Cl **00** *SC* **00** *P* *L* **#** **388**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *aGeneral*

Stylistic inconsistencies in reference to proper names.

SuggestedRemedy

"Capitalize the first letter of the words that form a field, a command, or an element name throughout their appearances (especially in text). This is also to avoid confusion and non-interoperability when "next" or "last" is actually the starting word of a field/element name. "

Proposed Response *Response Status* **U**

ACCEPT.

Response: Appreciate the acceptance of this comment which implies a lot of editorial work. However, a quick examination of D16-pre2 indicates that the acceptance has not been fully implemented.

Cl **00** *SC* **00** *P* **00** *L* **00** **#** **150**

Gubbi, Rajugopal Independent

Comment Type **TR** *Comment Status* **R** *CTA/M*

Remove Slotted aloha scheme from the draft ref: CID 537 - LB12, CID 387 - LB19, and CID 56 - LB22. What is the point in having slotted aloha access in addition to the backoff in CAP, TDMA in CFP? I don't see any justification in having yet another access scheme with WPAN. Why is this unncessary additional complexity being forced on to the implementors of this "low cost", "low complexity" and "low power" standard? If some future PHYs need it, let this be added as and when such a PHY is added to the 802.15.3 standard.

SuggestedRemedy

Make the change as requested.

Proposed Response *Response Status* **U**

REJECT. The open and association MCTAs were added to handle two concerns, the first was that new PHYs may not support efficient CCA detection. In this case, slotted aloha provides a contention access method that provides for the needs of the piconet. Another reason to used slotted aloha is that under certain conditions, it can be more efficient than using the CAP. Adding a new contention method to the MAC when a PHY group has been formed is probably not the best venue. At this time, the TG has many members who have expertise in the MAC available to review draft. In the future, when a new PHY is down-selected, there may not be as many people available who have the experience and knowledge of the TG3 MAC to be able to add a new contention method. Adding slotted aloha does not add much, if any complexity, the DEV needs the random number generatora and exponential increasing backoff for any contention based method. The DEV is already required to be able to send frames and look to see if it gets an ACK. Depending on the parameters used for either the CAP or the open and association MCTAs, the power usage may actually be lower using MCTAs for the DEVs in the piconet than using the CAP. MCTAs have an advantage over the CAP in that they can be put into multiple locations in the superframe allowing the PNC to potentially use the time more efficiently.

Cl **00** *SC* **00** *P* **00** *L* **00** **#** **151**

Gubbi, Rajugopal Independent

Comment Type **TR** *Comment Status* **R** *CTA/M*

Remove MCTA scheme from the standard ref: CID 536 - LB12, CID 513 - LB19, and CID 63 - LB22. Why can't the open and association be performed in CAP instead of devicing a new mechanism altogether for such a relatively low probability events? what is the point in having another collision based access mechanism inside a declared "collision free period (CFP)". If the concern is about a new PHY that may be added in the future, this mechanism can be added at the time of including the new PHY as allocations to a currently reserved stream ID (or DEVID) so that the legacy DEVs keep off of those slots and the new DEVs use them as per the new rules.

SuggestedRemedy

Make the change as requested.

Proposed Response *Response Status* **U**

REJECT. The open and association MCTAs were added to handle two concerns, the first was that new PHYs may not support efficient CCA detection. In this case, slotted aloha provides a contention access method that provides for the needs of the piconet. Another reason to used slotted aloha is that under certain conditions, it can be more efficient than using the CAP. Adding a new contention method to the MAC when a PHY group has been formed is probably not the best venue. At this time, the TG has many members who have expertise in the MAC available to review draft. In the future, when a new PHY is down-selected, there may not be as many people available who have the experience and knowledge of the TG3 MAC to be able to add a new contention method. Adding slotted aloha does not add much, if any complexity, the DEV needs the random number generatora and exponential increasing backoff for any contention based method. The DEV is already required to be able to send frames and look to see if it gets an ACK. Depending on the parameters used for either the CAP or the open and association MCTAs, the power usage may actually be lower using MCTAs for the DEVs in the piconet than using the CAP. MCTAs have an advantage over the CAP in that they can be put into multiple locations in the superframe allowing the PNC to potentially use the time more efficiently.

Cl **00** *SC* **00** *P* **00** *L* **00** **# 152**

Gubbi, Rajugopal Independent

Comment Type **TR** *Comment Status* **R** *IFS*

Replace MIFS with SIFS ref: CID 68 - LB22
- MIFS is less than SIFS
- it does not result in any significant time eficiency given the low probability of its use
- But introduces yet another IFS at the lowest level of MAC
- Mandates that the receive frames be processed within MIFS instead of SIFS since the worst case IFS is MIFS and hence drastically increases the complexity at the MAC and PHY

Remove MIFS and use SIFS in its place.

SuggestedRemedy

Make the change as requested.

Proposed Response *Response Status* **U**

REJECT. Using the MIFS instead of the SIFS with no-ACK frames can provide an improvement in the throughput of 8%. One of the key applications of 802.15.3 is streaming applications such as music and video which typically would be sent with either a no-ACK or Dly-ACK policy. At 55 Mb/s this is equivalent to 4.4 Mb/s, almost enough for an additional SDTV stream. This does require that the receiver process unload its input queue somewhat faster, but this can be handled in hardware.

Cl **00** *SC* **00** *P* **00** *L* **00** **# 153**

Gubbi, Rajugopal Independent

Comment Type **TR** *Comment Status* **A** *PHY/Timings*

Summarise all PHY timing parameters in one table in 11.2.7 ref: CID 69 - LB22 A summary all PHY dependent parameters (aCCADetectTime,aPHYSIFS-Time etc.) in a table with actual values at one place instead of spreading them all around the PHY clause is very desirable from implementors'view. An example would be Table-64 for MAC parameters. Although Table-120 provides a list of just the IFS parameters in a table, even there the for actual values the readers have to scrouge through the individual subclauses, which can easily be avoided.

SuggestedRemedy

Make the change as requested.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Make a table of all of the pZZZYyy parameters and their values, this will follow the format of table 65 in clause 8.

Cl **00** *SC* **00** *P* **00** *L* **00** **# 154**

Gubbi, Rajugopal Independent

Comment Type **TR** *Comment Status* **R** *ASIE*

Remove app-specific IE ref: CID 446, 477, 478 and 479 - LB19, CID 71 - LB22. Use of Vendor specific command is the answer to the issue that is intended to be solved through this app-specific IE. This is expecially since neither the standard nor an implementation of PNC can force the interpretation of bits in the currently undefined payload of this IE at each DEV which may be implemented by variety of vendors with their own "application" specific interpretations of those bits.

SuggestedRemedy

Make the change as requested.

Proposed Response *Response Status* **U**

REJECT. The ASIE is intended to be included in the beacon as an announcement. A command cannot be sent in the beacon so the vendor specific command would not be applicable to solve this need. The ASIE was put in to enable new functionality for some DEVs without breaking compatibility for all DEVs. Since the TG cannot possibly forsee all uses that might be required, this is left to be defined by the vendors.

Cl **02** *SC* *P* **34** *L* **# 347**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

The EESS#1 reference should read as follows: "Consortium for Efficient Embedded Security, Efficient Embedded Security Standards (EESS), EESS #1: Implementation Aspects of NTRUEncrypt and NTRUSign, Version 1.0, November 13, 2002. Available from http://www.ceesstandards.org." The SEC1 reference should read as follows: "Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Version 1.0, Certicom Research, September 20, 2000. Available from http://www.secg.org/." These changes were suggested to the technical editor on several occasions (lastly on Nov 22, 2002), but never implemented correctly.

SuggestedRemedy

change references as indicated.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. The security suites will be removed so this change no longer needs to be made.

Cl **03** *SC* *P* *L* **#** **350**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

Incorporate proper security notions throughout the Draft, defined in line with well-established cryptographic practice. We give an example of improper usage: in Clause 3, Page 5, line 21, 'authentication' is confused with 'authorization', since 'authentication' refers to 'evidence as to the true source of information or the true identity of entities' (see, e.g., the Handbook of Applied Cryptography, or Slide 2 of 02/114r5), whereas 'authorization' refers to 'assurance that an entity may perform specific operations'. This improper/sloppy use of terminology leads to misleading claims regarding security services offered. The following terms in Clause 3 need more accurate definitions: authentication, authentic data, integrity code, key establishment, key management, key transport, nonce, symmetric key.

SuggestedRemedy

I am - again - prepared to offer help, but this would assume flexibility and an open mind from the assistant security editor as well. Let us try again…

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Delete definitions for key management, key establishment, key transport, authentication, access control, authentic data, nonce, confidentiality, private key, public key, public-key certificate, signature verification, signed data, trusted third party.

Cl **05** *SC* **Clause 5.3.1.3** *P* **14** *L* **#** **352**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *PNCHndOvr*

What happens in the event of a handover of the child PNC, where the new child PNC is not part of the parent piconet?

SuggestedRemedy

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Add the ability to handover the dependent PNC as indicated in 03/032r8.

Cl **05** *SC* **Clause 5.3.2.1** *P* **15** *L* **#** **353**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *DepPN*

The procedure by which a child piconet ends its piconet is not described. If the child PNC uses the 'disassociate' command here fore as well, this has the inadvertent side-effect that not only the child piconet is ended, but also the child piconet controller is disassociated!

