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* **W**

ACCEPT.

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 **00** *SC* **00** *P* **00** *L* **00** # **91**

Freedman, Avraham Hexagon System Engi

Comment Type **TR** *Comment Status* **R** *aInterop*

I have a problem with this standard. I believe 15.3 should have been completely interoperable with 15.1, 15.3 and 11b. Although it seems that 15.3 has put some effort towards that goal, it did not take the last steps, whic are essential. The result is that 802 is now sending quite a confused message to the market. What device should the portable/mobile computer be equipped with? 11g? 15.1? 15.3? All of the above? Neither? Does 802.15 have any roadmap towards some kind of unification? Despite of that, I voted "approve", because I appreciate the effort put into the standard. However, I would like to see, or more importantly, I want RevCom to see the group rebuttal, and I hope some effort towards a more interoperable WPAN standard is going to be made.

SuggestedRemedy

Make the change as requested.

Proposed Response *Response Status* **W**

REJECT. The PAR for 802.15.3 identified a class of applications that required a MAC that was fundamentally different from 802.11's MAC, and so interoperability with 802.11 at a MAC level was not possible without seriously compromising the performance of 802.15.3. Although interoperability with other wireless standards is not required in the 802.15.3 PAR, Annex D in the standard does address the issue of interoperability with other IEEE wireless standards. The Annex indicates that it is possible for an implementer to build a DEV that could switch between 802.11b and 802.15.3, i.e. a dual-mode device. Not only that, specific choices in the selection of the PHY characteristics were made that make interoperability easier. In addition, some companies already have dual-mode solutions that can do both 802.15.1 and 802.11b with only a modest increase in the cost of the solution. These same techniques can be used to create dual-mode 802.15.3/802.15.1 implementations.

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* **5.3.10** *P* **19** *L* **#** **394**

Ho, Jin-Meng — Texas Instruments

Comment Type **TR** *Comment Status* **A** *aEditorial*

Incorrect statement in the last paragraph in line 47.

SuggestedRemedy

"Replace "In addition to the power save modes" with "Regardless of the power management mode"."

Proposed Response *Response Status* **W**

ACCEPT.

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* **W**

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.

Cl **06** *SC* **6.3.13** *P* **57** *L* **2** # **430**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *PNCHndOvr*

Parameters missing in Table 17.

SuggestedRemedy

"Create a new row as follows: NewPNCDEVAddress, MAC address, Any valid individual MAC address, The DEV address of the DEV being requested to assume PNC responsibilities. Create another new row as follows: HandoverCountdown, Integer, 0-NmbrHndOvrBcns-1, The number of beacons the old PNC will transmit before control of the piconet is turned over to the new PNC. Create yet another row as follows: NumberOfCTRBs, Integer, 0-255, The number of CTRBs, excluding requests for asynchronous channel time, currently being serviced by this PNC. Create one more row as follows: NumberOfSPSSets, Integer, 0-255, The number of SPS sets currently being serviced by this PNC."

Proposed Response *Response Status* **W**

REJECT. The DME already knows the mapping between DEVID and MAC address, in fact it is the DME and FCSL that map MAC addesses into DEVIDs, not the MAC or MLME. The other proposed parameters are not used by the DME. The handovder countdown is a local timing requirement of the MAC. The number of CTRBs is not passed to the DME because the CTRBs are used only by the MAC/MLME, 8.5.1.1 and 8.5.2.1. The number of SPS sets is only used by the MAC/MLME and is not used by the DME, 8.13.

Cl **06** *SC* **6.3.13** *P* **57** *L* **5** # **429**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PNCHndOvr-e*

Parameter misnaming in Table 17 in lines 5-6.

SuggestedRemedy

"Change "PNCCapableDEVID" to "NewPNCDEVID"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.3.13.1** *P* **57** *L* **32** # **431**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PNCHndOvr-e*

Parameter misnaming and parameter missing in lines 32-38.

SuggestedRemedy

"Rename "PNCCapableDEVID" to "NewPNCDEVID", and after this parameter add "NumberofDEVs,"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.3.13.2** *P* **58** *L* **6** # **434**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *PNCHndOvr*

Parameters missing (6-9.

SuggestedRemedy

"After "NumberOfDEVs," add "NmbrHndOvrBcns," and "DEVInfoSet,"."

Proposed Response *Response Status* **W**

REJECT. The MSC in figure 98 shows that the MLME-PNC-HANDOVER.indcation is only used at the beginning and end of the handover process. At the beginning of the handover, the NmbrHndOvrBcns and the DEVInfoSet are not known by the new PNC. At the end of the handover process, the NmbrHndOvrBcns has no meaning and the DEVInfoSet has already been passed to the new PNC. If the .indication says that the handover process has been canceled, then neither of these parameters are required either.

Cl **06** *SC* **6.3.13.5** *P* **59** *L* **19** # **436**

Ho, Jin-Meng Texas Instruments

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

Parameter list missing in line 19.

SuggestedRemedy

"Add the following parameters in the parentheses: NewPNCDEVID, NewPNCDEVAddress, HandoverCountdown."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Add NewPNCDEVID and NewPNCDEVAddress, the HandoverCountdown is a timing parameter local to the MAC/MLME and doesn't have significance here.

Cl **06** *SC* **6.3.15** *P* **62** *L* **23** # **437**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PNCHndOvrACL*

Ambiguous Valid range for ResultCode in Table 19 in lines 23-25.

SuggestedRemedy

Clarify in 6.3.15.4.2 what result would correspond to a ResultCode of DENIED.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. The DENIED code is no longer necessary due to changes in the ACL handover command. Delete 'DENIED'.

Cl **06** *SC* **6.3.15.1.2** *P* **63** *L* **48** # **438**
Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PNCHndOvrACL*

Incomplete statement in lines 48-49.

SuggestedRemedy

"After "security information" add "about the DEV specified by the QueriedDEVID as" and change "that DEV" to "the DEV of TrgtID"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change "that DEV" to "the DEV of TrgtID". The request command asks for all of the security information that is managed by the QueriedDEVID, not just information about the QueriedDEVID.

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* **W**

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.

Cl **06** *SC* **6.3.18** *P* *L* # **490**
Ho, Jin-Meng Texas Instruments

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

Missing subclauses.

SuggestedRemedy

Create a new subclause to define an MLME-TERMINATE-STREAM.indication primitive.

Proposed Response *Response Status* **W**

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.

Cl **06** *SC* **6.3.18** *P* *L* # **488**
Ho, Jin-Meng Texas Instruments

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

Missing subclauses.

SuggestedRemedy

Create new subclauses to define MLME-MODIFY-STREAM.indication and MLME-MODIFY-STREAM.response primitives.

Proposed Response *Response Status* **W**

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.

Cl **06** *SC* **6.3.18** *P* *L* # **486**
Ho, Jin-Meng Texas Instruments

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

Missing subclauses.

SuggestedRemedy

Create new subclauses to define MLME-CREATE-STREAM.indication and MLME-CREATE-STREAM.response primitives.

Proposed Response *Response Status* **W**

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.

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* **W**

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.

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* **W**

ACCEPT.

Cl **06** *SC* **6.3.18.1** *P* **70** *L* **47** # **483**

Ho, Jin-Meng Texas Instruments

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

"Incorrect parameter range in Table 22 in lines 47-50: The actual result of a request is contained in the "ReasonCode" instead of the "ResultCode". How is a ResultCode of FAILURE generated?"

SuggestedRemedy

"Change the "Valid range" of "ResultCode" as follows: RESPONSE_RECEIVED, TIMEOUT. Change the corresponding "Description" to "Indicates if the request has received a response (an ACK in the case of stream termination) or timed out." "

Proposed Response *Response Status* **W**

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

Cl **06** *SC* **6.3.18.3** *P* **71** *L* **34** # **487**

Ho, Jin-Meng Texas Instruments

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

Missing parameter in lines 34-44.

