Panasonic, Samsung, Sony, Toshiba

Introducing Next generation Secure Memory Technology

Panasonic, Samsung, Sony, Toshiba

November 2012

Conditions of Publication

Contents

1. Overview

NSM (Next generation Secure Memory initiative) technology provides security on flash memory robust enough to be used for HD-quality content. This new technology enables users to consume their content on any device with mobility as well as on their lock-in devices, such as smartphone, tablet, DTV, etc. Consumers will be able to download content securely into Licensed Media. Licensed Media means a storage device (SD Memory Card, embedded memory or HDD) with secure flash memory that supports NSM technology.

1.1 Benefits of NSM technology

The NSM technology has been basically constructed on media binding concept, which is generally more flexible than device binding, a way that limits content consumption only on lock-in devices (and most DRM solution's approach at present).

As found in user's natural desire, content needs to belong to users so that they can consume it on any device and anywhere. In this sense, media binding enables users to have better experiences by consuming the content in the way they want by using their own physical media. At the same time, media-based content distribution requires a robust security system to address security concerns such as media cloning, content key disclosure, and so forth. In order to accomplish the advantages of the media binding aspect, the NSM technology focuses on various security enhancements such as anti-cloning and revocation of disclosed secrets.

In fact, security concerns raised from security weakness of playback devices and storage devices cloning attacks have been preventing download services from happening for premium content distribution. As a solution to meet user's desire and content owner's requirement at the same time, media binding can be considered.

We believe this can empower package-based media market to step forward because this is a business model that can satisfy both content providers and users, provided that security concerns on premium content distribution through storage devices is adequately resolved.

Through the NSM Technology, much more robust environment for premium content distribution can be realized, and therefore, time-to-market for premium content can be shortened as an additional benefit for users' content consumption.

1.2 Content consumption scenarios

With the fast advancements in mobile devices, movie consumption scenario is rapidly expanding from the conventional living room environment to mobile environment. This trend reflects consumers' strong demand for content consumption on mobile devices, especially on Android-based smartphones and tablets, the security level of which is not considered to be high enough to consume valuable movie content. Also, users want to see content in HD-quality even on mobile devices because they are so accustomed to HD-quality from HDTVs and Blu-ray™ movies.

It is often expected that cloud-based streaming service will be the future of content distribution. However, it is not likely to happen at least for a few years for mobile devices, especially for HD-quality content. In this case, a secure download service can be a good complementary to streaming services. Streaming HD-quality content through mobile carriers' network will cause significant burden to network itself, even if it is possible. Also, users will be required to pay significant additional network cost to realize this scenario, and using a Wi-Fi network greatly limits the mobility of mobile devices. Therefore, storing content in Licensed Media is the most affordable and efficient solution for users to consume HD-quality content on mobile devices securely at this moment.

Generally, NSM technology can be used for the following cases:

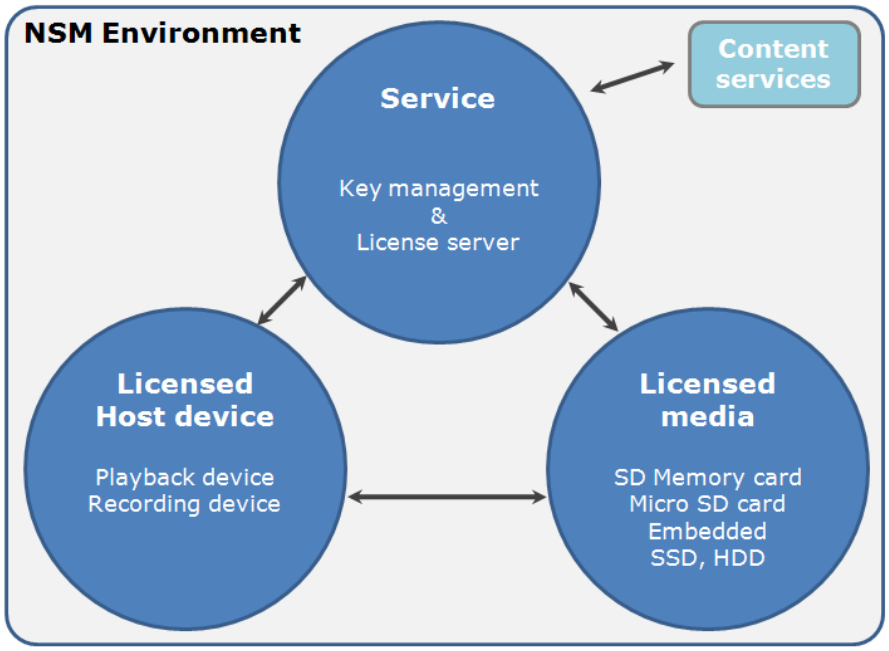
1. **Packaged media**: Content providers can pre-load content into Licensed Media and sell as packaged content. This can be considered as an expansion of optical media such as DVD and Blu-ray™ because secure memory can be used on mobile devices as well as conventional BD players and TVs.