SuggestedRemedy

The disassociation command for child piconets should distinguish the child PNC from the child piconet (by using the proper DEVID as of Clause 7.2.3). I could not find this in the text, but might have overlooked this.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. On page 15, line 36 add 'A child piconet ends its piconet with the shutdown procedure and then uses the stream termination command to release the resources in the parent piconet. When the child PNC shuts down its piconet, it is not required to leave the parent piconet.' Add text to clause 8.2.6 as follows:
8.2.6.3 Dependent PNC termination of a dependent piconet

After stopping piconet operations for its own piconet {xref 8.2.6}, a child PNC shall inform its parent PNC that it no longer requires channel time for child piconet operations by sending the parent PNC a channel status request command terminating the CTA used for the child piconet.

After stopping piconet operations for its own piconet {xref 8.2.6}, a neighbor PNC shall inform its parent PNC that it no longer requires channel time for neighbor piconet operations by sending a disassociation request command to the parent PNC. Upon receiving a disassociation request command from a neighbor PNC, a parent PNC shall remove the CTA used by the neighbor piconet.

Cl **05** *SC* **Clause 7.2.1** *P* **109** *L* **#** **355**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *FrmFrmt*

change the Frame Control Field, such as to allow flexibility in the security services provided. Comment: in the current draft, the security services that are provided on frames statically depend on the frame type (beacon, ACK, command, and data frame). Conceptually, the communicating device should decide how to protect the frames it sends (although it might keep the requirements and capabilities of the recipient devices in mind). Additionally, this would allow considerable efficiency gains for applications where one requires only data authenticity or data confidentiality, but not both (since one would save a factor two in computational workload and, potentially, bandwidth). More flexibility would be provided by allowing a SEC field of 3 bits, which would allow the following 8 possibilities for frame protection to be indicated: SEC = Encr x Auth, where Encr={ON, OFF} and where Auth={0, 32-bit, 64-bit, 128-bit}. (Here, Encr=ON and Auth=64 would correspond to encrypting data and providing a 64-bit integrity check hereover, whereas, e.g., Encr=OFF and Auth=0 would correspond to having no security at all.). This security services indicator might be arranged at the frame level, but there is ample room for specifying this in the frame control field (it costs 3 bits including the SEC bit that is already provided in the current Draft D15).

SuggestedRemedy

Change the draft in line with the flexible security services identifier example given above and adapt all impacted text. See also the last slide of document 02/290 that was already presented in July 2002 (IEEE 802 meeting in Vancouver).

Proposed Response *Response Status* **W**

REJECT. The symmetric key encryption is sufficient for the PAN space without adding additional complexity.

Cl **06** *SC* **6.3.11.2** *P* **55** *L* **#** **425**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *SEC*

Definition for MLME-SECID-UPDATE.confirm missing!

SuggestedRemedy

Create a subclause to define the MLME-SECID-UPDATE.confirm primitive.

Proposed Response *Response Status* **U**

REJECT. No frames are sent or received as a result of the MLME-SECID-UPDATE.request primitive and the only information that might need to be passed back to the DME would be if there was a memory failure of some kind that prevented the DME from being able to update or add the data, which is outside the scope of the MLME commands.

Response: The XXX.confirm primitive is needed because there could be INVALID_PARAMETERS!

Cl **06** *SC* **6.3.17.3** *P* **68** *L* **25** **#** **480**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *Probe*

Incorrect parameter list in lines 25-30.

SuggestedRemedy

"Remove "InfoElementMap," and 'ProbeTimeout" from the list as they do not the .indication primitive."

Proposed Response *Response Status* **U**

REJECT. The Probe command that is sent by the MLME-PROBE.response primitive can also contain a request for information. Therefore the .response command needs these two parameters.

Response: Add a statement to this effect.

Cl **06** *SC* **6.3.18.1** *P* **69** *L* **6** **#** **484**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTA/Isoch*

"Ambiguous Description in lines 6-7: What is "the target of the MLME.request" in the case of a side-stream, the PNC or the non-PNC DEV on the other side of the stream? "

SuggestedRemedy

Resolve the ambiguity.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. The probe command is always sent as a peer-to-peer command (i.e. as a 'side-stream'). If a DEV sends a probe to the PNC, the PNC responds with information about itself, not with information about another DEV. The only way to find probe information about a DEV is to send the probe command directly to the DEV. Therefore, the TargetID in this MLME will become the DestID in the first probe command frame that is sent.

Response: Add a statement to this effect.

Cl **06** *SC* **6.3.18.1** *P* **70** *L* **34** **#** **482**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTA/Isoch*

Incomplete Description in Table 22 in lines 34-40.

SuggestedRemedy

"In the MinNumTUs row, after "number of TUs" add "per CTA". In the DesiredNumTUs row, after "number of TUs" add "per CTA". In the AvailableNumTUs row, delete "Either" and after "number of TUs" add "per CTA"."

Proposed Response *Response Status* **U**

ACCEPT.

Response: Lines 4-20, page 150 (D16-pre2): These two fields sometimes are for 'per CTA" (lines 5 and 7) and other times are for "per CTA Rate Factor" (line 12). Moreover, for "per CTA Rate Factor", the definition is done through non-normative text style "For example". An undefined term "sub-rate superframes" is also used.

More importantly, do not use CTRq TUs to specify CTAs as explained in a related response to the resolution on CID 677. Instead, specify each CTA in units of microseconds and do not let the "CTA Rate Factor" get involved in the specification of CTAs. There is no need here to further distinguish the cases of "super-rate allocation" and "sub-rate allocation", which would only complicate the definition and employ again yet undefined terms.

The CTA concepts are the core of this MAC, and cannot afford to be ill defined.

Cl **06** *SC* **6.3.21.1** *P* **78** *L* **15** **#** **496**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *Scan/Remote*

Incorrect reference in Table 25 in line 15. There is no need to define a new set of PiconetDescription just for remote scanning purposes.

SuggestedRemedy

"Change "Table 26" to "Table 6"."

Proposed Response *Response Status* **U**

REJECT. The remote piconet description set corresponds to the data that is passed in the Remote Scan Response command. Some of the data (beginning with SuperframeDuration) is not passed in the command and so cannot be passed up by the primitive.

Response: In Table 25 of D16-pre2, change "Set of remote piconet descriptions" to "Set of RemotePiconetDescriptions". Also under "Description" in the same row, add "Remote" right before "PiconetDescriptionSet".

Cl **06** *SC* **6.3.24** *P* **85** *L* **19** **#** **513**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *PM*

Missing subclauses.

SuggestedRemedy

Create new subclauses to define MLME-PS-SET-INFORMATION.indication and MLME-PS-SET-INFORMATION.response primitives.

Proposed Response *Response Status* **U**

REJECT. The participation of the PNC DME is not required to respond to this command as required by the draft standard. Thus the .indication and .response primitives are not required in this instance.

Response: Although MLME primitives are not exposed in the air, these two primitives should be still defined for the sake of consistency: The presence of XXX.confirm suggests that the DEV DME maintains the PS Set information, and hence in a similar way the PNC DME keeps the requested PS Set information.

Cl **06** *SC* **6.3.24** *P* **86** *L* **26** **#** **514**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *PM*

Missing subclauses.

SuggestedRemedy

Create new subclauses to define MLME-PS-SET-CONFIGURE.indication and MLME-PS-SET-CONFIGURE.response primitives.

Proposed Response *Response Status* **U**

REJECT. The participation of the PNC DME is not required to respond to this command as required by the draft standard. Thus the .indication and .response primitives are not required in this instance.

Response: Although MLME primitives are not exposed in the air, these two primitives should be still defined for the sake of consistency: The presence of both XXX.request and XXX.confirm together with their parameters suggests that the DEV DME decides on the PS Set information, and hence in a similar way the PNC DME decides on the requested change to the PS Set information.

Cl **06** *SC* **6.3.24** *P* **87** *L* **22** **#** **515**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *PM*

Missing subclause.

SuggestedRemedy

Create a new subclause to define an MLME-PM-MODE-CHANGE.indication primitive.

Proposed Response *Response Status* **U**

REJECT. The participation of the PNC DME is not required to respond to this command as required by the draft standard. Thus the .indication primitive is not required in this instance.

Response: This primitive is needed for similar reasons to those stated in CommentID 514.

Cl **06** *SC* **6.3.5** *P* **37** *L* **52** **#** **404**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *Assoc*

"Incorrect parameter range in Table 9 in lines 50-54: The actual result of an association request is contained in the "ReasonCode" instead of the "ResultCode"."

SuggestedRemedy

"Change the "Valid range" of "ResultCode" as follows: RESPONSE_RECEIVED, TIMEOUT. Change the corresponding "Description" to "Indicates if the association request has received a response or timed out."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. "Change the "Valid range" of "ResultCode" as follows: SUCCESS, TIMEOUT. Change the corresponding "Description" to 'Indicates if the primitive completed successfully or timed out.' In line 47, change "the result of the attempted association" to 'the reason why the attempted association failed as indicated in the association response command or indicates that the association was successful.'

Response: To be consistent with the definitions of other primitive, change "SUCCESS" to "COMPLETED". Also change "the primitive completed successfully" to "the association primitive exchange has completed".

Cl **06** *SC* **6.3.7.1** *P* **43** *L* **#** **409**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *SEC/Auth*

"Incorrect parameter range in Table 11 in lines 51-52: The actual result of an authentication request is contained in the "ReasonCode" instead of the "ResultCode"."

SuggestedRemedy

"Change the "Valid range" of "ResultCode" as follows: RESPONSE_RECEIVED, TIMEOUT. Change the corresponding "Description" to "Indicates if the authentication request has received a response or timed out." "

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Change the "Valid range" of "ResultCode" as follows: COMPLETED, TIMEOUT. Change the corresponding "Description" to "Indicates if the authentication request has received a response or timed out."