SuggestedRemedy

"After "CTR-TU," add "Priority," to the parameter list."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.3.18.4** *P* **72** *L* **11** # **489**

Ho, Jin-Meng Texas Instruments

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

Missing parameter in lines 11-15.

SuggestedRemedy

"Before "ResultCode" add "ReasonCode," to the parameter list."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.3.2.2.1** *P* **31** *L* **42** # **398**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *Scan*

Incomplete statement.

SuggestedRemedy

"Replace "or when it" with " when the desired BSID or PNID is found, or when the MLME"."

Proposed Response *Response Status* **W**

REJECT. The DEV is required to scan through all of the requested channels before it returns the .confirm. One reason for this is that DEV might find multiple piconets with the same PNID or BSID and it should report to the DME all of the relevant piconets that it defines.

Cl **06** *SC* **6.3.20.2** *P* **76** *L* **6** # **492**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *ChnlStatus*

Missing parameters in lines 6-8.

SuggestedRemedy

"After "OrigID" add to the parameter list ", MeasurementWindowSize, TXFrameCount, RXFrameCount, RXFrameErrorCount, RXFrameLostCount"."

Proposed Response *Response Status* **W**

REJECT. These parameters are not coming from the requestor, rather the DME is keeping track of the channel status so that it can compute channel time requests and to determine which PHY data rates to use.

Cl **06** *SC* **6.3.20.2.1** *P* **76** *L* **14** # **493**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *ChnlStatus*

Incomplete statement in lines 14-15.

SuggestedRemedy

"After "DEV" add "and performing the requested channel measurement"."

Proposed Response *Response Status* **W**

REJECT. The MAC/MLME does not perform any measurements, rather the DME responds via MLME-CHANNEL-STATUS.respone primitive with the numbers that it has been collecting over a previous measurement window size.

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* **W**

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.

Cl **06** *SC* **6.3.21.1** *P* **78** *L* **31** # **497**

Ho, Jin-Meng Texas Instruments

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

Redundant Table --Table 26: There is no need to define a new set of PiconetDescription just for remote scanning purposes.

SuggestedRemedy

Delete Table 26 and adjust the numbering for subsequent tables accordingly.

Proposed Response *Response Status* **W**

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.

Cl **06** *SC* **6.3.21.2** *P* **79** *L* **6** # **498**

Ho, Jin-Meng Texas Instruments

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

Missing parameters from the parameter list in lines 6-8.

SuggestedRemedy

"After "ChannelList," add to the parameter list all the parameters that appear in the next primitive, MLME-REMOTE-SCAN.response."

Proposed Response *Response Status* **W**

REJECT. The scan has not yet been performed when this primitve is issued, see Figure 131, so these parameters are not yet available.

Cl **06** *SC* **6.3.21.2.1** *P* **79** *L* **14** # **499**

Ho, Jin-Meng Texas Instruments

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

Incomplete statement in lines 14-15.

SuggestedRemedy

"After "PNC" add "and performing or denying the requested remote scan"."

Proposed Response *Response Status* **W**

REJECT. The DME controls the scan process and it happens after it receives the the MLME-REMOTE-SCAN.indication primitive as illustrated in Figure 131.

Cl **06** *SC* **6.3.21.2.2** *P* **79** *L* **19** # **500**

Ho, Jin-Meng Texas Instruments

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

Incomplete wording in lines 19.

SuggestedRemedy

"Change "may send" to "sends"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.3.21.4.2** *P* **80** *L* **26** # **502**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *Scan/Remote-e*

Incorrect and unnecessary statements in lines 26-29.

SuggestedRemedy

"Delete the statements beginning from "If unsuccessful" to "on its behalf.". Also note that the parameter "REQUEST_DENIED" is contained in the "ReasonCode" but not the "ResultCode"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.3.22.1** *P* **81** *L* **14** # **503**

Ho, Jin-Meng Texas Instruments

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

Incomplete Description in Table 27 in line 14.

SuggestedRemedy

"After "PNID" add "/BSID"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.3.23.3.2** *P* **83** *L* **44** # **508**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *TPC-e*

Incorrect statement in line 44.

SuggestedRemedy

"After the "ACK was" delete "not"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.3.24** *P* **84** *L* **2** # **509**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PM-e*

"Incorrect wording: The words "PS modes" in this draft sometimes means power save (PS) modes only and sometimes means power management (PM) modes which include ACTIVE mode."

SuggestedRemedy

"Change "PS mode" to "PM mode", "PS modes" to "PM modes" and "PS-MODE" to "PM-MODE" throughput this subclause, including the tables therein. "

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Throughout sub-clause 6.3.24 and its tables, when the term 'PS mode' refers to all four modes use 'PM mode' instead, including in the naming of the MLMEs. This will affect the MSCs and some of the text in clause 8 as well.

Cl **06** *SC* **6.3.24** *P* **84** *L* **2** # **512**

Ho, Jin-Meng Texas Instruments

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

Incorrect Valid range in the first row of Table 29: HIBERNATE is one of the PS modes.

SuggestedRemedy

"Either delete "HIBERNATE," or expand "PS" into "SPS, PSPS"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change the name from PSSwitchOperation to PSMode to match the frame formats. The frame formats in 7.5.7.1 only specify 3 states because PS is used to switch to PSPS, SPS or both SPS and PSPS.

Cl **06** *SC* **6.3.24** *P* **84** *L* **2** # **510**

Ho, Jin-Meng Texas Instruments

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

Unspecific Valid range and Description in Tables 29 and 30.

SuggestedRemedy

"Replace "As defined in…" with specific valid range or description."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. It is extremely difficult to keep normative definitions synchronized between separate sections of the standard. To avoid this problem, the standard tries to define any given requirement only once and to then cross reference to it in the text where appropriate. This makes the standard easier to maintain and less likely to have errors. However, there is one problem with the valid range cross-references in Table 29 and 30. Add to 7.5.7.2 'The PS set indices are defined as:
0x00 -> APS set
0x01 -> PSPS set
0x02-0xFD -> DSPS sets
0xFE-> Unallocated SPS set
0xFF -> Reserved'

Also add a xref to 8.13 to all of the 7.5.7 xrefs that don't have it already.

Cl **06** *SC* **6.3.24** *P* **84** *L* **2** # **511**

Ho, Jin-Meng Texas Instruments

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

Naming inconsistencies: The names of some parameters in Tables 29 and 30 and the following primitives are different from those of the corresponding fields defined in 7.5.7 for the related commands.

SuggestedRemedy

"Throughout 6.3.24, change 'PSSwitchOperation" to "NewPMMode", "PSSetOperation" to "OperationType", "PSStructureSet" to "PSSetStructureSet", "DEVIDMapLength" to "BitmapLength", and "DEVIDMap" to "DEVIDBitmap"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Throughout 6.3.24, change 'PSSwitchOperation" to "PMMode", "PSSetOperation" to "OperationType", "PSStructureSet" to "PSSetStructureSet" (this change is especially essential since it means a set of sets), "DEVIDMapLength" to "BitmapLength", and "DEVIDMap" to 'DEVIDBitmap'

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* **W**

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.

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* **W**

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.

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* **W**

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.

Cl **06** *SC* **6.3.24.3** *P* **86** *L* **7** # **223**

Lynch, Jerry XtremeSpectrum

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

[PM] Small changes to support new TrgtID field in the PS Mode change command.

SuggestedRemedy

Add parameter TrgtId to MLME-PS-MODE-CHANGE.request. Add TrgtId to table 29, page 84: TrgtId, Integer, as defined in 7.5.7.1.

Proposed Response *Response Status* **W**

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

Cl **06** *SC* **6.3.24.7.2** *P* **88** *L* **17** # **516**

Ho, Jin-Meng Texas Instruments

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

Incorrect statement in lines 17-18.

SuggestedRemedy

Replace the first statement as follows: The DME is informed of the PM mode change to ACTIVE.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Replace the first sentence with 'The DME is informed of the PS mode change to ACTIVE.'

Cl **06** *SC* **6.3.3** *P* **32** *L* **36** # **399**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *Start*

Incorrect parameter range in Table 7 in line38.

