**List of changes to the draft standard**

October 14, 2007

SUBJECT: Changes to IEEE P1619.1/D24, Draft Standard for Authenticated Encryption with Length Expansion for Storage Devices

References: IEEE P1619.1/D23, Draft Standard for Authenticated Encryption with Length Expansion for Storage Devices, dated August 2007.

The following list contains the changes made to IEEE P1619.1 in going from draft number D23 to the new draft number D24.

Changes that were done according to a comment:

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 41 | 1.3 | (1.3 line 20)<br>or<br>s/b<br>and | | Done |
| 103 | 3.2 | Can a source be given for the "Authoritative Dictionary of IEEE Standards"? Is it available on the web? | Provide source | Added bibliography entry for the Authoritative Dictionary as follows: [B6] IEEE 100, The Authoritative Dictionary of IEEE Standards Terms, Seventh Edition, New York, Institute of Electrical and Electronics Engineers, Inc. |
| 105 | 3.2 | Should the use of a KEK be specifically restricted to ONLY encrypting another key. | "A cryptographic key used only for encrypting other cryptographic keys." | Changed |
| 22 | 3.3 | The "H" in the acronyms SHA and SHS<br>stands for "Hash" in the relevant NIST<br>documents. | Consider replacing "hashing" with "hash"<br>for SHA and SHS. | Changed all instances of SHS and SHA to use 'Hash', and to use leading capitals (e.g., "Secure Hash Standard") to indicate a proper noun |
| 49 | 3.3 | (3.3 line 27)<br>mode encryption | | Removed "mode encryption" following "counter" |
| 53 | 3.3 | (3.3 line 30)<br>FIPS PUB Federal Information Processing Standards Publication<br>Delete; not used once two references are corrected to match how they are<br>introduced in section 2. | | Deleted |
| 52 | 3.3 | (3.3 line 40)<br>SHS secure hashing standard<br>Delete; not used | | Deleted |
| 50 | 3.3 | (3.3 line 41)<br>Add XTS abbreviation | | Added: XTS: Xor-encrypt-xor with tweak and ciphertext stealing |
| 108 | 4.1 | "Archives" is the wrong word here, it implies too much. | "..securely stores and retrieves information." | Changed |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 110 | 4.1 | Suggest making "information" more specific to match Figure 1. | "storage of encrypted records and metadata produced by the&" | Changed (Note that the Storage Medium may contain plaintext records as well...) |
| 112 | 4.1 | Annex C is informative and therefore cannot contain requirements. | Either make it normative or change this sentence. | Changed to: See Annex C for a documentation summary. |
| 114 | 4.1 | What does the dotted line around the cryptographic mode imply? It cannot be an optional feature as surely at least one mode is needed in a system. | Clarify | Removed dotted line around cryptographic mode, and the term 'cryptographic mode'. |
| 17 | 4.1 | Figure caption needs to be on the same page as the figure. | Adjust document pagination to include figure caption on the same page as the figure. | See #2 |
| 58 | 4.1 | (4.1 line 30)<br>Move the cryptographic unit bullet to be the 4th bullet | | Moved |
| 59 | 4.1 | (4.1 line 1)<br>In figure 1, need to include "Tweak" going into the cryptographic module to cover XTS figure 3. | | Added Tweak as input into the Cryptographic Mode box of the Cryptographic Unit |
| 60 | 4.1 | (4.1 line 1)<br>Keep figure 1 caption on same page as figure | | See #1 |
| 130 | 5.1 | What span is the Maximum Total Plaintext in Table 2 measured over? | Define span as encryption session as in 6.5.3. | Added following text as footnote to Table 2 (in reference to the Maximum Total Plaintext column): "Applies to all data encrypted during the lifetime of a particular cipher key" |
| 63 | 5.1 | (5.1 line 28)<br>modes<br>s/b<br>routines | | Changed |
| 62 | 5.1 | (5.1 line 30)<br>of the CCM-128-AES-256 cryptographic mode.<br>A routine is not part of a mode. Try<br>"implementing the CCM-128-AES-256 cryptographic mode." | | Changed |
| 67 | 5.1 | (5.1 line 1)<br>Table 2<br>0 or 16 to 268-1<br>Unclear if this means<br>(0 or 16) to 2^68-1<br>or<br>(0) or (16 to 2^68-1) | | Added comma: 0, or 16 to 268-1 |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 66 | 5.1 | (5.1 line 1)<br>Table 2<br>12 or 16 to 2^61-1<br>Unclear if this means<br>(12 or 16) to 2^61-1<br>or<br>(12) or (16 to 2^61-1) | | Added comma: 12, or 16 to 261-1 |
| 131 | 5.2 | Clarify the difference between the IV in e) and g), and name one of them CBC-IV as per the glossary. | Clarify (also needed in 5.4) | Added following note after list in 5.2: "NOTE—The IV used for the CBC-MAC computation of CCM does not correspond to the CBC-IV used in CBC-HMAC (see 5.4), even though the names are similar. The CBC-MAC portion of CCM uses a “CBC-IV” of all zeros, as compared to CBC-HMAC, which uses a unique CBC-IV for each invocation." |
| 65 | 5.2 | (5.2 line 10)<br>(hereafter referenced as the CCM document)<br>Delete this extra level reference (ehre and in the text below) and just refer to NIST SP 800-38C directly (like item a) refers to NIST FIPS 197 rather than "the AES document") | | Changed |
| 69 | 5.2 | (5.2 line 13)<br>256-bit<br>s/b<br>256-bit (32-byte) | | Changed |
| 70 | 5.2 | (5.2 line 20)<br>Generate IVs according to 6.5<br>s/v<br>IV computation with further requirements from 6.5<br>(to match 5.3) | | Changed |
| 64 | 5.2 | (5.2 line 28)<br>footnote 3 For information on references, see Clause 2.<br>Delete this unnecessary footnote | | The IEEE Style Manual does recommend such a footnote, but this comment has come up often enough that we'll delete it and let the IEEE editors decide whether to add it back in before publication. |
