List of changes to the draft standard

October 14, 2007

SUBJECT: Changes to IEEE P1619/D18, Draft Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

References: IEEE P1619.1/D17, Draft Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices, dated July 2007.

The following list contains the changes made to IEEE P1619 in going from draft number D17 to the new draft number D18.

Changes that were done according to a comment:

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
6	Ball, Matthew V	3.2	Place reference in parentheses	Change 'Galois field, see Menezes et. al. [B7]' to 'Galois field (see Menezes et. al. [B7])'	Fixed in text
5	Ball, Matthew V	3.2	Remove 'see' within bibliographic reference	Change '[see B12]' to '[B12]'	Fixed in text
8	Ball, Matthew V	5.1	Missing 'a'	Insert 'a' between 'In particular,' and 'single data unit'	Fixed in text
10	Ball, Matthew V	6	The sentence starting "The reason is that..." and to the end of the paragraph is informative	Move this informative text into a NOTE that immediately follows the paragraph	Fixed in text
3	Ball, Matthew V	3.1.1	Link to 3.3 is no longer valid	Change (see 3.3) to (see 4.3.1)	Fixed in text
13	Ball, Matthew V	D.4.3	XTC-AES-128 is the wrong name	Change XTC-AES-128 to XTS-AES-128	Fixed in text
9	Ball, Matthew V		The word 'attacker' implies a physical attack on a person.	Consider replacing 'attacker' with 'adversary' throughout the document	Replaced
81	Coordination, Editorial		Meets all editorial requirements. All MEC issues were fixed and the IEEE Word Template for drafts was used - thank you.		No change required
90	Cummings, Roger	4.1	This needs to include a definition of a hexadecimal format (as used in 5.1)	Add a similar sentence a d example to that for binary.	Fixed in text

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
94	Cummings, Roger	5.1	On what basis are tweak values incremented? On a data block basis, data unit basis? Obviously I think it may obvious to most people but it doesn't actually say anywhere!	"Each data unit is assigned a tweak value which is a non-negative integer. Consecutive data units are assigned tweak values in a monotonically increasing sequence, starting from an arbitrary non-negative integer."	Fixed in text
93	Cummings, Roger	5.1	Is a block REQUIRED to be 128 bits? The reference line is the closest to a requirement, and the encryption & decryption procedures seem to assume it.	Include in the block definition a clear requirement that a block shall be exactly 128 bits.	Fixed in text
89	Cummings, Roger	3.1.1	"(see 3.3)" is incorrect	should be "(see 4.3.1)"	Fixed in text
95	Cummings, Roger	5.3.2	"The key is parsed as a concatenation of two fields of equal size called Key1 and Key1"	Correct	Fixed in text
96	Cummings, Roger	5.4.2	Left term should be P, not C	C <- XTS-AES-Dec(Key, C, i)	Fixed in text
101	Cummings, Roger	7.1.1	Should the text elements in the Key Backup structure support I18N & L10N? Should a language tag be incorporated into the structure?	If the text is restricted to US-ASCII, say so, and provide a reference.	All text is US-ASCII
100	Cummings, Roger	7.1.2	What character set and encoding is used for the text in the StructureID, and other elements identified as text in the Key Backup structure? The W3C XML standard referenced defines ISO10646.	Specify that text is UTF-8, or some such other encoding scheme and add a specific reference.	All text is US-ASCII
88	Cummings, Roger	Intro	The introduction makes two references to "threats", but there is no text that references threats anywhere in body of the standard.	Either those references should be removed, or else the details of the threats covered should be included in the body of the draft standard.	"Dictionary attack" removed. Copy-pased is described in annex.
24	Elliott, Robert C	3.1	(3.1 line 10) Standards s/b Standards Terms		Fixed in text