SuggestedRemedy

"Delete "PICONET_DETECTED,"."

Proposed Response *Response Status* **W**

REJECT. The PNC is required in clause 8 to do a final scan prior to starting the piconet and so it may find all of the channels busy.

Cl **06** *SC* **6.3.3.2.2** *P* **33** *L* **47** # **400**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *Start*

The second statement in lines 47-48 is not applicable since the MLME/MAC is directed to start a piconet at a SPECIFIC channel.

SuggestedRemedy

"Delete the statement "If all of the channels for the PHY…set to PICONET_DETECTED."."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change 'If all of the channels for the PHY are occupied' to be 'If the requested channel is occupied'. The PNC is required to do a final scan before starting the piconet.

Cl **06** *SC* **6.3.5** *P* **37** *L* **14** # **401**

Ho, Jin-Meng Texas Instruments

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

Incorrect naming and reference in Table 9 in lines13-15 and the following primitives.

SuggestedRemedy

"Change "CapabilityField" to "OverallCapabilities" in Table 9 and in the parameter lists of the following MLME-ASSOCIATE.request and MLME-ASSOCIATE.indication primitives, and change the corresponding field name "Capabilities" to "Overall Capabilities" in 7.5.1.1. Also change "As defined in 7.4.12" to "As defined in 7.5.1.1 under "Type" and "Valid range" in Table 9."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Resolve as indicated in CID 297.

Cl **06** *SC* **6.3.5** *P* **37** *L* **40** # **403**

Ho, Jin-Meng Texas Instruments

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

"Incorrect parameter in Table 9 in lines 40-41: "AssociationStatus" is reported when a DEV receives a beacon containing a DEV Association IE. However, the DEV Association IE, and hence the "AssociationStatus", does not live up to the intent that any associated DEV can determine the DEVs currently associated with the PNC by having the PNC send a DEV Association IE in the beacon each time a DEV is associated or disassociated. Namely, any given associated DEV may not be able to determine the DEVs that had associated with the PNC earlier than it did, because that DEV, before associating with the PNC, could have missed the DEV Association IEs broadcasting the association status of those DEVs."

SuggestedRemedy

"Replace the "AssociationStatus" parameter with an "AssociationList" parameter, where "AssociationList" lists the DEVIDs and MAC addresses of all the DEVs associated with the PNC at the time the corresponding "Association List" IE is broadcast in the beacon, which occurs whenever a DEV is associated with or disassociated from the PNC."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. After a DEV gains membership in the piconet, i.e. after it associates if authentication is not required or after it authenticates if authenticationis required, the PNC broadcasts the PNC info command that contains not only the DEVID and DEV addresses of every DEV in the piconet, it also contains their capabilities. The complete list of DEVs in the piconet might make the beacon too long, so the standard uses the broadcast of the PNC info command, which can be fragmented, to communicate the list of DEVs in the piconet. This is described in 8.3.3. No change is required for the draft because this functionality is already provided.

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* **W**

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.'

Cl **06** *SC* **6.3.5.5** *P* **40** *L* **10** # **406**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *Assoc*

Incorrect wording in line 10. Incorrect parameter in line 18.

SuggestedRemedy

"Change "other associated DEVs" to "an associated DEV". Replace "AssociationStatus" with "AssociationList"."

Proposed Response *Response Status* **W**

REJECT. The list of active DEVs in the piconet is passed to the DME via the MLME-PNC-INFO.confirm, see also the resolution of CID 403. This MLME is used to notify DEVs that are already in the piconet that a new DEV has joined. The DEVs that are already in the piconet should already have the membership information, if not they can request in a directed frame from the PNC using the PNC Info Request command.

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* **W**

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."

Cl **06** *SC* **6.3.7.4.1** *P* **45** *L* **19** # **410**

Ho, Jin-Meng Texas Instruments

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

Incorrect statements in lines 19-20.

SuggestedRemedy

"After "there is no" add "authentication". Replace "shall" with "is" (2 occurrences). Change "SUCCESS" to "RESPONSE_RECEIVED"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. "After "there is no" add "authentication". Replace "shall be set to" with "is" (2 occurrences). Change "SUCCESS" to "COMPLETED".

Cl **06** *SC* **6.3.7.8.1** *P* **47** *L* **19** # **413**

Ho, Jin-Meng Texas Instruments

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

Incorrect statements in lines 19-20.

SuggestedRemedy

"Replace "shall" with "is" (2 occurrences). Change "SUCCESS" to "RESPONSE_RECEIVED"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. "Replace "shall" with "is" (2 occurrences). Change "SUCCESS" to "COMPLETED"."

Cl **06** *SC* **6.3.8.1** *P* **48** *L* **6** # **415**

Ho, Jin-Meng Texas Instruments

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

Incomplete parameter list in lines 6-9.

SuggestedRemedy

"After "TrgtID," add "SECID,"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.3.8.2** *P* **48** *L* **26** # **416**

Ho, Jin-Meng Texas Instruments

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

Incomplete parameter list in lines 26-29.

SuggestedRemedy

"After "OrigID," add "SECID,"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. A DEV is always requesting the current symmetric key associated with a security relationship when using the request key command. By sending a request key command to the TrgtID DEV, the security manager will know which relationship (TrgtID-OrigID) to reference for the key. The request key indication provides the OrigID and should also provide the TrgtID contained in the frame so the DEV can determine whether this message if for the piconet security manager or the peer security manager. Add TrgtID following the OrigID parameter in the request key indication MLME. The target DEV must send back the current SECID with the latest symmetric key. For the distribute key command, the originating security manager must designate the SECID value along with the symmetric key. To complete the protocol, the receiving DEV needs to send back the SECID that it received. Add SECID field to the frame format in Figure 60, 61, and 62. On page 141, lines 38-39, remove the second sentence of the first paragraph of section 7.5.2.5, "The SECID is the unique identifier for the security relationship with which the distributed key is associated."

Cl **06** *SC* **6.3.8.2.2** *P* **48** *L* **40** # **418**
Ho, Jin-Meng Texas Instruments

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

Incorrect specification in lines 40-41.

SuggestedRemedy

"Replace the paragraph as follows: Upon receipt of the MLME-REQUEST-KEY.indication with the ResultCode set to SUCCESS, the DME issues an MLME-REQUEST-KEY.response to the MLME."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.3.8.3.1** *P* **49** *L* **4** # **419**
Ho, Jin-Meng Texas Instruments

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

Incorrect specification in line 4.

SuggestedRemedy

Replace line 4 as follows: with the ResultCode set to SUCCESS.

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.3.9.1** *P* **50** *L* **27** # **420**
Ho, Jin-Meng Texas Instruments

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

Incomplete ResultCode Value range in Table 13 in lines 27-28.

SuggestedRemedy

"After "SUCCESS," add "FAILURE","."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.3.9.2.2** *P* **51** *L* **24** # **421**
Ho, Jin-Meng Texas Instruments

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

Misspelling in line 24.

SuggestedRemedy

"Replace "REQUEST" with "DISTRIBUTE"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.5.1** *P* **91** *L* **25** # **517**
Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *MAC/PIB*

Unspecific Definition in Table 33.

SuggestedRemedy

"Replace "As defined in…" with specific definition."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change 'MaxAssociations' to be 'MaxAssociatedDEVs' to match the name in 7.5.1.1. Also change this name in 6.3.5 as well.

Cl **06** *SC* **6.5.3** *P* **92** *L* **35** # **518**
Ho, Jin-Meng Texas Instruments

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

Missing mode in Table 35 in lines 35-36.

SuggestedRemedy

"Under "Octets Definition" add "0x02 = mode 2"."

Proposed Response *Response Status* **W**

REJECT. There are only two security modes defined in the draft, modes 0 and 1.

Cl **06** *SC* **6.6** *P* **94** *L* **31** # **519**
Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *MAC-SAP-e*

Incorrect Description in Table 39 in lines31-32.

