SMPTE REGISTERED DISCLOSURE DOCUMENT

Cinelink 2 Specification

The attached document is a Registered Disclosure Document prepared by the proponent identified below. It has been examined by the appropriate SMPTE Technology Committee and is believed to contain adequate information to satisfy the objectives defined in the Scope, and to be technically consistent.

This document is NOT a Standard, Recommended Practice or Engineering Guideline, and does NOT imply a finding or representation of the Society.

Errors in this document should be reported to the proponent identified below, with a copy to eng@smpte.org.

All other inquiries in respect of this document, including inquiries as to intellectual property requirements that may be attached to use of the disclosed technology, should be addressed to the proponent identified below.

Proponent contact information:

Reiner Doetzkies
Texas Instruments
6550 Chase Oaks Blvd.
Plano, TX 75023

Email reiner@ti.com

Approved April 12, 2010

Table of Contents

Page

Introduction

Cinelink 2 is a protocol used to protect copyrighted images between a playback server and DLP Cinema® projector system. The images are protected on a local video data link via an AES key stream generator operating in counter mode.

1 Scope

This document provides details of the implementation of the Cinelink 2 Link Encryption from Texas Instruments.

2 Conformance Notation

Normative text is text that describes elements of the design that are indispensable or contains the conformance language keywords: "shall", "should", or "may". Informative text is text that is potentially helpful to the user, but not indispensable, and can be removed, changed, or added editorially without affecting interoperability. Informative text does not contain any conformance keywords.

All text in this document is, by default, normative, except: the Introduction, any section explicitly labeled as "Informative" or individual paragraphs that start with "Note:"

The keywords "shall" and "shall not" indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.

The keywords, "should" and "should not" indicate that, among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.

The keywords "may" and "need not" indicate courses of action permissible within the limits of the document.

The keyword "reserved" indicates a provision that is not defined at this time, shall not be used, and may be defined in the future. The keyword "forbidden" indicates "reserved" and in addition indicates that the provision will never be defined in the future.

A conformant implementation according to this document is one that includes all mandatory provisions ("shall") and, if implemented, all recommended provisions ("should") as described. A conformant implementation need not implement optional provisions ("may") and need not implement them as described.

Unless otherwise specified, the order of precedence of the types of normative information in this document shall be as follows: Normative prose shall be the authoritative definition; Tables shall be next; followed by formal languages; then figures; and then any other language forms.

3 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this registered disclosure document. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this recommended practice are encouraged to investigate the possibility of applying the most recent edition of the standards indicated below.

SMPTE 291M-2006, Television — Ancillary Data Packet and Space Formatting

SMPTE 292-2008**,** 1.5 Gb/s Signal/Data Serial Interface

SMPTE 372-2009, Dual Link 1.5 Gb/s Digital Interface for 1920 × 1080 and 2048 × 1080 Picture Formats

AES, FIPS PUB 197, Advanced Encryption Standard. U.S. Department of Commerce/National Institute of Standards and Technology. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

4 Glossary of Terms and Acronyms

292: SMPTE interface specification for HD-SDI (used interchangeably with HD-SDI)

AES: Advanced Encryption Standard

DLP: Digital Light Processing

DVI: Digital Visual Interface

HD-SDI: High Definition Serial Data Interface (used interchangeably with 292)

LE keys: Link Encryption keys

TLS: Transport Layer Security

5 System Description

A system block diagram of a typical Cinelink 2 system is given in Figure 1.

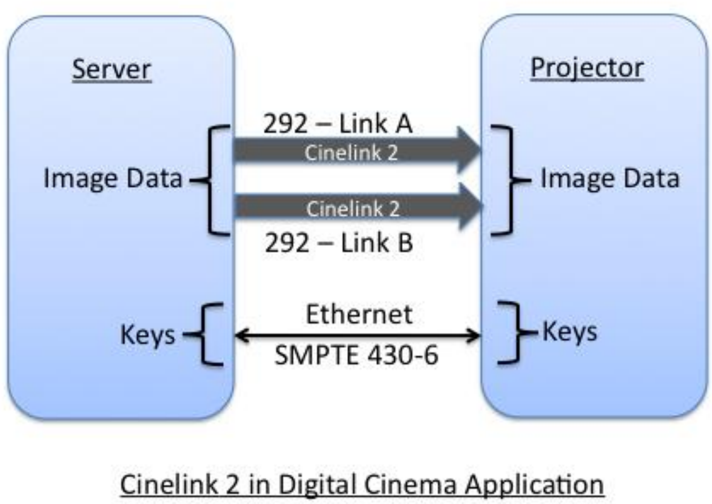

Figure 1 – Cinelink 2 Typical Application

A Cinelink 2 system consists of an encryption engine in the server, a channel, and a decryption engine in the projector. The encryption engine is depicted in Figure 2.

