Media Identifier
Management Technology
Specification

Intel Corporation

International Business Machines Corporation

Panasonic Corporation

Toshiba Corporation

Revision 0.85 Preliminary Release

September 27, 2010

NOT FOR LICENSE OR IMPLEMENTATION AT THIS TIME

This page is intentionally left blank.

Preface

Notice

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. IBM, Intel, Panasonic, and Toshiba disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

This document is an intermediate draft and is subject to change without notice. Adopters and other users of this specification are cautioned that products based on it may not be interoperable with the final version or subsequent versions thereof.

Intellectual Property

Implementation of this specification requires a license from the 4C Entity, LLC.

Contact Information

Please address inquiries, feedback, and licensing requests to the 4C Entity, LLC:

- Licensing inquiries and requests should be addressed to 4C-Services@4CEntity.com.
- Feedback on this specification should be addressed to 4C-Services@4CEntity.com.

The URL for the 4C Entity, LLC web site is http://www.4CEntity.com.

This page is intentionally left blank.

Table of Contents

List of Figures

This page is intentionally left blank.

List of Tables

This page is intentionally left blank.

Chapter 1
Introduction

1. Introduction

1.1 Purpose and Scope

The *Content Protection for eXtended Media Specification* (CPXM) defines a robust and renewable method for protecting content stored on a number of physical media types. CPXM technology is an enhanced version of Content Protection for Recordable Media (CPRM) technology. The specification is organized into several "books". The *CPXM Specification: Introduction and Common Cryptographic Elements* book provides a brief overview of CPXM, and defines cryptographic procedures that are common among its different uses. The media specific book provides further details of how to adapt CPXM technology onto a particular media. The application specific book provides additional details for using CPXM technology to protect content stored on the media.

CPXM technology consists of the following books, under the general title *CPXM Specification:*

- *Introduction and Common Cryptographic Elements*
- *Media specific* book
- *Application specific* book

This document describes an additional feature of CPXM, which is Media Identifier Management Technology (MIMT). MIMT is designed to ensure global uniqueness of the Media Identifier and to prevent duplication of the Media Identifier. This additional feature works with CPXM technology and is common to each application.

The use of this specification and access to the intellectual property and cryptographic materials required to implement it will be the subject of an addendum license to the CPXM License Agreement. A license authority referred to as the 4C Entity, LLC is responsible for establishing and administering the content protection system based in part on this specification.

This document is an abridged version and for evaluation purposes only.

1.2 Document Organization

This document is organized as follows:

- Chapter 1 provides an introduction.
- Chapter 2 lists abbreviations and acronyms used in this document.
- Chapter 3 describes adaptation to SD Memory Card.

1.3 References

This book shall be used in conjunction with the following publications. When the publications are superceded by an approved revision, the revision shall apply.

4C Entity, LLC, *CPXM License Agreement* (Unpublished)

4C Entity, LLC, *MIMT addendum to the CPXM License Agreement* (Unpublished)

4C Entity, LLC, *CPXM Specification: Introduction and Common Cryptographic Elements, Revision 0.85*

4C Entity, LLC, *CPXM Specification: SD Memory Card Book Common Part, Revision 0.85*

4C Entity, LLC, *CPRM Specification: SD Memory Card Book Common Part, Revision 0.961*

4C Entity, LLC, *Content Protection System Architecture White Paper, Revision 0.81*

SD Group, *SD Memory Card Specifications, Part 3: Security Specification, Version 3.10*

1.4 Future Directions

The current document describes MIMT for SD Memory Card. In future revisions, MIMT elements for other media may also be specified.

1.5 Notation

Except where specifically noted otherwise, this document uses the same notations and conventions for numerical values, operations, and bit/byte ordering as described in the *CPXM Specification: Introduction and Common Cryptographic Elements* book.

Chapter 2
Abbreviations and Acronyms

2. Alphabetical List of Abbreviations and Acronyms

The following abbreviations and acronyms are used in this document:

4C	4 Companies (IBM, Intel, Panasonic, and Toshiba)
AKE	Authentication and Key Exchange
CBC	Cipher Block Chaining
CPRM	Content Protection for Recordable Media
CPXM	Content Protection for eXtended Media
DNN	Device Node Number
ECB	Electronic Codebook
ID	Identifier
ID_{cm}	Controller Manufacturer Identifier
ID_{mck}	Media Controller Key Identifier
ID_{media}	Media Identifier
LLC	Limited Liability Company
lsb	Least Significant Bit
K_{app}	Application Key
K_{auth}	Authentication Key
K_m^0	Media Key
K_{mc}	Media Controller Key
K_{mcu}	Media Controller Unique Key
K_{mu}	Media Unique Key
MIMT	Media Identifier Management Technology
MKB	Media Key Block
msb	Most Significant Bit
N_{mcu}	Media Controller Unique Number
N_s	Secret Number
SD	Secure Digital
TBD	To Be Determined
XOR	Exclusive-OR

This page is intentionally left blank.

