High-bandwith Digital Content Protection System Revision 1.0 Erratum

Revision 19 March 2001

Notice

This document is an erratum for the previously-published specification:

High-bandwidth Digital Content Protection System, Revision 1.0, Intel Corporation, February 17, 2000.

On page 23, the first paragraph of Section 2.7 has been changed as highlighted below:

> The transmitter signals the receiver to begin the third part of the authentication protocol through the previously reserved control signal CTL3 in the DVI interface. This is done with a single high-going pulse, during the vertical blanking interval, of sufficient width that it may be distinguished from bit errors on the channel or any effects due to resynchronization events in the receiver.

On page 9, the second paragraph has been changed as highlighted below:

> Authentication fails if the topology maximums are exceeded. All video transmitters check to see if the KSV of any attached device is found in the current revocation list, and, if present, the authentication fails. The video transmitter verifies the integrity of the current revocation list by checking the signature of the system renewability message (SRM) using the Digital Content Protection LLC public key L[1]. Failure of this integrity check constitutes an authentication failure.

On page 9, the last paragraph has been changed as highlighted below:

> The video transmitter enables data encryption when the first part of the authentication protocol successfully completes.

On page 10, the paragraph below Figure 2-3 is updated to further clarify the behavior of index, *i*, for the values K_i, M_i, and R_i. This index value equals 1 for the first frame after any successful authentication (or re-authentication) of which CTL3 is asserted. Furthermore, this index does not advance for frames of which CTL3 is not asserted (i.e. when encryption is disabled). The following is the paragraph with the changes highlighted:

> The third part of the authentication protocol, illustrated in Figure 2-3, occurs during the vertical blanking interval preceding the frame for which it applies. Each of the two devices calculates new cipher initialization values, K_i and M_i, and a third value R_i. The index, *i*, represents the encrypted frame number, starting with the value of one for the first video frame for which content protection is enabled after any completion of the first and (if applicable) second parts of the authentication protocol. K_i is a 56-bit key used to initialize the HDCP cipher for encryption or decryption of the RGB information for the video frame. M_i is a new 64-bit initialization value for the HDCP cipher. R_i is a 16-bit value used for link integrity verification, and is updated for every 128th frame, starting with the 128th frame. The video transmitter verifies this value against its own calculations to insure that the video receiver is still able to correctly decrypt the information. This verification is made at the rate of once every two seconds, plus or minus one-half second. It is required that the R_i' read operation complete within 250 milliseconds from the time that it is initiated by the video transmitter. Failure for any reason causes the video transmitter to consider the DVI link to be unauthenticated.

On page 11, additional clarification has been added for changes from State A0 to State A1. The following is the paragraph with the changes highlighted:

> **Transition A0:A1.** A trigger event initiates the authentication protocol. Trigger events include hot plug detection of an attached video receiver, completion of certain phases of the operating system startup, or a software request.

On page 12, the description of State A3 has been changed as highlighted below:

> **State A3 Validate Receiver.** The video transmitter reads R_0' from the video receiver and compares it with the corresponding R_0 produced by the video transmitter during the computations of State A2. If R_0 is equal to R_0', then data encryption is immediately enabled. The video transmitter must allow the video receiver up to 100 ms to make R_0' available from the time that *Aksv* is written. The video transmitter also checks the current revocation list for the video receiver's KSV *Bksv*. If *Bksv* is in the revocation list, then the video receiver is considered to have

failed the authentication. Note: checking the revocation list for *Bksv* may begin as soon as the *Bksv* has been read in State A1, asynchronously to the other portions of the protocol, but is must complete prior to the transition into the authenticated state (State A4).

On page 13, an additional paragraph has been added after all of the state and transition descriptions. The following is the additional paragraph with the additions highlighted:

> Note that in some implementations, the trip from the point in State A3 where encryption is enabled to State A4 may be sufficiently long to miss one or more verification timer events. For improved usability, such implementations may alternatively handle the link integrity check process (i.e. State A5) asynchronously from the rest of the state diagram. In such cases, the transition into State A5 may occur from any state for which encryption is currently enabled. Also, the transition from State A5 returns to the appropriate state to allow for undisrupted operation.