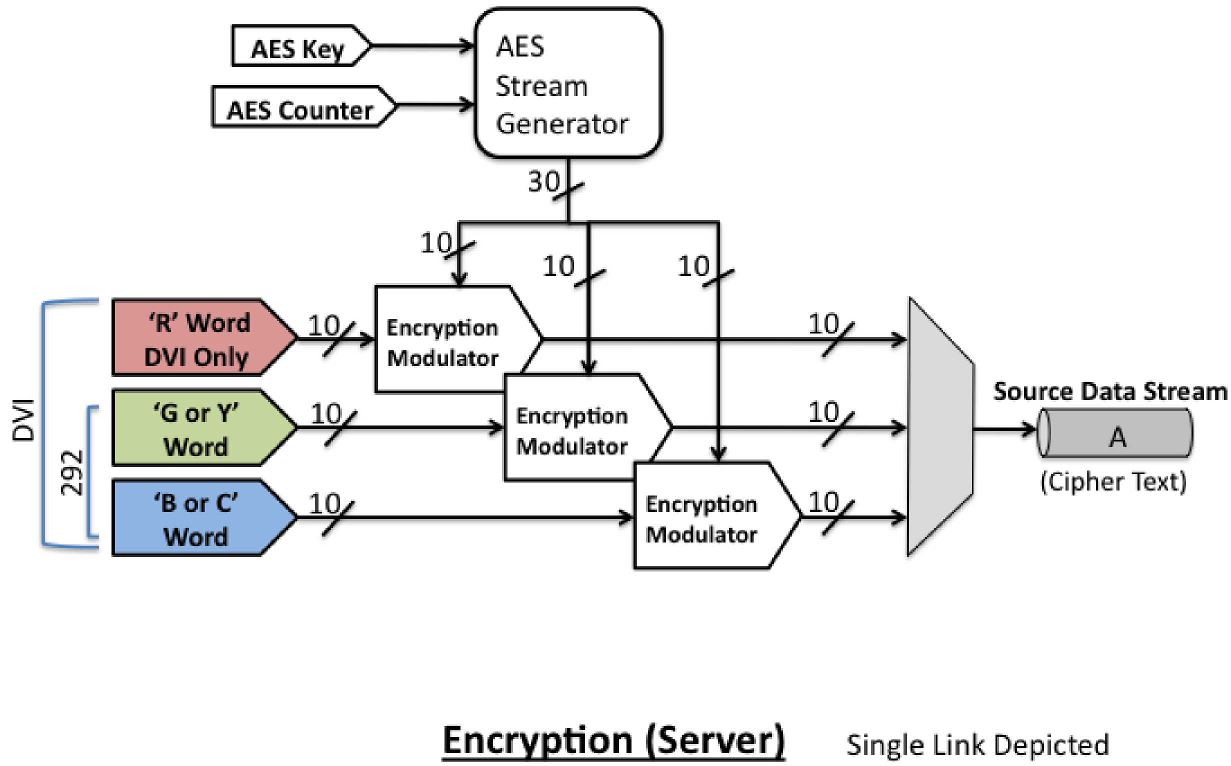

Figure 2 – Encryption Engine

The basic structure of the encryption and decryption engine is symmetric. The decryption engine is depicted in Figure 3.