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
23	Elliott, Robert C	3.1	(3.1 line 10) Seventh Edition, s/b Seventh Edition [B5],		Fixed in text
26	Elliott, Robert C	5.1	(5.1 line 33) single s/b a single		Fixed in text
32	Elliott, Robert C	6	(6 page 15 line 1) data unit s/b the data unit		Fixed in text
41	Elliott, Robert C	7.2	(7.2 line 13) Key s/b the Key		Fixed in text
40	Elliott, Robert C	7.2	(7.2 line 13) Document s/b The Document		Fixed in text
42	Elliott, Robert C	7.3	(7.3 line 5-6) (see http://www.w3.org/2001/04/xmlenc#aes256-cbc) Convert into a bibliography entry and cross reference it from here; that should eliminate the large spaces in line 5.		Fixed in text
22	Elliott, Robert C	4.1)	(4.1) Add a convention for hexadecimal numbers (subscript 16), since they are used in 5.1.		Fixed in text
27	Elliott, Robert C	4.3.1	(4.3.1 line 17) physical block s/b logical block		added "or logical"
28	Elliott, Robert C	5.3.1	(5.3.1 page 11 line 5) In figure 1, increase the line weights		Done
29	Elliott, Robert C	5.4.1	(5.4.1 page 13 line 7) In figure 3, increase the line weights		Done
31	Elliott, Robert C	5.4.2	(5.4.2 line 26+) In 5.3.2, the numbered steps are indented to the right. 5.3.2 and 5.4.2 should be consistent.		Fixed in text

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
30	Elliott, Robert C	5.4.2	(5.4.2 line 22) Pm s/b Cm		Fixed in text
38	Elliott, Robert C	7.1.1	(7.1.1 page 15 footnote 3) i.e., the tweak value that corresponds to the first data unit in the archive should be inside ()		Fixed in text
37	Elliott, Robert C	7.1.1	(7.1.1 page 15 footnote 3) contiguous s/b i.e., a contiguous		Fixed in text
36	Elliott, Robert C	7.1.1	(7.1.1 page 15 footnote 3) encrypted data s/b the encrypted data		Fixed in text
35	Elliott, Robert C	7.1.1	(7.1.1 page 15 footnote 3) ability s/b the ability		Fixed in text
34	Elliott, Robert C	7.1.1	(7.1.1 page 9 footnote 3) initial s/b the initial		Fixed in text
33	Elliott, Robert C	7.1.1	(7.1.1 line 15) XML s/b The XML		Fixed in text
39	Elliott, Robert C	7.1.5	(7.1.5 line 18) TransformName s/b Transform Each table is an "element" with the name of its subclause (with spaces removed).		Fixed in text
44	Elliott, Robert C	AnnexB	(AnnexB line 13) material. s/b material (other test vector headers have no ending .)		Fixed in text

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
43	Elliott, Robert C	AnnexB	(AnnexB line 9) ; s/b .		Fixed in text
50	Elliott, Robert C	D.2	(D.2 page 34 line 12) chaining then an s/b chaining, an		Fixed in text
49	Elliott, Robert C	D.2	(D.2 page 34 line 11) key s/b same key		Fixed in text
48	Elliott, Robert C	D.2	(D.2 page 34 line 12) will necessarily yield s/b yields		Fixed in text
47	Elliott, Robert C	D.2	(D.2 page 34 line 5) tags then any s/b tags, any		Fixed in text
53	Elliott, Robert C	D.3	(D.3 page 35 line 19) "the group" What group?		replaced by "P1619 workgroup"
52	Elliott, Robert C	D.3	(D.3 page 35 line 15) better granularity s/b finer granularity		Fixed in text
51	Elliott, Robert C	D.3	(D.3 line 41) is required s/b are required		Fixed in text
55	Elliott, Robert C	D.4	(D.4 page 38 line 19) attack, s/b attack		Fixed on page 32
54	Elliott, Robert C	D.4.2	(D.4.2 line 6) value,. s/b value.		Fixed in text

