Access Control in Multimedia Broadcasting for Mobile Terminals

Shinji Ishii[†], *Kouichi Ito, Hidetaka Kuwano, Akihito Akutsu, and Toshiharu Morizumi*

Abstract

This article explains access control technology and content protection technology that will serve as content security measures when multimedia broadcasting is provided as a pay service. High-quality audio-visual streaming services based on ISDB-Tmm (integrated services digital broadcasting, terrestrial mobile multimedia) are planned for 2012. They are expected to include realtime services and storage-based services.

1. Introduction

ISDB-Tmm (integrated services digital broadcasting, terrestrial mobile multimedia), which will be used for multimedia broadcasting services that are scheduled to begin in Japan in 2012, can be considered to be one of the most advanced commercial schemes in terms of security technology supporting the content business and in terms of using the combination of broadcasting and communication. This article mainly explains the functional requirements for the content security technology, including what conventional technology is inherited and the potential for developing the conventional technology. Notices from the Japanese Ministry of Internal Affairs and Communications (MIC) and relevant standard specifications are also mentioned.

2. Content security technology

In the content business, the distribution of valuable content requires guarantees that the content will be used only as permitted. Content security technology serves to satisfy this requirement.

The multimedia broadcasting services are scheduled to include subscription-based services. Since the beginning of subscription-based digital broadcasting services, it has been possible to use the conditional access system (CAS) to restrict content viewing to the receivers used by contract-holders.

Businesses that handle products and digital content and apply security technology for digital transactions used in electronic payments are now common. Digital content differs from food products and other such goods in that its value as a commercial product remains the same even after use. Therefore, digital content must include a function for limiting its use to within the usage rights. Digital rights management (DRM) is one system that includes functions for both electronic payment management and content usage rights management.

For multimedia broadcasting, the realtime broadcasting service and the storage-based broadcasting service described in an MIC report [1] are assumed. Those services take advantage of the features of CAS and DRM. The service and access control technology requirements for the two services are described in **Table 1**.

3. Notices and standards related to ISDB-Tmm

ISDB-Tmm has been systematized and expanded, beginning with BS (broadcast satellite) in 2000 and then CS (communication satellite, ISDB-S) and terrestrial digital broadcasting (ISDB-T). It is important that these broadcast media were effectively configured so that they could be received by the same receivers.

† NTT Cyber Solutions Laboratories
Yokosuka-shi, 239-0847 Japan

Table 1. Access control technology for multimedia broadcasting.

	Service requirements		Applicability of CAS/DRM	
	Realtime service	Storage-based service	CAS	DRM
Multicasting	Video distribution system with unlimited number of distributions	Access control does not work during storage.	◎	Unicast distribution; facility requirements correspond to transaction volume.
Realtime viewing	Video output can begin right after stream selection.	Viewing can begin only after the content has been stored and decrypted.	◎ Realtime (except for contract update)	A few seconds are required for license issuing.
Content storage	Not needed (personal-use recording permitted)	Anytime, anywhere within the usage rights	—	◎
Diversity of sales	Channel and program unit	Content unit	○	○
Setting of usage rights	Channel and program unit	Content unit	○	◎

Table 2. Comparison of content security schemes (access control).

		Multimedia broadcasting	Current broadcasting (ISDB-T)	IPTV (for reference)[*1]
Realtime	Scrambling	Scrambling key change (several seconds to several tens of seconds) MPEG2-TS packet unit[*2] (IPTV is MPEG2-TTS)		
		MIC Notice No. 40 Standardization: Association of Radio Industries and Businesses (ARIB)		Not specified by MIC Private sector standardization: IPTV Forum
	Encryption algorithms	MULTI2 64-bit block encryption AES, Camellia 128-bit block encryption	MULTI2 64-bit block encryption	Set independently by operator (realtime retransmission with consent of broadcasters) Usually AES, etc.
Storage-based	Encryption scheme	Mainly in units of content, usually files		
		Not specified by MIC	Not used	Not specified by MIC
	Encryption algorithm	Standardized by ARIB		Private sector standardization: IPTV Forum
		Not specified. ARIB STD-B25, Part 4 Encryption algorithm or equivalent recommended	Not specified. ARIB STD-B25 at least DES or equivalent recommended	AES
ITU international standardization status		Nothing directly, but it is possible to refer to ARIB STD-B25 from BT.1306 System C.		X.1191 describes an overview and requirements

Likewise, it is important to utilize new cryptanalysis technology as the processing power of computers increases.