2. **Online services**
   A. EST (Electronic sell-through): Users can download content and store it in secure memory. This content can be played on any devices that support the NSM technology, but cannot be copied illegally.
   B. Rental and subscription services: The NSM technology supports various types of use cases as widely used in the market today. Sell-through content, rental content, and subscription service content can be recorded all in one medium.
   C. MoD (Manufacturing on Demand): Content vending machines, kiosks, etc.

3. **Additional services**
   A. Digital Copy: Content providers can make a new business model by allowing users to copy Blu-ray™ content to Licensed Media for a reasonable price.
   B. Broadcast recording: Users can record broadcast content securely.

1.3 NSM service model

NSM provides not only flash memory-based security, but also total security service environment including:



Service

Various services NSM provides for secure content usage (key and license management).

Licensed Host Device

Devices that can play and record encoded content safely (TVs, smartphones, tablets, BD players, etc).

Licensed Media

Storage devices with secure flash memory that support NSM technology.

Harmonization with existing services

NSM services can be used for other existing content services or incorporate existing services into NSM services. Also, developing new service models by combining NSM services with existing services is possible. For example, an existing content service can use their own service model and still can use NSM technology as a medium.

The NSM Technology supports two types of content protections: Copy Protection System For Self-Encoding Content and Copy Protection System For Prepared Content. The Copy Protection System for Self-Encoding Content is targeting for SD and HD-quality content

distribution and HD-quality broadcast recording, and the Copy Protection System for Prepared Content is for HD-quality premium content distribution. In the current NSM scope, the Copy Protection System for Self-Encoding Content includes a broadcast recording scenario and the Copy Protection System for Prepared Content covers others such as EST (Electronic Sell-Through), MoD (Manufacturing on Demand), Digital Copy, and so on.

2. AV Format

The AV format supported by the Licensed Host Device is defined to ensure interoperability of content stored in Licensed Media, especially for content stored in removable media

2.1 MP4 and TS based format

NSM defines two types of AV formats: one is NSM native mp4 file format and another is NSM TS recording file format. Each AV format would be applied to both the Copy Protection System for Self-Encoding Content and Copy Protection System for Prepared Content. Usage examples of these AV formats are shown in Table 2-1.

Table 2-1: Usage of each AV format

AV format	Copy Protection Type	Usage
NSM mp4 file format	For Self-Encoding Content	* Self-encoding application * Distribution of prepared SD and HD quality content e.g. Broadcast recording, EST, MoD
	For Prepared Content	* Distribution of prepared HD-quality content e.g. Digital Copy, EST, MoD
NSM TS Recording file format	For Self-Encoding Content	* Self-encoding application e.g. Broadcast recording
	For Prepared Content	* Distribution of prepared HD-quality content e.g. Managed Copy

Note that when the file system where the upper limit of one file's size is $(4*2^{30} -1)$ bytes (e.g. FAT32) is used, the file larger than $(4*2^{30} -1)$ bytes should be split into multiple files and then recorded on the media.

2.2 NSM mp4 file format

This format is defined so that video and audio elementary stream assets of a service provider can be reused for the NSM mp4 file format, and mainly used in a content distribution service like Digital Copy, EST, MoD, etc.