SuggestedRemedy

"Change "Data portion of the MSDU" to "MSDU portion of the primitive"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.6.1** *P* **94** *L* **41** # **520**
Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *MAC-SAP-e*

Incorrect statement in line 41.

SuggestedRemedy

"Change "asynchronous MAC" to "asynchronous MSDU"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.6.1.2** *P* **95** *L* **8** # **521**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *MAC-SAP-e*

Incorrect statement in lines 8-11.

SuggestedRemedy

"Change "MSDU" to "MPDU" and "media" to "medium". Change "with an error" to "with the ResultCode set to INVALID_ACK_POLICY"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.6.2** *P* **95** *L* **15** # **522**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *MAC-SAP-e*

Incorrect statement in lines 15-16.

SuggestedRemedy

"Delete "due to a transmission timeout"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **06** *SC* **6.6.4.2** *P* **96** *L* **30** # **524**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *MAC-SAP-e*

Incorrect statement in lines 30-34.

SuggestedRemedy

"Change "MSDU" to "MPDU" and "media" to "medium". Rephrase the statement containing "as a stream source"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. "Change "MSDU" to "MPDU" and "media" to "medium".
Change 'If the StreamIndex for the request is not assigned to the DEV as a stream source,' to be 'If the StreamIndex for the request does not correspond to an existing stream with the DEV as the source,'

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* **W**

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.'

Cl **07** *SC* **7.2** *P* **108** *L* **53** # **530**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *FrmFrmt*

Misnaming in line 53.

SuggestedRemedy

"Rename "pMaxFrameSize" to "pMaxFrameBodySize" throughout the draft."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **07** *SC* **7.2.1** *P* **109** *L* # **531**

Ho, Jin-Meng Texas Instruments

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

This MAC does not accommodate VBR streams well.

SuggestedRemedy

"Use b11-b13 for a non-PNC DEV to request additional channel time for transferring remaining buffered data of the stream to which this frame belongs, when this frame is the last frame sent by this non-PNC DEV in the current superframe."

Proposed Response *Response Status* **W**

REJECT. Requiring the PNC to monitor all of the frames sent between devices is not feasible. Also, the use of the bits by the PNC is not clearly defined.

Cl **07** *SC* **7.2.7.4** *P* **113** *L* **#** **536**

Ho, Jin-Meng — Texas Instruments

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

Wording missing in lines 35 and 37. This causes ambiguity in the case of secure frames.

SuggestedRemedy

"Before "payload" add "Frame" and change "payload" to "Payload"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change 'payload field' to 'Frame Payload field' in this subclause, 2 places lines 35, 37.

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* **W**

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

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* **#** **544**

Ho, Jin-Meng — Texas Instruments

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

"Incorrect definition for "Burst" and hence for "Max Burst" in lines 50-51: Suppose five frames of consecutive sequence were transmitted but the second and fourth frames were not correctly received. The "burst" should include the third frame, even though this frame was correctly received, because the third frame would most likely be still sitting in the receive buffer in waiting for the missing second frame and hence occupied the receive buffer space--which the 'Max Burst" field was to indicate."

SuggestedRemedy

"Redefine the "Max Burst" field accurately."

Proposed Response *Response Status* **W**

REJECT. The Max Burst refers to the size of the remaing buffer on the receiver, so therefore it would include frame 3 in the example. The Max Burst is re-negotiated each time Dly-ACK is used. In the example, if the buffer held 8 frames, after the first burst, 3 would be filed (frames 1, 3 and 5) and so the next Max Bust would be set to 5 instead of 8. If there no more space available, the DEV would set Max Burst would be equal to 1.

Cl **07** *SC* **7.3.2.2** *P* **119** *L* **#** **546**

Ho, Jin-Meng Texas Instruments

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

Unwarranted field: The Max Frames field provides no more information than the Max Burst field.

SuggestedRemedy

Delete the Max Frames field and all references to it.

Proposed Response *Response Status* **W**

REJECT. The two fields 'max burst' and 'max frames' have two different uses. 'Max burst' indicates how many frames of the pMaxFrameSize length the destination can handle in one dly-ACK burst sequence. This value represents a buffering limitation in the destination DEV, i.e. what is the total storage capacity for data frame payloads that can be alloted before the destination MAC needs to get chance to process a burst. The destination may also be designed to arbitrate memory between different streams, e.g. every stream get a limited amount of memory, or every stream gets access to more memory for a limited time. The source DEV may send more frames than 'max burst' if their total frame body lengths are shorter than or equal to pMaxFrameSize * max burst. The 'max frames' field indicates another limitation in the destination DEV. The receiver function may only be able to store a certain amount of the 16 bit MPDU-IDs. There may also be a limitation of storage capacity for headers. These two limitations may also be per stream, totally, or any other implementation dependent limitation. A common application domain for 802.15.3 is low cost, low power, limited footprint devices with very limited amount of memory, so the protocol must provide a method to communicate such restrictions between the destination and source devices.

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* **W**

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.

Cl **07** *SC* **7.3.3.1** *P* **120** *L* **#** **549**

Ho, Jin-Meng Texas Instruments

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

Incomplete definition in lines 45-46.

SuggestedRemedy

"After "command block" add "and an FCS field"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Delete 'consists of a single command block and'

Cl **07** *SC* **7.3.4.1** *P* **122** *L* **#** **550**

Ho, Jin-Meng Texas Instruments

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

"Confusing naming: "Data" is already used to denote frames of type "Data", and now is also used to designate the frame payload of Data frames."

SuggestedRemedy

"Rename "Data" to "MSDU Payload" whenever it references the "Data" field of a Data frame."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. "Rename "Data" to "Data Payload" whenever it references the "Data" field of a Data frame."

Cl **07** *SC* **7.4** *P* **124** *L* **#** **551**

Ho, Jin-Meng Texas Instruments

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

"Confusing naming: "Data" is further used to represent the information field of information elements!."

SuggestedRemedy

"Rename "Data" to IE Payload" whenever it references the "Data" field of an IE."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **07** *SC* **7.4.1** *P* **125** *L* **32** # **554**

Ho, Jin-Meng — Texas Instruments

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

"Confusing definition in line 32: Do not use the word "associated with" since it already has a special meaning. Also, the channel time may be used by the DEV to send data from other streams than indicated by the Stream Index, as specified in Clause 8."

SuggestedRemedy

Rephrase the statement as follows: The Stream Index indicates the stream to which the channel time is allocated. The allocated DEV may use this channel time to send data belonging to other streams when this allocated stream has no more data to send.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change to 'The stream index, 7.2.5, indicates the stream corresponding to the channel time allocation.'

Cl **07** *SC* **7.4.11** *P* **130** *L* **3** # **561**

Ho, Jin-Meng — Texas Instruments

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

Incorrect statement in lines 3-4.

SuggestedRemedy

"Change "about certain characteristics of the CTAs" to "of certain characteristics of an allocated CTA"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change "about certain characteristics of the CTAs" to "of certain characteristics of a CTA". An allocated CTA would be an allocated channel time allocation, which would be redundant.

Cl **07** *SC* **7.4.13** *P* **131** *L* **29** # **566**

Ho, Jin-Meng — Texas Instruments

Comment Type **TR** *Comment Status* **A** *TPC*

"The current TX power" is actually referencing the "Current TX Power" field, but is not obvious at all without appropriate Capitalization."

SuggestedRemedy

Capitalize the first letters of the words forming proper names throughout this draft!

Proposed Response *Response Status* **W**

ACCEPT.

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* **7.4.16** *P* **133** *L* **34** # **444**

Ho, Jin-Meng — Texas Instruments

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

Incorrect value in line 34.

SuggestedRemedy

"Change "254" to "252"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **07** *SC* **7.4.4** *P* **126** *L* **19** # **555**

Ho, Jin-Meng Texas Instruments

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

"This IE does not serve the purposes it was intended for. The DEVs "newly" associated with the PNC and announced via this IE would not necessarily be known to DEVs that are associated later on (i.e., after the announcement of this IE."