| 26 | 5.3 | The capitalization of "counter" in the heading is not consistent with Table 1. | Capitalize "Counter" and "Mode" here, or else use lower case "counter" in Table 1. | Capitalized "Counter" and "Mode" to be consistent with SP 800-38D and the original GCM spec by McGrew and Viega. |
| 74 | 5.3 | (5.3 line 11)<br>256-bit<br>s/b<br>256-bit (32-byte) | | Changed |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 71 | 5.3 | (5.3 line 16)<br>Since 800-38D is not done, this note might not remain true. Eliminate all references to 38D and just refer to the McGrew document. | | Changed first part of note to: The document entitled "The Galois/Counter Mode of Operation" by Mcgrew and Viega does not allow... |
| 80 | 5.3 | (5.3 line 19)<br>"At least 16 bytes" doesn't mention the upper limit of 2^61-1 mentioned in the table. | | Changed to: e) The length of the IV shall be either 12 bytes, or between 16 bytes and 261-1, inclusive. |
| 79 | 5.3 | (5.3 line 19)<br>The length of the IV shall be either 12 bytes or at least 16 bytes.<br>Move this into the a)b) list | | Done |
| 27 | 5.4 | This line could be interpreted to allow, for example, the truncation of SHA-256 outputs to 160 bits. Is this intended? | Consider inserting "Output length of the SHA algorithm, i.e.,"& | Changed item as follows: c) The MAC length (i.e., Tlen) shall match the output length of the underlying hash function (e.g., 160 bits (20 bytes) for SHA-1, 256 bits (32 bytes) for SHA-256, or 512 bits (64 bytes) for SHA-512) |
| 28 | 5.4 | Some of the sentences end in periods, some don't. | Add periods to items b), c), d), e), and f). | The list was reworked to make each statement a sentence with a keyword (e.g., 'shall', 'may') |
| 29 | 5.4 | Would padding have to occur within the plaintext record formatter? | Consider replacing "the cryptographic unit" with the plaintext record formatter of the cryptographic unit". | Changed note as follows: NOTE— Even though the plaintext record is required to be a multiple of 16 bytes, the host record may be any size if the plaintext record formatter of the cryptographic unit provides padding to produce plaintext records that are a multiple of 16 bytes |
| 6 | 5.4 | "of an CBC-AES-256-HMAC-SHA" should be "of a CBC-AES-256-HMAC-SHA" | Make requested correction. | Changed |
| 136 | 5.4 | "there" should be "their" | Correct | See #31 |
| 7 | 5.4 | "there" should be "their". | Make requested correction. | See #31 |
| 73 | 5.4 | (5.4 line 31)<br>(see 4.5.1 for a discussion on padding)<br>That section doesn't mention padding. | | Changed to: "4.3 Plaintext record formatter" |
| 85 | 5.4 | (5.4 line 8)<br>needs only to support<br>s/b<br>is only required to support | | Changed |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 33 | 5.5 | Would padding have to occur within the plaintext record formatter? | Same as for comment on Page 15, Line 2. | Changed note to: Even though the plaintext record is required to be at least 16 bytes long, the host record may be smaller if the plaintext formatter of the cryptographic unit provides padding. |
| 137 | 5.5 | "allow there reconstruct during decryption" is most confusing. AAD may not be encrypted, and may be stored whole so it doesn't have to be reconstructed. | Clarify handling of AAD | See #31 (with changes from CBC to XTS) |
| 84 | 5.5 | (5.5 line 12)<br>FIPS PUB 180-2<br>s/b<br>NIST FIPS 180-2 | | Changed |
| 88 | 5.5 | (5.5 line 3)<br>Delete "with 512-bit (64-byte) key." which is implied by the definiton of HMAC-SHA-512 | | Deleted |
| 89 | 5.5 | (5.5 line 4)<br>One row should mention the IV is 16 bytes (each other mode mentions its IV size) | | Added: c) The IV length shall be 128 bits (16 bytes). |
| 36 | 6.4 | The period is missing for this sentence. | Add a period. | Added period |
| 141 | 6.4 | Missing space | "See B.2 for a" | Changed (see #37) |
| 37 | 6.4 | A space is missing after "B.2". | Add a space. | Added space |
| 19 | 6.4 | key-wrapping key is not defined | Use key-encrypting key | Changed |
| 92 | 6.4 | (6.4 line 14)<br>v2.1[B18]<br>s/b<br>v2.1 [B18] | | Changed |
| 45 | 3.2.0 | (3.2.0 line 8)<br>CBC-HMAC<br>should be spelled out:<br>cipher block chaining with keyed-hash message authentication code (CBC-HMAC): | | Changed name and reordered definitions to be alphabetical |
| 46 | 3.2.0 | (3.2.0 line 11)<br>CBC-HMAC-SHA<br>should be spelled out<br>cipher block chaining with keyed-hash message authentication code using secure hash algorithm (CBC-HMAC-SHA): | | Changed name and reordered definitions to be alphabetical |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 47 | 3.2.0 | (3.2.0 line 15)<br>CBC-IV<br>s/b<br>cipher block chaining<br>initialization vector (CBC-IV): | | Changed name and reordered definitions to be alphabetical |
| 44 | 3.2.0 | (3.2.0 line 26)<br>Delete 'mode encryption" | | Changed name and reordered definitions to be alphabetical |
| 48 | 3.2.0 | (3.2.0 line 28)<br>(See NIST SP 800-38D)<br>should reference the McGrew document per section 2, not 38D which is just a<br>bibliography reference. | | Changed |
| 55 | 3.2.0 | (3.2.0 line 5)<br>NOTE-See 4.2.3<br>Add . at end of each note | | Changed 3 occurrences |
| 51 | 3.2.0 | (3.2.0 line 20)<br>3.2.0.secure hashing standard (SHS): See NIST FIPS 180-2.<br>Delete; not used | | Deleted |
| 54 | 3.2.1 | (3.2.1 line 22)<br>Add definition for:<br>Xor-encrypt-xor with tweak and ciphertext stealing (XTS): | | Added: Xor-encrypt-xor with tweak and ciphertext stealing (XTS): The cryptographic mode of operation described in IEEE P1619. |
| 57 | 3.4.2 | (3.4.2 line 10)<br>"followed by the subscript 16."<br>Subscript 16 is never used | | Removed all references to hexadecimal numbers in this paragraph, and replaced it with the following text: Binary numbers are represented by a string of one or more binary digits, followed by the subscript 2. For example, the decimal number 26 is represented as 00011010_2 in binary. |
