# Comments on ETG 17-005

# Color coding of comments

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | P | Blue with black text | Proposed resolution that should be discussed, hopefully briefly. |
|  |  |  |  | O | Yellow with black text | Needs discussion to resolve. |
|  |  |  |  | R | White with grey text | Resolved. |

# The Comments

| **#[[1]](#footnote-1)** | **Page** | **Section** | **Imp.[[2]](#footnote-2)** | **Status** | **Comment/Recommendation** | **Resolution** |
| --- | --- | --- | --- | --- | --- | --- |
| FB1 | ii | ToC 2.2.1 | E | R | Spell out LLE as Link Layer Encryption and then abbreviate elsewhere in ToC? | Proposed Resolution: Added the (LLE) abbreviation to the title so it comes before the TOC. |
| H-2 | 0 | Cover Page | E | R | Fix the freakin’ cover page that Word destroyed. | Resolution: Fixed in R1. |
| H-1 | 0 | 0 | E | R | Fix the page number formatting throughout. | Resolution: Fixed in R1. |
| H0 | 0 | 0 | T | O | Incorporate appropriate changes (see other comments) to cover TDMA CC LLE in this document. | Discuss, no specific changes for this, just wanted to make sure we all agree. |
| MS01 | 1 | 1 | E | R | The text says this is an addendum to BBAC but the document is not structured as an addendum that can be used in combination with the parent document.  MSI prefers that this particular document contain the agreed upon technical material associated with the LLE application of a TDMA Trunking Voice Channel and a TDMA Trunking Control Channel. This consensus material in this document would then be used by the editors of various other TIA documents to be published.  Recommendation: Replace text about this being an addendum with text describing the intended content of this document. Here is a suggested modification:  The scope of this document describes the specifications for link layer security provided by encryption of TDMA data bursts over the TDMA air interface. This document includes an overview of link layer encryption for TDMA, a section to specify link layer encryption of bursts containing voice, a section for site procedures in the RF sub-system, and a section for information elements used for link layer encryption. Link layer security is generally applied to the data transmitted over the TDMA air interface including voice, control, and other signaling fields. It is not a substitute for end-to-end encryption of voice messages that is separately specified in TIA-102.AAAD for the block encryption protocol (ref. (2)). Other parts of the TIA-102 suite of standards provide link layer security specifications for other parts of a system, such as for FDMA channels, that are outside of the scope of this document. A precise explanation of the scope of this addendum is given as follows. | Proposed Resolution: Looks like this is the same paragraph with “addendum” edited out. I’ve made equivalent changes with some editorial differences to the intro.  Agreed Resolution: Get rid of the word standard in referring to this document.  Resolution: Done, removed “standard” and replaced it with “document” where appropriate.  Accepted in R5. |
| MS02 | 1 | 1.1 | E | R | This document is not written as an addendum. Recommend rewording this paragraph as follows:  The scope of this document is link layer security for TDMA channels specified in the Two-Slot TDMA suite of standards. Link layer security applies encryption to fields of sensitive data transmitted over the TDMA air interface to protect the data from interception and interpretation by unauthorized receivers. The encryption function is often labeled as link layer encryption. The sensitive data that is to be encrypted on the air interface includes digital voice, control signals that affect calls, and data signals that affect RF sub system operation. The protection of sensitive data uses a cryptographic function that is synchronized with a time value so that sensitive data cannot be copied and replayed on the channel for any unauthorized purpose. This document includes an overview of the link layer security cryptographic operations; as well as specifications for link layer encryption of voice, data, and control; site procedures for the RF sub system; and relevant information elements used for link layer encryption. The scope of this document does not include link layer encryption of FDMA channels, or end-to-end encryption of digital voice. Both of those items are covered in other standards in the TIA-102 suite of standards. Together the combination of end-to-end encryption of messages with link layer security of TDMA and FDMA channels provides improved security for systems using the TIA-102 suite of standards that includes resistance to interception, eavesdropping, misdirection, message replay, spoofing, and traffic analysis. | Proposed Resolution: Looks like this is the same paragraph with “addendum” edited out. I’ve made equivalent changes with some editorial differences to the intro.  Same as MS01. Agreed to close. |