SuggestedRemedy

"If this IE is to enable any given DEV associated in the piconet to be aware of all the other DEVs associated in the same piconet, rename it to "Association List" and redefine it such that it covers all the associated DEVs."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. This IE is only used to notify the existing members of the piconet about a new member that has just joined. DEVs that join the piconet after this DEV will find out about the existing DEVs in the piconet when the PNC broadcasts the PNC Info command after the new DEV joins the piconet. See also the resolution of CID 403. No change required for the draft since the requested capability is provided by the PNC Info command.

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* **W**

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}."

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* **W**

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.

Cl **07** *SC* **7.4.8** *P* **129** *L* **3** # **559**

Ho, Jin-Meng Texas Instruments

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

Incomplete specification in line 3.

SuggestedRemedy

"Add "a PSPS, " before "an SPS"."

Proposed Response *Response Status* **W**

REJECT. The PCTM bit is not used for PSPS DEVs because they listen to all of the system wake beacons and the beacons that follow any missed system wake beacons.

Cl **07** *SC* **7.5** *P* **135** *L* **9** # **449**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *Cmd*

The final statement of the first paragraph contradicts with its previous statement.

SuggestedRemedy

Delete this final statement.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change 'The PNC or destination DEV shall not respond to any command from a DEV that is not allowed to be sent as indicated in Table 53. The PNC or destination DEV may transmit an ACK following reception of the frame if the ACK policy is set to Imm-ACK.' to be 'The PNC or destination DEV shall ignore any command from a DEV that is not allowed to be sent as indicated in {xref Table 53}. The PNC or destination DEV shall transmit an Imm-ACK following reception of the frame if the ACK policy is set to Imm-ACK.'

Cl **07** *SC* **7.5.1.1** *P* **137** *L* **9** # **453**

Ho, Jin-Meng Texas Instruments

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

"Confusing naming in Figure 49 and the following text in lines 9 and 14: There is already a "Capability" information element, and here there are a "Capabilities" field, a "DEV Capabilities" field, and a "PNC Capabilities" field."

SuggestedRemedy

"In Figure 49 change "Capabilities" to "Overall Capabilities" and in lines 14-15 change "The capabilities" to "the Overall Capabilities". Also change "CapabilityField" in clause 6.3.5 and Table 9 to "OverallCapabilities"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. In Figure 49 change "Capabilities" to "Overall Capabilities" and in lines 14-15 change "The capabilities" to "the Overall Capabilities"

Cl **07** *SC* **7.5.2.1** *P* **139** *L* **#** **461**

Ho, Jin-Meng — Texas Instruments

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

Missing definitions.

SuggestedRemedy

"In Figure 4, after "OID Length" add "(=L sub m)". In the following text, define "Length", "OID" and "OID Length" fields."

Proposed Response *Response Status* **W**

ACCEPT.

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* **7.5.4.2** *P* **145** *L* **15** **#** **465**

Ho, Jin-Meng — Texas Instruments

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

Confusing naming in Figure 69 and the following text in lines 15 and 27.

SuggestedRemedy

"Change "Capability" to 'Overall Capabilities" (2 occurrences). Make the corresponding changes in 7.5.1.1."

Proposed Response *Response Status* **W**

ACCEPT. See also CID 453

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* **W**

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.'

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.

Cl **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* **W**

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.

Cl **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* **W**

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

Cl **07** *SC* **7.5.5.1** *P* **151** *L* **#** **571**

Ho, Jin-Meng — Texas Instruments

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

Ambiguous definition for the Target ID List Type field in lines 36-38: What is the additional information conveyed by this field? Does an asynchronous CTA request not always replace a previous asynchronous request?

SuggestedRemedy

Delete the Target ID List Type field and the paragraph defining it.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. It is possible that the asynchronous request will not replace the previous requests. This is described in 8.5.2.1 and should have been cross-referenced here. Add a cross-reference to 8.5.2.1 after 'all previous asynchronous requests'

Cl **07** *SC* **7.5.5.1** *P* **151** *L* **#** **572**

Ho, Jin-Meng — Texas Instruments

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

Ambiguous definition for the CTR time unit in lines 40-42.

SuggestedRemedy

"Change "for its request" to "for the CTA(s) it is requesting". After "units of CTA" delete "time". After "allocate" change "CTA time" to "CTAs". Delete the next statement "It also…"."

Proposed Response *Response Status* **W**

ACCEPT.

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* **W**

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.'

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* **W**

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."

Cl **07** *SC* **7.5.5.1** *P* **152** *L* **#** **478**

Ho, Jin-Meng — Texas Instruments

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

Confusing naming.

SuggestedRemedy

"Rename "CTR interval type" to "Rate Type" and "CTR Interval" to "Rate" throughout the draft."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Using 'rate' would be confusing with data rate. Rename "CTR interval type" to "CTA Rate Type" and "CTR Interval" to "CTA Rate" throughout the draft.

Cl **07** *SC* **7.5.5.1** *P* **152** *L* **#** **477**

Ho, Jin-Meng — Texas Instruments

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

Confusing naming.

SuggestedRemedy

"Rename "CTR type" to "Power Type" throughout the draft."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Rename "CTR type" to "CTA PM Type" throughout the draft.

Cl **07** *SC* **7.5.5.1** *P* **152** *L* **#** **573**

Ho, Jin-Meng — Texas Instruments

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

Incomplete definition in lines 45-46.

SuggestedRemedy

"After "CTR TUs" add "per CTA"."

Proposed Response *Response Status* **W**

ACCEPT.

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* **W**

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.'

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* **W**

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.'

Cl **07** *SC* **7.5.6.4** *P* **156** *L* **#** **582**

Ho, Jin-Meng — Texas Instruments

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

Incomplete definition in Figure 86.

SuggestedRemedy

"Expand Figure 86 to define "Piconet Description" such that it covers all the parameters (fields) listed in Table 6."

Proposed Response *Response Status* **W**

REJECT. The purpose of the remote scan request is to determine the level of potential interference on the current channel and other channels without disturbing the coordination function of the PNC. It also gives the PNC a longer 'reach' in finding out who might be the potential interferers. The PNC does not need this additional information to be able to determine the interferrence levels. This information is included in the scan process because the DEV might join one of the piconets that it finds.

Cl **07** *SC* **7.5.7.1** *P* **157** *L* **14** **#** **588**

Ho, Jin-Meng — Texas Instruments

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

"Incorrect range for the "PS mode" field: HIBERNATE is one of the PS modes."

SuggestedRemedy

"Either delete "Hibernate mode" or expand "PS mode" into "SPS mode" and "PSPS mode"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change 'PS mode' to be 'SPS mode' and change this in figure 144, also on page 216 line 4, page 217 line 19 and page 281, line 13.

Cl **07** *SC* **7.5.7.1** *P* **157** *L* **2** # **586**

Ho, Jin-Meng Texas Instruments

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

"Incorrect naming: As noted by this commenter earlier, the term "PS mode" is used to mean "PM mode" (power management mode), which includes ACTIVE mode and other modes (i.e., PS modes), and truly PS mode."

SuggestedRemedy

Change PS to PM (power management) when it references all power management modes.

Proposed Response *Response Status* **W**

ACCEPT.

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* **W**

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.'

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* **W**

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.

Cl **08** *SC* **8.1** *P* **161** *L* **30** # **597**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *MSC-e*

"Incorrect illustration in the last paragraph in lines 30-33 and Figure 95: A returned MLME-XXX.confirm does not necessarily contain a ResultCode of SUCCESS, because the result may be something other than SUCCESS or because the result may be encoded in the ReasonCode rather than the ResultCode as is the case in many primitives."

SuggestedRemedy

Delete this paragraph and Figure 95.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change 'SUCCESS' to be 'COMPLETED' in the figure and in the text.

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* **W**

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"

Cl **08** *SC* **8.11.2.1** *P* **212** *L* **53** # **764**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *TPC*

"Incorrect field name in line 53, page 212."