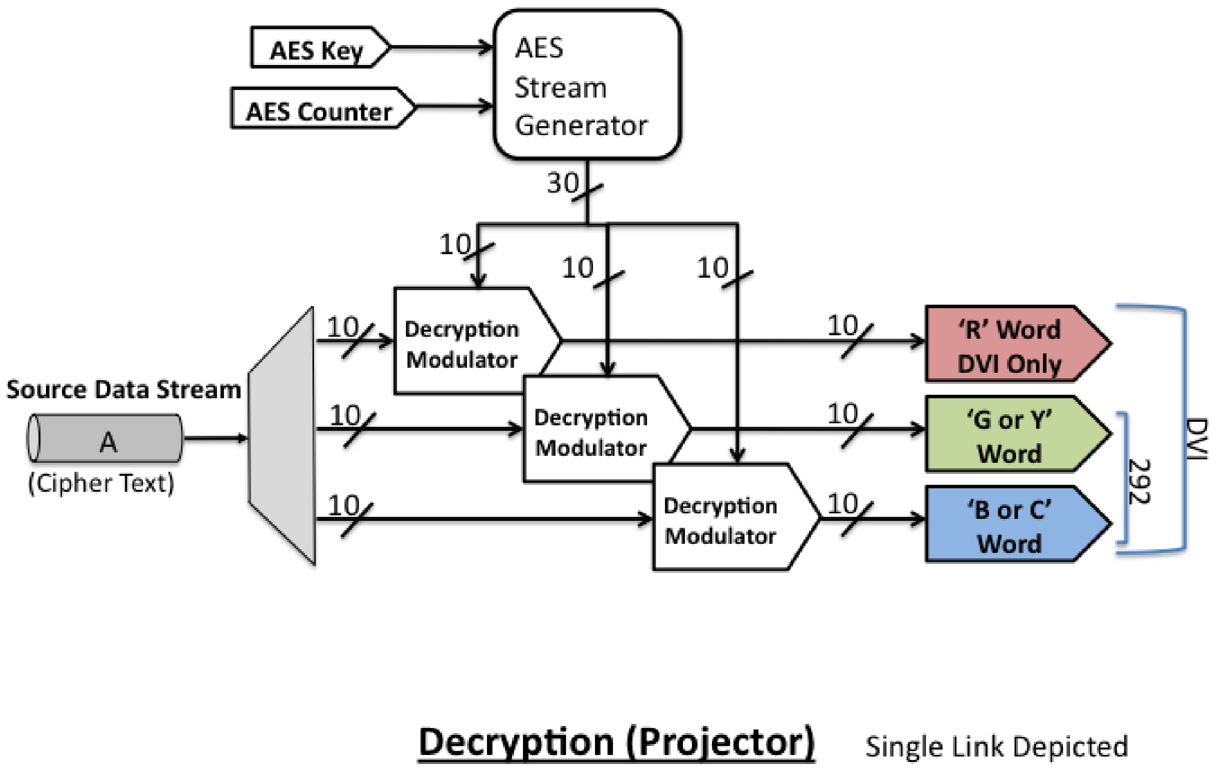

Figure 3 – Decryption Engine

The encryption/decryption engine structure consists of an AES stream generator block and three modulator/demodulators. The AES stream generator creates two or three (depending on the mode) 10-bit streams of random numbers at the input pixel rate based on an AES core operating in counter mode with an input of the 128-bit AES key and the 128-bit AES counter. The AES random number streams then modulate/demodulate the incoming input pixels to encrypt/decrypt them.

A HD-SDI link has a set of 8 prohibited codes not for use other than sync words. These hex values are 000h, 001h, 002h, 003h, 3FCh, 3FDh, 3FEh, and 3FFh. Thus, the encryption engine must not generate any of these invalid codes. The structure of the engine allows for invalid codes to be detected and discarded in the AES random number stream before modulating/demodulating the incoming data. The presence and discarding of invalid codes will require the AES core to operate 0.8% faster than the source data bit stream.

For dual-link HD-SDI, each channel is encrypted/decrypted independently.

For DVI source data streams, invalid code detection and discarding is not required and will be disabled.

A secured TLS Ethernet connection is used for key exchange between the server and projector. The details of this connection are beyond the scope of this specification.

All SMPTE image formats defined by the normative references are supported by Cinelink 2.

5.1 AES Counter Definition

Table 1 defines the AES counter. Note that the least significant bits of the counter are the cipher block count.

The definition of the AES counter is given Table 1.

Table 1 – AES Counter

TI AES COUNTER DEFINITION		
AES INPUT BIT	AES INPUT NAME	DESCRIPTION
[127:126]	LINK_NUMBER_[1:0]	0=SINGLE LINK OR LINK A OF DUAL LINK, 1= LINK B OF DUAL LINK, 2-3= RESERVED
[125:120]	RESERVED	0=DEFAULT
[119:56]	LE_ATTRIBUTE_DATA_[63:0]	ATTRIBUTE DATA EXTRACTED FROM LE KEY
[55:32]	FRAME_COUNT_[23:0]	NUMBER OF FRAMES FROM THE PREVIOUS KEY CHANGE, RESET TO ZERO AT KEY CHANGE
[31:16]	LINE_COUNT_[15:0]	ACTIVE VIDEO LINE NUMBER, RESET TO ZERO FOR THE FIRST LINE OF EVERY FRAME
[15:0]	CIPHER_BLOCK_COUNT_[15:0]	NUMBER OF CIPHER BLOCKS, RESET TO ZERO FOR THE FIRST BLOCK OF EVERY LINE