Chapter 3
SD Memory Card Adaptation

3. SD Memory Card Adaptation

3.1 Introduction

This chapter describes how to adapt MIMT to SD Memory Cards to prevent duplication of the Media Identifier.

3.2 Roles

An SD Memory Card consists of a Media Controller and a memory. The Media Controller is designed to read and write data in the memory and to exchange data with the Host. To produce an SD Memory Card, the following roles are involved. In some cases, multiple roles may be performed by a single manufacturer.

- Controller Manufacturer: A Controller Manufacturer provides a Media Controller to the Card Assembler. The Controller Manufacturer shall have the MIMT license from the 4C Entity, LLC.
- Memory Manufacturer: A Memory Manufacturer provides non-volatile memory for the SD Memory Card. The Memory Manufacturer is not required to have the MIMT license.
- Card Assembler: A Card Assembler assembles an SD Memory Card from a Media Controller provided by a Controller Manufacturer and memory provided by a Memory Manufacturer. The Card Assembler shall have the MIMT license from the 4C Entity, LLC.

The overview of relationships among those three roles and the 4C Entity, LLC are described in Figure 3-1.

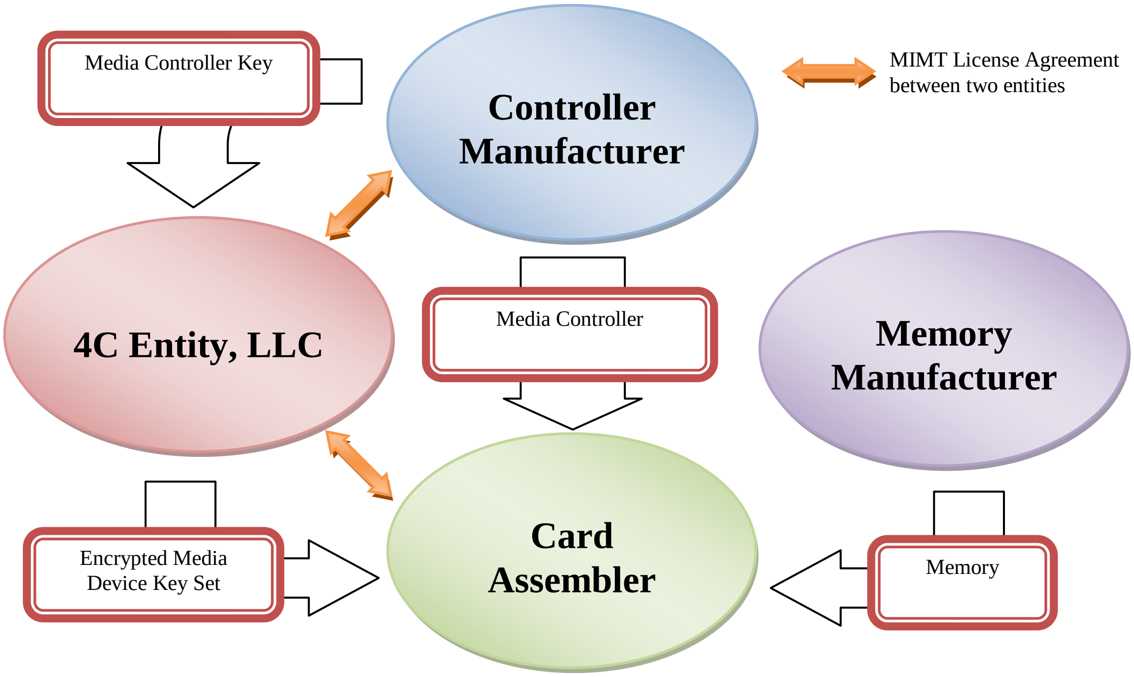


Figure 3-1 Relationship among three roles and 4C Entity, LLC

3.3 Components

This section shows components for the MIMT specification. The following components are stored in the Media Controller:

- Media Controller Key Identifier
- Media Controller Unique Number
- Media Controller Key
- Media Controller Unique Key

In addition to the values above, the Media Controller stores the following values in the Media Controller or in the memory:

- Media Device Key Set
- Authentication Key
- Random Number Key
- Device Node Number

The Media Controller Key Identifier and Media Controller Unique Number include one Controller Manufacturer ID given by the 4C Entity, LLC. Details are described in Sections of this document with those names. Table 3-1 describes treatment of these components.