On page 20, in the first paragraph of this page, has been changed as highlighted below:

> The values that must be exchanged between the video transmitter and the video receiver are communicated over the I^2C serial interface of the DVI interface. The video receiver or video repeater must present a logical device on the I^2C bus for teach T.M.D.S. link that it supports. No equivalent interface to video transmitters is specified. The eight-bit I^2C device address (including the read/write bit, "x") for the primary link is 0111010x binary, or 0x74 in the usual hexadecimal representation of I^2C device addresses where the read/write bit is set to zero. The device address for the secondary link is 0x76. Table 2-2 and Table 2-3 specify the address space for these devices, which act only as slaves on the I^2C bus. Multi-byte values are stored in little-endian format.

On page 23, the paragraph above Figure 2-10 has been changed as highlighted below:

> In order to minimize the number of bits that must be transferred for the link integrity check, a second read format must be supported by all video receivers and by video transmitters that do not implement a hardware I^2C master. This access, shown in Figure 2-10, has an implicit offset address equal to 0x08, the starting location for *Ri'*. The short read format may be uniquely differentiated from combined reads by tracking STOP conditions (P) on the bus. Short reads must be supported with auto-incrementing addresses.

On page 21, the Bksv register definition has been changed as highlighted below:

> Video receiver KSV. This value may be used to determine that the video receiver is HDCP capable. Valid KSVs contain 20 ones and 20 zeros, a characteristic that must be verified by the video transmitter hardware before encryption is enabled. This value must be available any time the receiver's HDCP hardware is ready to operate.

On page 21, the *Bcaps* register definition is incomplete. Bits 3, 2, 1, and 0 should be specified as reserved, with read value zero.

On page 21 and 22, the implementation-specific debug registers are expanded to 32 bytes and placed at offset 0xE0-0xFF. The following are updated Tables 2-2 and 2-3 with the changes highlighted:

Offset (hex)	Name	Size in Bytes	Rd/ Wr	Function
0x00	*Bksv*	5	Rd	Video receiver KSV. This value must always be available for reading, and may be used to determine that the video receiver is HDCP capable. Valid KSVs contain 20 ones and 20 zeros, a characteristic that must be verified by video transmitter hardware before encryption is enabled.
0x05	Rsvd	3	Rd	All bytes read as 0x00
0x08	*Ri'*	2	Rd	Link verification response. Updated every 128th frame. It is recommended that graphics systems protect against errors in the I^2C transmission by re-reading this value when unexpected values are received. This value must be available at all times between updates. R_0' must be available a maximum of 100 ms after *Aksv* is received. Subsequent R_i' values must be available a maximum of 128 pixel clocks following the assertion of CTL3.
0x0A	Rsvd	6	Rd	All bytes read as 0x00
0x10	*Aksv*	5	Wr	Video transmitter KSV. Writes to this multi-byte value are written least significant byte first. The final write to 0x14 triggers the authentication sequence in the display device.
0x15	Rsvd	3	Rd	All bytes read as 0x00
0x18	*An*	8	Wr	Session random number. This multi-byte value must be written by the graphics system before the KSV is written.
0x20	*V*	20	Rd	Twenty-byte SHA–1 hash value used in the second part of the authentication protocol for video repeaters.
0x34	Rsvd	12	Rd	All bytes read as 0x00
0x40	*Bcaps*	1	Rd	Bit 7: Reserved. Read as zero. Bit 6: REPEATER, Video repeater capability. When set to one, this device supports downstream DVI connections as permitted by the Digital Content Protection LLC license. Bit 5: READY, KSV FIFO ready. When set to one, the device has built the list of attached KSVs and appended the verification value *V*. This value is always zero during the computation of *V*. Bit 4: FAST. When set to one, this device supports 400 KHz transfers. When zero, 100 KHz is the maximum transfer rate supported.
0x41	*Bstatus*	2	Rd	Refer to Table 2–4 for definitions.
0x43	KSV FIFO	1	Rd	Key selection vector FIFO. Used to pull KSVs from devices with downstream DVI outputs. Must be read in a single, auto-incrementing access. All bytes read as 0x00 for video receivers (REPEATER == 0).
0x44	Rsvd	124	Rd	All bytes read as 0x00
0XC0	dbg	64	Rd/ Wr	Implementation-specific debug registers. Confidential values must not be exposed through these registers.