Placing importance on the balance between consideration of implementing the ISDB-T system for cell phones and mobile terminals and effective use of secure-client modules already in wide use for cell phones etc. in multimedia broadcasting as well, the relevant MIC Notices have been compiled as Technical Conditions for Multimedia Broadcasting Systems for Mobile Terminals. That served as the basis for Ministerial Ordinance and Notice revisions. The results relevant to content security are listed and compared with current broadcasting and Internet protocol television (IPTV) in **Table 2**.

ISDB-Tmm was revised in an April 2010 Notice [2] related to the conventional digital broadcasting (ISDB-T) base. For the encryption algorithm used in

Table 3. Content protection methods.

Broadcast system	Entry control, etc.
Broadcasting channel	Content encryption
Communications channel	Content encryption
Receiver function	Content encryption
Storage memory	Content encryption
Renderer	Compliance by receiver manufacturers
External display	Use of HDCP (high-bandwidth digital content)* or other display device specifications that allow content encryption (* example of a de facto standard)

the scrambling method for realtime broadcast content, AES (advanced encryption standard) and Camellia, which differ in basic structure from 128-bit block encryption and have been thoroughly analyzed for encryption strength, were added to the MULTI2 64-bit block encryption to mitigate particular encryption risks. Broadcasters can select from among those three algorithms for their implementations. Moreover, "Conditional Access System Specifications for Digital Broadcasting" in Part 4 of ARIB STD-B25 was newly established as a standard specification (ARIB: Association of Radio Industries and Businesses; STD: Standard). Furthermore, "Multimedia Broadcasting Conditional Access System (CAS) Operation and Receiver Specifications" in section 5 of ARIB TR-B33 and "Content Protection for Multimedia Broadcast" in section 8 are set as technical reports (TRs).

4. Access control

Most content must be protected by a certain minimum strength of security throughout the process from the moment the broadcaster obtains the content until the broadcast (including content complementation) and during the viewing or use at the receiver until the content is deleted. Content security technology requires content protection technology.

4.1 Content protection technology

The methods for protecting content from the time of broadcast up to storage in the receiver's memory device are described in **Table 3**. Even if the receiver is owned by a legitimate contract holder, any weakness in its security might be exploited in an attempt to use the content in ways outside the content rights. The strength of content protection depends largely on the implementation of the rendering function (video decoding etc.), which is the main target of such threats.

Broadcasters and receiver manufacturers agreed specific compliance rules that are based on the content rights holder's consent for using and implementing content protection functions in the receiver on the basis of those rules.

One approach that is being considered allows combinations of validity period for viewing, number of replays, and other such use content usage rights restrictions to be set as Rights Management and Protection Information (RMPI) so that the conditions for content use can be selected for each item of content.

4.2 Access control requirements

Since the broadcast content is transmitted via a broadcasting channel, the signal might be received by anyone within the broadcasting service area. Conditional access is technology for restricting use of content to only the receivers for which there is a subscription contract for pay services etc.

In the conditional access method (**Fig. 1**) for the content, the scrambling key for decrypting the content, *Ks*, is encrypted and broadcast as the ECM (Entitlement Control Message) in sync with the content packets (by multiplexing). The ECM includes the subscription contract information and the corresponding scrambling key (*Ks*). Because the scrambling key is broadcast in sync with the video and audio, the receiver can use that key to play the video and audio immediately after a channel for which a contract exists has been selected. The subscription contract information for each receiver is sent to the receiver as the EMM (Entitlement Management Message) via the broadcasting channel or communications channel. In this way, the most recent contract information is updated in the EMM and viewing control for a very large number of users can be achieved by reference to the ECM that is broadcast in sync with the content.