Response: To be consistent with the definitions of other primtives, change "if the authentication request has received a response or timed out" to "if the authentication primitive exchange has completed or timed out".

Cl **07** *SC* **7** *P* **107** *L* **17** **#** **528**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **X** *FrmFrmt*

Incorrect specification in line 17.

SuggestedRemedy

Delete the last statement of the 3rd paragraph.

Proposed Response *Response Status* **U**

This text replaces the 3rd paragraph of clause 7 on page 107 lines 14-17:
'For a frame to be correctly received by the MAC it shall pass the frame check sequence, have a protocol revision supported by the MAC, have a DestID equal to DEVID, BcstID, McstID or when applicable the PNCID or UnassocID, and have a PNID equal to the PNID of the piconet with which the DEV is synchronized. The MAC shall ACK all correctly received frames with ACK policy set to either Imm-ACK or Dly-ACK and DestID is the DEVID or when applicable the PNCID. If a DEV correctly receives a frame from an unassociated DEV it may ignore the frame and may choose not to respond to the frame. If authentication is required and a DEV correctly receives a frame from an unauthenticated DEV, it shall ignore the frame and shall not respond to the frame, except for the ACK, if the ACK policy is set to either Imm-ACK or Dly-ACK.'

Response: Change "frame check sequence" to "FCS validation", add "a" after the first "equal to", change "DestID is" to "DestID set to" (incorrect grammar), change "except for the ACK, " to "except with an appropriate ACK".

Cl **07** *SC* **7.2.7.4** *P* **113** *L* **# 535**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *FrmFrmt/FCS*

Word missing in line 30.

SuggestedRemedy

"After "MAC frame" add "Body" and change "frame" to "Frame"."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Change 'MAC frame' to 'Frame Payload' (see figure 8 for definition of Frame Payload).

Response: Under 7.2.1 and 7.2.4 of D16-pre2, change the first "information" to "an MSDU or a fragment thereof". The term "information" is not defined at all--what information?
Also change the heading of 7.2.4 to "Secure Frame Payload" ("field" is not used in the headlings of other related subclauses). Remember to capitalize the first letter of ALL words forming a proper name.

Cl **07** *SC* **7.2.7.5** *P* **113114** *L* **# 356**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *FrmFrmt/FCS*

the description of the FCS field is completely unclear. It is unclear whether the provision of a CRC check and the verification hereof are inverses of one another: conversion between bit strings and polynomials and encoding/decoding procedures lack clarity and precision. Moreover, statements as 'in the absence of transmission errors …' (Page 114, line 2) lack meaning.

SuggestedRemedy

replace the text by an unambiguous and clear description of the encoding/decoding procedures.

Proposed Response *Response Status* **W**

REJECT. This text is well accepted and is essentially the same as the text in 802.11.

Cl **07** *SC* **7.3.1.1, Figure 13** *P* **115116** *L* **# 360**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *FrmFrmt/Bcn*

The piconet controller should indicate in its piconet mode field (see Figure 13) the security policy the piconet adheres to. Currently, it only indicates whether security is ON or OFF, but this does not sufficiently indicate other security characteristics, such as the minimum bit-security level at which access control in the piconet is arranged. This information, in the current D15 draft contained in the Security Requirements Field (see Table 54), logically belongs in the piconet mode field and should be moved there.

SuggestedRemedy

Change the Draft D15 text to accommodate for this sound security policy principle and adopt impacted text, both in Clause 7.3.1.1 and in Clause 7.5.2.2. See also the discussion in document 02/364r2.

Proposed Response *Response Status* **W**

REJECT. This information is already passed to DEVs in the authentication process in the authentication response command. While it allows the DEV to know before it joins what is the level of security, this provides only part of the information that the DEV needs when selecting a piconet.

Cl **07** *SC* **7.3.2.2** *P* **119** *L* **# 545**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *ACK/Dly*

"Ambiguous specification in line 50: What does "frames of pMaxFrameSize" mean? Practically, the recipient DEV has to assume that the frames to be sent are of maximum allowable size in setting the value for the Max Burst field."

SuggestedRemedy

"Delete "of pMaxFrameSize"."

Proposed Response *Response Status* **U**

REJECT. While it would be clear to some implementers that this is for pMaxFrameSize, others may not make this interpretation. If it is obvious that these are all of pMaxFrameSize, then it doesn't change the specification to explicitly indicate that they are of that size here.

Response: Add "of Frame Payload length equal to" before "pMaxFrameSize" (which is a number).
A related comment: It would improve both parsing time and encoding efficiency to absorb the Dly-ACK request into the 2-bit ACK policy field.

Cl **07** *SC* **7.4.16** *P* **133** *L* # **362**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

One can save 1 byte in the public-key object by listing sequence numbers in decreasing order and reserving the first bit of the sequence number field to indicate whether one received the first fragment of the public key or not. The current encoding is wasteful (see also comment on encoding of Fragment Control Field).

SuggestedRemedy

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. The public key IE will be removed from the draft.

Cl **07** *SC* **7.4.16** *P* **133** *L* # **364**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

The public-key object types should distinguish between X509 certificates for the RSA-OAEP and the ECQMV security suite, since not doing so would block the use of 'lazy evaluation' techniques.

SuggestedRemedy

re-introduce this distinction.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Add 'RSA X.509' and 'ECC X.509' above 'X.509'.

Cl **07** *SC* **7.4.6** *P* **127** *L* **39** # **818**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PN/ChngParm*

"States "For a piconet that has pseudo-static CTAs, NbrOfChangeBeacons shall be at least four."

SuggestedRemedy

Should reference the MAC parameter: mMaxLostBeacons.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Change "For a piconet that has pseudo-static CTAs, NbrOfChangeBeacons shall be at least four." to be "For a piconet that has pseudo-static CTAs, NbrOfChangeBeacons shall be at least {xref mMaxLostBeacons}."

Response: Change "eight" in the following sentence to either "mMaxLostBeacons + 4" or "2 x mMaxLostBeacons".

Cl **07** *SC* **7.4.8** *P* **129** *L* **14** # **560**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PM/Hibernate*

"Incorrect specification: How could a PCTM IE sent in a beacon make a HIBERNATE DEV switch to ACTIVE mode, given that the PNC has no definite knowledge of when that DEV is going to enter the AWAKE state?"

SuggestedRemedy

Resolve the issue.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. The PCTM IE is placed in the beacon until the HIBERNATE DEV either a) repsonds to the IE with a PS mode change command or b) the ATP of the DEV expires and the PNC disassociates the DEV. Thus the DEV will either respond or it will be removed from the piconet.

Response: In 7.4.8 after "bitmap" (line 46) add a comma.

Cl **07** *SC* **7.5.2.2** *P* **140** *L* # **361**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

In Table 54, bit b1 shall be set to 0 if the piconet intends to operate at (at least) the 80-bit security level and to 1 if the piconet intends to operate at the 128-bit security level.

SuggestedRemedy

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Add a field '80 bit security required' with the definition 'If the 80-bit security required bit is set to 1, the security manager shall only authenticate DEVs with a security suite that is stated to provide at least 80-bit security in Table 96 while it operates as the security manager.' Add a column to table 96 with title 'At least 80 bit claimed secuity' and put X's in all of the columns.

Cl **07** *SC* **7.5.2.5** *P* **141** *L* # **370**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *SEC/Key*

The request key response command should return all the keys that are shared with the requesting device, including information on the group of devices the key is shared with. Currently, no freshness is provided either.

SuggestedRemedy

This will be provided separately.

Proposed Response *Response Status* **W**

REJECT. The request key response command will return only the key that was requested, see the resolution of CID 416. Freshness is ensure with the CCM nonce, Annex B.

Cl **07** *SC* **7.5.4.4** *P* **146** *L* **#** **468**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PNCHndOvr*

"Ambiguous definition for the "Sequence Number" field in line 14."

SuggestedRemedy

Rephrase the definition as follows: The Sequence Number field specifies the number of frames that have been sent prior to this frame by this DEV in the response to the request.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Rephrase the definition as follows: 'The Sequence Number field specifies the number of frames that have been sent prior to this frame by this DEV in the response to the request. Thus the first frame has a Sequence Number of 0 while the last frame has a Sequence Number equal one less than the Total Number of Frames.'

Response: After "equal" add "to".

Cl **07** *SC* **7.5.4.4** *P* **146147** *L* **#** **366**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *PNCHndOvr/SEC*

If 'ACL info handover' is enabled, only the so-called 'manual certificate modes' of the supported security suites shall be used, since implementing this ACL transfer mode is sufficient for continuing the smooth operation of the piconet in the event of a PNC handover. All the other presently defined modes in Draft D15 miss a proper justification and should be removed.

SuggestedRemedy

Remove all verification information formats that do not represent these so-called 'manual certificates'. Moreover, completely remove the following clauses: Clauses 10.3.2.2-10.3.2.3, Clauses 10.4.2.2-10.4.2.5, and Clauses 10.5.2.2-10.5.2.5.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. The ACL handover command will be changed to use LV elements so that no restrictions are placed on the data or verification methods. The command will be renamed to Security Information Exchange command.

Cl **07** *SC* **7.5.4.4** *P* **146147** *L* **#** **367**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *PNCHndOvr/SEC*

Table 56, Clause 7.5.4.4: The security suite is encoded using a 5-bit field and as an OID in Clause 10. This is inconsistent.

