White Paper

SDSD-CPRM

Flexible Protection for Digital Content

December 2007

Executive Summary

SDSD-CPRM is a new extension to the SD Memory Card that addresses the difficulties that authorized sharing of protected digital content poses. It uses Content Protection for Recordable Media (CPRM) methods defined by 4C Entity to separate encrypted digital content from the keys that release (decrypt) it. The *SDSD-CPRM* separate delivery mechanism greatly benefits the consumer, content provider, and device manufacturer. The consumer can freely manage and distribute encrypted content, the content provider is able to deliver and protect content, and the device manufacturer can develop products with a common SD Memory Card interface.

This paper reveals the flexibility that *SDSD-CPRM* provides for the authorized sharing and movement of digital content along with a detailed explanation of the CPRM implementation.

Contents

Introduction

Today's digital devices are more capable and mobile than their predecessors. Features on these devices allow the user to access various forms of digital content. In most cases, the consumer is looking for high quality entertainment such as music, movies, and streaming video. As a result, online sales of music and video have boomed. By 2010, it is expected that online sales of digital music will represent one-quarter (25%) of all music purchased worldwide[1]. Additionally, consumer online sales for streaming video are expected to reach $3.2 billion USD in 2007[2].

The personal computer (PC) is the most common device used to access digital content as nearly three out of four U.S. homes own a PC[3] and nearly fifty percent (50%) of those homes have access to broadband internet[4]. Entertainment has transformed the PC into a multimedia platform with the ability to watch streaming or downloaded video, listen to music, create and store content, and deliver content to other devices. In many cases, the PC is used to manage and store a library of downloaded entertainment. Along with the PC, the vision for the future digital living room will extend digital content to all aspects of home entertainment. This future digital home environment will provide many opportunities for content providers, application developers, and device manufacturers.

Mobile phone products have also transformed from communication oriented devices to mobile entertainment devices. Many mobile phones have the ability to access the internet, play downloaded music, and watch streaming video. Worldwide sales of music to mobile phone users are expected to reach $32.2 billion USD by 2010[5]. As a result, downloaded content has increased the need for additional storage on a mobile device. Thus, many mobile phones have added an SD Memory Card expansion slot. It is expected that over twenty-four percent (24%) will have this feature by 2008[6].

To provide the consumer with flexible access to all forms of digital content, there must be a way to ensure that the content is: high quality, easy to store and maintain, sharable with a similar digital device, and copyright holder friendly. Currently, it is difficult to distribute protected digital content between similar devices. This paper discusses a new extension to the SD Memory Card specification that is an ideal solution to the above problem, *SDSD-CPRM* (Secure Digital with Separate Delivery).

SDSD-CPRM utilizes Content Protection for Recordable Media algorithms, defined by the 4C Entity SD-SD specifications, to encrypt content so that it is separated from the keys that release (decrypt) it. This paper shows how encrypted content is distributed along with an explanation of the *SDSD-CPRM* separate delivery mechanism.

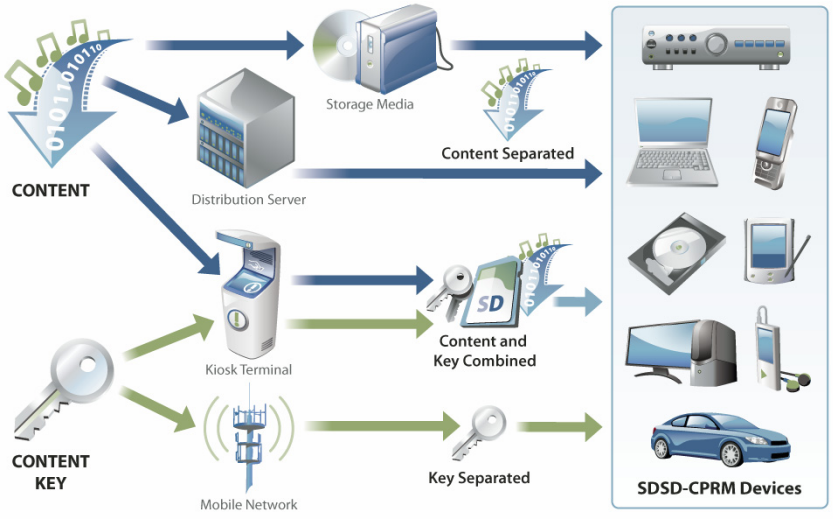
1. International Federation of the Phonographic Industry
2. In-Stat Market Data Research
3. Nielsen Media Research
4. Pew Internet and American Life Project Research
5. Gartner Research
6. International Data Corporation Research

Delivering Content

The separate delivery capability of *SDSD-CPRM* provides broad access to a variety of digital content for the consumer and in turn, tremendous opportunities for the content provider. Encrypted content is available in many forms; downloaded from the internet or mobile network to storage media (hard disk drive (HDD) or flash device) and in programmed form (CD, DVD, or flash device). The keys that unbind the content are similarly available but must be programmed to the SD Memory Card or *SDSD-CPRM* device.