SuggestedRemedy

"Change "piconet maximum transmit power field" to "Max TX Power Level field". Change "maximum power level" to "Max TX Power Level"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **08** *SC* **8.11.2.1** *P* **213** *L* **2** # **767**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *TPC*

"Incorrect field name in line 2, page 213."

SuggestedRemedy

"Change "piconet maximum transmit field" to "Max TX Power Level field"."

Proposed Response *Response Status* **W**

ACCEPT.

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* **W**

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.

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* **214** *L* **54** # **249**

Odman, Knut XtremeSpectrum

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

[PM] The rule in SPS that beacon announcements shall be done in N subsequent wake beacons, in stead of just N subsequent beacons starting with the wake beacon, makes PNC implementation complicated. All this calls for a unified rule for PSPS and SPS: If you miss your wake beacon, listen to the next beacon. The requirement can be relaxed for SPS

SuggestedRemedy

Add text after description of wake beacon:□"A DEV that does not correctly receive its wake beacon shall listen to the following beacon if it's in PSPS or HIBERNATE mode, and it should (may?) listen to the following beacon if it's in SPS mode".

Proposed Response *Response Status* **U**

ACCEPT IN PRINCIPLE. Resolve as indicated in CID 309. This resolution removes the requirement that the PNC align the announcements to the SPS DEV's wake beacons. Instead it aligns it with one and sends the rest in the following beacons.

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** *P* **215** *L* **9** # **774**

Ho, Jin-Meng Texas Instruments

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

Incomplete specification in Table 63.

SuggestedRemedy

"After "All other CTAs" add "and intervals" (between CTAs)."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. After "All other CTAs" add "and unallocated time (between CTAs)."

Cl **08** *SC* **8.13.1** *P* **215** *L* **50** # **777**

Ho, Jin-Meng Texas Instruments

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

"Incomplete specification in line 50, page 215."

SuggestedRemedy

"After "desired system wake beacon interval" add "which may or may not be honored by the PNC"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Following line 51 on page 215, add 'The PNC uses the wake beacon interval information from all particpating PSPS DEVs to determine the system wake beacon interval. The actual system wake beacon interval may not correspond to any of the PSPS DEVs desired wake beacon interval.'

Cl **08** *SC* **8.13.1** *P* **215** *L* **53** # **778**

Ho, Jin-Meng Texas Instruments

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

"Incomplete specification in lines 53 and 54, page 215."

SuggestedRemedy

"After "requirement changes" add "However, the PNC may not be able to honor the system wake beacon interval desired by the DEV if that interval is different from the interval requested by other DEVs also in PSPS mode."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Resolve as indicated in CID 777.

Cl **08** *SC* **8.13.2.2** *P* **217** *L* **15** # **780**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PM/SPS-e*

"Incorrect term in line 15, page 217."

SuggestedRemedy

"Change "power save mode" to "power management mode"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. The terms power management and power save were used interchangeably but this is confusing. The TG has agreed to change all the occurances of 'power management' to be 'power save' for consistency.

Cl **08** *SC* **8.13.2.2** *P* **218** *L* **13** # **793**

Ho, Jin-Meng Texas Instruments

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

Incorrect statement in lines 13-14.

SuggestedRemedy

"Change "and shall request that the PNC" to ". The PNC shall"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change 'field to ‘PS’ and shall request that the PNC terminate the stream, 8.5.1.3.' to be 'field to ‘PS’. The DEV shall also send a Channel Time Request command to terminate the stream, {xref 8.5.1.3}.'

Cl **08** *SC* **8.13.2.2** *P* **218** *L* **2** # **789**

Ho, Jin-Meng Texas Instruments

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

"Unwarranted specification in lines 2-4, page 218."

SuggestedRemedy

"Delete the words "and a channel time request…terminated"."

Proposed Response *Response Status* **W**

REJECT. The sentence does not add any specifications (no shalls, mays or shoulds). This sentence was added to clarify the purpose of the MCTA and its length. It is intended as an aid to the implementers but does not place any restrictions on them.

Cl **08** *SC* **8.13.2.2** *P* **218** *L* **6** # **791**

Ho, Jin-Meng Texas Instruments

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

"Unwarranted specification in lines 6-7, page 218."

SuggestedRemedy

"Delete the statement "The SPS DEV may send…following the PS change command."."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **08** *SC* **8.13.2.3** *P* **219** *L* **49** # **797**

Ho, Jin-Meng Texas Instruments

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

"Ambiguous term in line 49, page 219: What are "wake CTAs"?"

SuggestedRemedy

Clarify the term.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change 'wake CTAs' to be 'CTAs'

Cl **08** *SC* **8.13.3** *P* **220** *L* **45** # **799**

Ho, Jin-Meng Texas Instruments

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

"Ambiguous wording in line 45, page 220."

SuggestedRemedy

"Add "positively" before "acknowledged"."

Proposed Response *Response Status* **W**

REJECT. This standard only has positive acknowledgement, there is not an negative acknowledgement. Thus any acknowledgement is a positive one.

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* **W**

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.

Cl **08** *SC* **8.14** *P* **225** *L* **47** # **816**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *ASIE*

"Ambiguous specification in lines 47-52, page 225: What is the "application data identifier field"?"

SuggestedRemedy

Clarify the ambiguity.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. This field is no longer used (and hasn't existed for at least 3 drafts). Delete the sentences "If the application data identifier field was set to "0" in the request, the MAC shall assign a new application data identifier that is different from that assigned to other current ASIEs. The "0" value application data identifier shall not be assigned to any ASIE. If the requested application data identifier belongs to an existing ASIE, the MAC shall modify the persistence of that ASIE, and reply with the same application data identifier in the indicate. If the repeat field an existing ASIE is set to "0", the PNC shall terminate the existing ASIE."

Cl **08** *SC* **8.15** *P* **226** *L* **36** # **817**

Ho, Jin-Meng Texas Instruments

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

"Undefined parameter in Table 64 in line 36, page 226: This revision does not define or reference "mMinProcessedCTAs"."

SuggestedRemedy

Define or delete this parameter.

Proposed Response *Response Status* **W**

ACCEPT. The parameter will be deleted as indicated in CID 144.

Cl **08** *SC* **8.2.1** *P* **162** *L* **42** # **600**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *Scan*

"Incorrect statements in lines 42-46: The interval "mMinChannelScan" should not be referenced to reception of a frame--how long would the searching DEV have to stay in the channel if no frame was ever received?"

SuggestedRemedy

"Delete "While searching, if any frame is received,", Capitalize the first letter of the following article, and further delete the words "from the time…as part of the MLME-SCAN.confirm primitive"."

Proposed Response *Response Status* **W**

REJECT. The DEV stays on the channel after it receives a frame so it can find the beacon associated with the piconet. If no frame is found, it stays on the channel for the ChannelScanDuration specified in the MLME-SCAN.request.

Cl **08** *SC* **8.2.2** *P* **163** *L* **29** # **601**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *Start*

"Incorrect statements in lines 29-36: The Start procedure follows the Scan procedure immediately, and hence there is no point to require the DEV to perform another scan."

SuggestedRemedy

Delete all the statements other than the first one from the third paragraph of this subclause.

Proposed Response *Response Status* **W**

REJECT. The PNC may be required to scan multiple channels during the scan procedure. Thus selected channel may have not been scanned very recently and the new PNC could end up starting in a channel that has since become occupied. This takes a little longer but piconet startup is an infrequent event and scanning helps to prevent possible collision.

Cl **08** *SC* **8.2.3** *P* **164** *L* **23** # **603**

Ho, Jin-Meng Texas Instruments

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

"Ambiguous terms in lines 23-25, page 164."

SuggestedRemedy

"Change "capability field" to "PNC Capabilities field" and "capabilities information" to "PNC Capabilities information"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **08** *SC* **8.2.3** *P* **165** *L* **14** # **605**

Ho, Jin-Meng Texas Instruments

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

"Ambiguous terms in lines 14-15, page 165: What is "PNC related traffic" and what is "non-PNC related traffic"?"