| FB2 | 2 | 1.2 | E | R | Is the word “Field” needed with IEMI, I-OEMI, and S-OEMI in the list? | Nah, I’ll take it out. See FB3. |
| FB3 | 2 | 1.2 | E | R | Add LLE and LLS to the Abbreviation list? | Sure, but I don’t see LLS anywhere, so I’m not doing that. |
| FB4 | 4 | 2.1 Fig 1 | T | R | In the cloud it says “Infrastructure”. Is “RFSS” appropriate here? | Response: I’d prefer not to make this change. It really is infrastructure as it can be a whole network, not necessarily just elements of the same RFSS. Discuss.  Proposed Resolution: No change. |
| FB5 | 4 | 2.1 Fig 1 Bullets 5 & 6 | E | R | Should the word “Arrows” be used in place of “Flow”? The combination of arrow symbols make up a “flow”. Or is this too nitpicky? | Response: Too nitpicky.  Proposed Resolution: No change. |
| H1 | 4 | 2 | E | R | “Black Flow: Indicates an information flow carrying encrypted information.”  Suggest changing to:   * Black Flow: Indicates an information flow carrying FEC encoded encrypted information. | Resolution: No change. |
| MS03 | 4 | 2.1 | E | R | Figure 1 - The diagram is missing a label for SU2 on the group of 3 SUs on the left hand side. | Done in R1, Thanks. |
| H2 | 5 | 2.1 | T | R | First Paragraph: “When transmitting link layer protected…”  LLE IV has changed since this draft. Should now refer to LLE Overview (LLEIV). IV is now Downlink frequency, data/time, and source indicator. | Proposed Resolution: See markup in R1. Couple small changes added in R2. |
| H4 | 5 | 2.1 | T- | R | The site identifying part of the initial vector identifies the Wide Area Communications Network (WACN), System, RF Subsystem (RFSS), Site ID, Color Code/NAC[[3]](#footnote-3), and Direction of the transmission, and the time coordinate identifies the time of the transmission to a granularity of TDMA slots.  Suggest changing to micro slots..  The site identifying part of the initial vector identifies the Wide Area Communications Network (WACN), System, RF Subsystem (RFSS), Site ID, Color Code/NAC[[4]](#footnote-4), and Direction of the transmission, and the time coordinate identifies the time of the transmission to a granularity of TDMA micro slots (7.5 ms). | Resolution: Done in R1. |
| H3 | 5 | 2.1 | T | R | “Table 2 identifies the information content of the *four* logical…” Remove the word “four” to accommodate TDMA CC LLE. | Resolution: Done in R1. |
| MS04 | 5 | 2.1 | T | R | Par 1 states: “using a site identification and time coordinate as an initial vector input for the encryption”.  This statement should be updated to align with the information in the latest Overview document. Note that paragraph 4 also references site identification information.  From Overview R12:  2.3  The 128-bit Link Layer Encryption Initial Vector (LLEIV) comprises the following fields (Channel Frequencies 24 bits each; Source Indicator 2 bits; Time Value 40 bits). The defined portions yield 66 information bits in the IV. The remaining bits are defined to be zero.  3.1.3  Each channel type (e.g., trunking control, TDMA traffic) or information element to be encrypted has a defined method of developing a “Crypto-Synch” word, and of translating the crypto-synch into an initial vector (IV)  3.4.1  The LLE Initial Vector is illustrated in **Error! Reference source not found.** and contains: Downlink Freq 24 bits; Time 40 bits; Source Indicator 2 bits. | Proposed Resolution: slightly heavy rewrite. See markup in R1. |
| MS05 | 5 | 2.1 | E | R | The footnote is no longer necessary. A decision has already been made to remove the NAC/Color Code from the IV. Additionally, any other references to NAC/Color Code within the context of an IV component elsewhere in the document should be removed. | Thanks, removed in R1. |
| FB6 | 6 | Table 3 | E | R | First use of ESS in the document. Used elsewhere as well. Should be added to list of Abbreviations. | Done, thanks. |
| H5 | 6 | 2.1 | T | R | Table 2: Add a line for the CC LCCH: See H-EC-1, below. | Proposed Resolution: See H-EC-1 |
| H6 | 6 | 2.1 | T | R | Table 3: Add lines for OECI and IECI Bursts. See H-EC-2 below. | Proposed Resolution: See H-EC-2 |
| H7 | 7 | 2.2.1 | E | R | Figure 2 caption is bulleted for some reason. | Resolution: Not Anymore. Fixed. |
| H8 | 7 | 2.2.2 | E+ | R | This essential material is present in the LLE Overview. We can keep it here, or refer to the definition there. Discuss. | Discuss.  Keep it here. |