| 106 | 3.4.3 | Concatenation does not seems to be used in the document. | Remove 3.4.3 | See #56 |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 56 | 3.4.3 | (3.4.3 line 13)<br>"3.4.3 Concatenation<br>The concatenation operator (\|\|), represented as two vertical pipes, joins two bit strings such that the left operand occupies the lower addresses of the result, and the right operand occupies the upper addresses. If the result is interpreted as an integer, the left operand contains the most-significant bits and the right operand contains the least-significant bits.<br>NOTE-This is consistent with the big-endian convention.<br>Example:<br>00112 \|\| 10102 = 001110102"<br>Delete; \|\| is never used. | | Deleted |
| 18 | 4.2.1 | The term "policies" is used and even emphasized, but no further definition or explanation could be found in the document. | Provide information on what is meant by the term "policies." | Added following definition to 3.2: policies: In cryptography, a set of rules that defines aspects of the management of a cryptographic system (e.g., encryption, decryption, or bypass rules). |
| 115 | 4.2.2 | "is a tape drive" is not good description | "is contained in a tape drive" | Changed |
| 116 | 4.2.2 | "is a disk drive" is not good description | "is contained in a disk drive" | Changed |
| 117 | 4.2.5 | The medium also stores metadata per the figure. | "encrypted records and metadata" | Changed |
| 122 | 4.5.1 | Subclause 4.5 is self-referential | Use "the following subclauses" as in 4.6.1 | Changed (Note, however, that there is precedent for this strange self-referential form in other standards, such as those of INCITS/T10.) |
| 61 | 4.5.3 | (4.5.3 line 34)<br>AAD and IV<br>s/b<br>IV and AAD<br>to match the rest of the paragraph | | Changed |
| 23 | 4.6.2 | Does this sentence apply to the first<br>case, i.e., if the cryptographic unit<br>validates the MAC before returning<br>the plaintext? | Consider combining with the previous<br>paragraph or otherwise clarifying. | Preceded sentence with "If the cryptographic unit is capable of returning plaintext before validating the MAC, then" |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 24 | 4.6.2 | Similar to the previous comment<br>it's not clear whether the cryptographic<br>unit is supposed to have the option of<br>supporting the special signal "PASS"<br>in the first case as well as the second,<br>where it's required. | Reorder text or revise to clarify. | Changed first part of sentence to "If the cryptographic unit is capable of returning plaintext before validating the MAC, then …". Also updated parallel text in Table C.1 |
| 25 | 4.6.3 | It's not clear whether "ordering verification" refers to lines<br>41 and 42, or to something else in B.3, or to something else altogether. | Indicate the meaning of "ordering verification" in the text, and consider including a definition in Clause 3. | Changed 4.6.3 heading to "Ordering verification"; Changed first sentence of 4.6.3 to "During decryption, a cryptographic unit should performing ordering verification by checking that each IV or AAD is consistent…"; Removed hyphen in phrase "ordering verification". |
| 93 | A | (A line 22)<br>Add "Available from..." for [B9] | | Changed to: [B9] IETF RFC 3766, Determining Strengths For Public Keys Used For Exchanging Symmetric Keys, available from the World Wide Web site http://www.ietf.org/rfc/rfc3766.txt, April 2004. |
| 39 | B.4 | The reader may not immediately remember which modes use counter mode. | Consider inserting something like '', as occurs in CCM and GCM,''. | Added "(e.g., GCM, CCM)" following the word 'mode' |
| 94 | B.4 | (B.4 line 41)<br>Note, however, that such implementations<br>s/b<br>Such implementations<br>(avoid using Note outside real NOTEs) | | Changed |
| 95 | B.4 | (B.4 line 50)<br>Note that CBC<br>s/b<br>CBC<br>(avoid using Note outside real NOTEs) | | Changed |
| 96 | B.7.1 | (B.7.1 line 17)<br>It is noted that the bound<br>s/b<br>The bound<br>(avoid using Note outside real NOTEs) | | Changed |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 98 | D.1 | (D.1 line 20)<br>KEY3 (XTS only) last 512 bits of the cipher key<br>Key3 is never used in the test vectors; HMK is used instead | | Changed |
| 99 | D.1 | (D.1 line 27)<br>Key 3<br>s/b<br>HMK | | Changed |
| 100 | | The second paragraph of the Introduction states "legislation that requires the encryption of sensitive information". This isn't completely accurate, encryption is often stated only as a remedy. | "legislation that requires the protection of sensitive information." | Changed |
| 1 | | The caption for this figure should appear on the same page as the figure. | The caption for this figure should appear on the same page as the figure. | Figure now linked to caption |
| 10 | | change "consolidates" to "processes" | | Changed |
| 143 | | "partially decrypted plaintext" contradicts the body of the standard | Use same wording as in the body | Changed "partially decrypted plaintext" to "plaintext" |
| 144 | | Wording improvement suggestion | "Use of a corrupted" | Changed |
| 147 | | CIV isn't used in 5.4. CBC-IV is, but not consistently. | Clarify term | Clarified term CBC-IV in both 5.4 and in the CIV and NON acronyms in the test vectors |
| 146 | | AAD is used in the test vectors, but doesn't appear in the list of abbreviations | Add AAD | Added |
| 3 | | Meets all editorial requirements. If possible, please submit the source files for all graphics in Tiff format. | | Diagrams are available in Visio format, and can also be converted to TIFF |