Figure 1 illustrates how content and keys are delivered separately or combined.

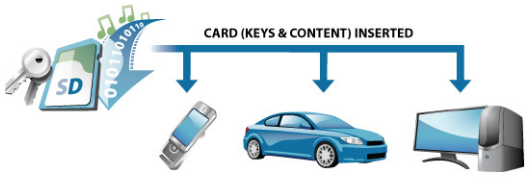
Figure 1. Content Delivery with SDSD-CPRM



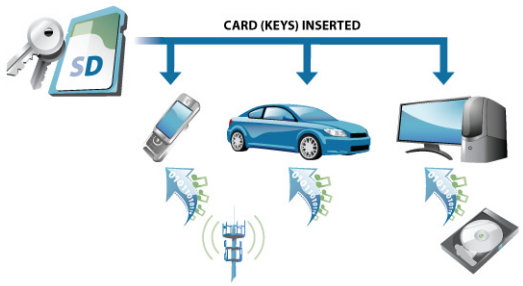
Moving Content

There are various ways to move, distribute, restore, and backup content between similar *SDSD-CPRM* devices. This results in multiple paths for the movement of encrypted content and keys. The following illustrates and explains five common use scenarios.

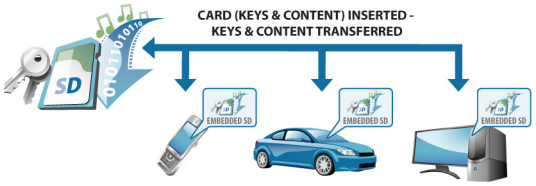
Scenario 1: Keys and encrypted content reside on an SD Memory Card. The SD Memory Card is inserted into the *SDSD-CPRM* device. The device is able to play the content.



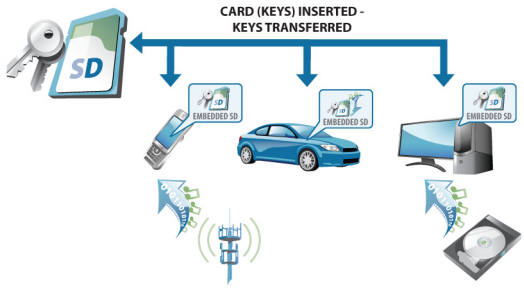
Scenario 2: Keys for the content, Key Library, reside on an SD Memory Card. The SD Memory Card is inserted into the *SDSD-CPRM* device. The receiving device has the encrypted content or has access to it from another source (HDD, PC, LAN, Mobile, etc.).



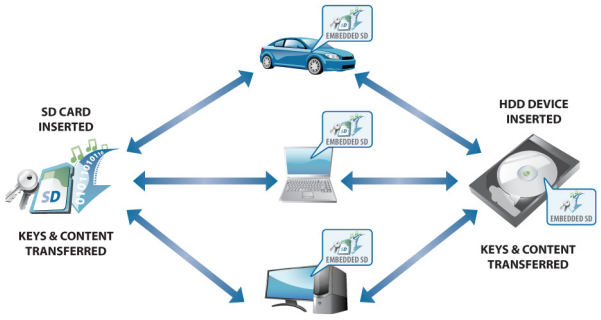
Scenario 3: Encrypted content and associated keys reside on an SD Memory Card. The SD card is inserted into the *SDSD-CPRM* device where it transfers the content and keys to the embedded SD memory. The SD Card is now removable.



Scenario 4: Keys for the content, Key Library, reside on an SD Memory Card. The SD card is inserted then transfers the keys to the *SDSD-CPRM* device with embedded SD memory. The receiving device has the encrypted content or accesses it from another source (HDD, PC, LAN, Mobile, etc.). At this point, the SD Memory Card is removable.