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
21	Elliott, Robert C	General)	(General) An informative annex should be included documenting the LRW algorithm last defined in 1619/D5, including its test vectors. Producers have created implementations of LRW (as of 7/26/2007, google still finds more hits on "LRW" than "XTS"), and what they implemented needs to be documented in a document that isn't going to disappear. Since XTS is the preferred algorithm, it would be confusing for LRW to defined as part of a new standards effort (e.g. 1619a); it should be easy to port the D5 text into an informative annex as part of completing this project. It can be presented as historical background, and the usage constraints that led to XTS should be mentioned (don't include the tweak key as the plaintext data encrypted with that same tweak key, and ensure that the tweak key is a fully random value).		We agreed that this will be best served by a separate document
82	Griffin, Robert W	1.3	The document is inconsistent in terms of citing references, at times using square brackets following the author name, at other times including a "see ..." followed by the square brackets, such as in section 1.3 (also section 3.2).	Use only square brackets following author name, removing the "see ..." clause.	Partially fixed. This specific comment reflects 2 different uses.
76	Griffin, Robert W	7.3	Line 13, page 13 refers to XTS-AES-512. XTS-AES-512 is not defined as an allowed transform in the standard.	"XTS-AES-512" on page 13 should be "XTS-AES-256".	Fixed in text
78	Griffin, Robert W	D4.3	Typo, line 2, page 32: "XTC-AES-128"	should be "XTS-AES-128".	Fixed in text

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
63	Hibbard, Eric A	5.1	Grammatical problem.	Too many sentences started with "In particular". Suggest dropping this phrase.	Changed to "for example"
62	Hibbard, Eric A	5.1	Grammatical problem.	Change "In particular, single data unit does not necessarily correspond" to something like "In particular, a single data unit does not necessarily correspond"	Fixed in text
61	Hibbard, Eric A	5.1	Grammatical problem.	Change "When encrypting tweak value using AES, the tweak" to something like "When encrypting a tweak value using AES, the tweak"	Fixed in text
60	Hibbard, Eric A	5.1	Grammatical problem.	Change "This standard applies to encryption of data stream divided" should be changed to something like "This standard applies to encryption of a data stream divided"	Fixed in text
66	Hibbard, Eric A	6	Grammatical problem.	Change "if XTS-AES key consists of 512" to "if the XTS-AES key consists of 512"	Fixed in text
65	Hibbard, Eric A	6	Incorrect section referrences.	Change "5.3.2 and 5.4.2" to "5.3 and 5.4"	Fixed in text
64	Hibbard, Eric A	5.4.2	This sentence is more cumbersome than it needs to be.	Change "An illustration of the decrypting the last two blocks Cm-1Cm in the case that Cm is a partial block (b>0) is provided in Figure 4." to "The decryption of the last two blocks Cm-1Cm in the case that Cm is a partial block (b>0) is illustrated in Figure 4."	Fixed in text
67	Hibbard, Eric A	7.1.1	Grammatical problems.	There is an extra period following the footnote number. Also, the contents of the footnote have several wording problems.	Reworded
68	Hibbard, Eric A	D.3	Incorrect reference.	Change "C.1" to "D.2"	Fixed in text
59	Hibbard, Eric A	D.4	Incorrect acronym used.	"XTC-AES-128" should be "XTS-AES-128"	Fixed in text

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
75	Holoman, Stuart		The sentence "All numbers in this Annex are hexadecimal" is, in fact incorrect. Number usage outside the specific examples are normal base-10 numbers; e.g., "XTS-AES-128", "32 bytes" in line 13, and many more. That sentence should be expanded as indicated. However, if the "Vector #" is part of the specific example, then vector numbers greater than 10 (base 10) should be changed to the hexidecimal equivalent; e.g. "Vector 10" would be "Vector a", "Vector 17" would be "Vector 11".	Change sentence to read "All numbers within specific examples in this Annex are hexidecimal."	Fixed in text
74	Holoman, Stuart		plural usage	Change "two application" to read "two applications".	Fixed in text
15	Karocki, Piotr	5.1	Here we have also hexadecimal numbers. So sentence in 4.1 (page 8, line 21: "Decimal and binary numbers are used within this document.") is not correct.	Change: "Decimal and binary numbers are used within this document." To: "Decimal, binary and hexadecimal numbers are used within this document." Add, at end of 4.1: "Hexadecimal numbers are represented by a string of one or more hex digits followed by the subscript 16. Thus, the same decimal number 26 may also be represented 1A16."	Fixed in text
17	Karocki, Piotr	7.1.1	Do "refers to the size of the element and not to the size of the encoding." mean "refers to the size of element, and not to the size of encoded element" ?		Yes, the stated interpretation is correct.

