INTEROPERABLE CONTENT PROTECTION FOR DIGITAL TV

B.J. van Rijnsoever and J.P. Linnartz

Philips Research
Prof. Holstlaan 4, Eindhoven, The Netherlands

ABSTRACT

Interoperability in digital TV is still hampered by proprietary content protection systems. The OPIMA specification offers a generic solution for multimedia terminals, in which the end-user's terminal is adapted to a content protection system by downloading a corresponding plug-in. This paper describes the OPIMA solution and shows how it can be applied to digital TV.

1. INTRODUCTION

Many digital TV service providers sell their content under the control of a conditional access (CA) system [1][2][3]. These systems encrypt the MPEG-2 [4] signal before broadcast and send decryption keys to the digital TV terminals (set-top boxes or integrated TV sets) of paying end-users. The terminals decrypt the signal and manage cryptographic keys and content access rights.

Although standards exist for the embedding of CA systems in the MPEG-2 multiplex [1][5], the CA system messages themselves are proprietary. A CA system provider wants full control over his system so that he can ensure its security.

Many digital TV terminals have been designed to work with a specific CA system. Such terminals limit the choice of the end-user to service providers who use that same CA system. In addition new service providers cannot easily use the installed base of terminals to deploy their services.

This lack of interoperability between CA systems and multimedia terminals is a well-known problem, and a number of techniques has been developed that offer partial solutions. In SimulCrypt solutions [6], the same content item is independently protected by several CA systems. The terminal chooses the CA system it can cope with. If these systems use the same content encryption mechanism, it is sufficient to broadcast the encrypted content only once. Each CA system however continues to use its own control messages, so that these are transmitted for all CA systems in parallel. The disadvantage of SimulCrypt solutions is that they do not scale well to a large number of different CA systems.

In MultiCrypt solutions, the end-user's terminal is instantiated to work with a specific CA system. This is achieved by inserting a module that implements all functions that are specific for that CA system. In digital TV, the DVB 'Common Interface' [7] and the OpenCable 'Point of Deployment' [8] are examples of this approach. These existing examples of MultiCrypt in digital TV have the disadvantage that they work with an expensive physical module, namely a PC card. Before an end-user can access a service, he or she first has to obtain such a physical module which is a serious impediment for the deployment of the service.

This paper presents a MultiCrypt solution for interoperability between CA systems and digital TV terminals, based on the OPIMA (Open Platform Initiative for Multimedia Access) specification [9]. The scope of OPIMA is multimedia in general, so it is much wider than digital TV alone. This solution uses a software plug-in (with the option to use a smart card in addition). Downloading of a software plug-in allows for much faster deployment.

Section 2 reviews content protection in digital TV, Section 3 introduces OPIMA, and Section 4 shows how OPIMA can be used in the context of digital TV.

2. DIGITAL TV CONTENT PROTECTION

CA systems enforce conditional content access by encryption or, equivalently, scrambling. Content decryption keys are provided only to authorized end-users. A CA system manages products, access rights and end-users. Products are sellable items like a subscription to a TV service or a pay-per-view program. A CA system may package products in many different ways that are deemed appealing for end-users. An access right is the right of an end-user to access (e.g., watch or record) a product. A CA system may define the access rights in a very detailed way by imposing restrictions. A CA system manages end-users like any commercial system manages its clients. In addition however, it is a characteristic of a CA system that end-users may try to illegitimately extend their access rights to others (e.g., by passing on content decryption keys). To prevent this, access rights are enforced by some tamper resistant environment inside (or connected to) the end-user's terminal. A smart card is an example of such an environment.

Conditional access systems for digital TV are proprietary systems. Many CA systems are however based on standards. Standardization of CA protocols facilitates interoperability between CA systems and end-user

0-7803-6536-4/00/$10.00 (c) 2000 IEEE

terminals through sharing of components. MPEG and regional standards bodies like DVB, ATSC and OpenCable have defined CA protocols. These protocols specify the encryption of content and the transfer of CA control messages in the MPEG-2 transport stream (TS), see Figure 1. The control messages themselves are proprietary for the CA system.

Two types of CA control messages are distinguished. Entitlement Control Messages (ECMs) transfer content decryption keys to the tamper resistant environment in the end-user's terminal. The content decryption key will be made available for decryption if a corresponding access right exists. An Entitlement Management Message (EMM) transfers a content access right to the tamper resistant environment of a specific end-user. In addition, EMMs are used for key management.

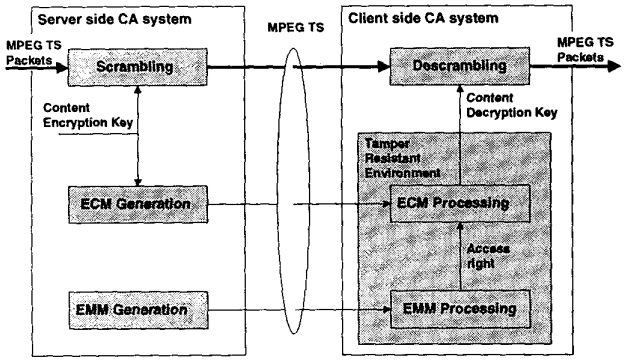

Figure 1: MPEG-2 CA system.

