References are to version D3d1

Page 334 line 1 Delete 11.4.5.1
Add new TLV on page 338
‘Data encryption setting’
‘This parameter indicates whether SAs are mandated for transport connections and for the Secondary Management connection’

Table 1:

Type	Length	Value	Scope
9	1	0x00, no SAs requires 0x01, SA mandated all other values reserved	REG-RSP

Rationale: We mandate the implementation of authentication and encryption so the old TLV is obsolete. But we need a TLV for turning encryption on/off

Page 326 line 5 Delete (uint16,uint16) or change it (preferred) to (uint8,uint8,uint8).
Page 326 line 14
change ‘TEK Key exchange and the KEK length.’ to ‘TEK exchange algorithm.’
line 44
Change title of table 121 to read ‘TEK Exchange Algorithm Identifyer’.
In table on line 51 change triple DES EDE,128 to read ‘3DES EDE with 128 bit key’

Page 327 in section 11.2.21
Change length field to be 3*n.
Change Value field to read:
A list of byte triplets identifying a collection of cryptographic suites. Each triplet represents a supported cryptographic suite. The first byte in the triplet identifies shall be the Data Encryption Algorithm Idenfier encoded as in <ref to table 119>. The second byte in the triplet shall be the Data Authentication Algorithm Idenfier encoded as in <ref to table 120>. The third byte shall be the TEK Exchange Algorithm Identifier encoded as in table <ref to table 121>.

Change table 122 to read ‘Allowed Cryptoggraphic Suite encodings’ Change the value column to read ‘0x010001’. Add to the Description to ‘...tion & 3DES,128

On page 328 line 27 change ‘pairing ...’ to read ‘Cryptoraphic suite employed within the SA.’

On page 174 starting line 35. Delete Entire paragraph beginning ‘This specification.....’
Rationale : Effort to allow AES in standard

On p. 174 line 55-56 change ‘and ...’ to read ‘and ‘strong symmetric algorithms to perform key exhanges between SS and BS.’

On p. 175 l.1 change ‘Privacy’ to ‘The PKM protocol’

p. 175 l. 42. Change sentence ‘A primary...’ to read ‘Each SS establishes a Primary Security association during the SS initialization process.’
Rationale: The old sentence is a relic from DOCSIS days.

Page 175 Replace paragraph starting line 48 with
‘A Security Association’s shared information shall include the Cryptographic Suite employed within the SA. The shared information may include Traffic Encryption Keys and Initialization Vectors. The exact content of the SA is dependent on the SA’s Cryptographic Suite.‘
Rationale: most of the paragraph is crap

Page 175 line 58, Change paragraph to read
‘Each SS with encryption enabled shall establish an exclusive Primary Security Association with its BS. The SAID of any SS’s Primary Security Association must be equal to the Basic CID of that SS.’

Insert subsectionunder SA reading
Cryptographic Suite
A Cryprographic Suite is the SA’s set of methods for data encryption, data authentication and TEK exchange. A Cryptographic Suite is specified as described in <11.2.20>.

Change ‘BS ensures’ page 176 line 5 to ‘BS shall ensure’.
Page 176 line 8 Delete entire paragraph.
Rationale: Section is fluff except for last sentence, but this is already covered by the authorization state machine.

Delete section 7.3.1.1.1 ‘Preliminary comment .....’
Rationale Standards do not need preliminary comments

Insert section ‘Mapping of Connections to Security Associations’ after SA section (7.1.3)
If a BS mandates the SS to apply SAs to all transport connections and to the Secondary Management connection the following rules for mapping the connections to SAs apply:
1. All transport connections shall be mapped to an existing SA.
2. All uplink transport connections shall be mapped to the Primary SA.
3. Downlink transport connections may be mapped to any SA.
4. The Secondary Management Connection shall be mapped to the Primary SA.
Note that the TEK exchange of the
The actual mapping can be acheived either by including the SAID of an existing SA in the DSA-XXX messages together with the CID or by performing dynamic SA mapping as described in section <ref 7.4>. No explicit mapping of Secondary Management connection to the Primary SA is required.

Rationale: Rules needed for CID and SA mapping. They were vaguely stated in on of the deleted sections.

Page 176 Delete Entire section 7.2 Operational overview together with subsection 7.2 Operational overview
Rationale: The same information is given in 7.3.

Page 177 Delete 7.3.1 ‘State models’

Rationale: It is empty
Promote 7.3.1.1 to 7.3.1
Page 177 lines 21 Delete sentence ‘The state models....’
Rationale ‘ Difference between specification and implementation should be clear at this level
Page 177 before line 24 insert heading H3 ‘SS authorization and AK exchange overview’

Page 177 delete lines 34-38

Page 60 line 49 delete row with SS Identification
page 60 line58 delete entire paragraph

Pages 318 line 20-319 line 65
Delete it all. Rehash Type values for remaining TLVs

page 177 Delet lines 57-60, on line 61 delete rest of item starting from ‘binding’

On page 178 line 15 change 4-bit to 2-bit.