Video:	MPEG-4 AVC
Audio:	MPEG-4 AAC
Subtitle:	Bitmap based

3GPP-based metadata box is applied for the NSM mp4 file format, and a new mp4 box is also added for extension such as storage of thumbnails.

2.3 NSM TS recording file format

This format supports two recording modes - direct recording of the digital broadcasting (*1) and MPEG-4 AVC transcode recording (*2).

Video:	Broadcasting dependent (*1)
	MPEG-4 AVC (*2)
Audio:	Broadcasting dependent (*1)
	MPEG-4 AAC (*2)
Subtitle:	Broadcasting dependent (*1)
	Bitmap based (*2)

3. Architecture

3.1 Electronic Sell-Through (EST)

This section describes the components and the flow in the case of EST. Licensed Media can also be used for other types of video distribution services, such as Manufacturing on Demand (MoD) or Digital Copy.

Figure 3-1 illustrates the overall architecture for EST.

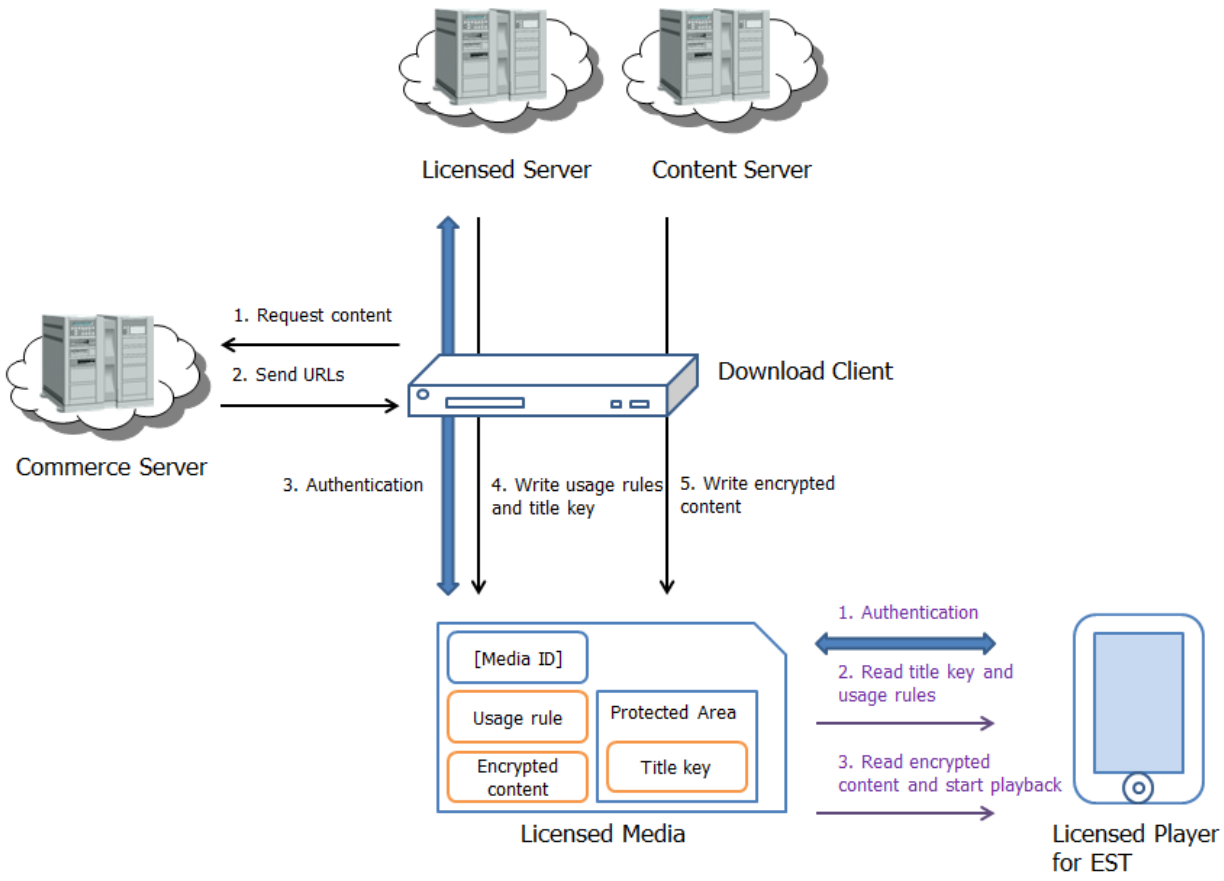


Figure 3-1 Components and flow in the case of EST

3.1.1 Components

Commerce Server

The Commerce Server is a server that provides the main function of online storefront such as product display and payment.

Content Server

The Content Server is a server that stores and distributes encrypted content.

Licensed Server

The Licensed Server is a server that distributes usage rules and content encryption keys. The server has a function to authenticate Licensed Media.

Licensed Media

The Licensed Media is a storage device with secure flash memory that complies with NSM specifications. The Licensed Media has a Media ID, which is uniquely assigned to each Licensed Media, and a Protected Area, which is an area of data storage that ensures the integrity and secrecy of the stored data.

Download Client

The Download Client performs content downloading onto the Licensed Media.

Licensed Player for EST