Table 3-1 Treatment of MIMT components

Component	Location where stored	Assigner/Generator	Required secrecy and integrity level
Media Controller Key Identifier (16 bytes)	Media Controller (Recommended)	Controller Manufacturer	None
Media Controller Unique Number (6 bytes)	Media Controller	Controller Manufacturer	Integrity
Media Controller Key (16 bytes)	Media Controller	Controller Manufacturer	Highly Confidential
Media Controller Unique Key (16 bytes)	Media Controller	Controller Manufacturer	Highly Confidential
Media Device Key Set	Memory	4C Entity, LLC	Highly Confidential
Device Node Number (5 bytes)	Memory	4C Entity, LLC	None
Authentication Key (16 bytes)	Memory	Host Devices	Highly Confidential
Random Number Key (16 bytes)	Memory	Card Manufacturer or 4C Entity, LLC	Highly Confidential
Controller Manufacturer ID (1 byte)	Media Controller (Media Controller Key Identifier and Media Controller Unique Number)	4C Entity, LLC	Integrity

The components above are stored in either the Media Controller or the memory. The area in which CPXM components are stored is described in Section 3.3 of *CPXM Specification: SD Memory Card Book Common Part*. Mapping of the CPXM components to the MIMT compliant SD Memory Card is depicted in Figure 3-2. Each component is stored in either the Media Controller or the memory except the Media Identifier. The Device Node Number of the Media Identifier is stored in the memory. On the other hand, the Media Controller Unique Number of the Media Identifier is stored in the Media Controller. 16 Authentication Keys, the Random Number Key and the Media Device Key Set are encrypted with the Media Controller Unique Key and stored.