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
18	Lang, Kenneth	5.3.2	The text "two fields of equal size called Key1 and Key1 such that" should read "two fields of equal size called Key1 and Key2 such that"	The text "two fields of equal size called Key1 and Key1 such that" should read "two fields of equal size called Key1 and Key2 such that"	Fixed in text
19	Lang, Kenneth	5.4.2	The text "two fields of equal size called Key1 and Key1 such that" should read "two fields of equal size called Key1 and Key2 such that"	The text "two fields of equal size called Key1 and Key1 such that" should read "two fields of equal size called Key1 and Key2 such that"	Fixed in text
79	Schwarm, Stephen C	4.1	You carefully define the representations of decimal and binary numbers but do not include hex which is used in the next section.	line 28 change "Decimal and binary numbers" to "Decimal, hexadecimal and binary numbers" line 32 add Hexadecimal numbers are represented by a string of 0, 1, 2, ... A, B, ... F characters followed by the subscript 16.	Fixed in text
80	Schwarm, Stephen C	5.1	Be consistent in the use of upper case letters in hexadecimal numbers. This may not be the only place	line 34 change "byte array 9a" to "byte array 9A"	Change to lower case
84	Sheehy, David B	4.1	Hexadecimal numbers are used in this document.	Text should be added to 4.1 to describe them. For example, "Hexadecimal numbers are represented in their usual 0, 1, 2, ... format followed by the subscript 16". Note that section 5.1 uses this format while Appendix B does not. This should be reconciled.	Notation for hex numbers added. Description in Annex B already states that numbers are hexadecimal. Adding subscript will make the text very hard to read.
86	Sheehy, David B	5.4.1	The 'j' is missing from XTS-AES-blockDec()	Should read P <- XTS-AES-blockDec(Key, C, i, j)	Fixed in text
87	Sheehy, David B	5.4.2	The assignment should be to "P" and not "C".	Should read P <- XTS-AES-Dec(Key, C, i) the assignment should be to "P" and not "C"	Fixed in text
85	Sheehy, David B	D.4.3	Old term used in document	"XTC-AES-128" s/b "XTS-AES-128"	Fixed in text
2	Snively, Robert N	D.3	Cross-reference to clause C.1 appears to be incorrect.	Update the reference, probably to D.2.	Fixed in text

List of changes requested but not accepted

October 14, 2007

SUBJECT: Rejected comments on IEEE P1619

This document identifies the negative comments from the balloting group on IEEE P1619, draft number D17, that could not be accepted, together with the reasons why.

These were as follows:

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
11	Ball, Matthew V	6	The requirement that "An XTS-AES key shall not be associated with more than one key scope" is not cryptographically necessary and is overly restrictive. In particular, a RAID application might use the same key for several hard disks, with each hard disk using an independent key scope. This application would be disallowed by this requirement.	Consider changing this sentence as follows: "An XTS-KEY key shall only be associated with key scopes that do not have overlapping tweak values."	Too big a change at this stage of the standard.
4	Ball, Matthew V	3.1.1	The definition for 'key scope' is probably not sufficiently broad for inclusion into the IEEE Dictionary.	Consider replacing the definition of 'key scope' as follows: key scope: a set of data units protected by a particular key. NOTE - See 4.3.1 and Clause 6	We require the current definition
7	Ball, Matthew V	3.1.2	The term 'XTS-AES' is undefined	Add following definition (or similar): XTS-AES: The cryptographic mode of operation that uses the XTS transform with the AES block cipher.	There is no precise meaning to XTS outside of the XTS-AES context
12	Ball, Matthew V		page ii: We may consider adding a few more keywords	Consider adding these keywords: AES, XTS, hard drive, and XML	The existing keywords are sufficient