The Licensed Player for EST is a playback host that plays content on the Licensed Media. The Licensed Player has a function to authenticate Licensed Media.

3.1.2 Flow

This section describes how the Download Client downloads content to the Licensed Media and how the Licensed Player plays content on the Licensed Media.

Recording procedure

1. The Download Client requests content from the Commerce Server.
2. The Commerce Server sends the URLs of the Licensed Service and Content Server to the Download Client.
3. The Download Client initiates an authentication between the Licensed Server and the Licensed Media. Then, the server and the Licensed Media authenticate each other and create a secure authentication channel between them.
4. The License Server writes the content encryption key for the requested content in the Protected Area on the Licensed Media through the secure authentication channel and writes the usage rules for the requested content on the Licensed Media and binds them with the Media ID.
5. The Download Client downloads encrypted content from the Content Server to the Licensed Media.

Playback procedure

1. The Licensed Player for EST and the Licensed Media authenticate each other and create a secure authentication channel between them.
2. The Licensed Player for EST reads the content encryption key for the

downloaded content from the Protected Area on the Licensed Media through the secure authentication channel. Then, the player reads the usage rules for the downloaded content and the content encryption key from the Licensed Media.

3. The Licensed Player for EST verifies the usage rules for the downloaded content. If the verification is successful, the player decrypts the encrypted content and decodes it.

3.2 Broadcast recording

This section describes the components and the flow in the case of broadcast recording. Figure 3-2 illustrates the overall architecture for broadcasting recording.