5.2 AES Stream to Plaintext/Ciphertext Mapping Definition

The AES core generates a 128-bit output for each AES key and AES counter input. These 128-bit output blocks are called cipher blocks. The conversion of these 128-bit cipher blocks into 10-bit random number streams in the presence of invalid codes is illustrated for 10-bit data words in the following Figure 4. In the AES stream invalid codes are defined to be 3FFh, 3FEh, 3FDh, 3FCh, 3FBh, 3FAh, 3F9h, and 3F8h. When an invalid code in the AES stream is detected, it is simply discarded and replaced with the next code in the stream. Note that 8 bits from each cipher block are not used.

Figure 4 illustrates the AES to data word mapping for SMPTE 292 source data.

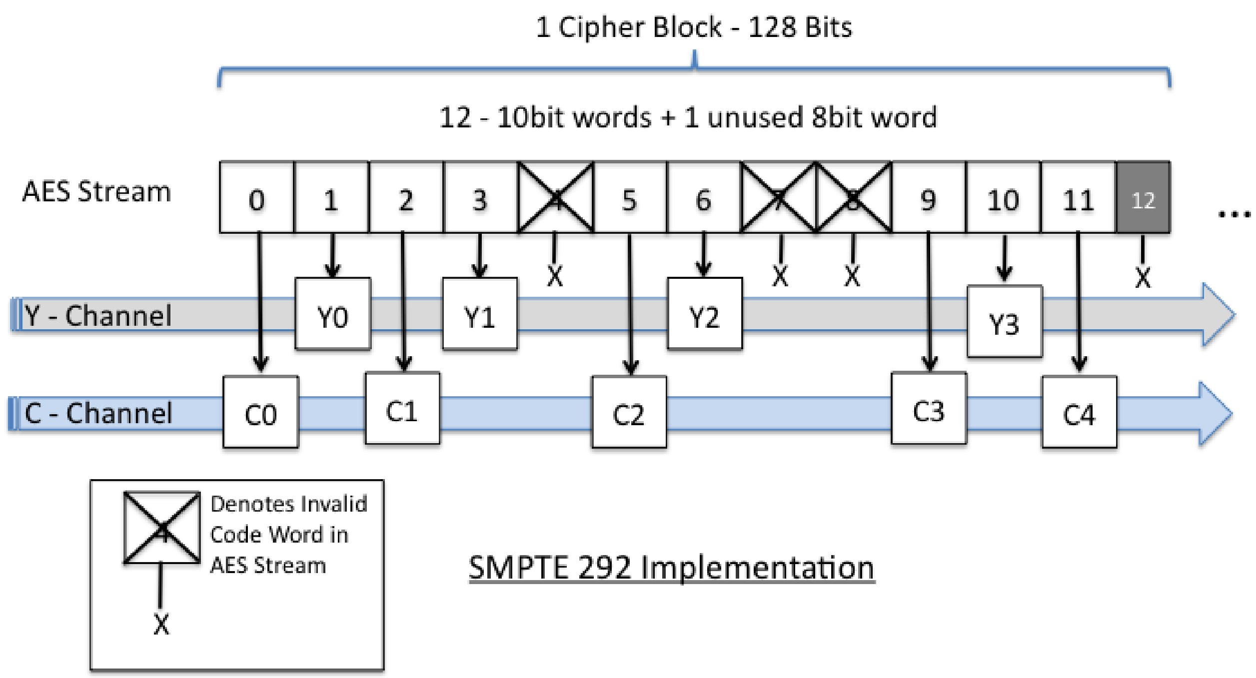

Figure 4 – AES to data word mapping for 292

Figure 5 illustrates the AES to data word mapping for DVI source data.