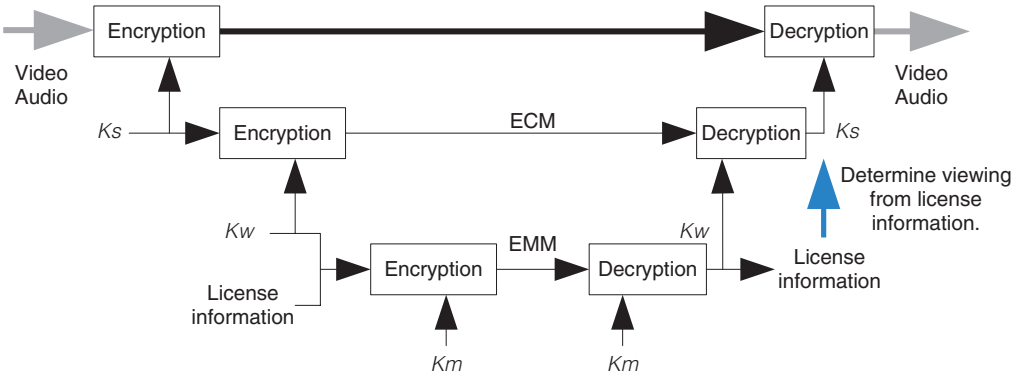

Fig. 1. Overview of CAS.

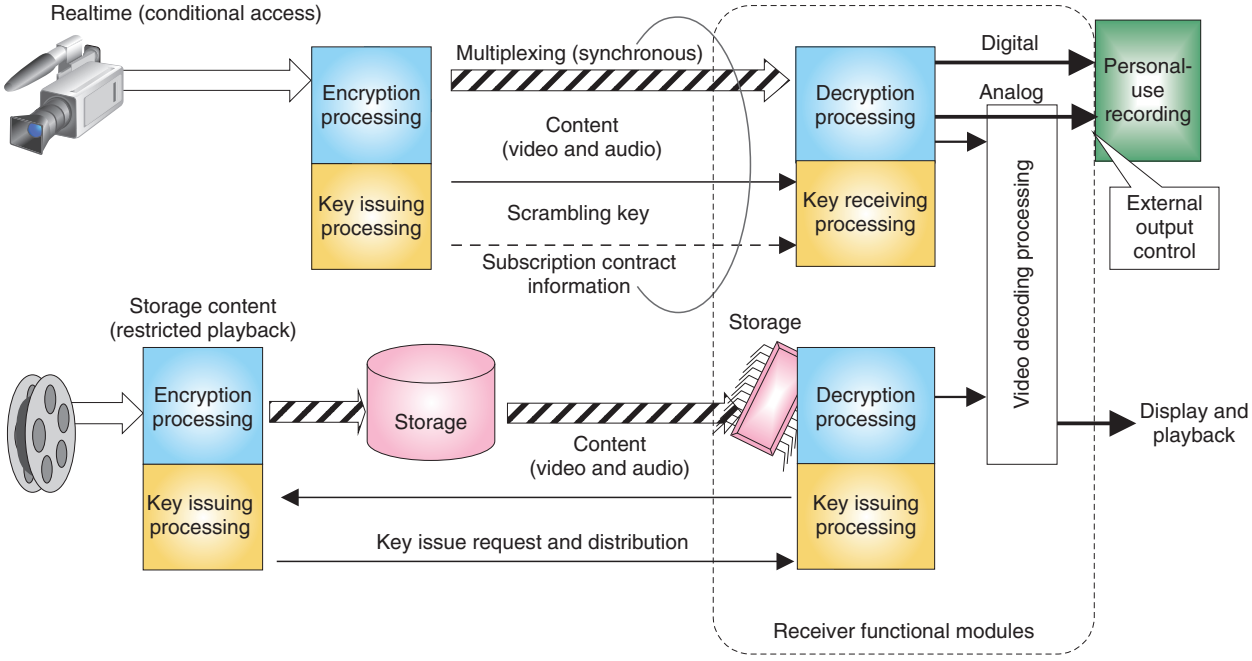

Fig. 2. Content security system.