SuggestedRemedy

Define the terms.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change: "The new PNC shall begin using the PNCID for all PNC related traffic, but it shall continue to use its previously assigned DEVID for all non-PNC traffic." To: "The new PNC shall begin using the PNCID as the SrcID for all beacon or command frames transmitted. The new PNC shall use the PNCID or its previously assigned DEVID as the SrcID for all data frames transmitted."

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* **W**

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

Cl **08** *SC* **8.2.3** *P* **167** *L* **18** # **610**

Ho, Jin-Meng Texas Instruments

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

"Ambiguous terms in line 18, page 167."

SuggestedRemedy

"Add "PNC" before "capabilities field"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **08** *SC* **8.2.5** *P* **169** *L* **43** # **614**

Ho, Jin-Meng Texas Instruments

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

Incomplete statements in lines 43-45.

SuggestedRemedy

"Change "the neighbor" to "After the association request is accepted, the neighbor". After "by the PNC" add "in the Association Response command"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **08** *SC* **8.3.1** *P* **173** *L* **11** # **627**

Ho, Jin-Meng Texas Instruments

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

"Undefined parameter in line 11, page 173."

SuggestedRemedy

"Define "aAssocRespConfirmTime"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change the name to mAssocRespConfirmTime which is defined in 8.15, Table 64.

Cl **08** *SC* **8.3.1** *P* **173** *L* **24** # **629**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *Assoc*

"Incorrect statement in lines 24-25, page 173: As noted elsewhere by this balloter, the DEV Association IE does not serve the purposes it was intended for. The DEVs "newly" associated with the PNC and announced via this IE would not necessarily be known to DEVs that are associated later on (i.e., after the announcement of this IE. The balloter has suggested to replace the "DEV Association IE" with an "Association List IE" that lists all the DEVs associated with this PNC."

SuggestedRemedy

"Rephrase the statement "The PNC after…" as follows: The PNC after acknowledging this second request shall send a beacon containing an Association List IE that includes the requesting DEV. Change "the DEV association information element" in line 27 to "an Association List IE that includes itself". Change "DEV association IE" in lines 28, 29, and 30 to "Association List IE"."

Proposed Response *Response Status* **W**

REJECT. The PNC info command provides the requested functionality as described in 8.3.3. Thus the DEV association IE does not need to be expanded. See also the resolution of CID 403.

Cl **08** *SC* **8.3.1** *P* **174** *L* **35** # **630**

Ho, Jin-Meng Texas Instruments

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

Incorrect illustration in Figure 103.

SuggestedRemedy

"Change "association IE" to "Association List IE" and "ack with" to "ACK with"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change 'ack with' to 'Imm-ACK with'. (2 places) The association IE is sufficient for this process as the PNC info command will be used to update the new DEV with the complete membership in the piconet as described in 8.3.3. See also the resolution of CID 403.

Cl **08** *SC* **8.3.1** *P* **174** *L* **49** # **634**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *Assoc*

"Redundant information in line 49, page 174: The PNC Information command contains all the information in the "DEV Association IE"."

SuggestedRemedy

Delete this requirement or expand this procedure to replace the requirement that the PNC send a beacon containing a DEV Association IE to reflect the association status of a newly associated DEV.

Proposed Response *Response Status* **W**

REJECT. The association IE serves two purposes. The first is to tell other DEVs in the piconet that a new DEV has joined. The second, perhaps more important purpose is that this IE is used to complete the association process for the requesting DEV. When the DEV receives this IE in the beacon, it knows that it has successfully associated.

Cl **08** *SC* **8.3.2** *P* **175** *L* **13** # **637**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *PNService*

"Ambiguous statements in lines 13-19: After a DEV disassociates from the PNC, should the PNC update the Piconet Services IEs via a beacon or a Piconet Services command?"

SuggestedRemedy

Clarify the ambiguity.

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Add to the end of line 19 'After a DEV disassoicates from the piconet, the PNC shall delete the DEV's Piconet Services IE from its own record.' Note: All of the other DEVs will see the disassoicate announcement and can update their own internal storage by deleting the entry if they kept it.

Cl **08** *SC* **8.3.4** *P* **176** *L* **14** # **643**

Ho, Jin-Meng Texas Instruments

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

"Ambiguous statement in lines 14-15, page 176."

SuggestedRemedy

"Change "for the disassociating DEVs" to "with the disassociated DEV as the SrcID or DestID"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **08** *SC* **8.3.4** *P* **176** *L* **14** # **642**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **R** *Assoc*

"Incorrect specification in line 14, page 176."

SuggestedRemedy

"Change "DEV Association IE" to "Association List IE which no longer includes the newly disassociated DEV"."

Proposed Response *Response Status* **W**

REJECT. DEVs that remain associated already know the members of the piconet (or they can find out by requesting this information from the PNC with the PNC info command). They do need to know when a DEV is disassociated and the association IE provides this information.

Cl **08** *SC* **8.3.4** *P* **176** *L* **43** # **644**

Ho, Jin-Meng Texas Instruments

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

Incorrect illustration in Figure 104 and Figure 105.

SuggestedRemedy

"Change "beacon with association IE" to "Beacon with Association List IE no longer including DEV-2", change "ack" and "ACK" to "Imm-ACK", and "ASSOCIATE-INFO" to "ASSOCIATION-INFO". Delete "DEVID=DEV-2, status=disassociated", "DEVID =DEV-2", and "Status = disassoc"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change "ack" and "ACK" to "Imm-ACK", and "ASSOCIATE-INFO" to "ASSOCIATION-INFO" As indicated in the resolution of CID 642, the association IE is sufficient to inform the DEVs in the piconet that a DEV has disassociated from the piconet. See also the resolution of CID 403.

Cl **08** *SC* **8.4.3** *P* **179** *L* **8** # **650**

Ho, Jin-Meng Texas Instruments

Comment Type **TR** *Comment Status* **A** *CAP/BkOff*

"Incorrect statement in lines 8-10, page 179."

SuggestedRemedy

"Delete the statement "This avoids the problem…"."

Proposed Response *Response Status* **W**

ACCEPT.

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* **W**

ACCEPT IN PRINCIPLE. Rename CFP to CTAP - 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* **W**

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.

Cl **08** *SC* **8.4.4.1** *P* **180** *L* **13** # **657**

Ho, Jin-Meng Texas Instruments

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

"Ambiguous specification in lines 13-14, page 180: It is not clear if dynamic CTAs may be allocated to isochronous streams."

SuggestedRemedy

"Before "Asynchronous CTAs" add "Dynamic CTAs may be allocated for isochronous streams."."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. On page 179, line 52 at the end of the paragraph add 'Dynamic CTAs may be used for both asynchronous and isochronous streams.'

Cl **08** *SC* **8.4.4.2** *P* **180** *L* **51** # **664**

Ho, Jin-Meng Texas Instruments

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

"Incomplete statement in lines 51-52, page 180."

SuggestedRemedy

"After "associated DEV" add "known to be in the AWAKE state"."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. After the sentence on line 51, add to the paragraph. "However, it is possible that the target DEV will not be receiving during the CTA if it is in a power save mode, {xref 8.13} or if it is not receiving multicast traffic, {xref 6.3.19.1}"

Cl **08** *SC* **8.4.4.2** *P* **181** *L* **24** # **666**

Ho, Jin-Meng Texas Instruments

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

"Incorrect specification in lines 24-25, page 181: How does the PNC indicate in its Channel Time Response command that it will not update the channel time request?"

SuggestedRemedy

"Clarify and rephrase the statement "If the PNC…additional channel time."."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Change 'If the PNC ... additional channel time.' to be 'If the source DEV requires additional channel time it will need to use the stream modification procedure, 8.5.1.2.'