Changes that followed the principle of the comment:

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 42 | 2 | (2 line 6)<br>Reference footnote 2 from all the NIST entries | | According to the IEEE Style Manual, only the first reference needs a footnote. Moved footnote 2 to the first NIST reference and changed NIST webpage to reference only the base url: <http://csrc.nist.gov> (NIST has redesigned their webpage, and I don't think the old link still works, or will work in the long-term) |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 109 | 4.1 | Why "simple"? | Either explain limitations further or remove | The intent was to show that the CU *may* perform key management, but is not primarily responsible in doing to. Changed to: A cryptographic unit that performs data formatting, encryption, and decryption, and that may perform cryptographic key management (see 4.2.4). |
| 111 | 4.1 | "facilitates interchange" directly contradicts the introduction, and is preceded by a dangling "This". | "The documentation will provide sufficient information to allow optimal use and detailed security evaluation of the cryptographic unit and its environment." | (the word 'will' is taboo). Changed to: "The documentation provides sufficient information to allow optimal use and detailed security evaluation of the cryptographic unit and its environment." |
| 113 | 4.1 | The last two sentences of this paragraph are not clear enough, and introduce unnecessary terminology (such as physical and logical). | "Multiple components shown below may exist within a single equipment, and multiple instantiations of the same component may exist within a single system." | Changed to: Multiple components shown in Figure 1 may exist within a single embodiment, and multiple instantiations of the same component or subcomponent may exist within a single system. |
| 118 | 4.4 | Typo | "decryption routine has cryptographically" | In this text, we need to make sure to allow implementations that check the MAC after returning some plaintext. Changed to: "The plaintext record de-formatter shall only use information that the decryption routine is able to cryptographically verify using a message authentication code (MAC)." |
| 128 | 5.1 | Though this document defines multiple modes, and allows one or more to be support in a cryptographic unit, it contains no rules for how multiple may be used. May the same key be used for 2 modes in one session? Silly I know, but no covered. | Our position is that each cryptographic unit should support only one mode at a time. Ideally for us, each product should support one mode, and the product info should tell the application which mode is being used. Anything else means that the system may change things underneath us and we will not know what happens. | The concerns of mode control (i.e., which mode is active) are probably better handled in other standards, such as T10/SSC-3 for tape drives, or T13 for disk drives. Added the following text to the end of 4.5.3: "For encryption, the cryptographic unit shall associate each cipher key with a single cryptographic mode, and shall not use this cipher key in any other cryptographic mode. The key manager should associate each cipher key with a single cryptographic mode." |
| 129 | 5.1 | Can we please number these modes? | I'd rather product data sheets claim support for '1619.1 mode 3' rather than 'CBC-AES-256-HMAC-SHA-256 as specified in 1619.1". | We're working on defining algorithm numbers in other standards bodies, such as T10 and IANA. Putting numbers into this standard is probably not a good idea, and it's a little late to add them now. SISWG will provide guidance on numbering these algorithms separately. |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 81 | 5.3 | (5.3 line 12)<br>Tag<br>Define that "Tag" in gcm corresponds to "MAC" in table 2. | | Changed line to: b) The MAC length shall be 128 bits (16 bytes). The MAC shall be used as the Tag defined in the GCM algorithm. |
| 16 | 5.4 | Inconsistent use of FIPS 198 identifier. | FIPS 198a is used elsewhere. | Changed "FIPS 198a" to "FIPS 198" (The only thing named 'FIPS 198a' is the filename for FIPS 198 -- the document itself only uses 'FIPS 198') |
| 134 | 5.4 | The reference in e) is incorrect. | Padding is discussed in 4.3 & 4.4, but there needs to be a requirement somewhere on the boundary to be padded to. See the Note on page 15 line 1 for a possible place. | Reference changed to 4.3. The padding boundary is only a requirement of the particular cryptographic mode, which is why 5.4 specifies a boundary of 16 bytes. See #73. |
| 135 | 5.4 | The confusion on encrypted versus ciphertext record is further evidenced here. Use consistent terminology. | Identify the encrypted record in Fig 2 and either remove the "record" next to ciphertext. | Text reworked to more consistently use the term 'ciphertext record' where appropriate. Figure 2 is correct, according to the intention of the P1619.1 architecture. See also #30 |
| 31 | 5.4 | The end of the sentence is a little awkward. | Replace "there" with "their", or reword to something like "if there is enough information elsewhere to reconstruct them for the decryption routine." | Replaced sentence with following (and similar change for sentence following Figure 3): In Figure 2, the dotted lines around the 'AAD' and 'CBC-IV' boxes indicate that it is optional to include these fields within an encrypted record if there is enough information elsewhere to reconstruct the AAD and CBC-IV for the decryption routine. |
| 30 | 5.4 | Is a ciphertext record different than ciphertext? | Consider replacing "Ciphertext Record" with "Ciphertext" in Figure 2. | The terms "ciphertext record" and "ciphertext" are subtly different in that ciphertext is the generic result of encrypting plaintext, but a ciphertext record is the result of encrypting a plaintext record (and has the same length). As a counterproposal, what if we added a definition for "ciphertext record" as follows: "ciphertext record: The result of encrypting a same-length plaintext record using a cryptographic mode of operation. See also: ciphertext; cryptographic mode of operation; plaintext record." |
| 138 | 5.4 | Tweak is not identified as an input in the text, but is shown in Figure 3 | Add tweak to list of inputs | Tweak' is already listed as an input, in the same line describing the IV. |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 77 | 5.4 | (5.4 line 28)<br>HMAC using SHA-1, SHA-256 or SHA-512<br>s/b<br>Integrity algorithm: HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-512 | | Changed to: b) The HMAC shall use one of the following hashing functions (see NIST FIPS 180-2):<br>1) SHA-1;<br>2) SHA-256; or<br>3) SHA-512. |
| 78 | 5.4 | (5.4 line 29)<br>MAC length:<br>Describe which of these sizes applies to HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512 | | Changed to:c) The MAC length (i.e., Tlen) shall match the output length of the underlying hash function (e.g., 160 bits (20 bytes) for SHA-1, 256 bits (32 bytes) for SHA-256, or 512 bits (64 bytes) for SHA-512). |