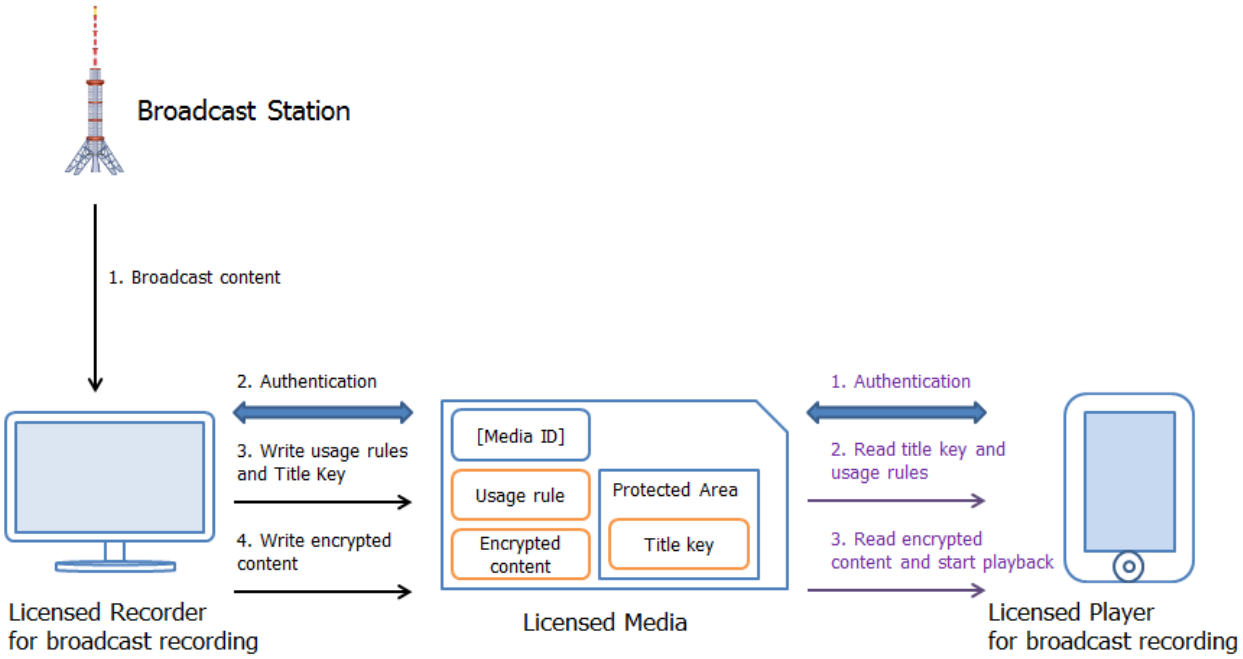


Figure 3-2 Components and flow in the case of broadcast recording

3.2.1 Components

Broadcast Station

The Broadcast Station is a station that is established to broadcast television programs.

Licensed Media

The Licensed Media is an SD Memory Card that complies with NSM specifications. The Licensed Media has a Media ID, which is uniquely assigned to each Licensed

Media, and a Protected Area, which is an area of data storage that ensures the integrity and secrecy of the stored data.

Licensed Recorder

The Licensed Recorder is a recording host that records broadcast content on the Licensed Media. The recorder has a function to authenticate Licensed Media.

Licensed Player for broadcast recording

The Licensed Player for broadcast recording is a playback host that plays broadcast content on the Licensed Media. The Licensed Player has a function to authenticate Licensed Media.

3.2.2 Flow

This section describes how the Licensed Recorder records broadcast content on the Licensed Media and how the Licensed Player for broadcast recording plays content on the Licensed Media.

Recording procedure

1. The Licensed Recorder receives broadcast content, such as CAS (Conditional Access System) protected broadcast program, from the broadcast station.
2. The Licensed Recorder and the Licensed Media authenticate each other and create a secure authentication channel between them.
3. The Licensed Recorder generates and writes a content encryption key in the Protected Area on the Licensed Media through secure authentication channel. The Licensed Recorder also creates usage rules based on the rules of the upstream copy protection system and writes those rules on the Licensed Media, binding them with the Media ID.
4. The Licensed Recorder creates encrypted content from the original content using the content encryption key and writes that encrypted content on the Licensed Media.

Playback procedure

1. The Licensed Player for broadcast recording and the Licensed Media authenticate each other and create a secure authentication channel between them.
2. The Licensed Player for broadcast recording reads the content encryption key for the downloaded content from the Protected Area on the Licensed Media through the secure authentication channel. Then, the player reads the usage rules for the downloaded content.
3. The Licensed Player for broadcast recording verifies the usage rules for the downloaded content. If the verification is successful, the player decrypts the encrypted content using the content encryption key.

3.3 Advantages

3.3.1 Anti-cloning of content

The NSM technology has a great advantage in anti-cloning of content, which is accomplished by multiple security ID layers. For more information about anti-cloning of content, see Chapter 4, "Anti-Cloning".

3.3.2 Content encryption key protection using PKI-based authentication

Content encryption keys are stored in the Protected Area of the Licensed Media in a secure manner. The Protected Area is a secure storage that exists in the Licensed Media and can be accessed only if the authentication is successful. When the Licensed Player plays content, it is required to perform the authentication in order to obtain Content encryption keys. A PKI (Public Key Infrastructure-based) technology is used as an authentication technology.