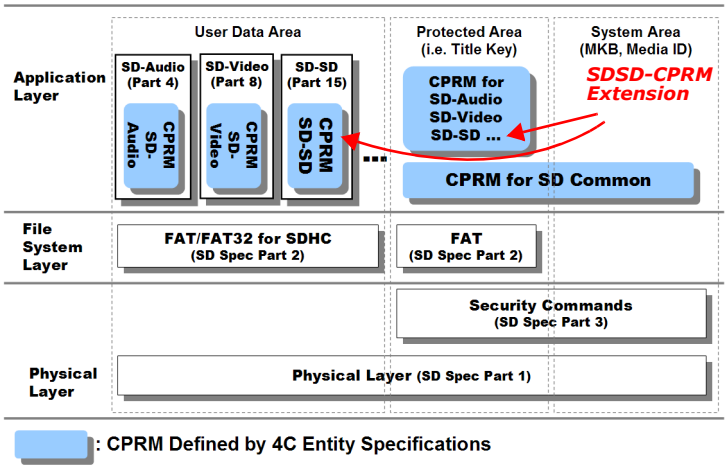
Scenario 5: Encrypted content and associated keys reside on an external storage device with embedded SD memory (SD Memory Card or Hard Disk Drive). The external storage device transfers the keys and content to the *SDSD-CPRM* device with embedded SD memory. After transfer, the external storage device is removable.



The SD Memory Card Extension

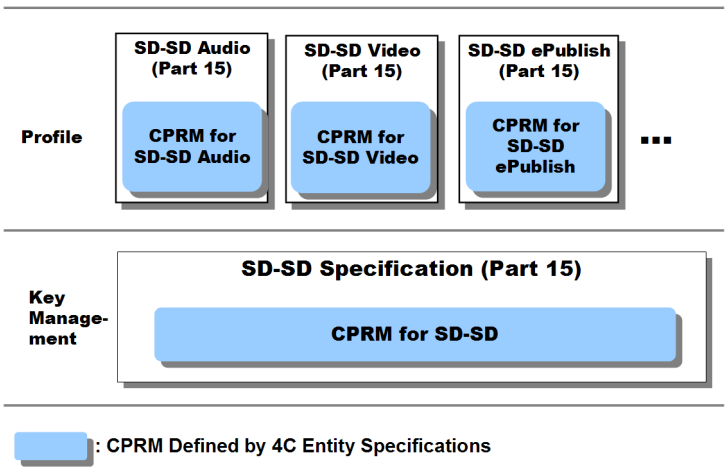
SDSD-CPRM is an extension to the SD Memory Card specification. It adds the ability to independently maintain and store encrypted digital content. The SD Memory Card stores the keys that release (decrypt) the content for access by an *SDSD-CPRM* enabled device. CPRM (C2 Cipher) is used to encrypt/decrypt the digital content and keys. Figure 2 shows the layers of the SD Memory Card and the areas affected by the *SDSD-CPRM* extension.

Figure 2. SD Memory Card Layers with SDSD-CPRM Extension



The *SDSD-CPRM* implementation uses one Media Key Block for all content types. Each content type has an associated profile. Currently, three profiles are approved or under consideration. Those include ***SD-SD Audio***, ***SD-SD Video***, and ***SD-SD ePublish***. These profiles define the implementation of CPRM used to encrypt a specific type of content. Additionally, key management uses CPRM to generate and encrypt the keys. See Figure 3 on page 6.

Figure 3. Current and Future CPRM Profiles for SDSD-CPRM



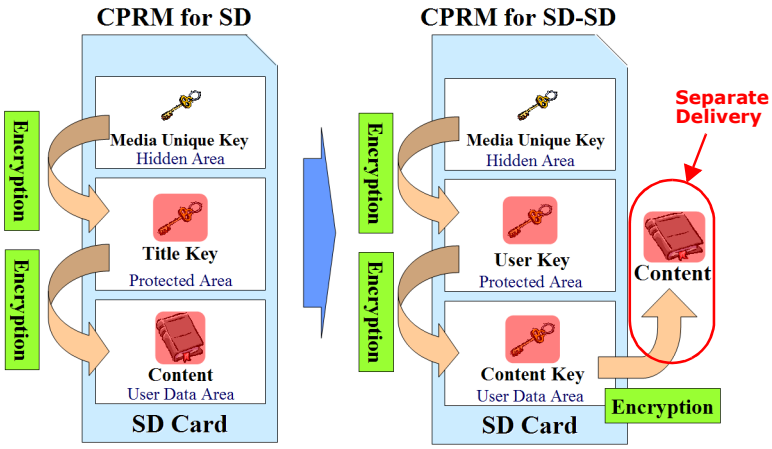
CPRM Differences for SD and SDSD-CPRM

The SD implementation of CPRM requires encrypted content to reside in the user data area of the SD Memory Card. The following steps define the encryption flow for SD (See Figure 4):