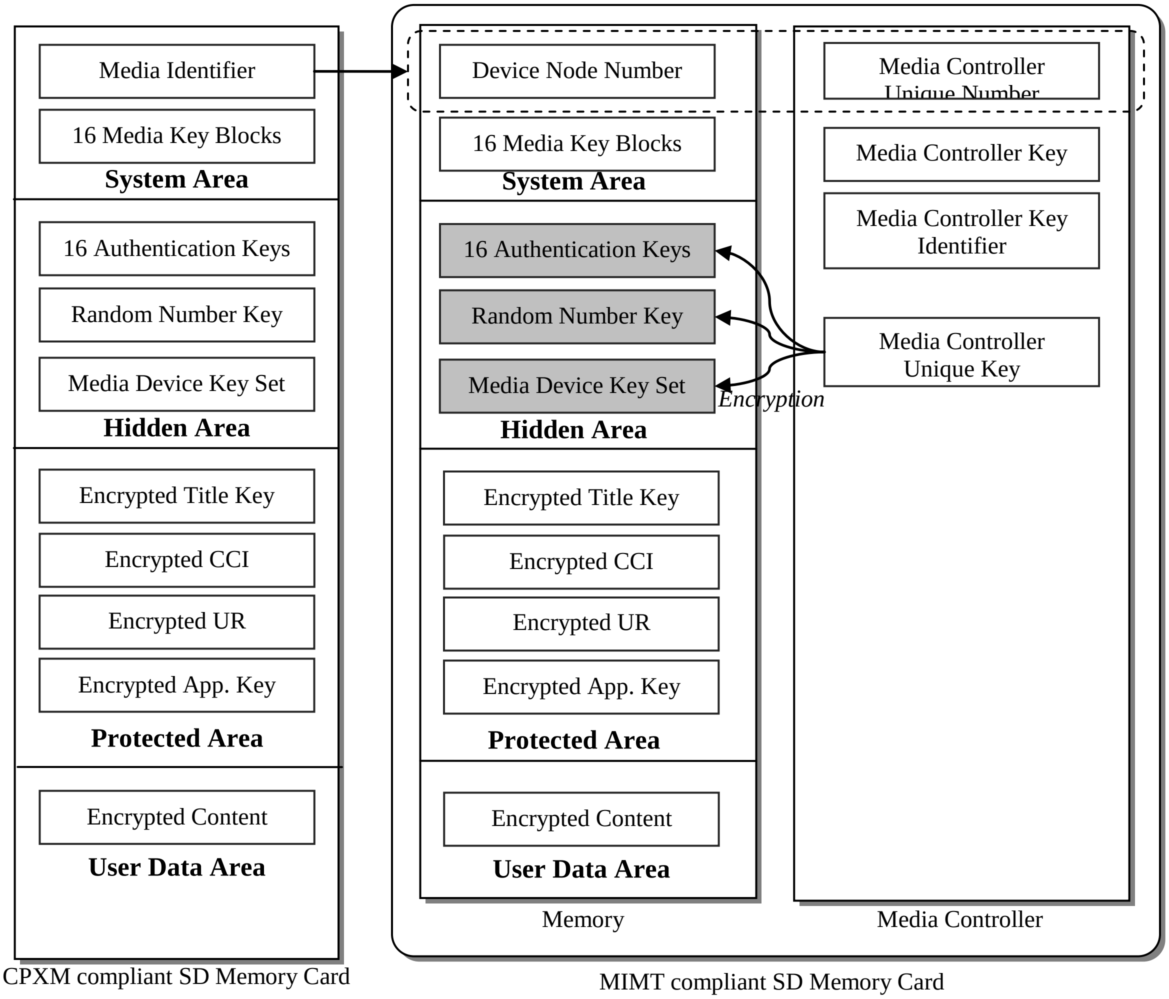


Figure 3-2 Mapping of CPXM components to MIMT compliant SD Memory Card

3.3.1 Controller Manufacturer Identifier

The Controller Manufacturer Identifier (ID_{cm}) is a unique 1-byte identifier assigned by the 4C Entity, LLC to each Controller Manufacturer. ID_{cm} is used as a part of Media Controller Key Identifier and Media Controller Unique Number.

3.3.2 Media Controller Key Identifier

The Media Controller Key Identifier (ID_{mck}) is an identifier for a Media Controller which shares the same Media Controller Key (K_{mc}) assigned by a Controller Manufacturer. The ID_{mck} is embedded in the Media

Controller. The ID_{mck} consists of 1-byte Controller Manufacturer Identifier (ID_{cm}) assigned by the 4C Entity, LLC and a 15-byte unique number (such as serial number) among Media Controllers produced by the Controller Manufacturer. To identify each unique Media Controller, the unique number shall be unique among all Media Controllers produced by a particular Controller Manufacturer and shall not be statistically unique, but shall be guaranteed unique. A pair of ID_{mck} and K_{mc} is sent to the 4C Entity, LLC in a secure manner. It is strongly recommended that the Media Controller Key Identifier be read by a vendor specific command of the Media Controller.

3.3.3 Media Controller Unique Number

The Media Controller Unique Number (N_{mcu}) is a 6-byte number that is embedded in a Media Controller when the Media Controller is manufactured. The Media Controller Unique Number consists of a 1-byte Controller Manufacturer Identifier and a 5-byte unique number assigned by the Controller Manufacturer. The Controller Manufacturer Identifier is defined in Section 3.3.1. The N_{mcu} shall be unique within all Media Controllers produced by a Controller Manufacturer and shall not be altered, rewritable or modifiable. This number shall be used as a part of the Media Identifier of the SD Memory Card.

3.3.4 Media Controller Key

The Media Controller Key (K_{mc}) is a 16-byte secret key embedded when the Media Controller is manufactured. K_{mc} shall be securely embedded in the Media Controller and shall not be altered, rewritable or modifiable. This key is used to encrypt CPXM components such as Authentication Keys and Media Device Keys in the SD Memory Card. The method to encrypt is described in Section 3.5.1. K_{mc} shall be treated as 4C Highly Confidential Information. A pair of K_{mc} and ID_{mck} is sent to the 4C Entity, LLC in a secure manner. It is allowed that one K_{mc} is stored in multiple Media Controllers. The number of Media Controllers which may have the same K_{mc} shall not exceed one million (1,000,000).[1]

3.3.5 Media Controller Unique Key

The Media Controller Unique Key (K_{mcu}) is a secret unique key in the Media Controller. K_{mcu} is used to bind the CPXM components to the Media Controller which has that K_{mcu}. K_{mcu} shall be statistically unique and uniquely assigned to each Media Controller. K_{mcu} shall be treated as 4C Highly Confidential Information. It is not necessary that each K_{mcu} is embedded as a value, that is, K_{mcu} may be calculated from K_{mc} and N_{mcu} in the Media Controller. The following formula is an example to calculate K_{mcu}.