SuggestedRemedy

Use the OID to indicate the security suite. This also removes the need to define verification information types, since this is implied by the OID of the security sub-suite.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Remove the field 'Security suite' from 'Verification Info Type field'. Add a new fields to the 'Verification Info Type field', 'OID Length' and 'OID' with the definitions 'The OID indicates the security suite of the ACL information, {xref 10.2.1}.' and 'The OID length is the length of the OID.' Add these definitions to 7.5.2.1 where they are missing as well.

Cl **07** *SC* **7.5.4.4** *P* **146147** *L* **#** **368**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *PNCHndOvr/SEC*

The description of the implementation of ACL transfer should not impose constraints on how the ACL transfer modes are represented in memory. Since this is the sole role of applying the SHA-1 function to public-keying material in this ACL transfers (the occasional bandwidth savings are negligible over time), this compression function shall not be specified, by lack of justification.

SuggestedRemedy

completely remove all Clauses that refer hereto.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. The ACL handover command will be changed to use LV elements so that no restrictions are placed on the data or verification methods. The command will be renamed to Security Information Exchange command.

CI **07** *SC* **7.5.4.5** *P* **147** *L* **53** **#** **469**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *Probe*

"Confusing naming and incorrect encoding of the fields in the Probe Command. Also it is not worth going through the encoding specified by Figure 75, which, in fact, would not fit with the case of binary encoding of an information element's ID (the ID is 8 bits long, while the Elements requested subfield has 31 bits."

SuggestedRemedy

"Rename the field name "Information elements" to "IEs Provided" and "Information request" to "IEs Requested" (m octets) in this subclause and in 8.9.2. Delete Figure 75 and the paragraph immediately about it. Replace the four paragraphs immediately below Figure 75 with the following paragraph: The IEs Requested field specifies the Element IDs of the information elements requested by this DEV, with each Element ID occupying one octet."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Rename the field name "Information elements" to "IEs Provided". However, when bit 0 is equal to zero, the other 31 bits are a binary represenation of the IE number, thus you can request less (one at time) up to an index of about 2^31, which is more than sufficient.

Response: The response accepts only the suggested remedy on the "Information elements" field, while rejecting that on the "Information request" field. After rereading the text defining the "Information request" field, this commenter still feels that the suggested remedy on that field should be adopted as well: Using two types of encodings for this field complicates implementation without offsetting benefits. (1) The biniary encoding method requires 4 octets, one octet more than needed in the suggested encoding method (2 octets for Length and 1 octet for the requested Element ID). (2) The bitmap encoding method accommodates only IEs of element ID < 32, which is not acceptable since there may be IEs whose element ID >= 32. It is incorrect to base the encoding on the currently defined IEs, as future revisions may add additional IEs within the allowed ID space.

With the encoding method as indicated in the suggested remedy, the Length field is to cover only the IEs Provided field which is variable in length.

CI **07** *SC* **7.5.5** *P* **150** *L* **#** **474**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTReq*

Ambiguous naming: CTR could be interpreted as either channel time request as defined in 7.5.5.1 or channel time response as defined in 7.5.5.2.

SuggestedRemedy

"Rename "Channel time request command" to "Channel Time Allocation (CTA) Request Command" and "Channel time response command" to "Channel Time Allocation (CTA) Response Command". Change "channel time request block (CTRB)" to "Channel Time Allocation Request Block (CTARB). Change "CTR" to "CTA request" throughout the draft. In fact, part of the draft (like 8.5) already uses "CTA"."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Change all CTR references to be "CTRq" to avoid confusion. If the response command needs an acronym, it will be ‘CTRsp’.

Response: This is really awkward.

Cl **07** *SC* **7.5.5.1** *P* **151** *L* **#** **570**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTA*

"Ambiguous definition in lines 20-29, page 152: The word "CTA" is used to mean both a single CTA and a collection of CTAs."

SuggestedRemedy

"Rephrase these two paragraphs as follows:
The Rate Type field is set to 0 for a subrate CTA request and 1 for a superrate CTA request. A subrate CTA request indicates a need for a CTA every N superframes where N > 1, while a superrate CTA request indicates a need for N CTAs in every superframe where N = 1 or N > 1.
The Rate field specifies the value of N referenced in the last paragraph. For a subrate CTA request, the Rate field value shall be a power of 2. A PNC shall support up to eight CTAs per superframe for each stream."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Change the paragraphs as follows:
(note CTR Interval will change names due to the resolution of another comment.)

The CTR Interval Type field shall be set to one for a subrate CTA request and zero for a super-rate CTA request. A subrate CTA request indicates a need for a CTA every N superframes where N is greater than one, while a super-rate CTA request indicates a need for N CTAs in every superframe where N equals one or N greater than one.

The CTR Interval field specifies the value of N, as described above. For a subrate CTA request, the CTR Interval field value shall be a power of 2. A PNC shall support up to eight CTAs per superframe for each stream."

Response: Lines 29-45, page 149 (D16-pre2): The terms "super-rate CTA" and "sub-rate CTA" are used but never defined in a normative fashion. The text here attempts to define these terms indirectly and others like "CTA Rate Factor" using a non-normative style "For instance". It is also confusing to say "CTAs appear in the beacon".

Rename "CTA Rate Factor" to "CTA Repetition", and change these lines as follows (suggested in the original comment):

The CTA Rate Type field is set to 0 for a subrate CTA request and 1 for a superrate CTA request. A subrate CTA request indicates a need for a CTA every N superframes where N > 1, while a superrate CTA request indicates a need for N CTAs in every superframe where N = 1 or N > 1.

The CTA Repetition field specifies the value of N referenced in the last paragraph. For a subrate CTA request, the CTA Repetition shall be a power of 2. A PNC shall support up to eight CTAs per superframe for each stream.

LIne 1, page 149 (D16-pre2): Delete "either" (incorrect grammar). In the following line, after "stream" add "index".

Cl **07** *SC* **7.5.5.1** *P* **151** *L* **#** **476**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTA*

"Ambiguous statement in lines 15-16: What is an "ACTIVE channel time allocation" and what is an "SPS (not just PS?) channel time allocation"?"

SuggestedRemedy

Clarify the ambiguity.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. In 7.5.5.1, page 152, after lines 15-16, add the following text:
'For subrate allocations, an ACTIVE allocation (specified by CTA type = 0) puts no restriction on the superframe of the first CTA specified by CTR interval. A DSPS allocation (specified by CTA type = 1) synchronizes all CTAs specified by the CTR interval with the DSPS set awake superframes of the DSPS set specified by the DSPS index. The value of the CTR interval shall be no smaller than the DSPS set's awake beacon interval.

The DSPS set index field is used to identify the DSPS set with which the CTR is associated, if the CTR is for a DSPS allocation. Only valid DSPS set indices, {xref 7.5.7.2}, are allowed for a DSPS allocation request. Otherwise, the field shall be set to 0 and shall be ignored on reception.'

Response: In D16-pre2, change "to request" (two instances) to "for requesting" in lines 20-21, and "puts" to "places" in line 22, page 149.

Cl **07** *SC* **7.5.5.2** *P* **153** *L* **18** **#** **574**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTRsp*

Incorrect definition in lines 18-19.

SuggestedRemedy

"Change "per CTR interval" to "per CTA", and "the requested stream" to "the specified isochronous stream"."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. On page 153, line 18, add 'In the case of a super-rate allocation, it is the number of TUs assigned in each superframe. In the case of a sub-rate allocation it is the number of TUs assigned in each of the sub-rate superframes.'

Response: See reply to resolution on CID 482.

Cl **07** *SC* **7.5.6.1** *P* **154** *L* **5** **#** **576**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *ChnlStatus*

Ambiguous definition in lines 5-6: How would this command be responded when the DestID is set to the BcstID?

SuggestedRemedy

Describe the response or delete the statement.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. On page 154, line 6, change ‘to the BcstID’ to be ‘to the BcstID with the ACK Policy field set to no-ACK.’ Add to page 205, line 45 ‘If the PNC sends a broadcast Channel Status Request command, i.e. the DestID is the BcstID, it is requesting that all DEVs that receive the command respond with a Channel Status Response command sent to the PNCID. Each DEV sends the response command when they get an opportunity, either in the CAP or in an MCTA.’

Response: After "i.e." add ", if". Change "it is" to "the PNC is", "receive" to "received", "sent to" to "addressed to", and "get an opportunity" to "have an opportunity to do so".

Cl **07** *SC* **7.5.7.5** *P* **159** *L* **25** **#** **593**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PM*

Incorrect wording in lines 25 and 27.

SuggestedRemedy

"Change "number PS set structures" to "Number of Supported PS Sets", and "The PS set structure" to "Each PS set structure"."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Change "number PS set structures" to "number of current PS sets", and "The PS set structure" to "Each PS set structure". Change 'Number of supported PS sets' to be 'Maximum Supported PS Sets' in Figure 92 and the following text. Also replace where it occurs in clause 8. Add a new field, "Number of Current PS Sets" with definition, 'The Number of Current PS Sets field is a count of the number of PS set structures in this command as well as the number of currently active PS sets in the piconet.'

Response: What is an "active PS set"? Does the last sentence mean "The ...field is the number of PS set structures in this command plus the number of..."? (The word "count" is not clear.)

Cl **07** *SC* **7.5.7.5** *P* **159** *L* **36** **#** **594**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PM*

Incorrect statement in lines 36-37.