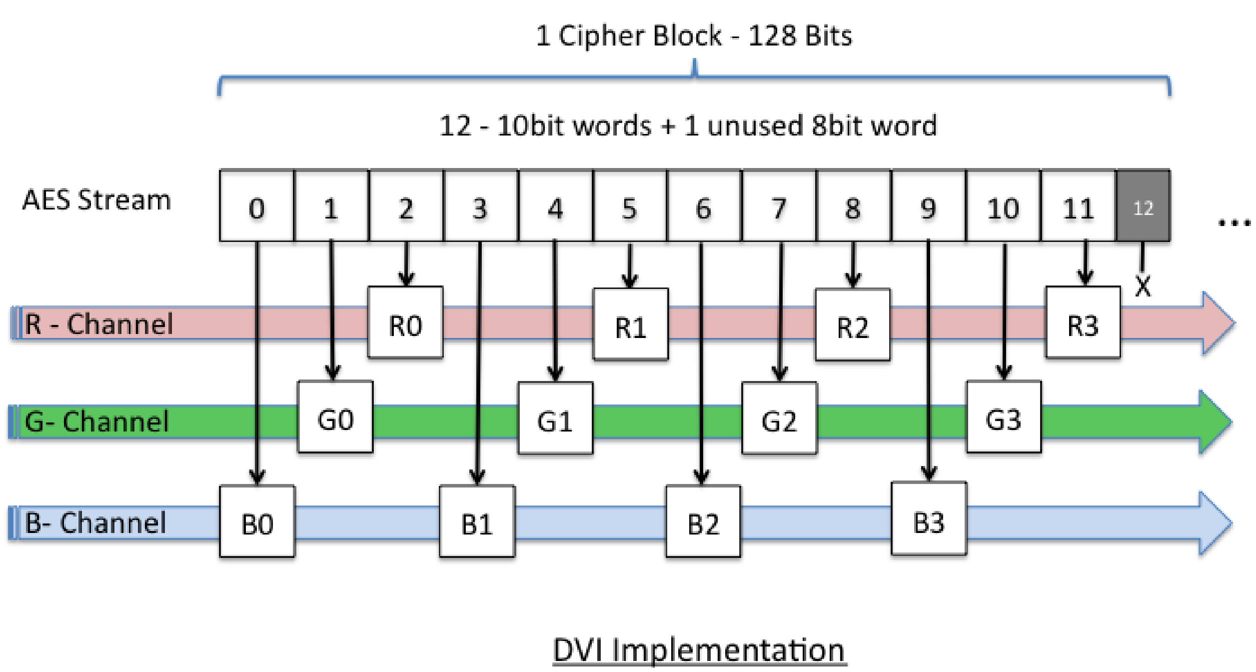

Figure 5 – DVI Mapping

The encryption/decryption engine is inherently a 10-bit engine and encrypts and decrypts in 10-bit words. To encrypt/decrypt 8-bit DVI video, the data must be mapped into the 10-bit words of the engine.

The exact mapping between the AES cipher blocks and the incoming pixel data for DVI video is as follows in Table 2.

Table 2 – DVI Image Mapping

AES INPUT BIT	8 BIT 4:4:4 DVI Video	
	PIX #	BIT
0	0	B_0
1	0	B_1
2	0	B_2
3	0	B_3
4	0	B_4
5	0	B_5
6	0	B_6
7	0	B_7
8	0	NOT USED
9	0	NOT USED
10	0	G_0
11	0	G_1
12	0	G_2
13	0	G_3
14	0	G_4
15	0	G_5
16	0	G_6
17	0	G_7
18	0	NOT USED
19	0	NOT USED
20	0	R_0
21	0	R_1
22	0	R_2
23	0	R_3
24	0	R_4
25	0	R_5
26	0	R_6
27	0	R_7
28	0	NOT USED
29	0	NOT USED
30	1	B_0
31	1	B_1
32	1	B_2
33	1	B_3
34	1	B_4
35	1	B_5
36	1	B_6
37	1	B_7
38	1	NOT USED
39	1	NOT USED
40	1	G_0
41	1	G_1
42	1	G_2
43	1	G_3
44	1	G_4

AES INPUT BIT	8 BIT 4:4:4 DVI Video	
	PIX #	BIT
45	1	G_5
46	1	G_6
47	1	G_7
48	1	NOT USED
49	1	NOT USED
50	1	R_0
51	1	R_1
52	1	R_2
53	1	R_3
54	1	R_4
55	1	R_5
56	1	R_6
57	1	R_7
58	1	NOT USED
59	1	NOT USED
60	2	B_0
61	2	B_1
62	2	B_2
63	2	B_3
64	2	B_4
65	2	B_5
66	2	B_6
67	2	B_7
68	2	NOT USED
69	2	NOT USED
70	2	G_0
71	2	G_1
72	2	G_2
73	2	G_3
74	2	G_4
75	2	G_5
76	2	G_6
77	2	G_7
78	2	NOT USED
79	2	NOT USED
80	2	R_0
81	2	R_1
82	2	R_2
83	2	R_3
84	2	R_4
85	2	R_5
86	2	R_6
87	2	R_7
88	2	NOT USED
89	2	NOT USED
90	3	B_0
91	3	B_1
92	3	B_2
93	3	B_3
94	3	B_4
95	3	B_5
96	3	B_6
97	3	B_7
98	3	NOT USED
99	3	NOT USED