Table 2-2. Primary Link HDCP Port (I^2C device address 0x74)

Offset (hex)	Name	Size (Bytes)	Rd/Wr	Function
0x00	*Bksv*	5	Rd	Video receiver KSV. See primary link comments. This value must match the value of Bksv for the primary link.
0x05	Rsvd	3	Rd	All bytes read as 0x00
0x08	*Ri'*	2	Rd	Link verification response. See primary link comments. This value will differ from the value of *Ri*' for the primary link.
0x0A	Rsvd	6	Rd	All bytes read as 0x00
0x10	*Aksv*	5	Wr	Video transmitter KSV. See primary link comments. This value must be programmed to the same value of *Aksv* for the primary link.
0x15	Rsvd	3	Rd	All bytes read as 0x00
0x18	*An*	8	Wr	Session random number. See primary link comments. This value must **differ** from the programmed value of *An* for the primary link.
0x20	Rsvd	160	Rd	All bytes read as 0x00
0xC0	dbg	64	Rd/Wr	Implementation-specific debug registers. Confidential values must not be exposed through these registers.

Table 2-3. Secondary Link HDCP Port (I^2C device address 0x76)

On page 41, Table A-3 has been changed as highlighted below:

	A1 – B1	A1 – B2	A2 – B1	A2 – B2
Km	5309c7d22fcecc	f6aee46089c923	4afe34dbec1205	a423d78b8676a7
REPEATER || An	034271c130c070403	0445e62a53ad10fe5	083bec2bb01c66e07	00351f7175406a74d
Ks	54294b7c040e35	4e60d941d0e8b1	2c9bef71df792e	1963deb799ee82
M_0	a02bc815e73d001c	e7d28b9b2f46c49d	8e1e91f6d8ae4c25	d05d8c26378a126e
R_0	8ae0	fb65	3435	4fd5
K_1	d692b7ee1d40e8	e46f51311a959a	f3e27849d067c1	65f793e160ec27
M_1	1dbf44e50f523e56	445b5c6eebf657ff	23d89127a5ee6c26	68be984885aafef7
Line 1, Pixel 1	R 59 G c0 B 3e	R 56 G bf B 8a	R 11 G 07 B d2	R b8 G 2c B 9c
Line 1, Pixel 2	R 9e G e5 B fe	R 2c G 26 B 03	R b1 G 8f B 7f	R 9b G 34 B e3
Line 1, Pixel 3	R 9a G f9 B 19	R 88 G 43 B dc	R 3c G fb B 8c	R 1c G fa B d7
Line 1, Pixel 4	R 5b G 5d B 6c	R 1d G db B bd	R a3 G 97 B 0c	R 00 G A0 B 08
Line 1, Pixel 5	R 55 G dc B de	R e6 G 32 B 13	R 38 G 94 B 3e	R ce G c3 B f4
Line 1, Pixel 6	R e5 G 87 B 63	R 36 G 34 B 24	R ac G 84 B da	R f4 G 36 B 27
Line 1, Pixel 7	R be G fc B c7	R 48 G 82 B 8f	R b8 G a4 B 73	R b6 G 36 B f7
Line 1, Pixel 8	R a1 G b5 B 65	R 99 G b9 B db	R 2f G c5 B c0	R 24 G bd B 8b
Horizontal Blank Re-Key				
Line 2, Pixel 1	R 12 G 6b B 14	R 9c G ac B 7b	R 6c G 64 B c7	R 73 G 9f B 2e
Line 2, Pixel 2	R 06 G 4a B 73	R 40 G 11 B d0	R ba G 05 B 8d	R f6 G 1e B 16
Line 2, Pixel 3	R f8 G bb B 15	R aa G 3c B e6	R 62 G 17 B ff	R e2 G 8c B 59
Line 2, Pixel 4	R cc G e6 B 21	R e6 G e9 B ac	R f1 G e5 B df	R d9 G 8a B 86
Line 2, Pixel 5	R 87 G 95 B 78	R 7a G d5 B 2e	R c2 G e6 B 92	R c5 G eb B 96
Line 2, Pixel 6	R d2 G 03 B f7	R 94 G 1f B 35	R 47 G a4 B 94	R c0 G b3 B ce
Line 2, Pixel 7	R 62 G 81 B 44	R a7 G 85 B 64	R 59 G b7 B a1	R eb G 26 B f3
Line 2, Pixel 8	R 80 G d8 B 75	R f7 G 45 B 16	R 9d G 96 B ea	R f4 G 9e B e1