By using this technology, even if Host Authentication Keys are leaked and used for a ripper tool, they are easily identified and revoked when the ripper tool is executed. This is because the Public Key Certificate of the Licensed Host Device is sent to the Licensed Media during the authentication.

3.3.3 Access control of the Protected Area

The Protected Area of the Licensed Media consists of multiple sub-divided blocks. Each block is assigned for the specific purpose, such as EST, MoD, Digital Copy, or broadcast recording. Access to each block can be controlled by host certificates that are used for PKI-based authentication.

Figure 3-3 shows an example of access control of the Protected Area.

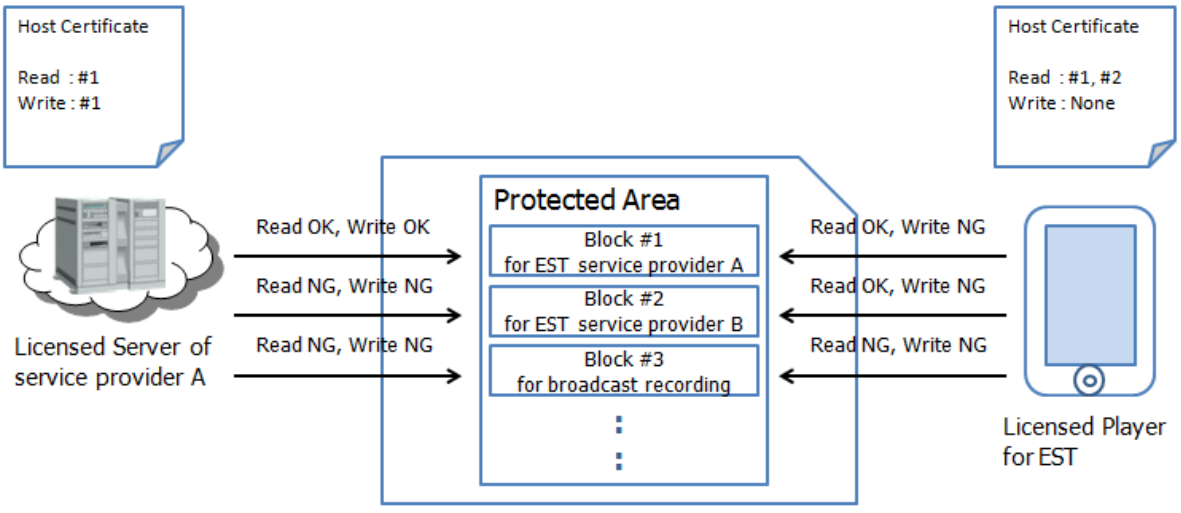


Figure 3-3 Access control of the Protected Area

4. Anti-cloning

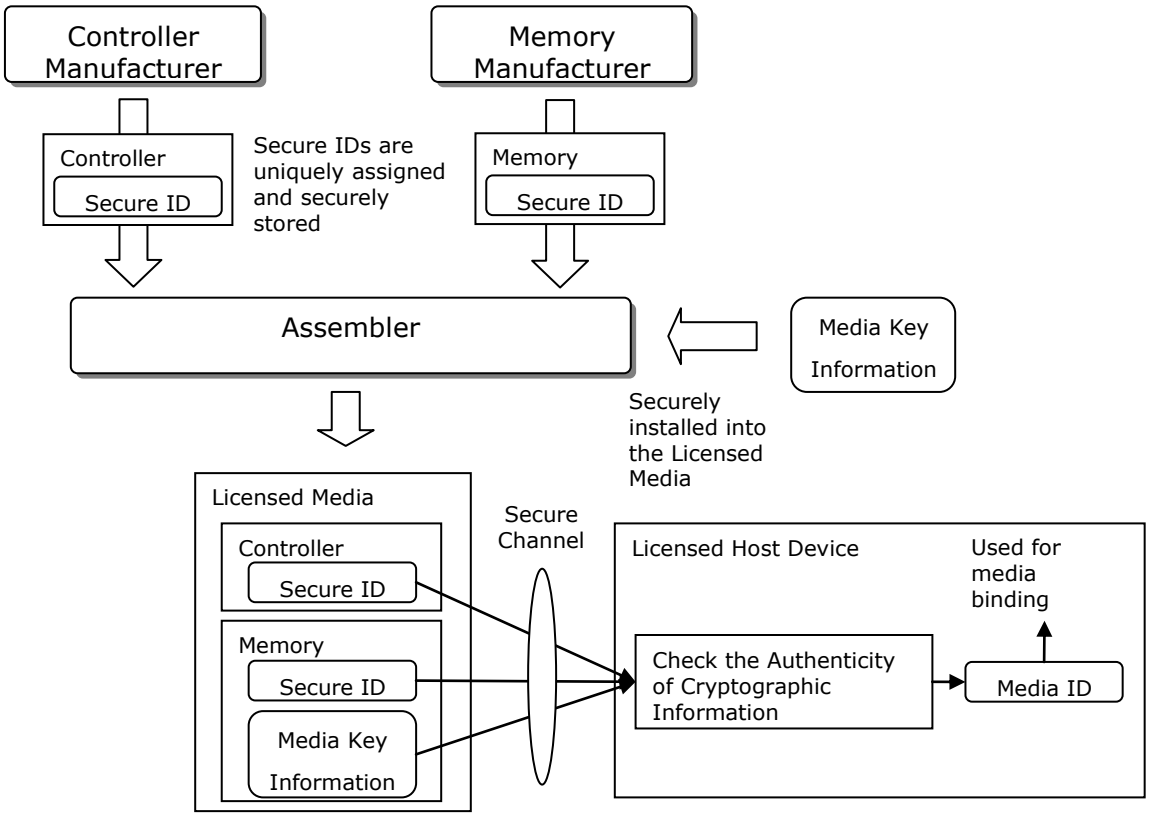
4.1 Background

Existing content protection systems for removable media use a Media Identifier (Media ID) for physical media to bind encrypted content and the media. The encrypted content is cryptographically bound to the Media ID so that unauthorized copy of the encrypted content cannot be played back from the other media. This approach is efficient as far as Media ID is not cloned. However, once uniqueness of Media ID becomes less ensured, the encrypted content can be copied and played back without cracking the content protection system. Especially, non-compliant media manufacturers can easily produce cloned media by just applying the same Media ID to multiple pieces of media for distributing pirated content.

4.2 Secure ID