| 76 | 5.4 | (5.4 line 33)<br>IV generation<br>s/b<br>IV computation<br>(to match 5.3) | | Changed sentence to:g) The cryptographic unit shall compute IVs, called CBC-IVs in the case of CBC-HMAC, according to one of the following methods (see NIST SP 800-38A, Appendix C) |
| 82 | 5.4 | (5.4 line 5)<br>there<br>s/b<br>their | | See #31 |
| 32 | 5.5 | It's not clear that the antecedent to "this method" is restricted to the case of variable length AAD. | Combine with previous paragraph. | Added the following (accidentally deleted) sentence in front of the sentence in question to mirror the structure found in the CBC-HMAC subclause: "If the cryptographic unit supports XTS-HMAC, then documentation shall describe the format of the AAD and the method used to determine where the AAD ends and the tweak starts." Also added to Annex C. |
| 35 | 5.5 | The end of the sentence is a little awkward. | Same as for comment on Page 16, Line 4. | See #31 |
| 83 | 5.5 | (5.5 line 12)<br>FIPS PUB 198<br>s/b<br>NIST FIPS 198a | | See #16 |
| 86 | 5.5 | (5.5 line 1)<br>AES key<br>s/b<br>cipher key | | (See #75). Changed to: a) The cipher key length shall be 1024 bits (128 bytes), consisting of the concatenation of the following parts, in order:<br>1) An AES key that is 512 bits (64 bytes), used as input into the XTS-AES-256 procedure (see IEEE P1619); and<br>2) An HMAC key that is 512 bits (64 bytes), used as input into the HMAC-SHA-512 procedure. |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 87 | 5.5 | (5.5 line 4)<br>Generate IVs according to 6.5...<br>s/b<br>IV computation with further requirements from 6.5, used as the tweak specified in IEEE P1619. | | Changed to:b) The cryptographic unit shall compute IVs according to 6.5. The IV is used as the tweak specified in IEEE P1619. |
| 90 | 5.5 | (5.5 line 6)<br>The cryptographic unit shall use the remaining bits of the cipher key as the HMAC-SHA-512 key in the MAC generation and verification routines. In HMAC-SHA-512, the resulting MAC shall be 64 bytes long. Since only HMAC-SHA-512 is defined, combine the generic and specific sentences into one. | | Deleted entire paragraph and put equivalent description into lettered-list (see #86 for text) |
| 91 | 5.5 | (5.5 line 5)<br>there<br>s/b<br>their | | See #31 |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 140 | 6.4 | "shall" needed in the sentence about key wrapping, also isn't key wrapping equally applicable to encryption? | Clarify | Removed the sentence in question because it was not meant to be a requirement, and it did not meaningfully contribute to the standard. Also, added the following text to the beginning of 6.4 to clarify key wrapping: "Key wrapping is the process of using a key encrypting key (KEK) to encrypt another cryptographic key (e.g., cipher key) using a key wrapping routine. Key unwrapping is the process of using a KEK to decrypt a previously wrapped cryptographic key. If the same KEK is used for both wrapping and unwrapping, then it is a symmetric KEK. If a different KEK is used for wrapping and unwrapping, then an asymmetric public KEK performs the wrapping and an asymmetric private KEK performs the unwrapping. ... The cryptographic unit may use any key wrapping routine for protecting the cipher key during import or export, or for archival within the storage medium or key manager. The cryptographic unit should only use key wrapping routines that have undergone peer review within the cryptographic community, such as those listed above. " |
| 120 | 4.5.3 | The definition of an encrypted record in this section is most confusing & needs to be reworked. Also the relationship of metadata as shown in Fig 1 with this section is not clear. | "The encryption routine produces an encrypted record that contains: a) Ciphertext; b) A message authentication code (MAC); c) Optionally an IV (or enough information that the complete IV can be recreated; d) Optionally the AAD (or enough information that the complete AAD can be recreated; e) Other information to support optional functions such as verification (see 4.5.6.3)." Also remove the metadata arrow from Fig 1. | Changed to reflect the suggestions for items a) through d). Adding the suggestion for e) is potentially misleading because the information used to perform Ordering Verification (as described in 4.6.3) needs to be contained within the AAD, IV, or ciphertext. |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 121 | 4.5.3 | Why the statement that the ciphertext has the same length as the plaintext record? This seems to be the only place this is mentioned. Is this a requirement? | Remove or make a firm requirement. | The ciphertext record needs to be the same length as the plaintext record, according to the P1619.1 model. It is possible to have host records and plaintext records that are not the same length, to achieve the behavior you're probably looking for. Added this sentence to 4.5.3: "The ciphertext record shall have the same length as the plaintext record." |
| 124 | 4.6.2 | Are there limits to how much plaintext can be returned before the MAC is verified. Can you get multiple records ahead in plaintext terms? | | There are no additional limits to the amount of plaintext that can be returned before the MAC is verified. Multiple records can be transferred before checking the MAC. However, there is value in requiring documentation of limits. The documentation requirements have been expanded as follows: "If the cryptographic unit is capable of returning plaintext before validating the MAC, then documentation shall define the special signal PASS, describe how the host and/or controller receive such a signal, and define limits for the number of host records and bytes of plaintext that the cryptographic may return before checking the MAC" |
| 34 | 5.5. | Is a ciphertext record different than ciphertext? | Same as for comment on Figure 2. | See #30 |
| 38 | A | NIST may finalize SP 800-38D in time to revise this entry. | Revise if possible. | While we want to use SP 800-38D if possible, the timing is such that even if 800-38D is released before P1619.1 is finalized, we won't have time to perform a thorough review to determine whether P1619.1 is compatible with 800-38D. However, such a change would be appropriate for an amendment to P1619.1. |
| 40 | B.6 | The seriousness of the vulnerability that Joux identified is not well reflected in this paragraph. The "certain circumstances" are more general for the Joux attack than for the Ferguson attack. | Revise the paragraph to cite the Joux observations on GCM (available on the NIST site) and to focus more attention on them. | Added bibliography entry for the Joux paper. Added reference to the Antoine Joux paper in B.6, but left paragraph otherwise unchanged. |
| 97 | B.8 | (B.8 line 46)<br>FIPS PUB 800-38A<br>s/b<br>FIPS SP800-38A | | Changed to NIST SP 800-38A |