AES INPUT BIT	8 BIT 4:4:4 DVI Video	
	PIX #	BIT
100	3	G_0
101	3	G_1
102	3	G_2
103	3	G_3
104	3	G_4
105	3	G_5
106	3	G_6
107	3	G_7
108	3	NOT USED
109	3	NOT USED
110	3	R_0
111	3	R_1
112	3	R_2
113	3	R_3
114	3	R_4
115	3	R_5
116	3	R_6
117	3	R_7
118	3	NOT USED
119	3	NOT USED
120	NOT USED	NOT USED
121	NOT USED	NOT USED
122	NOT USED	NOT USED
123	NOT USED	NOT USED
124	NOT USED	NOT USED
125	NOT USED	NOT USED
126	NOT USED	NOT USED
127	NOT USED	NOT USED

5.3 Link Encryption Key Message Definition

The Link Encryption Key (LE key) is a 128-bit pseudo-random number used as the key for AES stream generator operating in counter mode. The same LE key used for encryption is required for decryption.

The Link Encryption Attribute Data (LE attribute data) is a 64-bit parameter of the AES counter. It is required to use a random number for this parameter that changes when the LE key changes.

Each LE key will be identified by a 12-bit key ID. A LE Key ID of zero is defined as no encryption.

Note: SMPTE 430-6 ASM defines the LE key ID parameters of the LEKeyLoadMessage as a 32-bit word, however only a 12-bit word is supported by the process defined in this document. The upper 20 bits of the LE Key ID will therefore be ignored. Also, note that a LE Key ID of zero is not permitted by this document; thus, an error response shall be returned if a LE Key ID value of zero is sent via ASM.

All LE keys and LE attribute data for a movie may be sent before the start of the movie, or each individual LE key and LE attribute data may be sent before its corresponding movie clip. It is required that the LE key and LE attribute data be sent a minimum of 1 second before use.

The LE key and LE attribute data are sent from the server to the projector in a Link Encryption Key Message (LE key message) via the Ethernet connection. See SMPTE 430-6 ASM.

The current LE key ID as well as the next LE key ID for each video clip will be sent from the server to the projector via metadata .

The projector must be able to change LE keys, as identified by a new LE key ID within metadata, at any video frame boundary.

All LE keys and LE attribute data stored in the projector are stored in volatile memory. In the event of loss of power to the projector, the LE keys and LE attribute data must be re-loaded into the projector.

The LE Key data received from the server is mapped to the AES Key register in Table 3:

Table 3 – LE Key Data Mapping

ASM Message (Byte order received)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
AES Key	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3

The LE Attribute Data received from the server is mapped to the AES Counter register in Table 4:

Table 4 – LE Attribute Data Mapping

ASM Message (Byte order received)	0	1	2	3	4	5	6	7
AES Counter	4	5	5	7	0	1	2	3

5.4 Link Encryption Metadata Definition

The link encryption metadata is used to transfer unencrypted time critical data from the server to the projector.

The items required for the LE metadata are given in Table 5.

Table 5 – LE Metadata

LE KEY METADATA		
ITEM	DESCRIPTION	SIZE
NEXT_LE_KEY_ID	LE_KEY_ID OF THE NEXT KEY	12 BITS
CURRENT_LE_KEY_ID	LE_KEY_ID OF THE CURRENT KEY	12 BITS
CURRENT_FRAME_COUNT	NUMBER OF FRAMES FROM THE PREVIOUS KEY CHANGE, RESET TO ZERO AT KEY CHANGE	24 BITS
VERSION	CURRENTLY SET TO ZERO	6 BITS
LINK_NUMBER	0=SINGLE LINK OR LINK A OF DUAL LINK, 1= LINK B OF DUAL LINK, 2-3= RESERVED	2 BITS
AES_SYNC_WORD	THE VALID 10-BIT AES WORD DIRECTLY FOLLOWING THE AES WORD USED TO ENCRYPT THE LAST ACTIVE PIXEL OF THE LAST ACTIVE LINE OF THE PREVIOUS FRAME. THIS WORD IS USED BY THE PROJECTOR TO VERIFY SYNCRONIZATION OF THE SERVER AND PROJECTOR AES RANDOM NUMBER GENERATORS.	10 BITS

This data is used to execute LE key changes and to supply the projector with frame count and link number components of the AES counter.