To address the above issue, our technology adopts multiple robust Secure ID layers for the memory components (Memory) and the memory controller component (Controller) within a storage product (Licensed Media). The Secure IDs for both types of components (Memory and Controller) are utilized by the Licensed Host Device to identify and authenticate each piece of the Licensed Media. The aim to adopt multiple layers is to enhance the robustness against the case where each of the layers is compromised. The Secure ID in each layer is a bundle of Security Information uniquely assigned to each piece of the Licensed Media, and different types of Secure IDs are allocated to the Memory and the Controller according to the layers.

To authenticate the Secure IDs, Cryptographic Information derived from the Secure IDs and Media Key Information is transmitted from both the Memory and the Controller to the Licensed Host Device through a secure authenticated channel. The secure authenticated channel is based on a widely adopted cryptographic technology. If the authenticity of the Cryptographic Information is confirmed, the Licensed Host Device derives the Media ID.



4.3 Robustness

Our multi-layer security system provides a more robust anti-cloning technology against unauthorized copy than existing content protection systems. By means of the secure authenticated channel, any malicious alteration of the information is prevented. The Secure IDs retained in the Licensed Media are managed only by trustable entities. Any sensitive information is never disclosed to non-compliant and non-trusted entities in the transaction. Furthermore, cloned media cannot be produced even by the information which a compliant Licensed Host Device can retrieve.

5. References

ISO/IEC 14496-14:2003: Information technology - Coding of audio-visual objects - Part14: MP4 File Format

ISO/IEC 14496-3:2005: Information technology - Coding of audio-visual objects - Part3: Audio

ISO/IEC 14496-10:2009: Information technology - Coding of audio-visual objects - Part10: Advanced video coding