Cl **08** *SC* **8.4.4.5** *P* **182** *L* **39** # **672**

Ho, Jin-Meng — Texas Instruments

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

"Undesirable specification: The Aloha access algorithm defined in this subclause is undesirable in two folds: (1) The "binary backoff" nature of the contention algorithm, i.e., doubling the contention window after an inferred collision, in a PAN would unnecessarily increase the access latency, as an inferred collision could be a result of a non-collision event such as interference or bad channeling. Also, the backoff has a memory which could spread over a large number of superframes, and hence does not allow the PNC to adapt the CW to load changes for optimal channel throughput and access latency. Instead, re-randomizing the backoffs without doubling the CW among contending DEVs in every superframe would be more effective in avoiding collision, especially considering the generally low DEV population in a PAN, and hence in improving channel throughput and access delay. (2) Potentially each contending DEV may have to buffer a large number of MCTA definitions as announced in the beacon, and determine which of those MCTAs may be used for an initial transmission, a retransmission, and a retransmission again, ..., of a command frame, all within the same superframe. This would certainly increase the implementation cost."

SuggestedRemedy

"(1) The number "a" should not be individual functions of retransmission attempts by contending DEVs. Instead, it should be a parameter whose value is updated and annonced by the PNC in each beacon. To this effect, add two 1-octet subfields to the Piconet Synchronization Parameters field for encoding "a", one for use with Association MCTAs and one for use with Open MCTAs. "a" may be called Associaiton CW exponent and Open CW exponent, respectively. Eliminate the first branch of Equation (1) and the condition in the second branch. Each contending DEV shall redraw a backoff after receiving a beacon using the "a" value contained in that beacon, even if the previous backoff has not expired (and hence the DEV did not transmit in the previous superframe). A DEV shall regenerate a backoff for a retransmission within the same superframe using the same "a" value as in the initial transmission.
(2) Add a statement to limit the number of MCTAs (for each type, Association or Open) that may be used by any given DEV to two within each superframe. That is, only one retransmission is allowed by each DEV following a failed transmission in the same superframe."

Proposed Response *Response Status* **W**

REJECT. The Slotted Aloha backoff algorithm is well documented in the literature. Just as an associating DEV won't know the difference between a collision and interference, the PNC likely won't be able to tell the difference between a collision and interference either. In this case, the PNC won't know what value to set for the exponent of the back-off window, "a". Also, the suggested Remedy does not specify what algorithm the PNC will use to determine the parameter "a".

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* **W**

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.

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* **W**

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

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* **W**

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.

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* **W**

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.

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* **W**

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

Cl **08** *SC* **8.4.4.7** *P* **186** *L* **15** # **684**

Ho, Jin-Meng Texas Instruments

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

Incorrect illustrations in Figure 111.

SuggestedRemedy

"Change "SIFS" to "MIFS" after "Frame 1" and "Frame 2", respectively."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **08** *SC* **8.5** *P* **187** *L* **23** # **820**

Ho, Jin-Meng Texas Instruments

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

"Section 8.5 states "Each DEV shall support at least one isochronous stream." This is an uneccesary requirement to place on all DEVs. Some DEV applications may only have a need for asynchronous transfers."

SuggestedRemedy

Omit requirement from the spec.

Proposed Response *Response Status* **W**

ACCEPT. Also delete from the PICS.

Cl **08** *SC* **8.5.1.1** *P* **188** *L* **53** # **690**

Ho, Jin-Meng Texas Instruments

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

"Incorrect term in line 53, page 188."

SuggestedRemedy

"Change "CTA status command" to "CTA Status IE"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **08** *SC* **8.5.1.1** *P* **189** *L* **22** # **691**

Ho, Jin-Meng Texas Instruments

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

"Incorrect illustrations in Figure 114, Figure 115, and Figure 116."

SuggestedRemedy

"Change "ACK" to "Imm-ACK" (2 occurrences in each figure). Change "presence" to "reception". Change 'association frame" to "Association Request command frame". Change "ResultCode" to "ReasonCode" in each of these three figures (recall that the actual result is contained in the ReasonCode). Change "= FAILED" to "not equal to SUCCESS" in Figure 115."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. In figures 114, 115 and 116, Change "ACK" to "Imm-ACK" (2 occurrences in each figure). Delete"with ResultCode = ???" in each of these three figures.

On page 183, line 8, change "presence" to "reception" and change 'association frame" to "Association Request command".

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* **W**

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.

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* **W**

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.

Cl **08** *SC* **8.5.1.3** *P* **194** *L* **20** # **700**

Ho, Jin-Meng Texas Instruments

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

Incorrect illustrations in Figure 121.

SuggestedRemedy

"Change "ACK" to "Imm-ACK". Change "reason code = stream terminated" to "ReasonCode = Stream terminated by PNC". Move the text together with the arrow between the two lines connected to the "DEV-3 MLME" and DEV-3 DME" boxes down below the arrow with text "beacon with null-CTA SI = x"."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **08** *SC* **8.5.2.1** *P* **194** *L* **53** # **701**

Ho, Jin-Meng Texas Instruments

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

"Incorrect term in line 53, page 194."

SuggestedRemedy

"Delete "-SPS" and rename "CTR type" if needed."

Proposed Response *Response Status* **W**

ACCEPT.

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* **W**

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

Cl **08** *SC* **8.5.2.1** *P* **196** *L* **22** # **704**

Ho, Jin-Meng Texas Instruments

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

Incorrect illustration in Figure 122.

SuggestedRemedy

"Change "ACK" to "Imm-ACK" (2 occurrences)."

Proposed Response *Response Status* **W**

ACCEPT.

Cl **08** *SC* **8.6.3** *P* **197** *L* **49** # **821**

Ho, Jin-Meng Texas Instruments

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

"Spec does not define what determines a "Lost Beacon". Is it just not receiveing a beacon frame type at the expected time? Or if data within the beacon is wrong or unexpected (such as PNID, DestID, SrcID, Time Token), such that the beacon be ignored and lost beacon counter incremented? Some of this is implied but not explicitly specified."

SuggestedRemedy

"Add table or text to describe which info within a beacon must be valididated. Section 8.6.3, "Beacon Reception," would be a good location for such info."

Proposed Response *Response Status* **W**

ACCEPT IN PRINCIPLE. Add to page 197, line 53 'A lost beacon is defined as one for which the FCS is not valid or when a DEV has not received a beacon at the expected time.'

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* **W**

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.

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* **W**

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.

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* **W**

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}.

Cl **08** *SC* **8.7** *P* **200** *L* **14** # **719**

Ho, Jin-Meng Texas Instruments

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

"Incomplete statements in lines 14-16, page 200."

SuggestedRemedy

"Change "multiple SDUs" to "multiple MSDUs belonging to the same stream". Change "the SDUs" to "the MSDUs"."

Proposed Response *Response Status* **W**

ACCEPT.

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* **W**

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

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* **W**

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.'

Cl **08** *SC* **8.9.2** *P* **203** *L* **30** # **732**

Ho, Jin-Meng — Texas Instruments

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

"Incorrect field name in line 30, page 203."

SuggestedRemedy

"Change "ACK request" to "ACK Policy"."

Proposed Response *Response Status* **W**

ACCEPT.

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* # **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* *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* **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* **330** *L* **#** **825**

Ho, Jin-Meng — Texas Instruments

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

"Incorrect wording in lines 19-20, page 330."

SuggestedRemedy

"The polynomial generator, g(D), for the pseudo random binary sequence (PRBS) shall be."

Proposed Response *Response Status* **W**

ACCEPT.

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* **W**

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.

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.

Cl **E** *SC* **E.7.3.2** *P* *L* # **824**

Ho, Jin-Meng — Texas Instruments

Comment Type **TR** *Comment Status* **A** *ACK*

"In Table E.4, item MLF17, Acknowledgement and retransmission, appears to be associated with sub items MLF18.1 to MLF18.5."

SuggestedRemedy

"Either
a)renumber MLF17 as MLF18 or
b)renumber MLF18.x, with MLF17.x, where x is the respective subitem numbers."

Proposed Response *Response Status* **W**

ACCEPT. Renumber 18.x as 17.x and update the rest of the numbers in the table accordingly.