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
92	Cummings, Roger	4.3	The term "block" is seriously overloaded in this document. "Block-storage" appears in the title, 'physical block on the storage device" is included in the data unit definition, and then "logical block on the storage device" appears at the bottom of page 3 and at the top of page 9.	Is there a reason to use both physical and logical? I think not. Use only physical or logical but not both - perhaps use storage block. Create a definition of (data) block and include in 3.1 (and clearly state that any use of block with no adjectives means this definition).	Changing notation at this point will introduce more problems than it will fix.
91	Cummings, Roger	4.3	The rationale for a separate "special definitions" section is unclear.	Move the definition of data unit into 3.1	This was a request of IEEE editorial review
99	Cummings, Roger	6	What is the definition of "range"?	Use "LBA of the storage of that block on the media"?	Range is not necessarily related to LBA. As stated in the standard, the exact mapping from data units to underlying representation is beyond the scope.
98	Cummings, Roger	6	I'm not sure of the utility of stating that the tweak typically corresponds to the LBA. How does a user of the storage go about checking this requirement? What if different LBAs are seen by different users of the storage?	Delete reference to LBA, or add a flag in 7.4 that says the KeyScopeStart is based on the LBA?	KeyScope is not required to be based on LBA
97	Cummings, Roger	6	Does the last sentence need to be qualified by a scope? Within a single key scope? Within a single partition?	"An implementation compliant with this standard may or may not support multiple data unit sizes within a single key scope."	Scope is unrelated. The goal of the statement is to emphasize that the implementation supporting a single data unit size is still compliant.
102	Cummings, Roger	A	It's not clear why the references are split into Normative References and a Bibliography, and one of the references is duplicated.	Move the B1, B5, B12, B13 and B14 references as a minimum to Normative References.	The IEEE Style Manual requires a Normative References section for references that are necessary to implement the standard, and a Bibliography for references that are informative. The references B1, B5, B12, B13, and B14 don't appear necessary to implement the standard
25	Elliott, Robert C	5.1	(5.1 line 29) 9a s/b 9A		We switched to lower case

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
46	Elliott, Robert C	D.2	(D.2 page 34 line 2) After "ECB mode" add a cross refernce to NIST SP800-38A (where ECB is defined)		This is a general discussion and thus general understanding of ECB is sufficient, without the exact details in SP800-38A
45	Elliott, Robert C	D.2	(D.2 line 24-25) After "counter (CTR) mode or cipher 25 block chaining (CBC) mode" add a cross reference to NIST SP800-38A where these modes are defined		This is a general discussion and thus general understanding of ECB is sufficient, without the exact details in SP800-38A
57	Fenster, Yaacov	5.1	The text describes certain limits (shall not exceed 2^128-2). The text should include an explanation for the limits. I like the appendix with the discussion of the rationale, however I am looking for something a bit more down to earth for the person reading this text.		Calculations were decided to be out of scope
58	Fenster, Yaacov		Perhaps we should also supply a XSD for XML verification?		While an XSD may be useful, it is too late in this standard to add that now without a concrete proposal.
77	Griffin, Robert W	7.3	Is the cipherElement length correct in the XML example on page 14? The key is 512 bits. When wrapped using aes256-cbc, padding will extend the cipher text by 128 bits, and the pre-pended IV will add another 128 bits. Total cipher text length will then be 512 + 128 + 128 = 768 bits. When BASE-64 encoded, the encoded value will have approximately 128 characters. The example has approximately 150 characters.	Correct the calculation of cipherElement length.	Robert Griffin will investigate whether to keep his comment
83	Griffin, Robert W	D.5	The Meyer/Matyas text is no longer in print and may not be generally available to readers of the standard.	Cite alternative online or in-print resource for explanation of ciphertext stealing.	While it is true that this book is out-of-print, it is still easily available in second-hand markets.