1. The *Media Unique Key*, located in the hidden area of the SD Memory Card, encrypts the *Title Key*.
2. The *Title Key*, located in the protected area of SD Memory Card, encrypts the content.
3. The encrypted content resides in the user area of SD Memory Card.

Note: The encryption process is independent for SD-Audio and SD-Video (i.e., they cannot share a *Title Key*).

Figure 4. CPRM Differences for SD and SDSD-CPRM



The *SDSD-CPRM* implementation of CPRM does not require the encrypted content to reside on the SD Memory Card. This is accomplished by adding another step to the encryption process. The following steps define the encryption flow for *SDSD-CPRM* (See Figure 4 on page 6):

1. The *Media Unique Key*, located in the hidden area of the SD Memory Card, encrypts a *User Key* (instead of a *Title Key*).
2. The *User Key*, located in the protected area of the SD Memory Card, encrypts a *Content Key*.
3. The *Content Key*, located in the user area of the SD Memory Card, encrypts the content.
4. The encrypted content may reside in the user data area of the SD Memory Card or on another type of storage media (HDD, flash device, DVD, or CD). This defines the *Separate Delivery* capability of *SDSD-CPRM*.

Note: Different content types (*SD-SD* Audio, *SD-SD* Video, etc.) may share the same *User Key*.

Key Structure for SDSD-CPRM

As mentioned above, the *SDSD-CPRM* implementation generates a *User Key* and a *Content Key* for content encryption. The *User Key* has the following characteristics:

- Stored in protected space on the SD Memory Card
- Encrypts up to 100 Content Keys
- Independent of the *SD-SD* content type (Audio, Video, and ePublish)
- Used for the integrity of Usage Rules (i.e., Lets the recording device know if Usage Rules apply)

The *Content Key* is defined by the following characteristics:

- Stored in user space on the SD Memory Card
- Dependent on the *SD-SD* content type (Audio, Video, and ePublish)
- Embeds usage rules (General and *SD-SD* Audio)

General Usage Rules

By design, the movement of *SDSD-CPRM* encrypted content is not controlled. However, rules may apply to the movement of content keys that unbind the encrypted content. This gives the content provider the ability to limit access to protected content. These rules include:

- **Copy** - A function that controls how a *Content Key* is copied to an *SDSD-CPRM* device or SD Memory Card. The available settings are:
  - Unlimited copies are allowed
  - 1 to 14 copies are allowed
  - Not allowed
- **Move** - A function that controls how a *Content Key* is moved to an *SDSD-CPRM* device or SD Memory Card. The available settings are:
  - Unlimited movement
  - Move once
  - Not allowed
- **Time Basis** (not supported in revision 0.9) - *Content Key* is valid for a specified time

Note: There are no use restrictions on the *Content Key* when Usage Rules are not applied.

SD-SD Audio Usage Rules

SDSD-CPRM provides usage rules for legacy devices. *SD-SD* Audio content is capable of playing on legacy SD-Audio devices and is recordable to CD. The rules include:

- **Export to SD-Audio** - This function allows the *Content Key* to move from an *SD-SD* Audio device to an SD-Audio device. The *Content Key* is decrypted with the *User Key* and sent to the SD-Audio device for encryption as a *Title Key*. The *Content Key* is bound in the *SD-SD* Audio device and identified as exported to SD-Audio. The *Title Key* is also identified and marked as exported SD-Audio. Encrypted content is directly stored to the user data area of the SD-Audio device

Note: Both devices (*SD-SD* Audio and SD-Audio) can playback the associated content.

- **Re-Import from SD-Audio** - This function checks the SD-Audio *Title Key* and *SD-SD* Audio *Content Key* to ensure they are the same, unbinds the *Content Key* in the *SD-SD* Audio device, and then deletes the *Title Key* from the SD-Audio device

Note: The encrypted content on the SD-Audio device cannot play.