> K_{mcu} = AES_G(K_{mc}, N_{mcu} || a 10-byte Secret Number)
>
> where AES_G is defined in Section 2.3 of the *CPXM Specification: Introduction and Common Cryptographic Elements* book.

The AES_G cryptographic algorithm in this context may be replaced with another one-way function cryptographically stronger than one based on the 128-bit block AES cipher. The 10-byte Secret Number shall be generated by a random number generator and embedded in Media Controllers which have one Media Controller Key Identifier. The Secret Number shall be treated as 4C Highly Confidential Information. K_{mcu} is used to encrypt the Media Device Keys.

3.3.6 Media Device Key Set

The Media Device Key Set is a set of keys used for MKB updates and media authentication. Details are described in Section 3.1 of the *CPXM Specification: Introduction and Common Cryptographic Elements* book. Media Device Keys shall not be read from the SD Memory Card except in cases where Media Device Keys are in encrypted form described in Section 3.5.1. Media Device Keys shall not be stored outside of the Media Controller except in cases where Media Device Keys are in encrypted form described in Section 3.5.1.

[1] The 4C Entity, LLC does not issue more than one million sets of Media Device Keys encrypted with the same K_{mc}.

3.3.7 Authentication Key

The Authentication Key is a key derived from the Media Identifier and a Media Key calculated from an MKB and a Media Device Key Set. Details are described in Section 3.3.2.1 of the *CPXM Specification: SD Memory Card Book Common Part*. 16 pairs of MKB and the associated Authentication Key are stored in an SD Memory Card. The Authentication Keys shall not be read from the Media Controller and stored outside of the Media Controller except in cases where the Authentication Keys are in encrypted form described in Section 3.5.3.

3.3.8 Random Number Key

The Random Number Key is a key used to generate random numbers and described in the *CPXM Specification: SD Memory Card Book Common Part*.

3.3.9 Device Node Number

The Device Node Number (DNN) is an assigned value for Devices which use the same Media Device Key Set. The definition is described in Section 3.2.3 of the *CPXM Specification: Introduction and Common Cryptographic Elements* book. This number shall be used as a part of the Media Identifier of the SD Memory Card.

3.3.10 Media Key

The Media Key (K_m^0) is a key derived from an MKB and a Media Device Key Set. Details of the derivation are described in Section 3.2.4 of the *CPXM Specification: Introduction and Common Cryptographic Elements* book. Any Media Key shall not be read from the Media Controller and stored outside of the Media Controller.

3.4 Manufacturing flow

This is an example of the manufacturing flow.