| # | Sub clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|
| 21 | | Is the generation of encrypted records intended to be excluded from the definition of a session? | Consider revising to clarify; also, consider replacing "encryption operations" with something like "invocations of the encryption routine." | Changed definition of Encryption Session to: An interval in which a cryptographic unit generates encrypted records using a set of self-consistent variables, such as unique initialization vectors. |
| 9 | | change "that securely maintains" to "that may securely maintain" | | (Actually line 37). In principle this suggestion is correct in that the previous language implies a 'shall' requirement on the key manager. This ambiguity should be cleared up. However, 'may' isn't strong enough here. Changed to "that should securely maintain" |
| 11 | | The "shall" applies to "to unambiguously reconstruct the original host records or detect malicious tampering." and the latter is not possible in all cases. Perhaps this should be "attempt to detect any malicious tampering, and in the case where no tampering is detected shall allow unambiguous reconstruction of the original host records." | | This text was intended to only consider the case when a host record is contained within two or more plaintext records, and as such, needs clarification. Changed the sentence as follows: "If a host record is formed from two or more plaintext records, then Tthe cryptographic unit shall include sufficient information within the AAD, IV, or plaintext record to allow the plaintext record de-formatter (see 4.4) to unambiguously reconstruct the each of the original host records or detect malicious tampering." |
| 148 | | The test vectors for the different SHA lengths are not immediately obvious. Suggest amending the section titles to show coverage of the 3 cases. | Amend sections titles in D.4 | Changed title of D.4 to "D.4 CBC-AES-256-HMAC-SHA test vectors (including HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512)" |