Table A-3. Sample Authentication and Encryption Values (REPEATER = 0)

On page 42, Table A-4 has been changed as highlighted below:

	A1 – B1	A1 – B2	A2 – B1	A2 – B2
Km	5309c7d22fcecc	f6aee46089c923	4afe34dbec1205	a423d78b8676a7
REPEATER || An	134271c130c070403	1445e62a53ad10fe5	183bec2bb01c66e07	10351f7175406a74d
Ks	bc607b21d48e97	b7894f1754caaa	fe3717c12f3bb1	aac4147081a2d0
M_0	372d3dce38bbe78f	43d609c682c956e1	536dee1e44a58bf4	38b57ad3cdd1b266
R_0	6485	3f68	dd9b	7930
K_1	98b281e1876a9a	ffbfea4bc7fd2c	a1ec276b2ddaf0	0f0b83888e3209
M_1	016f9561e001f80d	2a067368042fa1aa	b365f8813c45db0b	06471e358f601ce4
Line 1, Pixel 1	R 33 G 4e B 55	R bc G 9c B a4	R 4a G c7 B d3	R c2 G c8 B 84
Line 1, Pixel 2	R d2 G 37 B 4e	R 43 G 19 B df	R 30 G a7 B ec	R 2f G 7c B 68
Line 1, Pixel 3	R 0e G 22 B f5	R b1 G e0 B 12	R 2d G 6e B 36	R 90 G 0b B e5
Line 1, Pixel 4	R c1 G 31 B 8f	R 27 G d0 B 5a	R e1 G 75 B b6	R 9e G de B 54
Line 1, Pixel 5	R dc G a1 B a7	R d8 G aa B 3d	R 94 G ff B fb	R 78 G cd B 8c
Line 1, Pixel 6	R 27 G e7 B c3	R 3f G 2a B 64	R 11 G aa B c1	R 38 G a5 B b8
Line 1, Pixel 7	R 56 G 3e B c9	R 2e G 00 B 0a	R 5c G 71 B 66	R 32 G ff B 1e
Line 1, Pixel 8	R 10 G dc B 2f	R f2 G 47 B 63	R be G 33 B 6f	R e4 G d9 B 0c
Horizontal Blank Re-Key				
Line 2, Pixel 1	R 73 G 03 B 22	R e4 G 97 B f1	R 0b G a7 B ec	R 62 G 0f B 61
Line 2, Pixel 2	R 69 G 01 B 36	R df G 15 B 0e	R 4f G 10 B 1e	R 33 G 73 B 52
Line 2, Pixel 3	R 3d G 27 B 53	R 2f G 44 B 7b	R fe G 16 b 16	R cd G 96 B fd
Line 2, Pixel 4	R fe G 41 B 50	R 0c G 9b B ae	R 52 G e6 B 35	R 53 G ea B d5
Line 2, Pixel 5	R a8 G 18 B 8d	R 93 G db B da	R db G 8d B b7	R 33 G a9 B 31
Line 2, Pixel 6	R 1a G 02 B 91	R a7 G f9 B 01	R 18 G f0 B d9	R cc G 34 B 86
Line 2, Pixel 7	R 8c G 29 B ce	R 1a G 39 B 9a	R f5 G 9a B 63	R 6e G e0 B bb
Line 2, Pixel 8	R 89 G cd B bf	R 4b G 54 B 00	R d4 G ac B aa	R d2 G fc B 4b

Table A-4. Sample Authentication and Encryption Values (REPEATER = 1)

On page 54, Table A-16 has been changed as highlighted below:

Sequence	Kx	Ky	Kz	Bx	By	Bz	Output
Load	0x089c923	0xf6aee46	0x0000000	0xad10fe5	0x5e62a53	0x0000144	
1	0x000ace8	0x2bbe222	0xa84ba32	0xf8ee8f0	0x5d68545	0x649180e	0xb24463
2	0xbe2db4d	0xced43e8	0x6cf4c5d	0x5e52253	0x8d0daa0	0xfbde86b	0x1fa15f
3	0x59aaa16	0x420acae	0x948ddf1	0xe59bdcc	0xd7951b1	0x092c03c	0x787a32
4	0x6716e27	0xc71eabf	0x728216a	0x84926be	0xcaad80c	0xec3a8a5	0xf27cef
5	0x2b8be74	0xc7b7cd8	0x1896efd	0x7d66727	0x5c571f8	0x8069a85	0x88a3ad
6	0x417f923	0xf719e90	0xd5c1459	0x76bb30d	0x5333af4	0xa18c913	0xd01f1b
7	0x6c1faa9	0xf7175fd	0x50bb276	0xd91bfa4	0x1a7d561	0x456e67c	0xdc6f7c
8	0x90a1447	0xad4dd26	0x59afdb6	0xa59b390	0x1794cd7	0x3453dff	0x9276f6
…	…	…	…	…	…	…	…
41	0x456a8de	0x218a73d	0xefe8143	0x4705e66	0xa0ab473	0x77d249d	0x40cba0
42	0x5bb75c0	0x9e32509	0xcd4d66f	0x4d4a0e2	0x02b580f	0x2b49a78	0x1a3445
43	0x692b31d	0x40c7b06	0xeb692c8	0x0d36661	0x3a20c13	0x8cf85c3	0x02f684
44	0x4ac7e44	0x584dad4	0x2606dca	0xb39da54	0xc47d057	0xdca5d5d	0xf7ef88
45	0x995c381	0xe782e99	0x500545a	0x0710574	0x54607a7	0x42e8a1e	0xf1a5cc
46	0x2a39ef6	0xb3509f9	0xbd26dfe	0x284e17f	0x439d9e4	0x4dd18ce	0x23402b
47	0xe937d30	0x7910780	0x03575d7	0xdf9ad7d	0x3c7791a	0x6ddd61f	0x95dc64
48	0xb9af224	0x04c8a5f	0x49c96b1	0x754caaa	0xb7894f1	0xfcce020	0xcdaa1d
Load	0x754caaa	0xb7894f1	0xfcce020	0xad10fe5	0x5e62a53	0x0000144	
1	0x1cfb5dd	0xce2b088	0x2eec032	0x93dabe7	0x5d68545	0x649180e	0x4bbc20
2	0xfa0338f	0xdd9d11d	0x26e8f45	0x91d34c5	0x8d0daa0	0xa42f29f	0x0c1351
3	0x11ffc1e	0xd8fc06f	0x846a9c2	0x575d169	0x5f1d290	0xd8d250e	0x14f5d7
4	0x004ea3a	0xb8ae70e	0x00f25c3	0x807911a	0x442cc5a	0x1f6d6e5	0xa0c9b8
5	0xffd1f46	0x63fcef9	0x59e2583	0x0965cff	0x912f65a	0x9fad256	0x28067a
6	0x86aa27f	0x1bfc986	0x7559055	0xd307ffb	0x11af6d1	0x4d14ec4	0xa73184
7	0xe438d81	0x2f72c2a	0x065bebb	0x2c48a34	0x00ed16b	0xb2430a6	0x62d500
8	0xdc88b2a	0x1b83e3e	0xc719f35	0x3530afd	0x2435827	0x62edd40	0xe4b982
…	…	…	…	…	…	…	…
49	0x6e1ecc7	0x2126ced	0xa7ac884	0x0a7c511	0x278da73	0x3c52476	0x2afbb7
50	0x9b7983d	0xd61a93c	0x560de7f	0x47467e0	0xf5c27f1	0x56257fb	0xbf090b
51	0x1848c4a	0x6946104	0x97436c5	0x0ac81df	0xac47979	0x84c004f	0x6fffc7
52	0xb9ff03e	0xfafd4f8	0x030217e	0xb570368	0x4a63c44	0x8c9e6ff	0x8f5af2
53	0x031fbfa	0x20c4236	0x7181797	0xa99940c	0x810cdc7	0x6eb5e1a	0xda43d6
54	0xc67ef5d	0xdee5ece	0xb3296c2	0xd4f4edd	0xe33bd04	0xcbee012	0xc409c6
55	0xa8244d2	0x3aef4b0	0x5c7f3ad	0x7eb9d86	0xa72a66e	0x5527b8c	0x3f82c9
56	0xe3a9d07	0xce2e311	0xa20cd64	0xe15b166	0x74e9482	0x6a048e0	0x6856e1

Table A-16. Block Module States During A1 - B2 Authentication (REPEATER = 1)