| H9 | 7 | 2.2.1 | E | R | xb(y) is equivalent to xy,b  Should all small x’s be capital?  Suggest:  Changing all small x’s to capital X’s | Withdrawn. |
| MS06 | 8-10 | 2.2.3 & 2.2.4 | T | P | These sections state that the IV = STP-MI. The components of both listed in 2.2.4 do not align with the description of the IV in the Overview (R12) document. Specifically, the ID and NAC information is used to derive the site keys and are no longer included in the IV. | Proposed Resolution: Rewrite of the section per following comments to bring it up to date.  Purged STP-MI in R2. |
| H10 | 8 | 2.2.3 | T | R | This is obsolete and should probably just refer to the LLEIV in the LLE Overview. | Proposed Resolution: Changed to reference Overview. Same as MS06. |
| H11 | 9 | 2.2.4 | T | R | WACN,System,RFSS ID, and Site ID are all obsolete fields, having been replaced by the downlink frequency. The rest of this is ok we think. Identify the source of the downlink frequency and replace the first 4 bullets with that. | Proposed Resolution: Done. |
| H12 | 9 | 2.2.4 | E | R | * + Remove “in” from sentence.   + For MAC PDUs, the Year SHALL be the year as of the beginning of the slot containing the burst in bearing the MAC PDU.   Suggestion:  Instead of separate statements for 4V, 2V and MAC PDU’s…can you just say ‘all slots’ …for each STP-MI variable to make it simpler? | Thanks, and No. Done in R1. |
| MS07 | 9 | 2.2.4 | E | R | In the descriptions of the Day, Hour, Minute and Microslot fields, the start and end ranges of assignable values are defined. However, the description of the Month field does not define the last value in the range of assignable values (1100). The end of range value of the Month field should be included, for consistency. | Proposed Resolution: Thanks. Done in R1. |
| H13 | 10 | 2.2.4 | T | R | NAC code is no longer used. Delete bullet | Resolution: Done in R1. |
| H14 | 10 | 2.2.4 | T | R | Direction indicator is now Source indicator. Should refer to LLE Source Indicator (SI) in LLE Overview. | Proposed Resolution: Done in R1. |
| H15 | 11 | 3.1.1 | T | R | “Let K be the TDMA Encryption Key” should be “Let K be the STEK of the TDMA channel per <LLE Overview>. Also, add STEK to list of abbreviations. | As marked up in the relevant paragraphs. |
| MS08 | 11 | 3 | T | R | In Figure 14 of the Overview document, there is text describing the Initial IV load event. For TDMA, this event is the start of the TDMA slot. This detail should be added to the TDMA document.  Additionally, the text for Load IV in the Overview document seems more relevant to the description of the Initial IV in Fig. 14. | Any thoughts on where to put it? Discuss.  MSI suggests 2.2.2.  Proposed Resolution: Made the change for the first part of the comment. Unclear on what is desired for the second. Suggest leaving it for TR8.  Agreed, added editor’s note. |
| MS09 | 11 | 3.1.1 | T | R | MSI proposes an alternate encryption schedule as follows: B, V0, V1, V2, V3. The rationale for this proposal is to make late-entry receive operation more efficient from the following standpoint:  In some cases for late-entry, it will be possible to successfully decode B without requiring the decode of the voice information. Therefore, putting V0 and V1 before B in the encryption schedule adds inefficiency when there is no valid voice information in V0 and V1. This proposal saves the act of fabricating bogus voice information to run through the front end of the encryption schedule in late-entry scenarios.  If this proposal is not accepted, there is still an editorial issue with section 3.1.1 that needs to be cleaned up. Steps 5 and 6 in the encoding schedule need to be swapped. | Resolution: Ok, we’re fine with this. Changes in encrypt and decrypt sections. |
| MS10 | 11 | 3.1.1 | E | R | Section 3.1.1 and 3.1.2 Recommend using the Prime notation on only the LLE encrypted data. This would require the editor to swap the order on the decode steps such that you compute V0 from V0’ as an example. | No. Why? What’s wrong with what’s there? Grumble.  In both sections, MSI wants V’ to consistently refer to encrypted or not encrypted. It doesn’t.  Agree to change in the next version.  Proposed Resolution: Done. Also changes to the section 3.1.3, using X and Y to refer to the input and output of the cryptosystem.  Accepted as modified. |
| H16 | 12 | 3.1.2 | T | R | “Let K be the TDMA Encryption Key” should be “Let K be the STEK of the TDMA channel per <LLE Overview>. This applies to both subparagraphs of this section. | Done. |