List of changes requested but not accepted

October 14, 2007

SUBJECT: Rejected comments on IEEE P1619.1

This document identifies the negative comments from the balloting group on IEEE P1619.1, draft number D23, that could not be accepted, together with the reasons why.

These were as follows:

| # | Name | Sub Clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|---|
| 14 | Hibbard, Eric A | 1.2 | Sentence is cumbersome. "In addition, this standard applies to other storage devices if these support storing extra metadata with each encrypted record." | "In addition, this standard applies to other storage devices, which are capable of storing extra metadata with each encrypted record." | We cannot easily change the Purpose without updating the PAR. Although the language is somewhat cumbersome, it does not appear ambiguous. |
| 102 | Cummings, Roger | 2 | Include NIST SP 800-38D inc this list given its prominence in Notes in section 5. | Create additional reference | SP 800-38D is a bibliography entry -- not a reference. The P1619.1 Task Group agreed to replace 38D with the original McGrew and Viega GCM spec because of uncertainty and incompatibilities within the latest 38D draft. |
| 15 | Hibbard, Eric A | 2 | IEEE P1619 refers to the project, but it is not clear that this is used for the actual standard. | Consider using IEEE 1619 | The 2007 IEEE Style Manual recommends the phrase "IEEE P1619" for a draft, and "IEEE std 1619" for an approved standard (see 10.4.3). Using "IEEE P1619" is consistent with the style manual |

| # | Name | Sub Clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|---|
| 8 | Geipel, Michael D | 3.2 | I strongly object to the sentence:<br>"The Authoritative Dictionary of IEEE Standards, Seventh Edition, should be referenced for terms not defined in this clause."<br>This is not a balloted standard. Rather, this is a collection of definitions found in IEEE standards that had been individually voted upon. As such, there is no requirement for consistancy. For example: in protocols, the terminology "frame" and "packet" are often used. If you look these terms up in IEEE 100, you will find a multiplicity of definitions, often contradictory. This NOT a criticism of the dictionary! Some IEEE protocols use "frames" to encapsulate "packet" data. Others use "packets" to contain "frames". If not defined in subclause 3.2, then a term should reference the actual standard in which it is defined.<br>One more relevant note: The seventh edition is IEEE 100-2000 (published in January 2000) and is not likely to be as useful as more recent standards references. A lot has changed since then... | Remove the sentence:<br>"The Authoritative Dictionary of IEEE Standards, Seventh Edition, should be referenced for terms not defined in this clause."<br>Either define terms in subclause 3.2 or reference an applicable standard in the body of the text. | This sentence is consistent with the IEEE 2007 Style Manual. After consulting the IEEE editorial staff, they asked that we keep the sentence as-is. If there is a particular term used in this standard that is ambiguously defined by the IEEE dictionary, please bring it to our attention and we will clarify it within the standard. |
| 5 | Snively, Robert N | 3.2 | At this point and numerous other points in sub-clause 3.2, the "Note" font and positioning is used for a statement that should be a reference. | Change the text "...secure hash algorithm family (See NIST FIPS 180-2.<br>Note -- See 5.4" to read:<br>"...secure hash algorithm family (See NIST FIPS 180-2). See 5.4.<br>This needs to be done for all such cases in clause 3.2. Make sure that the references are generated correctly so that they are active reference links in the PDF file. | This style is consistent with the IEEE 2007 Style Manual, subclause 10.5.2 "Construction of the definitions clause". According to this style, internal references should be set-off within NOTEs within definitions. |

| # | Name | Sub Clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|---|
| 107 | Cummings, Roger | 4 | I'm a little uncomfortable with the interleaving of models and requirements in this section. | Recommendation is to create a model section and then a separate requirements section. The requirements on documentation should be in a separate section. | (Note that Annex C contains all the documentation requirements in one place...) While this is a sound recommendation, it is unfortunately too late to implement this change without significant changes that would destabilize the draft. |
| 119 | Cummings, Roger | 4.4 | A firm requirement for the signal FAIL in the model section! | Suggest removing the requirement (it's stated again in 5.4) and adding the PASS/FAIL signals to Figure 1 | The similar requirements stated in 5.4 and 5.5 only apply to the CBC and XTS modes -- this requirement applies to all modes (and for slightly different circumstances). Added PASS and FAIL under the Status arrow going from the cryptographic unit to the controller. |
| 127 | Cummings, Roger | 4.7 | I don't believe that AAD affects the integrity & confidentiality, and thus shouldn't be listed here. | Remove AAD from here. Add requirement to ensure its integrity elsewhere. Also spell out KEK as it's used here for the 1st time. | AAD does affect the integrity of the encrypted record because AAD is used as part of the MAC computation. It does not affect the confidentiality, though, because it is not used as input into the encryption portion of the encryption routine (which is why disclosure is allowed, but modification is not)... Spelled out "KEK" |
| 68 | Elliott, Robert C | 5.1 | (5.1 line 1)<br>Table 2<br>MAC<br>s/b<br>HMAC-SHA | | The term 'MAC key' is used elsewhere in the document, where 'HMAC-SHA key' is not used anywhere. |
| 133 | Cummings, Roger | 5.3 | IV truncation sounds like a requirement but it's in a note. | Extract from note and change to "long IV shall be distilled back to 16 bytes". | Long IVs are not truncated -- they are hashed (or distilled). The requirement for distilling a long IV back down to 16 bytes is stated in the normative McGrew/Viega GCM reference. |
| 132 | Cummings, Roger | 5.3 | Does the NIST SP 800-38D need to be referenced in the sentence with the "shall" as well as the note? | Make 800-38D a requirement as well and add to the glossary. | See #38. We are not using SP 800-38D as a normative reference at this time because the current 38D draft is incompatible with P1619.1 |
| 75 | Elliott, Robert C | 5.4 | (5.4 line 27)<br>AES key<br>s/b<br>cipher key | | In CBC-HMAC, the cipher key is the concatenation of the AES key and the HMAC key. The AES key is 256-bits and the cipher key is either 416, 512, or 768 bits. |