SuggestedRemedy

"Change "non zero value" to "than 0 or 1", and "in this particular SPS set" to "in a particular SPS mode"."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Change "non zero value" to "than 0 or 1", This command returns a list of all the DEVs who are members of a particular PS set. It does not indicate that they are in a PS mode. The PS status IE(s) in the beacon contain the lists of the DEVs that are in PS mode for each of the sets. A DEV shall first join a set before it can change to either SPS or PSPS mode. Thus a DEV can be a member of a set but not be in a power save mode.

Response: Add to the draft the text beginning from "This command" to the end of the paragraph.

Cl **08** *SC* **8.10** *P* **208** *L* **16** **#** **753**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PN/ChngParm*

"Incorrect statement in line 16, page 208: Pseudo-static CTAs are actually changed when the superframe duration is changed."

SuggestedRemedy

"Change "pseudo-static CTAs" to "pseudo-static CTA blocks"."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. The CTA location does not change relative to the beacon and so the CTA does not change (CTAs only have meaning measured relative to the beacon). The location of the psuedo-static CTA relative to previous beacons will change, but the source and destination DEVs will be informed prior to that by the piconet parameter change IE. If there are pseudo-static CTAs, the piconet parameter IE will be sent at least mMaxLostBeacons prior to the change. Thus, even if the DEVs miss some of the announcements, they will either a) hear at least one of them or b) miss all but hear the first beacon with the new superframe duration. To clarify this, change "A PNC shall not change pseudo-static CTAs" to be "A PNC shall not change either the pseudo-static CTAs or the pseudo-static CTA blocks"

Response: CTAs only have meaning measured relative to the beacon? When a DEV send a CTA request command, it is requesting CTAs based on the superframe duration then in effect. When the superframe duration changes, the CTA changes as well to the very users of the CTA!

Cl **08** *SC* **8.13** *P* **214** *L* **40** **#** **769**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PM*

"Confusing and incorrect definitions for power management modes, power save modes, power states, and their relationships: ACTIVE mode is NOT a power save mode as is often confused throughout this draft. A DEV may be in "AWAKE" state beyond the time when it is either transmitting or receiving. For instance, a DEV may be in "AWAKE" state when the channel is idle. A DEV may not be in a "SLEEP" state even if it is neither transmitting nor receiving."

SuggestedRemedy

"Rewrite the first paragraph as follows:
There are four power management (PM) modes defined in this standard, ACTIVE, HIBERNATE, PSPS, and SPS modes. The latter three modes are collectively referred to as power save (PS) modes. A DEV that is in ACTIVE, HIBERNATE PSPS, or SPS mode is said to be an ACTIVE DEV, a HIBERNATE DEV, a PSPS DEV, or an SPS DEV, respectively. In any given PM mode, a DEV may have two power states, AWAKE and SLEEP states. A DEV in AWAKE state is able to transmit and receive and is fully powered, while a DEV in SLEEP state is not able to transmit or receive and consumes very low power. A DEV, regardless of its PM mode, is allowed to enter the SLEEP state during a CTA for which it is neither the source nor the destination, and between CTAs other than the beacon times and CAPs. A DEV is allowed to enter the AWAKE state during any time when it is in a power save mode."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Rewrite the first paragaph in 8.13 as follow: ‘There are four power management (PM) modes defined in this standard, ACTIVE, APS, PSPS, and DSPS modes. The latter three modes are collectively referred to as power save (PS) modes. A DEV that is in ACTIVE, APS, PSPS, or DSPS mode is said to be an ACTIVE DEV, an APS DEV, a PSPS DEV, or a DSPS DEV, respectively. In any given PM mode, a DEV may be in one of two power states, either AWAKE or SLEEP states. AWAKE state is defined as the state of the DEV where it is either transmitting or receiving. SLEEP state is defined as the state in which the DEV is neither transmitting nor receiving. A DEV, regardless of its PM mode, is allowed to enter the SLEEP state during a CTA for which it is neither the source nor the destination. A DEV is also allowed to enter the AWAKE state during any time when it is in a power save mode.’ The AWAKE and SLEEP states in the standard are defined based on their affect the operation of the piconet. The operation of the piconet is only affected by the DEV either transmitting or receiving. The state where the DEV is neither transmitting nor receiving but is still powered up is equivalent to the state where the DEV is completely turned off from the point of view of the other DEVs in the piconet. The only charactertistics that affect the piconet operation are that the DEV is either receiving or transmitting.

Response: 1. Change "either AWAKE or SLEEP states" to "either AWAKE or SLEEP state" (singular form for "state").

2. The following statements are incorrect: "AWAKE state is defined as the state of the DEV where it is either transmitting or receiving. SLEEP state is defined as the state in which the DEV is neither transmitting nor receiving."
A counter example: A DEV may have to stay awake (in its English sense) after an expected beacon is not received, yet the DEV will not necessarily be either transmitting or receiving. Replace these two sentences with the following (as suggested in the original comment): "A DEV in AWAKE state is able to transmit and receive and is fully powered, while a DEV in SLEEP state is not able to transmit or receive and consumes very low power."

3. The following statements intended to justify the current definition of AWAKE and SLEEP states are incorrect as well and should be deleted: "The AWAKE and SLEEP states in the standard are defined based on their affect the operation of the piconet. The operation of the piconet is only affected by the DEV either transmitting or receiving. The state where the DEV is neither transmitting nor receiving but is still powered up is equivalent to the state where the DEV is completely turned off from the point of view of the other DEVs in the piconet. The only charactertistics that affect the piconet operation are that the DEV is either receiving or transmitting." The AWAKE and SLEEP states of a DEV directly affect its own operation as well--the DEV would miss frames should it not know when to wakeup and would waste power should it not know when to sleep. The objective of power management is two folds--to enable a given DEV to know when it should enter which state and to enable other DEVs to know when that given DEV is able to transmit and receive and when that DEV is not able to do so.

Cl **08** *SC* **8.13** *P* **214** *L* **50** **#** **771**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **X** *PM/SPS*

"Confusing statement in lines 50-51, page 214."

SuggestedRemedy

"Change "A DEV that is in SPS mode may have multiple wake beacons" to "A DEV in SPS mode may be in multiple SPS sets and hence may have multiple wake beacons in the sense that each of those SPS sets may have its own wake beacon."

Proposed Response *Response Status* **W**

Change "A DEV that is in SPS mode may have multiple wake beacons" to "A DEV in SPS mode may be in multiple SPS sets and therefore may have multiple wake beacons because each of those SPS sets may have its own wake beacon."

Cl **08** *SC* **8.13** *P* **215** *L* **32** **#** **386**

Welborn, Matt XtremeSpectrum

Comment Type **TR** *Comment Status* **X** *PM/PSPS*

Small changes to support new TrgtID field in the PS Mode change command. Editorial: Switching to ACTIVE is the same procedure regardless of PS mode. Maybe lift out to the general clause?

SuggestedRemedy

8.13.1 page 216 line 12. (for PSPS) 8.13.2.2 page 217 line 31. (for SPS) 8.13.3 page 221 line 7. (for HIBERNATION) Add "with the PS Mode field set to ACTIVE and the TrgtID set to its own DEVID" Change Figure 146, page 224. Add param TrgtID=SrcID to MLME-PS-MODE-CHANGE.req and to PS mode change command

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Resolve as indicated in 03/032r3.

Cl **08** *SC* **8.13.3** *P* **221** *L* **12** # **806**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PM/Hibernate*

"Unambiguous specification in lines 12-13, page 221: The PNC cannot tell when the HIBERNATE DEV is going to be awake, so in which beacon should it send the PCTM IE to the HIBERNATE DEV?"

SuggestedRemedy

Resolve the issue.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. The PCTM IE is placed in the beacon until the HIBERNATE DEV either a) repsonds to the IE with a PS mode change command or b) the ATP of the DEV expires and the PNC disassociates the DEV. Thus the DEV will either respond or it will be removed from the piconet.

Response: Could not find the change in D16-pre2.

Cl **08** *SC* **8.2.3** *P* **165** *L* **23** # **606**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PNCHndOvr*

"Unnecessary restriction in line 23, page 165."

SuggestedRemedy

Delete this statement.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. However, the DEV needs to have the opportunity refuse handover, see the resolution of CID 139.

Response: But the statement is still in D16-pre2.

Cl **08** *SC* **8.4.4** *P* **179** *L* **26** # **651**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTA*

"Incorrect terms: Channel access in the CFP is not necessarily contention free, because open and association MCTAs are subject to Aloha-based contention."

SuggestedRemedy

Either modify the terms or add a statement to that effect.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Rename CFP to CTAP - channel time allocation period.

Response: Clause 4 says that CTAP stands for "channel time access period" but not "channel time allocation period".

Cl **08** *SC* **8.4.4.1** *P* **179** *L* **35** # **652**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *CTA*

"Incorrect specification regarding local selection in lines 35-38, page 179: Each CTA block contains a Stream Index that is tied to a specific stream."

SuggestedRemedy

"Rephrase the statement "The selection of a…" as follows: The source DEV of a CTA shall use that CTA to send data from the stream specified for that CTA, or to send data from other streams between the same source and destination DEVs if the specified stream has no more data to send."

Proposed Response *Response Status* **U**

REJECT. The proposed text is too restrictive. A DEV may have data pending for stream index 5 that is lower priority than stream index 3. The DEV would want to send data from stream index 3 in a CTA assigned to stream index 5 to improve the performance of its highest priority applications.

Response: After "their priorities" add "provided the recipient of the selected data is the destination DEV of this CTA".