This data is also used to verify the synchronization between the server and projector AES random number generators by comparing the AES_SYNC_WORD from the server (metadata) and the projector.

In a dual-link mode, there is no requirement on LE key change timing between the two links. In fact, each link may have a different key.

The projector shall generate the following status information relating to LE metadata.

- A “current LE key” error if the current LE key is not present in the projector memory.
- A “next LE key” error if the next LE key is not present in the projector memory.
- The LE key ID of the current LE key.
- The LE key ID of the next LE key.
- The type of Link Encryption being requested via metadata (none, Cinelink, or Cinelink 2)
- A AES synchronization error if the AES_SYNC_WORD from the metadata does not match the AES_SYNC_WORD generated in the projector

5.4.1 SMPTE 292 Link Encryption Metadata Definition

For a SMPTE 292 link, the LE metadata shall be based on the SMPTE 291M standard. The LE metadata shall be mapped into the user data area of the ancillary data packet. This ancillary data packet shall use the Type 2 data identification and is defined in Table 6.

Table 6 – Ancillary Data Packet

SMPTE 292 ANCILLARY DATA PACKET STRUCTURE FOR LE METADATA	
NAME	VALUE
ANCILLARY DATA FLAG	000H, 3FFH, 3FFH
DATA IDENTIFICATION	50H
SECONDARY DATA IDENTIFICATION	51H
DATA COUNT	0AH
USER DATA	LE METADATA
CHECKSUM	—

The LE metadata ancillary data packet shall be mapped into the vertical ancillary data area of the Y channel of HD-SDI and of the G and A channels of Dual link HD-SDI at least one full horizontal line prior to the first active video line.

The LE metadata is mapped into the ancillary data packet user data area as defined in the Table 7.

Table 7 – LE Metadata Packet

<table>
<tr><th colspan="11">SMPTE 292 ANCILLARY DATA PACKET USER DATA AREA DEFINITION</th></tr>
<tr><th>BITS</th><th>BIT 9</th><th>BIT 8</th><th>BIT 7</th><th>BIT 6</th><th>BIT 5</th><th>BIT 4</th><th>BIT 3</th><th>BIT 2</th><th>BIT 1</th><th>BIT 0</th></tr>
<tr><td>WORD 1</td><td rowspan="10">COMPLIMENT OF BIT 8</td><td rowspan="10">EVEN PARITY OF BIT 0 – BIT 7</td><td colspan="8">NEXT_LE_KEY_ID (7 : 0)</td></tr>
<tr><td>WORD 2</td><td>RSV</td><td>RSV</td><td>RSV</td><td>RSV</td><td colspan="4">NEXT_LE_KEY_ID (11 : 8)</td></tr>
<tr><td>WORD 3</td><td colspan="8">CURRENT_LE_KEY_ID (7 : 0)</td></tr>
<tr><td>WORD 4</td><td>RSV</td><td>RSV</td><td>RSV</td><td>RSV</td><td colspan="4">CURRENT_LE_KEY_ID (11 : 8)</td></tr>
<tr><td>WORD 5</td><td colspan="8">CURRENT_FRAME_COUNT (7 : 0)</td></tr>
<tr><td>WORD 6</td><td colspan="8">CURRENT_FRAME_COUNT (15 : 8)</td></tr>
<tr><td>WORD 7</td><td colspan="8">CURRENT_FRAME_COUNT (23 : 16)</td></tr>
<tr><td>WORD 8</td><td colspan="6">VERSION (5 : 0)</td><td colspan="2">LINK_# (1 : 0)</td></tr>
<tr><td>WORD 9</td><td colspan="8">AES_SYNC_WORD (7:0)</td></tr>
<tr><td>WORD 10</td><td>RSV</td><td>RSV</td><td>RSV</td><td>RSV</td><td>RSV</td><td colspan="3">AES_SYNC_WORD (9:8)</td></tr>
</table>

5.4.2 DVI Link Encryption Metadata Definition

For a DVI link, the LE metadata must be located in the active video area. The LE metadata shall be placed in an ancillary data packet. This ancillary data packet is located in a false active video line which is inserted as the first active video line of every frame. The false line should be black (R, G, B data should be zero) except for the metadata. If the projector detects the presence of an ancillary data packet on the first active video line, the projector shall capture the ancillary data packet and then discard the rest of the line. The server must not encrypt the ancillary data packet. The DVI ancillary data packet structure is defined in Table 8.