| H17 | 12 | 3.1.2 | E | R | Link Layer Encryption of 2V bursts SHALL proceed as follows, or by any method that produces equivalent results:  Let K be the TDMA encryption key;  Let V0, V1 be the 49-bit voice frames scheduled for transmission in the 4V Burst;  Compute V'i, the encrypted voice fields of the burst, and B', the encrypted ESS-B field of the burst as follows:  Suggest:  Change 4V to 2V and ESS-B to ESS-A in this section | ESS-A isn’t encrypted, butr you caught the cut and paste error. Done in R1. |
| MS11 | 12 | 3.1.1 | E | R | The decoding steps should use V0, V1, V2, V3… instead it specifies Vo, V1, V3, and V4. | I don’t see the “o”.  Fixed in R2. |
| H18 | 14 | 3.1.3 | E | R | “shall be encrypted as follows, *or method*…” should be “or by a method…” | Resolution: Done. |
| H19 | 15 | 3.1.4 | E | R | Figure 5 … MI has 73 bits…  Suggest changing figure to have MI bits from 0 -71 instead of 0-72 | Resolution: Thankis. |
| MS12 | 15 | Fig. 5 | T- | R | The flow diagram doesn’t show the complete story where FEC is performed. It shows the partition of hexbits prior to the FEC, and it shows the computation of the parity with is a portion, but not the entirety, of the FEC.  Suggest changing the block “Compute Parity” to “Compute FEC”, or something else that’s appropriately descriptive. | Ok. Used FEC. |
| H20 | 17 | 3.2 | E | O | I don’t find a spot in the overview where we did this (M47). Perhaps it belongs on page 17 of that document, in the bullets before figure 4. | Discuss.  See MS14. |
| H21 | 17 | 3.2 | E | R | Note that because the two MAC PDU streams carried by a TDMA channel are independent. Therefore, at any time that the channel is keyed, either slot can carry encrypted or unencryption PDUs without regard for the encryption of the other slot.  Suggest changing to:  Note that because the two MAC PDU streams carried by a TDMA channel are independent. Therefore, at any time that the channel is keyed, either slot can carry encrypted or unencrypted PDUs without regard for the encryption of the other slot. | unencrytion to unencrypted. Done in R1 |
| MS13 | 17 | 3.2 | E | R | Recommend deleting the work “because” in the first sentence | Resolution: OK. |
| MS14 | 17 | 3.2 | E | R | Regarding the editor’s note:  Based on MSI’s analysis of (M48) below, we concluded there is no need to add anything to the proposed standard for this case however, it may be beneficial to add some informative text in either the Overview or this TDMA LLE document. | Discuss.  Agree that text above the note is good. Delete editor’s note. Done in R2. |
| H22 | 18 | 3.2 | T | R | Does Table 5 really add anything anymore? It’s long and no one will ever read it. | Discuss and then remove.  MSI to draft a paragraph to replace the table.  Proposed Resolution: Added MSI text to replace what was there.  Agreed as in R4. |
| MS15 | 18 | Table 5 | E | R | The use of the term “Phase 1” in the Type column seems to be inconsistent. Based on how it’s being used, it appears the term should be renamed to “TDMA and FDMA”.  However, it is questionable why the Type column is actually needed. It’s not clear why showing where the MAC Messages originate from adds value. The first recommendation is to remove the Type column. If a decision is made to keep it, then the recommendation in the first paragraph applies. | Let’s kill the whole thing. Discuss with H22. See H22. |
| H23 | 19 | 3.2.1.1 | T | P | Figure 10: Add another figure for IECI and OECI MAC PDUs. Change “Figure 10 illustrates…” to “Figure 10 and 11 illustrate…”, and “The shaded areas in Figure to…” to “The shaded areas in the figures…” and similar grammatical changes in the section. Also add CRC-16 to the descriptive fields.  See H-EC-3 for the new figure. | Proposed Resolution in R1.  Figures are good. |
| H24 | 20 | 3.2.1.2 | T | R | Discuss M48. | See <S16. Delete the note. |
| MS16 | 20 | 3.2.1.1 | E | R | Regarding the editor’s note:  Based on MSI’s analysis, we concluded there is no need to add anything to the proposed standard for this case. We can withdraw the original comment. | Thanks. Resolved in R1.  MSI want’s more time to consider this.  MSI Proposes inverting the CRC and keeping the P bit. Changes in R5. |
| FB7 | 21 | 3.2.1.1 M48 | E | R | Users need take note of this one – Whether or not both slots might have to use the same mode; and the pro’s and/or con’s of it. Need to discuss this and hear more details. Keep in mind that it is not likely that any user has ever pondered this possibility…. | We’re not forcing both slots into the same mode. Since this is the issue, I think we’re ok.  Proposed Resolution: No change. |