Cl **08** *SC* **8.4.4.5** *P* **183** *L* **13** # **675**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTA*

"Incorrect specification in lines 13-16, page 183."

SuggestedRemedy

"Change "broadcast or unassigned" to "Association or Open". Delete "the open or association MCTA with the number r=". Change "ACK" to "Imm-ACK". Delete the last statement "After receiving" if "a", and hence the "backoff", is to be updated every superframe, as suggested earlier by this balloter."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. The comment that "broadcast or unassigned" should be changed to open or association. The rest of the suggested Remedy is not appropriate because it is based on a rejected suggestion from CID 672.

Response: Except the last sentence, the comment is independent of any other comment.

With reference to D16-pre2, delete "counting ra beginning with" in line 20 , page 185 (the DEV counts MCTAs but not ra), and delete "the open or association MCTA with the number r=" in lines 28-29 (the counter can only reach a number, but not an MCTA).

Cl **08** *SC* **8.4.4.6** *P* **183** *L* **38** **#** **677**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTReq*

"Incorrect illustrations in Figure 107, Figure 108, and Figure 109."

SuggestedRemedy

"Change "SIFS" to "MIFS" in Figure 107 (3 occurrences). Delete "CTR time unit" (which does not necessarily cover a whole frame plus MIFS due to variable frame sizes) from all the three figures. Change "SIFS" to "MIFS" after "Frame 1" and "Frame 2", respectively, in Figure 109."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Change "SIFS" to "MIFS" in Figure 107 (3 occurrences). Change "SIFS" to "MIFS" after "Frame 1" and "Frame 2", respectively, in Figure 109

Response: Change "SIFS" (the left two instances) to "MIFS" in Figure 107 in D16-pre2.

Delete "CTR time unit" in Figures 110-113 because, as partly pointed out in my original comment, the use of CTR time unit as the time unit for CTAs does not account for variable frame transmisison times nor retries within the same CTA. Transmission time may vary from frame to frame due to data rate (and potentially preamble) changes, the variable bit rate nature of the stream, and throughput considerations. For instance, an 1394 ISO packet may contain 0, 1, or 2 small MPEG cells (188 bytes). Such variable length packets themselves may be further aggregated either at the so-called FCSL or right at the MAC (even though the current spec has no such aggregation mechanism) to make efficient use of the 100 Mb/s plus data rates being specified in 802.15.3a which is to be using this MAC. On the other hand, a retry does not occur right after a prefixed CTR time unit. Note that if CTA is not specified correctly, this MAC will just fall apart.

Cl **08** *SC* **8.4.4.7** *P* **184** *L* **40** **#** **678**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *CTReq*

"Incomplete specification in lines 40-41, page 184."

SuggestedRemedy

"Change 'Including SIFS" to "Including MIFS/SIFS". Change "at least a SIFS" to "at least a MIFS/SIFS" (2 occurrences, one on the next page)."

Proposed Response *Response Status* **U**

REJECT. The DEVs need to have time to switch between transmit and receive between CTAs. A MIFS is not necessarily enough time to do this, therefore the SIFS time is required which is equal to the greater of the the TX/RX turnaround and the RX/TX turnaround times.

Response: I made this comment because I interpreted the statement to mean all the MIFSs and SIFSs in the CTA. I guess the author meant the trailing SIFS. Thus, before "SIFS" add "a trailing" in this sentence and others as well that exhibit this ambiguity.

Cl **08** *SC* **8.4.4.7** *P* **185** *L* **24** **#** **679**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTReq*

Incorrect specification in Equation (2).

SuggestedRemedy

"Change "/" to "x" and "* interval" to "x Superframe Duration"."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. The equation is confusing because it is missing parentheses. It should read:
MaxDrift = [clock accuracy (ppm)/1e6]*interval
A number in ppm is divided by 1e6 to get its fractional equivalent, thus 100 ppm is equal to 0.0001. The drift for a 10 ms interval with 100 ppm accuracy is 10 us.
Add parentheses to the equation to emphasize that the interval is multiplied by the fractional clock accuracy.

Response: In fact, the guard time includes another component--an uncertainty time due to the inaccuracy in determining the begining of the beacon preamble to which all the CTAs are referenced. This component is essentially independent of the superframe duration.

Values of this component, and the ppm in the clock drift component, should be specified for interoperability. That is, they should be listed as PIB parameters with specified values.

Cl **08** *SC* **8.4.4.7** *P* **185** *L* **39** **#** **682**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTReq*

Incorrect specification in Equation (3).

SuggestedRemedy

"Delete "+ SIFS"."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. (note: see 02/032r7 for formatted text). The inclusion of MIFS changed the CTR calculations, but the changes were not reflected in 8.4.4.6. '1)Change b3 in Figure 79 from "stream termination" to "MIFS CTRq TU". 2)Replace page 152, line 12 with: 'The MIFS CTRq TU bit indicates that the CTRq TU includes MIFS, not SIFS as described in 8.4.4.6. When the MIFS CTRq TU bit is set to one the PNC shall allocate SIFS-MIFS additional time to the CTA so that there is at least a SIFS duration between the last transmission in one CTA and the first transmission in the next. Otherwise, the SIFS is included in the CTRq TU.'
3)Move 8.4.4.6 after 8.4.4.7 since 8.4.4.6 refers to guard time. 4)Modify 8.4.4.6 as follows:
Calculating channel time requests
Each DEV sends channel time requests to the PNC to indicate the amount of channel time required for transmission.
The requesting DEV shall include the frame transmission time, if known a priori, and the ACK transmission time, if used, and MIFS or SIFS time as appropriate per frame or ACK when calculating channel time requests. Figure 1 (was #108) shows an example of channel time being requested for a CTA where Imm-ACKs are used.
When No-ACK is used, the channel time request is calculated differently because there is a MIFS in between each frame in the CTA instead of a SIFS. A channel time request that uses a CTRq TU with MIFS instead of SIFS shall set the CTRq TU MIFS bit to one to inform the PNC that it must add a time equal to SIFS-MIFS to the end of the CTA. This ensures that there is a SIFS between the end of transmission in one CTA and the start of the next. Figure 2 shows an example of a channel time request when no-ACK is used and the MIFS bit is set in the Channel Time Request command.
A CTRq TU in the CTA may cover more than one frame as shown in Figure 3. If the requesting DEV included SIFS-MIFS following the last MIFS as shown in Figure 3 it shall set the CTRq TU MIFS in the Channel Time Request to "0." IF SIFS-MIFS is not included in the CTRq TU, the CTRq TU MIFS bit shall be set to "1" and the PNC shall add SIFS-MIFS to the CTRq TU to calculate the duration of the CTA

Response: This new "MIFS CTRq TU" field is hopeless in cases of variable frame transmission times and retries as noted in my reply to resolution on CID 677. Do not use the CTRq TU as the time unit in specifying CTAs, and hence do not introduce this new field.

Cl **08** *SC* **8.5.1.2** *P* **191** *L* **35** **#** **697**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTA/Isoch-e*

Incorrect illustrations in Figure 117 and Figure 118.

SuggestedRemedy

"Change "ACK" to "Imm-ACK" (2 occurrences in each figure). Change "ResultCode" to "ReasonCode" in each of these two figures (recall that the actual result is contained in the ReasonCode). Change "= FAILED" to "not equal to SUCCESS" in Figure 118."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. In figures 117 and 118, Change "ACK" to "Imm-ACK" (2 occurrences in each figure). Delete "with ResultCode = ???" in each of these two figures. Add 'with Reason Code = success" to the channel time response command arrow in figure 117.

Response: Capitalize "success".

Cl **08** *SC* **8.5.1.3** *P* **193** *L* **19** **#** **699**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTA/Isoch-e*

Incorrect illustrations in Figure 119 and Figure 120.

SuggestedRemedy

"Change "ACK" to "Imm-ACK" in both figures. Change "ResultCode" to "ReasonCode" in each of these two figures (recall that the actual result is encoded in the ReasonCode)."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Change "ACK" to "Imm-ACK" in both figures. Change "SUCCESS" to "RESPONSE_RECEIVED" in each of these two figures. Ed. Note coordinate this code with new clause 6 name.

Response: Check against clause 6 that it is "RESPONSE_RECEIVED" but not "COMPLETED".

Cl **08** *SC* **8.5.2.1** *P* **195** *L* **12** **#** **702**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CTA/Async*

"Incomplete statement in line 12, page 195."

SuggestedRemedy

"After "superframe" add ", with any such CTA again announced by multiple CTA blocks each of which corresponds to a destination."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. After "superframe" add ", with any such CTA again announced by multiple CTA blocks that overlap in time but have different DestIDs.'

Response: "CTA blocks that overlap in time"? what does it mean? CTA blocks that have the same CTA Location and CTA Duration?

Cl **08** *SC* **8.6.4** *P* **198** *L* **10** **#** **712**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *Beacon*

Incorrect specification in Table 61.

SuggestedRemedy

"Under "Intended for" change "DestID" to "CTA source and destination DEVs"."

Proposed Response *Response Status* **U**

REJECT. The source DEV finds out information about the CTA in channel time request process. Some of the information is sent by the source to the PNC with the channel time request command and some of the information is passed back by the PNC to the source DEV with the channel time response command. The only DEV not involved in the negotiation is the destination and so it is the only intended target of this information element.

Response: Rephrase it as "Destionation DEVs".

Cl **08** *SC* **8.6.4** *P* **198** *L* **32** **#** **713**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *Beacon*

Incorrect wording or specification in lines 32-47.