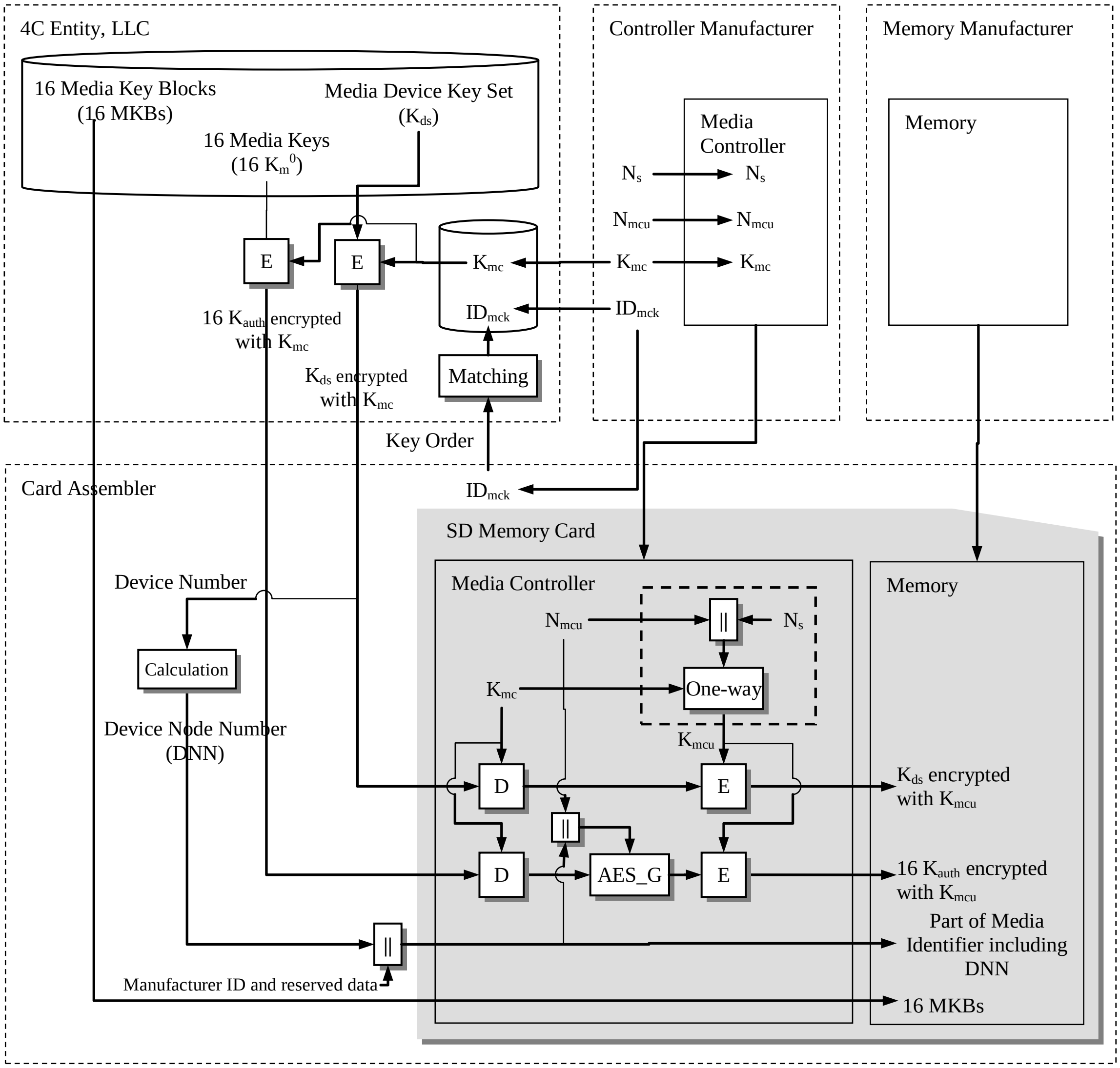
1. A Controller Manufacturer registers with the 4C Entity, LLC and receives one Controller Manufacturer Identifier.
2. The Controller Manufacturer produces Media Controllers. The Media Controller contains the following values:
   - Media Controller Key Identifier (ID_{mck})
   - Media Controller Unique Number (N_{mcu})
   - Media Controller Key (K_{mc})
   - Secret Number (N_s)

   The Media Controller Unique Key (K_{mcu}) can be calculated from K_{mc}, N_{mcu} and N_s which are embedded in this Media Controller.
3. The pair of a Media Controller Key Identifier and a Media Controller Key is sent to the 4C Entity, LLC in a secure manner specified by the 4C Entity, LLC.
4. The 4C Entity, LLC stores the pair of the Media Controller Key Identifier and the Media Controller Key in the database.
5. A Card Assembler gets a Media Controller with ID_{mck} from a Controller Manufacturer and a memory from Memory Manufacturers.
6. The Card Assembler orders a set of Media Device Keys for the SD Memory Card. The Card Assembler informs the 4C Entity, LLC of the Media Controller Key Identifier of the Media Controller.