4.3 Implementation requirements related to development and operating costs

The most important factor that is common to all security measures for application to commercial services for ordinary consumers is the cost-to-performance ratio. With respect to content protection, a much higher level of security is desirable to prevent loss of profit by the content provider. On the other hand, systems that have stronger content security are more expensive. Consequently, use of an excessively strong security function leads to a decrease in the user experience by lowering system performance, effectively increasing the cost of service provision. Furthermore, not all of the requirements are satisfied by security technology: legitimate use by the subscriber according to the terms of the legal contract with the service provider is related to effectively inexpensive provision of service at good quality. The actual implementation of the receiver functions takes this kind of security balance into account.

5. Security implementation technology

Because pay services are assumed for multimedia broadcasting services, the services can be implemented with security on the basis of ARIB STD-B25, the standard specifications for the technology currently being used for BS, CS, and terrestrial digital while addressing the following concerns.

- The receiver implementation shall not specify physical shapes.
- Because the broadcasting is done in a narrow bandwidth, the EMM, which is specific information for individual subscribers, shall be delivered mainly via a communications channel.
- Receiver cost should be reduced by sharing the security functions implemented in cell phones etc.

The content security system planned for multimedia broadcasting is illustrated in **Fig. 2**. The upper part of the figure shows a system for realtime broadcasting service and the lower part shows one for storage-based service.

Current commercial broadcasting does not include storage-based services, but ARIB TR-B27 [3] summarizes the results of studies on services for the digital broadcasting system based on a home server as a technical report. We consider that storage-based services can be implemented by specializing some of the service functions of the digital broadcasting system based on a home server. For storage-based services, it will be necessary to receive an encryption key. The issuing of the key is referred to as the issuing of a license. The main information contained in that license is 1) link information to the content, 2) a key for decrypting the content, and 3) RMPI that specifies the content usage rights.

6. Conclusion

Multimedia broadcasting is the newest service in digital broadcasting. Its technical architecture can be expected to engender services make the most of the advantages of telecommunication and broadcasting technologies through the fusion of cell phone and receiver functions. In addition to inheriting technology from the ISDB architecture, there is high cross-compatibility with the IPTV technical architecture, so services that implement horizontal integration of media can also be expected.

References

[1] http://www.soumu.go.jp/main_content/000041320.pdf (in Japanese).
[2] http://www.soumu.go.jp/main_content/000028353.pdf (in Japanese).
[3] http://www.arib.or.jp/english/html/overview/doc/4-TR-B27v1_0-2p3.pdf (in Japanese).

Shinji Ishii
Senior Research Engineer, NTT Cyber Solutions Laboratories.
He joined NTT in 1989 and engaged in developmental research on security systems for multimedia communications. Recently, he has been engaged in the development of copy protection systems and CAS for broadband communications and digital broadcasting.

Kouichi Ito
Senior Research Engineer, NTT Cyber Solutions Laboratories.
He joined NTT in 1985 and engaged in developmental research on geographic information systems. Recently, he has been engaged in CAS development for broadband communications and digital broadcasting.

Hidetaka Kuwano
Senior Research Engineer, Promotion Project 2, NTT Cyber Solutions Laboratories.
He received the B.S. and M.S. degrees in information engineering from Niigata University in 1993 and 1995, respectively. Since joining NTT Human Interface Laboratories in 1995, he has been engaged in R&D of video analysis, video structuring, and video OCR systems. He received the Young Engineer's Award from the Institute of Electronics, Information and Communication Engineers (IEICE) in 2000. He is a member of IEICE, the Information Processing Society of Japan, and the Institute of Image Information and Television Engineers.

Akihito Akutsu
Senior Research Engineer, Supervisor, Promotion Project 2, NTT Cyber Solutions Laboratories.
He received the B.E. and M.S. degrees in image science and engineering from Chiba University in 1988 and 1990, respectively. He has been engaged in research on IPTV systems, signal/knowledge processing aiming at video structurization, and user interfaces for interactive media.

Toshiharu Morizumi
Senior Manager, Technology and Solution Dept., mmbi, Inc.
He received the B.A. and M.M.G. degrees in media and governance from Keio University, Tokyo, in 1996 and 1998, respectively. After joining NTT Human Interface Laboratories in 1998, he engaged in R&D of application services over the broadband appliance and core technology of ISDB-Tmm. He moved to mmbi, Inc. in Oct. 2010.