SuggestedRemedy

"After "recipient of" change "the IE" to "an IE" (2 occurrences). Change "IEs" before "shall" to "IE" (3 occurrences). Change "subsequent" to "consecutive" (3 occurrences). In line 42, change "the first IE announcement shall be made in a system wake beacon" to "the IE shall be announced in a System Wake beacon and the following mMinBeaconInfoRepeat-1 beacons". In line 43, change "the IEs shall be sent in mMinBeaconInfoRepeat subsequent SPS set wake beacons" to "the IE shall be sent in a Next Wake beacon and the following mMinBeaconInfoRepeat-1 beacons".
Replace lines 46 and 47 as follows: "A CTA IE is considered to be intended for all DEVs if the SrcID or/and DestID contained in that IE is the BcstID or McstID, and otherwise for the pair of DEVs defined by the SrcID and DestID."

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. After "recipient of" change "the IE" to "an IE" (2 occurrences). Change "IEs" before "shall" to "IE" (3 occurrences). Change "subsequent" to "consecutive" (3 occurrences). Use 'at least' in all the references to the number of repeated beacons. In line 42, change "the first IE announcement shall be made in a system wake beacon" to "the IE shall be announced in a System Wake beacon and at least the following mMinBeaconInfoRepeat-1 beacons". Line 43 is modified as indicated in CID 309.
Replace lines 46 and 47 as follows: "A CTA Status IE is considered to be intended for all DEVs if the DestID contained in that IE is the BcstID or McstID. Otherwise the CTA Status IE is intended for the DEV defined by the DestID."
The standard does not allow the BcstID or McstID to be used for SrcID except that the BcstID is allowed for an MCTA, but this CTA is not announced with a CTA Status IE. The SrcID of the CTA status IE is informed of this information with a directed Channel Status Response command that requires and ACK. The CTA Status IE main purpose is to inform the destination, not source.

Response: Change "all DEVs" to "all or a group of DEVs" (McstID does not reference all).

Cl **08** *SC* **8.7** *P* **199** *L* **31** **#** **715**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *Frag*

"Ambiguous specification in line 31, page 199: The draft never defines a fragmentation threshold on a per stream basis, as implied by "the fragmentation threshold for the current isochronous stream or asynchronous data"."

SuggestedRemedy

Clarify the undefined phrase.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. On page 199, line 30 change 'Fragmentation is performed ... stream or asynchronous data.' to be 'Fragmentation may be performed at the transmitting DEV on each MSDU.' On line 31 change 'commands' to be 'commands, i.e. MCDUs,'. On page 199, line 34 delete 'for any reason and all the retransmissions shall obey the original fragmentation threshold of the MSDU/MCDU.' Change 'aMinFragmentSize' to be {xref pMinFragmentSize}.

Response: Change the last word of this paragraph from "piconet" to "PNC".

Cl **08** *SC* **8.8.3** *P* **200** *L* **37** **#** **720**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *ACK/Dly*

Ambiguous specification: The last paragraph of 8.7 is the only place indicating that MSDUs must be delivered to the upper layer in order when they are transmitted with the Dly-ACK mechanism.

SuggestedRemedy

"If this is the intent for Dly-ACK, restate it clearly in 8.8.3"

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Add text that indicates that Dly-ACK frames are passed up in order. See the resolution of CID 721.

Response: 1. Replace "Acknowledgment" with "ACK" in the headling to be consistent with the preceeding two headings.

2. Do not restrict Dly-ACK to isochronous streams only, especially considering the upcoming high data rate UWB based PHY. In fact, the last sentence of page 206 (D16-pre2) implies that asynchronous MSDUs may be sent with the Dly-ACK policy. Why are asynchronous MSDUs allowed to be delivered out of order?

3. Rename "Dly-ACK" to "Group-ACK" or "Block-Ack", as the name is misleading (the Dly-ACK frame is not delayed at all when in response to a Data frame with the Delayed ACK request set to 1) and impacts the understanding of this mechanism by most people and as this mechanism may be expected to be an important one in supporting the UWB based PHY.

4. In line 6, page 206 (D16-pre2), change "pMaxFrameBodySize MPDUs the source DEV may send in one burst. Because the receiver buffer requirement" to "MPDUs of Frame Payload size equal to pMaxFrameBodySize the source DEV may send between two . Because the receiver buffer size". Note that the term "burst" is not defined.

Cl **08** *SC* **8.8.3** *P* **200** *L* **44** **#** **721**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *ACK/Dly*

"Is the receiving MAC supposed to wait for any missing frames? If so, for how long? For instance, the sender sent 5 consecutive frames, of which frame 1 was not received by the recipient but was discarded by the sender after its last transmission (due to exceeding delay limit. Should the recipient hold all the received frames after frame 1 in waiting for frame 1? The issue is resolved in a similar mechanism defined in the latest 802.11e draft, which introduces a field in the frame requesting a Dly-ACK to indicate a Sequence Control value such that all frames with a smaller Sequence Control value have been discarded by the sender and hence should not be awaited by the recipient. This expedites the delivery of received frames to the upper layer in the case of missing frames at the recipient. "

SuggestedRemedy

Resolve this synchronization issue.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. On page 201, line 25 add the following as a new paragraph: 'The destination MAC shall deliver MSDUs for each isochronous stream in ascending MSDU number order to its FCSL. If necessary to accomplish this, a destination MAC may discard correctly received (and potentially acknowledged) frames. Asynchronous MSDUs shall be delivered to the FCSL in the order of reception.'

Response: 1. The new text still does not answer the questions raised in the original comments.

2. Why are asynchronous MSDUs allowed to be delivered out of order?

Cl **09** *SC* *P* *L* **#** **373**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *SEC/Key*

In the current draft, if devices do not yet share a key, these use the broadcast key. This creates a false sense of security.

SuggestedRemedy

Suggested remedy: correct this violation of proper security policy.

Proposed Response *Response Status* **W**

REJECT. The DEVs know that they are sharing information with all of the DEVs in the piconet. If this is unacceptable, they can use peer-to-peer security. In some cases a group key for the piconet is sufficient security because only one entity will authorize access.

Cl **10** *SC* *P* *L* **#** **376**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *MultiCast*

Allow multicasting, both secure and non-secure.

SuggestedRemedy

Suggested remedy: This will be provided separately.

Proposed Response *Response Status* **W**

REJECT. Authentication for multicast groups is outside of the scope of the PAR.

Cl **10** *SC* *P* *L* **#** **338**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

Throughout the draft, the security arguments should clearly distinguish between the different security suites defined. Moreover, each security suite shall refer to an external and vendor-independent standard for the claimed bit-security level. This applies both to the public-key based key establishment protocols (currently: ECC, RSA, and Lattice-based) and to the symmetric-key algorithms (currently: AES-CCM). If this evidence cannot be provided, the security suite shall be removed.

SuggestedRemedy

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Remove the security suites and update the draft consistent with the criteria listed in 03/032r3.

Cl **10** *SC* *P* *L* **#** **374**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *SEC*

Remove all unnecessary data expansion due to sending over and over again security status information.

SuggestedRemedy

This will be provided separately.

Proposed Response *Response Status* **W**

REJECT. This subject is appropriate for a follow-on PAR when there is more experience with a standard. This is an efficiency issue only.

Cl **10** *SC* *P* *L* *#* **375**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *aInterop/SEC*

Incorporate a way to have 802.15.3a devices interoperate with 802.15.3 devices, while using a more efficient symmetric security suite than the AES-CCM suite as in the current draft.

SuggestedRemedy

This will be provided separately.

Proposed Response *Response Status* **W**

REJECT. This standard only deals with TG3 and the encryption specification is adequate for these data rates.

Cl **10** *SC* **10.4** *P* *L* *#* **372**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *SEC*

The NTRUEncrypt security suite is not scalable (since it does not have a sub-suite using certificates). According to Annex C, only scalable solutions would be implemented with this standard. S.

SuggestedRemedy

specify a sub-suite of the NTRUEncrypt security suite using certificates. Failure to do so shall result in removal of the NTRUEncrypt security suite altogether.

Proposed Response *Response Status* **W**

REJECT. There is no reference in the draft for scalable security suites. The working group felt strongly that certificates should be optional, not required, based on the application space that 802.15.3 is addressing.

Cl **10** *SC* **Clause 10.2.1** *P* **284** *L* *#* **365**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *SEC*

The OIDs used in this standard all have the same prefix of 9 bytes. The OIDs can therefore be encoded more economically, by only encoding the sub-strings hereof that may differ. Thus, the OIDs for security sub-suites, currently encoded using 10 bytes, can be encoded using 2 bytes only. In fact, one could encode these sub-suites using an even more compact representation, by enumerating the OIDs for the sub-suites and encoding the corresponding integers as binary strings (this would allow encoding of OIDs as 1-byte strings). The current encoding is extremely wasteful.

SuggestedRemedy

adopt the efficient encoding of OIDs proposed above and do away with the current wasteful encoding.

Proposed Response *Response Status* **W**

REJECT. The extra 8 octets over the air have an inconsequential effect on the overall throughput of the piconet because they are sent infrequently. Futhermore, there are techniques to efficiently store these in memory.

Cl **10** *SC* **Clause 10.4** *P* *L* *#* **371**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

The changes to the NTRUEncrypt primitive in Clause 10.4 constitute far more than guarding against the padding scheme attack. This suggests that NTRUEncrypt is not robust.