7. The 4C Entity, LLC retrieves the Media Controller Key from the database. K_{mc} is identified by the Media Controller Key Identifier.
8. The 4C Entity, LLC assigns a Media Device Key Set which includes its Device Number to the order in Step 6.
9. The 4C Entity, LLC generates 16 pairs of Media Key Block and an associated Media Key.
10. The 4C Entity, LLC encrypts the Media Device Keys in the Media Device Key Set with the Media Controller Key.
11. The 4C Entity, LLC encrypts the Media Keys with the Media Controller Key.
12. The 4C Entity, LLC sends the encrypted Media Device Key Set, the Media Keys and the MKBs to the Card Assembler.
13. The Card Assembler prepares that part of the Media Identifier which is the remaining part other than the Media Controller Unique Number. This part of the Media Identifier contains the Device Node Number calculated from the Device Number in the Media Device Key Set. The details are described in Section 3.5.5.
14. The Card Assembler installs the set of encrypted Media Device Keys, the encrypted Media Keys, the MKBs and the part of Media Identifier described in Step 13 to the Media Controller specified by ID_{mck}.
15. The Media Controller decrypts the encrypted Media Device Keys with K_{mc} and re-encrypts the Media Device Keys with K_{mcu}. In this step, the Media Controller can verify the given Media Device Keys. The method used to verify is described in Section 3.5.1.
16. The Media Controller decrypts the encrypted Media Keys with K_{mc},
17. The Media Controller calculates the Media Identifier from the Media Controller Unique Number and the part of the Media Identifier described in Step 13
18. The Media Controller calculates the Authentication Keys from the Media Keys and the Media Identifier and encrypts the Authentication Keys with K_{mcu}.
19. The Media Controller writes the re-encrypted Media Device Keys, the encrypted Authentication Keys, the MKBs and the part of Media Identifier described in Step 13 to the memory.

There is a case where a Media Controller may calculate the Media Key by itself from the MKB or a part of the MKB given by the Card Assembler instead of performing Step 16. It is possible to check whether the Device Key and Media Key are correct, by checking the calculated Media Key with the decrypted Media Key in Step 16.

Figure 3-3 below is an overview of the media manufacturing flow described above. In this figure, E in a box indicates an encryption operation. Similarly D in a box indicates a decryption operation. One-way in a box indicates a one-way function operation.



Note that the area inside the dashed line in the Media Controller is an example implementation.

Figure 3-3 Overview of media manufacturing flow

3.5 Data Structure

This section describes data structure of components.

3.5.1 Delivery of Media Device Key Set

When a set of Media Device Keys is given from the 4C Entity, LLC, the order delivery format includes a check value for integrity checking. The check value is a result of a hash calculation of an entry of the Media Device Key Set. Each entry includes one check value. The Media Controller can verify it. Table 3-2 is a format of an entry of the Media Device Key Set in the order delivery format. Details of the order delivery format are described in the 4C Key Order Form document. The check value is calculated with the following formula:

Check value = AES_H(Data of Media Device Key Set)

where AES_H is defined in Section 2.2 of the *CPXM Specification: Introduction and Common Cryptographic Elements* book.

Table 3-2 Entry of Media Device Key Set in the Order delivery format

Bit **Byte**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
0	Data of Media Device Key Set							
…								
m-1								
m	Check value							
...								
m+15								

3.5.2 Encryption of Device Key

The Media Controller shall re-encrypt all Media Device Keys in a given Media Device Key Set with the Media Controller Unique Key when Media Device Keys are installed into an SD Memory Card. In case of Section 3.4, the re-encryption shall be done in Step 15. After receiving the Media Device Keys, the Media Controller shall not output the Media Device Keys unless these are encrypted with the Media Controller Unique Key. That is, the Media Device Key Set shall be encrypted with the Media Controller Unique Key by the AES cipher when the Media Device Key Set is stored out of the Media Controller, where the AES cipher is defined in Section 2.1 of the *CPXM Specification: Introduction and Common Cryptographic Elements* book. The AES cipher in this context may be replaced with another cipher cryptographically stronger than the 128-bit block AES cipher.

Although how to store a Media Device Key Set in an SD Memory Card is implementation specific, Table 3-3 is an example of a data structure for a Media Device Key Set in an SD Memory Card. The first pair of U Mask (0) and UV Number (0) corresponds to the first Media Device Key (0). In this case, each Media Device Key is encrypted with the Media Controller Unique Key in AES ECB mode defined in Section 2.1.1 of the *CPXM Specification: Introduction and Common Cryptographic Elements* book.