| MS17 | 21 | 4.1 | T | R | From previous discussions, I believe we agreed that TDMA VCHs SHALL be synchronized to the FDMA CCH for acceptable system performance. This statement needs to be added somewhere in the document. | Proposed Resolution: Added to paragraph of section 2.1  Agreed. |
| MS18 | 22 | 4.1  Table 6 | T | R | With the possible exception of the SYNC\_BCST message, I don’t see how these messages are relevant to LLE. Based on that we suggest removing these other messages from the table.  We also suggest noting somewhere that the Control Channel SYNC\_BCST is required for LLE.  Regarding a maximum periodicity spec,  Note that AABD-B currently says:  - SYNC\_BCST “shall be sent out at a rate of one every TSYNC\_BCST = 10 sec.  While an optimal value is endlessly debatable, we believe 10 seconds is too long.  We believe 3 seconds is a better value for LLE operation and this value is currently specified for other Control Channel Broadcast messages such as NET\_STS\_BCST and RFSS\_STS\_BCST and IDEN\_UP(\_VU). | Response: I’m fine with the timing of the sync\_bcst, however, the SU needs the others to get its site information, RFSS, etc. for the key derivation.  Discuss.  See markup in R2. |
| MS19 | 23 | 4.2 | E | R | Regarding the editors note:  Based on MSI’s analysis, we concluded there is no need to add anything to the proposed standard for this scenario. We can withdraw the original comment. | Thanks. Done in R1. |
| H25 | 24 | 5.1.2 | E | R | Section not required after changes to references above. | Withdrawn. |
| MS20 | 24 | 5 | E | R | May want to consider revising the section heading numbering in section 5 (e.g. numbering goes directly from 5 to 5.1.1) at some point | Done. Thanks. |
| MS21 | 24 | 5 | E | R | Regarding the Editors note:  Previous comments on the intentions for use of this document.  We agree the section on DUID encoding belongs in this document.  While the information about STP-MI and the direction indicator are common with FDMA, based on the recommended use of this document, it may still be useful to include that information in this document.  Discuss. | Discuss Fixed in R2. |
| MS22 | 24 | Table 7 | T | R | Based on our analysis, Motorola is fine with using the DUID to distinguish LLE 2V/4V bursts from clear 2V/4V bursts on the VCH. The only thing we propose doing is move the DUID assignment for the LLE 4V burst from %0001 to %0010 so we have an additional pair of orthogonal DUIDs available for future use. | Proposed Resolution: Agreed. Thanks. |
| H26 | 25 | 5.1.1 | T | R | Table 7 does not have TDMA-CC updated info.  Suggest:  Updating with TDMA-CC DUID values for LCCH with and without scrambling | Proposed Resolution: Done, also added the extra column that is in the TDMA CC document.  Closed. |
| MS23 | 25 | 5.1.2 | E | R | Regarding the editor’s note:  I believe previous discussions have concluded that the NAC/CC is not included in the STP-MI. | Correct, but this whole thing is wrong.  Proposed Resolution: Replaced with section from Overview.  Closed. |
| MS24 |  |  |  | R | The Null Information MAC message may be used to fill unused space in a PDU carrying other MAC messages. The Null Information MAC message contains a variable sized Null field that is filled with zeros. We feel that it will be better security practice to have the encoding element fill the null field with a random bit pattern rather than using al zeros. Otherwise, an analyzer could postulate where the null fields occur and use the known plaintext as a launching point for discovery of the key stream through cryptoanalysis. | Agreed, needs to be a cryptographically sound random number.  Update in next revision.  ‘  Proposed Resolution: Added suitable text to section 3.2.1.2 |

Extended (H-EC-1)

|  |  |  |
| --- | --- | --- |
| Logical Control Channel (LCCH) | MAC PDUs containing MAC Messages | Protected if MAC Messages require protection. |

Extended (H-EC-2)

|  |  |  |
| --- | --- | --- |
| Inbound Encoded Control Information | MAC PDU in IECI | Parity, DUID, Ramp, Guard, Sync and Pilot |
| Outbound Encoded Control Information | MAC PDU in OECI | Parity, DUID, ISCH |

Extended (H-EC-3)



1. Company initials (up to 2) and a sequential number to identify the comment. [↑](#footnote-ref-1)
2. IMP: Importance. E = Editorial – Fix it if you agree. T- = Minor Technical – Fix it if you agree. T = Significant Technical – Discuss it if you don’t agree, T+ = Major Technical – could result in a negative ballot if not resolved. [↑](#footnote-ref-2)
3. The TDMA Color code is synonymous with the FDMA NAC. [↑](#footnote-ref-3)
4. The TDMA Color code is synonymous with the FDMA NAC. [↑](#footnote-ref-4)