Move page 179 lines 13-26 to before page 178 line 32

Before page 178 line 33 insert new heading H3 ‘ TEK exchange overview’

Page 178 lines 37- 45 Delete starting from ‘A key request includes...’ to end of line 45.

Page 178 lines 48-55 Delete starting from ‘This key...’ to end of line 55.

On page 180 promote Sections 7.3.1.1.2 and 7.2.1.2
Page 180 Delete lines 33-36 as they provide no essential information

Page 198 line 23-24 Delete ‘(EDE...)’ and ‘(TEK...)

Page 198 line 58/59 replace ‘use an SS’s active AK(s) ‘ to ‘use a HMAC_KEY_U derived from the SS’s active AK(s)’
Page 198 line 61 change ‘authenticated with’ to authenticated with a HMAC_KEY_U derived from’

Page 199 line 1. Replace ‘an active AK ’ with ‘a HMAC_KEY_D derived from an ative AK’
Page 199 line 1- 2. Replave end of sentence ‘,and when encrypting the TEK in Key Replies’ with ‘The BS shall use a KEK derived from an active AKwhen encrypting the TEK in the Key Reply messages.’
page 199 line 5 before ‘;’ add ‘to derive the KEK and the HMAC_KEY_D’
page 199 line 6 before ‘.’ add ‘to derive the KEK and the HMAC_KEY_D’

Page 199 line 40 change ‘both primary and multicast’ to ‘all SAs’

Page 199 line 47-48 delete ‘(the TEK....)’

Page 203 line 6 Change Heading 7.6.1 to read ‘Data encryption with DES’

Page 203 line 8 Change ‘Privacy ‘ to ‘Data on connections associated with SAs with the Data Encryption Algorithm Identifier in the Cryptographic Suite equal to 0x01’

Page 203 line 12 Delete sentence
Page 203 line 3. Add sentence after the existing one ‘All SS and BS implementations must support the method of packet data encryption defined in < ref to 7.6.1>, encryption of the TEK as specified in <ref to 7.6.2> and message digest calculation as specified in <ref to 7.6.3>.

Rationale: Removing the optionality of ‘privacy’ implemetation alleviates interoperability issues.

Page 203 lines 14-16 The CBC IV shall be calculated as follows:
In the dowlink the CBC shall be initialized with the 64 least significant bits of the sum modulo 2^64 of the IV parameter included in the keying information and the contents of the PHY sycnronization field in the DL-MAP message during the time between the arrival of this DL-MAP message and the the arrival of the next one.
In the uplink the CBC shall be initialized with the 64 least significant bits of the sum modulo 2^64 of the IV parameter included in the keying information and the contents of the PHY sycnronization field in last DL-MAP message received prior to the UL-MAP message in which the uplink transmission were commanded.

Reasoning: The IV could be just the the IV+the frame number modulo 2^64 but as the PHY synch field in PHY dependent this defintion is about as good as I could come up with. Please come up with more elegant wording! For the uplink the case with no frames causes side effects when it comes to the wording.

Page 255 Replace Figure 131 with

Table 2: PHY Synchronization Field

Syntax	Size	Notes
PHY Synchronization Field( ){		
Frame Duration Code	8 bits	
Frame Number	24 bits	
}		

Page 203 Line 33 add ‘with 3DES’ to title

Page 203 Add before line 36 This method of encrypting the TEK shall be used for SA with the TEK Exchange Algorithm Identifier in the Cryptographic Suite equal to 0x01.

Page 203 line 58. Add sentences ‘ The downlink authentication key HMAC_KEY_D and shall be used for authenticating messages in the downlink direction.The uplink authentication key HMAC_KEY_U and shall be used for authenticating messages in the uplink direction.

Page 204 Insert heading H4 on before line 9 ‘DES Keys’

Page 204 Move lines 18-19 before line 15

Page 204 Add heading H4 before the text on line 15 ‘ The keying..’ reading ‘3DES KEKs’

Page 204 Replace line 21- 45/46 with
< begin replacement>
The 3DES KEK used to encrypt the TEK is derived from a common AK. The KEK shall be derived as follows:

KEK=Truncate(SHA(K_PAD_KEK | AK),128)
K_PAD_KEK=0x53 repeated 64 times i.e. a 512 bit string.

Truncate(*x*,*n*) denotes the result of truncating *x* to its left-most *n* bits.
SHA(*x*|*y*) denotes the result of applying the SHA-1 function to the concatenated bit strings *x* and *y*.
The key material of 3DES consists of two distinct DES keys. The 64 most significant bits of the KEK shall be used in the encrypt operation. The 64 least significant bits shall be used in the de-crypt operation.

<H4> ‘HMAC authentication keys’
The HMAC authentication keys are derived as follows:
HMAC_KEY_D=SHA(H_PAD_D|AK)
HMAC_KEY_U=SHA(H_PAD_U|AK).

with
H_PAD_D=0x3A repeated 64 times
and
H_PAD_U=0x5C repeated 64 times.

<end replacement>

Page 204 line 54 Question to editors “ what does F4 stand for ? I guess not hurricane strength”

Page 205 line 7 change ‘Privacy’ to ‘the protocol’
Rationale: the word privacy is no good.