Table 3-3 Example of data structure for Media Device Key Set

Bit **Byte**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
0	10_2		U Mask (0)					
1	UV Number (0)							
…								
5								
6	10_2		U Mask (1)					
7	UV Number (1)							
...								
11								
. . .	. . .							
1944	10_2		U Mask (324)					
1945	UV Number (324)							
...								
1949								
1950	Media Device Key (0)							
…								

1965	
1966	Media Device Key (1)
...	
1981	
. . .	. . .
7134	Media Device Key (324)
...	
7149	

3.5.3 Encryption of Authentication Key

The Media Controller shall encrypt 16 Authentication Keys with the Media Controller Unique Key when Authentication Keys are calculated in an SD Memory Card. In case of Section 3.4, the encryption shall be done in Step18. After Authentication Keys are calculated, the Media Controller shall not output the Authentication Keys except when the Authentication Keys are encrypted by the Media Controller Unique Key with the AES cipher. That is, the Authentication Keys shall be encrypted with the Media Controller Unique Key when the Authentication Keys are stored out of the Media Controller, where the AES cipher is defined in Section 2.1 of the *CPXM Specification: Introduction and Common Cryptographic Elements* book. The AES cipher in this context may be replaced with another cipher cryptographically stronger than the 128-bit block AES cipher.

Although how to store Authentication Keys in an SD Memory Card is implementation specific, Table 3-4 is an example of a data structure for 16 Authentication Keys in an SD Memory Card. In this case, each Authentication Key is encrypted with the Media Controller Unique Key in AES ECB mode.

Table 3-4 Example of data structure for 16 Authentication Keys

Bit **Byte**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
0	1st Authentication Key							
…								
15								
16	2nd Authentication Key							
...								
31								
. . .	. . .							
240	16th Authentication Key							
255								

3.5.4 Media Controller Key Identifier

Table 3-5 shows the structure of the Media Controller Key Identifier for the case of MIMT compliant SD Memory Cards.

Table 3-5 Structure of Media Controller Key Identifier

Bit **Byte**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
0	Controller Manufacturer Identifier							
1	Unique number							
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								

3.5.5 Media Identifier

The Media Controller shall return the Media Identifier upon request from Host Devices. MIMT compliant SD Memory Cards shall use the following data structure as the Media Identifier instead of the one described in Section 3.3.1.1 of the *CPXM Specification: SD Memory Card Book Common Part*.

Table 3-6 shows the structure of the Media Identifier for the case of MIMT compliant SD Memory Cards.

Table 3-6 Structure of Media Identifier

	Bit Byte	7	6	5	4	3	2	1	0
	0	Manufacturer ID assigned by the 4C Entity, LLC							
	1	Reserved for SD Card Association							
	2								
	3								
Media Controller Unique Number	4	Controller Manufacturer Identifier (ID_{cm}) assigned by the 4C Entity, LLC							
	5	Unique number assigned by Controller Manufacturer							
	6								
	7								
	8								
	9								
	10	Reserved (00_{16})							
	11	Device Node Number of Media Device Key Set							
	12								
	13								
	14								
	15								

The Media Identifier consists of the following values:

- Manufacturer ID: The first 1-byte field of the Media Identifier which is given by the 4C Entity, LLC to each Card Assembler. This value is the same as the Manufacturer ID defined in the *CPRM Specification: SD Memory Card Book Common Part*.
- Reserved for SD Card Association: The following 3-byte field of the Media Identifier which is assigned by the SD Card Association.
- Media Controller Unique Number: The following 6-byte field of the Media Identifier which is assigned by the Controller Manufacturer. The Media Controller Unique Number consists of the Controller Manufacturer Identifier and a unique number as described in Section 3.3.3.
- Reserved: The following1-byte field of the Media Identifier is reserved and filled with 00_{16}.
- Device Node Number of the Media Device Key Set: the last 5-byte field of the Media Identifier which is given by the 4C Entity, LLC. The value is recorded when the Media Device Key Set is installed by a Card Assembler.

3.6 Changes of processes

This section describes changes of processes defined in the *CPXM Specification: SD Memory Card Book Common Part*.

3.6.1 Authentication and Key Exchange (AKE)

In the AKE process described in Section 3.4.1 of the *CPXM Specification: SD Memory Card Book Common Part*, the Media Controller in MIMT compliant SD Memory Cards shall read the encrypted Authentication Key (K_{auth}) from the memory and decrypt it before using K_{auth}.

3.6.2 Update MKB process

In the Update MKB process described in Section 3.9 of the *CPXM Specification: SD Memory Card Book Common Part,* the Media Controller in MIMT compliant SD Memory Cards shall read the encrypted Media Device Key Set from the memory and decrypt its Media Device Key to be used for MKB process before step (3-2) in the Update MKB process. The Media Controller in MIMT compliant SD Memory Cards shall also encrypt the new K_{auth} and replace the old encrypted K_{auth} with the new encrypted K_{auth} when K_{auth} is replaced.