SuggestedRemedy

One should have credible evidence that NTRUEncrypt, as defined in this D14 draft specification, is robust, including independent confirmation of the claimed security level, both for the cryptographic primitive, the padding scheme, and the key establishment protocol around it. Failure to do so shall result in the removal of the security suite.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Remove the security suites and update the draft consistent with the criteria listed in 03/032r3.

Cl **10** *SC* **Clause 10.4.1.1** *P* **300** *L* *#* **377**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

The NTRUEncrypt Security Suite should be complete and specify domain parameters, security parameters, and scheme options (see EESS #1, Draft 5). Some of these items are missing, such as the wrapping tolerance, message padding method, private key space, and key generation primitive.

SuggestedRemedy

Completely specify the NTRUEncrypt security suite.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Remove the security suites and update the draft consistent with the criteria listed in 03/032r3.

Cl **11** *SC* **11.4.4** *P* **331** *L* *#* **826**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PHY*

"There is an inconsistency between equation (8), which defines x_init, and Table 126. The vector x_init specifies the initial state for the scrambler as x_init = [x_(n-1)^i ... x_(n-15)^i], whereas Table 126 specifies the seed for the scramble as x_15 ... x_0. First, x_15 ... x_0 represents 16 bits, but only 15 bits are need to specify the initial state.
Second, how does x_15 through x_1 map onto [x_(n-1)^i ... x_(n-15)^i]?"

SuggestedRemedy

Specify the mapping or correct the notation.

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Change x^15 to be x^14 in table 126. Let n=15 in the xinit matrix and map x_(n-1) to x_14, etc. in the text.

Response: After "equation (8)" add "is".

Cl **B** *SC* **Annex B.1** *P* *L* **# 332**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

The specification of the CCM mode does NOT match the specification of this mode in 802.11 Tgi (contrary to the message conveyed by the 802.11/802.15 liaison Dan Bailey at the closing ceremony of the IEEE 802 meeting in Hawaii and all the way back in Sydney, when we were voting in symmetric key cipher suites to be used). See also the 802.11 Tgi submissions as of March 6, 2002 (02/001r1) and as of May 28, 2002 (02/001r2). See also Draft D2.5 of 802.11 Tgi that was released in Nov 2002 (Clause 8.3.4.4). Moreover, the AES-CCM mode specification in 802.11 TG I DOES match the officially submitted specification of this mode to NIST, with as reference "R. Housley, D. Whiting, N. Ferguson, Counter with CBC-MAC (CCM), submitted to NIST, June 3, 2002. Available from http://csrc.nist.gov/encryption/modes/proposedmodes/." Following the official NIST-submission would have obvious advantages, as this would allow single-chip implementations for devices that support both 802.11 and 802.15; it would allow proper cryptographic scrutiny of AES-CCM by the brightest cryptographic minds in the community without the need to translate the impact of their cryptanalysis on our current 'twisted' specification; it would also allow for simplified integer arithmetic.

SuggestedRemedy

adapt the AES-CCM mode as specified in the current draft, such as to follow the official NIST submission specification. This is relatively straightforward, since it merely comes down to reformatting blocks in the presently described specification.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Resolve as indicated in CID 333.

Cl **B** *SC* **Annex B.1.2** *P* **354** *L* **# 333**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

the encoding of the integers L and M in the authentication flags octet (see Figure B.2) follows highest-order bit last conventions for encoding an octet as integer, whereas the length encoding (see Figure B.3) follows lowest-order bit last conventions (e.g., 0xFEFF corresponds to 216-28). The current inconsistency in integer representation conventions unnecessarily increases the complexity of implementing integer arithmetic.

SuggestedRemedy

Suggested remedy: use lowest-order bit last conventions everywhere throughout all security specifications (e.g., 802.11 does this.)

Proposed Response *Response Status* **W**

ACCEPT.

Cl **B** *SC* **Annex B.1.2** *P* **355** *L* **2426** **# 334**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

(and elsewhere): To avoid ambiguity, 'concatenation' should read 'right-concatenation'; similarly, 'appending' should read 'right-appending'.

SuggestedRemedy

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. The terms 'right' and 'left' are ambiguous. Change 'concatenation' to be 'concatentated as the higher order octets' and 'appending' with 'appending as the higher order octets'

Cl **B** *SC* **Annex B.1.2** *P* **355** *L* **42** **# 335**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *SEC*

The last operation (on the XOR of Bn and Xn) has as output Xn+1 rather than T (since the tag T corresponds to a certain prefix of Xn+1 only).

SuggestedRemedy

Proposed Response *Response Status* **W**

REJECT. The proposed resolution (in document 03/046r1) only replaces the equation with a sentence. Either are correct, but the equation is less likely to lead to misinterpretation. Finally, first M octets is unambiguous whereas 'left' and 'right' are open to interpretation.

Cl **B** *SC* **Annex B.1.3** *P* **356** *L* **2930** **# 336**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

To avoid ambiguity, 'concatenation' should read 'right-concatenation'. Similarly, 'first' should read 'leftmost'.

SuggestedRemedy

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. The terms 'right' and 'left' are ambiguous. Change 'concatenation' to be 'concatentated as the lower order octets'.

Cl **B** *SC* **Annex B.1.4** *P* **356** *L* **39** **#** **337**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

m is the plaintext, not the encrypted message.

SuggestedRemedy

change 'encrypted message m' to 'encrypted message'. Alternatively, define the cipher-text in a more formal way and refer thereto. See also 02/469r0.

Proposed Response *Response Status* **W**

ACCEPT.

Cl **C** *SC* **Anex C.2** *P* **364366** *L* **#** **342**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

(and Pages 368-369, Annex C.5): The security arguments should be based on proper security analysis and not merely on an ad-hoc informal argument (the latter might have been common place 20 years ago, but cryptography has moved on). Currently, the security analysis for the key establishment mechanisms based on NTRUEncrypt and RSA are based on such ad-hoc informal analysis. The security analysis of ECMQV is even obscured! (witness the reference on Page 368, line 21 to 'The security suite specifications in this document are able to specify other algorithms).

SuggestedRemedy

Replace the ad-hoc security analysis of the public-key mechanisms by proper security arguments, both for each of the public-key mechanisms in the current Draft D15 standard, and for the symmetric-key based mechanisms, such as authenticated key transport, data encryption and authentication, and key updates.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. The security suites will be removed so this change no longer needs to be made.

Cl **C** *SC* **Annex C.1.2** *P* **363** *L* **#** **340**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

although the network size is restricted to at most 256 devices at any instance, this is not true over time (since devices may join and leave the network in an ad-hoc fashion and may not have met before). Thus, the security solution should scale arbitrary sets of devices (which may not have met before at all), rather than to a fixed set of limited size.

SuggestedRemedy

adapt the text accordingly.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Add text that indicates that the ACL will potentially contain more than 256 DEVs as you may want to keep track of DEVs that move in and out of the piconet. 'Although there is a fixed upper bound of fewer than 255 DEVs in a piconet, the security solution might need to scale to arbitrary sets of DEVs, rather than to a fixed set of limited size. DEVs join and leave the network in an ad-hoc fashion and in some cases, will not have previously communicated with the other DEV(s).'

Cl **C** *SC* **Annex C.1.3** *P* **364** *L* **#** **341**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *SEC*

specify the security threat model that is assumed at system set-up. Without a proper indication of the threats considered, one cannot draw conclusion on the security provided by the 802.15.3 WPAN.

SuggestedRemedy

Proposed Response *Response Status* **W**

REJECT. Annex C is an informative annex and information on the threat models is not required for proper implementation of the standard.

Cl **C** *SC* **Annex C.1.4** *P* **364** *L* **#** **343**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **A** *SEC*

The selection criteria described in this clause miss any rationale. We give two examples: (1) 'time to market': not all the security suites are robust and time-tested security technology, witness the recent changes to NTRUEncrypt from Draft D11 towards D14 that were necessitated by recent attacks on their padding scheme and the non-acceptance of the NTRUEncrypt technology in any standard that is not controlled bt NTRU, Inc. (2) 'market suitability': to-date, there is not even a single published review of the adequacy of any of the protocols in the standard for 802.15.3 applications.

SuggestedRemedy

completely remove this clause, as it is misleading.

Proposed Response *Response Status* **W**

ACCEPT.

Cl **C** *SC* **Annex C.2** *P* **364** *L* **34** **#** **344**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *SEC*

1the '802.15.3 security model' to which this clause refers is nowhere to be found!

SuggestedRemedy

provide an adequate security model (the current wording is misleading).

Proposed Response *Response Status* **W**

REJECT. Annex C is an informative annex. The security model is not required to correctly implement the standard. The security model is outside of the scope of the standard.

Cl **C** *SC* **Annex C.5** *P* **368369** *L* **#** **346**

Struik, Rene Certicom Corporation

Comment Type **TR** *Comment Status* **R** *SEC*

The RSA-based and NTRUEncrypt-based public-key establishment protocols that are claimed to be based on TLS, but do deviate from this protocol in so many aspects that the suggestions as if the security analysis for TLS would also automatically apply to the ad-hoc variant of TLS used for the RSA- and NTRUEncrypt-based protocols is misleading.

SuggestedRemedy

Provide a proper and adequate rationale that the variant of TLS used for the RSA-based and NTRUEncrypt-based public-key key establishment protocols is as secure as the underlying cryptographic primitives.

Proposed Response *Response Status* **W**

REJECT. Annex C is an informatve annex. The analysis in Annex C is felt to be a proper analysis. The annex details the ways in which the present method differs from TLS and addresses those issues.