Table 8 – DVI Ancillary Data Packet

DVI ANCILLARY DATA PACKET STRUCTURE FOR LE METADATA	
NAME	VALUE
ANCILLARY DATA FLAG	000H, 3FFH, 3FFH, 000H, 3FFH, 3FFH
DATA IDENTIFICATION	50H
SECONDARY DATA IDENTIFICATION	51H
DATA COUNT	0AH
USER DATA	LE METADATA
CHECKSUM	—

The checksum is calculated in the same manner as for the SMPTE 292 metadata as defined by SMPTE 291M standard.

Table 9 defines how the LE metadata ancillary data packet is mapped into the DVI red and green channels.

Table 9 – DVI LE Metadata Packet Mapping

DVI ANCILLARY DATA PACKET BIT MAPPING										
METADATA	BIT 9	BIT 8	BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
DVI BUS	RED1	RED0	GRN7	GRN6	GRN5	GRN4	GRN3	GRN2	GRN1	GRN0

The LE metadata is mapped into the ancillary data packet user data area as defined in Table 10.

Table 10 – DVI Ancillary Data Packet, User Data

DVI ANCILLARY DATA PACKET USER DATA AREA DEFINITION										
BITS	BIT 9	BIT 8	BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
WORD 1	COMPLIMENT OF BIT 8	EVEN PARITY OF BIT 0 – BIT 7	NEXT_LE_KEY_ID (7 : 0)							
WORD 2			RSV	RSV	RSV	RSV	NEXT_LE_KEY_ID (11 : 8)			
WORD 3			CURRENT_LE_KEY_ID (7 : 0)							
WORD 4			RSV	RSV	RSV	RSV	CURRENT_LE_KEY_ID (11 : 8)			
WORD 5			CURRENT_FRAME_COUNT (7 : 0)							
WORD 6			CURRENT_FRAME_COUNT (15 : 8)							
WORD 7			CURRENT_FRAME_COUNT (23 : 16)							
WORD 8			VERSION (5 : 0)						LINK_# (1 : 0)	
WORD 9			AES_SYNC_WORD (7:0)							
WORD 10			RSV	RSV	RSV	RSV	RSV	AES_SYNC_WORD (9:8)		

5.4.3 Link Encryption Key Change Timing Requirements

The timing requirements for LE key change timing are defined in Table 11.

Table 11 – LE Key Timing

LE KEY CHANGE TIMING REQUIREMENTS	
REQUIREMENT NAME	VALUE
MIN DELAY BETWEEN LE KEY CHANGES	1 SECOND
MAX PROCESSING TIME FOR LE KEY MESSAGES	30 SECONDS

Note that the “max processing time for LE key messages” parameter defines the time required for the projector to decrypt the message and make the LE key available for use decrypting pixel data. The stated times are based upon the successful acknowledgement of the key received message.

5.5 Encryption Modulator and Decryption Demodulator Definition

The encryption modulator shall encrypt the plaintext using the AES key stream.

The SMPTE 292 modulator is defined such that given plaintext in the range of 4 to 1019 and AES key stream in the range of 0 to 1015 the modulator will generate encrypted ciphertext in the range of 4 to 1019. Thus only valid codes will be transmitted down the channel. The decryption modulator shall decrypt the ciphertext using the AES key stream.

The DVI modulator is used with full range plaintext and AES key stream data.

The same function both encrypts and decrypts.

The SMPTE 292 modulator/demodulator is defined below.

Encryption: Ci = 292_LUT (Mi + Ei)

Decryption: Mi = 292_LUT (Ci + Ei)

The DVI modulator/demodulator is defined below.

Encryption: Ci = DVI_LUT (Mi + Ei)

Decryption: Mi = DVI_LUT (Ci + Ei)

Mi: Input data of the encryption modulator and output data of the encryption demodulator

Ci: Encrypted data

Ei: Pseudo random number from the stream converter

292_LUT: The 11-bit in/10-bit out LUT mapping defined in Appendix A.

DVI_LUT: The 11-bit in/10-bit out LUT mapping defined in Appendix A.

Annex A LUT Definition (Normative)

Defined by the equation below:

$$Y= [((917 – X) – 4) \text{ MOD } (1016)] + 4$$

Y = Output Data
X = Input Data of Range (0 – 2047)

For a table of the data see Annex B.

Annex B LUT Data (Normative)

[See Annex B in the zip file]

Annex C Bibliography (Informative)

SMPTE 430-6-2008, D-Cinema Operations — Auditorium Security Messages for Intra-Theater Communications