- **Export to CD** - This usage rule allows decrypted content to record externally to a CD. The available settings are:
  - Unlimited recordings are allowed
  - 1 to 254 recordings are allowed
  - Not allowed

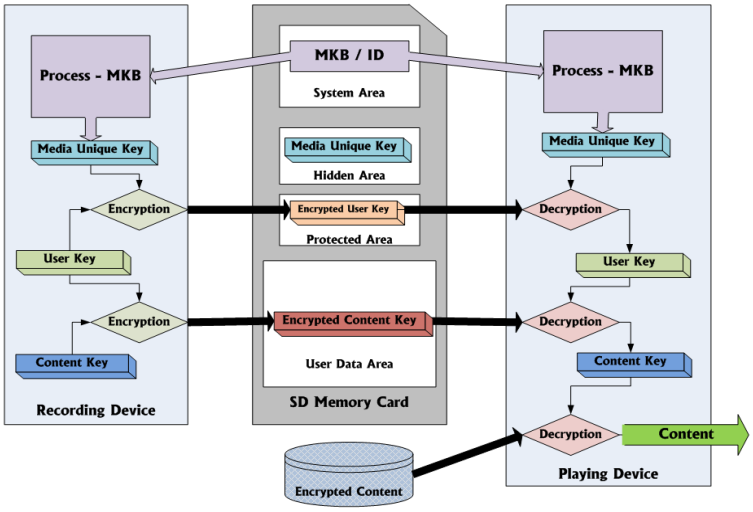
Key Management - Recording/Playback

The separate delivery capability of *SDSD-CPRM* simplifies the CPRM process for the consumer and content provider. Encrypted content, by nature, is free from any restrictions to its movement or delivery and is, therefore, easier to manage. However, the keys that release (decrypt) the content must adhere to certain use requirements pertaining to the CPRM process. The key management system must be able to:

- Access Protected Area of the SD Memory Card using CPRM
- Generate/Manage User Key and Content Key using CPRM
- Pass Keys to other SDSD-CPRM devices using CPRM

Figure 5 displays the CPRM flow from a Recording Device to the Playing Device.

Figure 5. CPRM Flow - Record and Play



Toshiba Corporation's MQbic™ Digital Rights Management System is an example of a key management system for *SDSD-CPRM*.

Key Library

A typical use for an SD Memory Card is to maintain the key library for various forms of content (Audio, Video, and ePublish). Table 1 shows the memory capacity required to store an associated number of keys.

Table 1. Key Library Capacity

Required Memory Capacity	Number of Keys*
128KB	500
256KB	1,000
1MB	5,000
2MB	10,000
5MB	25,000
10MB	50,000
20MB	100,000
30MB	150,000
50MB	250,000

*200 Bytes per Key (Content Key + Meta Data)

Conclusion

SDSD-CPRM is a flexible solution for consumers and content providers. The separate delivery capability provides the consumer with many ways to distribute and maintain digital content. Built-in CPRM functions give content providers and developers the capacity to furnish digital content while preserving their intellectual property rights. Additionally, digital device manufacturers can develop and market products that have a common and low cost SD Memory Card interface.

IBM, Intel, Panasonic and Toshiba formed the 4C Entity in 1999 to address the interoperability challenge of sharing premium content. 4C Entity is the industry organization leading the development, adoption and promotion of interoperable standards for sharing premium content. 4C Entity technologies are critical to enabling users to share premium content among devices built by multiple manufacturers.

The SD Card Association (SDA) is an open industry standards organization established in January 2000 by Matsushita Electric (Panasonic), SanDisk and Toshiba, and is supported by a consortium of more than 1000 companies. The SDA's mission is to set industry standards and promote SD Memory Card acceptance in a variety of applications.

References

SD Card Association (http://www.sdcard.org)

1. SD Specification Part 15, Separate Delivery Specification v1.10
2. SD Specification Part 15, Audio Profile Specifications (Addendum to Separate Delivery Specification v1.0)
3. SD Specification Part 15, Video Profile Specifications (Addendum to Separate Delivery Specification v1.0)

4C Entity (http://www.4centity.com)

1. CPRM Specification, SD Memory Card Book: SD-Separate Delivery Part (SD-SD), Rev. 0.9
2. CPRM Specification, SD Memory Card Book: SD-Separate Delivery Audio Part (SD-SD Audio), Rev. 0.9
3. CPRM Specification, SD Memory Card Book: SD-Separate Delivery Video Part (SD-SD Video), Rev. 0.9

Notice