| # | Name | Sub Clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|---|
| 72 | Elliott, Robert C | 5.4 | (5.4 line 24)<br>NIST FIPS 198<br>s/b<br>NIST FIPS 198a | | See #16 |
| 125 | Cummings, Roger | 4.6.2 | Another firm requirement for the signal FAIL in the model section! | See previous comment | See #119 |
| 123 | Cummings, Roger | 4.6.2 | Rework the inputs to reference the encrypted record structure defined above, and identify source of the inputs if not from that record. | Rework. Cover where IV & AAD come from. | While it is true that it's a little hard to infer where these inputs come from, the standard does describe this in other sections, and reworking this text now would be somewhat risky. Note that the IV and AAD do not have to come from the encrypted record -- in fact, they can come from just about anywhere. |
| 126 | Cummings, Roger | 4.6.3 | Verification is a requirement, and should be specified in more detail elsewhere. | | While it's true that "verification of the MAC" is a requirement, it is not a requirement to verify the correct ordering of decrypted host records. This is left only as a recommendation. See #25 for similar discussion |
| 142 | Cummings, Roger | 6.5.3.4 | should in the 2nd sentence of c) needs to be a "shall" | Make Change | This is getting too far into the implementation details. From a cryptographic standpoint, it is sufficient to simply cease encrypting data -- notification of this event is handled in other ways. In many cases, the IVs are large enough that it is not possible for a cryptographic unit to wrap the IV (other limitations kick in first...), so the cryptographic unit does not need to handle this case. |

| # | Name | Sub Clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|---|
| 145 | Cummings, Roger | | Annex C is informative and therefore cannot contain requirements, but its referenced in many requirements in the body of the document. | Make Annex C normative | Annex C is a restatement of normative text already contained in the main body. Making this normative would result in the possibility of disagreement between the main body and this annex, and would create an ambiguity as to which has precedent. By making Annex C informative, the main body becomes the sole possessor of normative text in regards to documentation. The other alternative (not taken here) would be to remove all documentation references in the main text, and only keep them in a normative Annex C. |
| 20 | Chen, Lidong | | MAC generation and verification are integral features of the modes in this document. | Incorporate MAC generation into the definition. | While this statement is true, the definition for 'cryptographic modes of operation' needs to be general enough for inclusion into the IEEE Authoritative Dictionary, and, in general, modes of operation do not have to include a MAC. |
| 13 | Goodman, Brian G | | Make the font match the rest of the document in lines 40-44. | | It does not appear that the font on lines 40-44 is different (The IEEE editorial staff will pick up these types of errors where they do exist) |
| 12 | Goodman, Brian G | | Why allow more than 16 bytes then? Why not make line 24: "shall either be 12 or 16 bytes." and deleted the caveat on lines 25/26? | | The original GCM draft by McGrew and Viega allowed longer IVs. There are some IV constructions that distill low-entropy sources into a higher-entropy 128-bit IV. |
| 101 | Cummings, Roger | 1 | "Full interchange" needs more definition to be useful. | "Complete interoperability of media between multiple products requires&." | Changing the Scope likely requires a new Project Authorization Request (PAR), and is difficult to do at this stage. |

| # | Name | Sub Clause | Comment | Proposed Change | Resolution Detail |
|---|---|---|---|---|---|
| 2 | Hars, Laszlo | | (1) The scope of the standard is too restrictive, excluding important applications, which could have been covered with minor modifications (e.g. authentication by other means).<br>(2) The standardized algorithms need too much resources, which make them unsuitable for other than magnetic tape storage (or similar devices), although the title, scope and abstract aims at general usage. | | 1) If the scope of this standard is too restrictive, please feel free to propose a PAR that better fits your proposed project 2) We welcome proposals for such algorithms, and would be happy to address them in a related standard or amendment |
| 104 | Cummings, Roger | 3.2 | The numbering of items in the glossary is incorrect. | Use the third level | See #4 |
| 4 | Snively, Robert N | 3.2 | The sub-clause numbers do not appear to be incrementing correctly for the definitions included in the entire sub-clause 3.2. Please either correct the incrementing of the sub-clause numbers or remove them from the definitions section. | Please either correct the incrementing of the sub-clause numbers or remove them from the definitions section. | This is a printing issue with the IEEE Word Template and will be resolved by IEEE editors before publication. |
| 139 | Cummings, Roger | 5.5 | Make the dotted line in the figure match the legend, they're not easy to spot! | Clarify both Fig 2 & Fig 3 | This is a printing issue that will be resolved during IEEE publishing. |
| 43 | Elliott, Robert C | 3.2.0 | (3.2.0 line 2)<br>All the definitions are "3.2.0." | | See #4 |