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
1	Hars, Laszlo		Customers usually read only the Title, Abstract, Scope and Purpose of a standard to see if it fits to their (perceived) needs. In the case of the proposed P1619 standard they could get the wrong idea about its applicability and advantages. Not even the Introduction covers sufficiently these important considerations. A reader has to scroll down to Page 27 (Annex D) to get some information about the applicability of the standard. In this form of the introductory sections the standard causes marketing, sales, perceptional difficulties for many companies: Customers demand it implemented even where it is not applicable (e.g. nothing tells here that Tapes are better served with P1619.1). For most applications the standardized XTS-AES encryption mode is viewed as better than other specialized solutions, even though they can be more secure and/or better performing, less expensive. The proposed new language below tells immediately if a certain application is better served by P1619.1, by some access control mechanism or by other techniques. Without the necessary (minimal) changes we cannot support the current text.	New Purpose: (drop two imprecise words) This standard defines specific elements of an architecture for cryptographically protecting data stored in constant length blocks. Specification of such a mechanism provides a tool for implementation of secure and interoperable protection of data residing in storage. New Abstract: This standard specifies cryptographic transform and key archival methods for protection of stored data in devices, where 1. The encrypted data is freely accessible 2. The data layout has to remain unchanged 3. There are no other metadata available than the location of the data blocks 4. Data is accessed in fixed sized blocks, independently from each other.	The wording was discussed at length during multiple meetings and the current wording represents the reached consensus.
73	Holoman, Stuart		The word "terabytes"	Change "terabytes" to "tebibytes"	The statement does not explicitly refer to power of 2 size
72	Holoman, Stuart		IEEE STD 1541-2002 Clause 4.1: "exabyte"	Change "exabyte" to "exbibyte"	This is why the word "approximately" was added to text

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
71	Holoman, Stuart		IEEE STD 1541-2002 Clause 4.1: "petabyte"	Change "petabyte" to "pebibyte"	This is why the word "approximately" was added to text
70	Holoman, Stuart		IEEE STD 1541-2002 Clause 4.1 states that "The SI prefixes shall not be used to denote multiplication by powers of two." The reference to "terabyte" meaning 2**40 should reflect this standard.	Change "terabyte" to "tebibyte"	This is why the word "approximately" was added to text
69	Holoman, Stuart		In the The Authoritative Dictionary of IEEE Standards, Seventh Edition, the word "byte" is "usually associated with being eight (8) bits but not always. In some other IEEE standards the word "octet" often replaces "byte". Rather than change all references to "byte" in this document, perhaps adding a specific definition would suffice.	Add sub-clause "3.1.3 Byte: exactly eight (8) consecutive or contiguous bits."	From both common usage and examples from the standard, it is clear that a byte refers to 8 bits.
16	Karocki, Piotr	2	I think footnotes should be renumbered (reset count to 1 on each page).		Passed mandatory editorial review. Changing this now might create more issus.
14	Karocki, Piotr	4.3	Why definition of "data unit" is not in clause 3.1?		Specific requirement of editorial review comm

#	Name	Sub clause	Comment	Proposed Change	Resolution Detail
56	Lockhart, Robert A		The following statements should be clarified: The number of 128-bit blocks in the data unit shall not exceed 2^128-2. The number of 128-bit blocks should not exceed 2^20. Is the data unit a block on the media or the number of 128 bit segments on the media? Does the second sentence mean the number of 128-bit blocks on the media is not to exceed 2^20 (i.e. 16MB) or does it mean that a data block within a sector should not exceed 16MB? Please clarify this statement		Data unit is defined. The second sentence is "should" while the first one in "shall".
20	Noll, Landon C	5.1	I have found that the sentence "The number of 128-bit blocks should not exceed 2^20" frequently confuses people. The sentence does not state what should not exceed 2^20 128-bit blocks. Some read the previous sentence and speculate this might be a further restriction on the data unit size. Some have no idea what is being recommended.	Change the sentence to explicitly state what should not exceed 2^20 128-bit blocks.	The second sentence clarifies the first. While in the first one it is "shall", the second is "should".