3. OPIMA

OPIMA is a specification that enables interoperability between content protection systems and multimedia terminals. The scope of OPIMA is very wide. Various parties from the consumer electronics industry, the IT industry, and academia have contributed to OPIMA. OPIMA is not restricted to digital TV and includes for example delivery of music through the Internet.

The goal of OPIMA is to create an open market for content delivery. In digital TV and other application areas, content protection systems tend to prevent the development of a horizontal market in which the end-user can use his or her multimedia terminal to access the content offerings of all service providers. Traditionally a terminal supports only one content protection system which severely limits the number of services that can be accessed.

The solution provided by OPIMA is a MultiCrypt solution, see Figure 2. In a MultiCrypt solution, a generic multimedia terminal is instantiated for a specific Intellectual Property Management and Protection (IPMP) system by downloading a corresponding software module or by inserting a corresponding hardware module. The module implements all functions that differ between different IPMP systems.

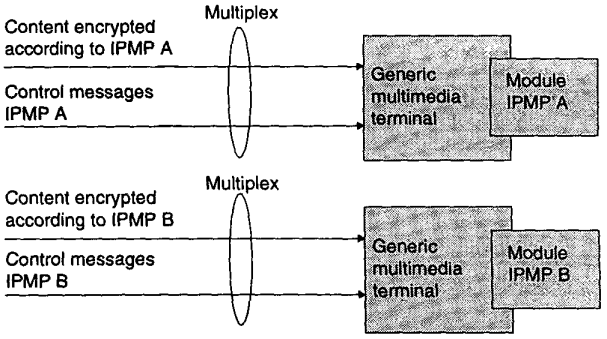

Figure 2: MultiCrypt

OPIMA defines the OPIMA peer model of a multimedia terminal, see Figure 3. The OPIMA Virtual Machine (OVM) guarantees the security of the IPMP plug-ins. These plug-ins embody content access rights and the identity of the end-user, so they must be protected from attacks by for example the end-user. How the OVM implements this protection is not defined by OPIMA; it is left as a task for an application domain that adopts OPIMA.

The OVM implements two application programming interfaces (APIs). The Application Services API enables the use of OPIMA by independent applications. Using this API, an application like for example a software player may request access to a specific content item identified by a URL.

The IPMP Services API enables MultiCrypt. It allows downloaded IPMP plug-ins (or, modules) to access the functionality of the multimedia terminal. The IPMP plug-in implements all functionality that is specific for a specific IPMP system in an application domain. Functions that are common in an application domain (like transmission and storage formats and possibly also content decryption) are implemented by the OVM.

The IPMP Services API also allows for communication with a smart card at the command level [10]. This means that the IPMP module in Figure 2 may be a combination of software plug-in and a smart card.

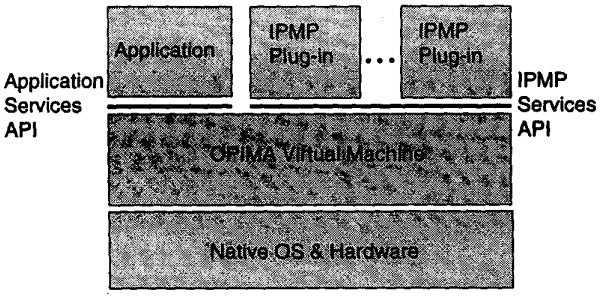

Figure 3: OPIMA peer model

OPIMA defines Secure Socket Layer (SSL) as the secure plug-in download protocol [11]. The SSL protocol is a secure authenticated channel between plug-in server and OPIMA peer. The protocol ensures the secrecy and the integrity of plug-in code during downloading. Also it allows mutual authentication of server and OPIMA peer. The server will verify that the OPIMA peer is a trusted peer and vice versa. This requires that the plug-in server and the OPIMA peer use certificates authenticated by a common certification authority.

4. APPLICATION OF OPIMA TO DIGITAL TV

A digital TV terminal may implement an OPIMA Virtual Machine, and CA system specific processing of control messages may be implemented as an IPMP plug-in. The IPMP Services API offers the plug-in access to all terminal functions it needs. The API is abstract in the sense that it is independent of the type of content or the type of multiplex that is protected by the CA system. All content or multiplex specific functions are implemented by the terminal, so there is a decoupling of content protection control on the one hand and content processing, multiplexing and transmission on the other hand.

The IPMP Services API also offers access to a standard smart card. Many CA systems use a smart card. The smart card serves as a store for access rights and cryptographic keys. Further it implements all processing of ECMs and EMMs. In that case one of the tasks of the IPMP plug-in is formatting of smart card commands and interpreting of results.

The subsections below describe how the OPIMA model supports the main CA process: content decryption and updating of access rights.

4.1 Content decryption

The process of content decryption is initiated by the end-user who selects a service protected by a CA system. Tables in the MPEG-2 Transport Stream indicate which CA system is used for the protection. If this CA system is not available in the terminal, a plug-in download procedure may be initiated, see Section 3. After the corresponding plug-in and, if applicable, a corresponding smart card have been obtained, the following procedure is executed between plug-in and OVM:

1. Using the *abstractAccessToContent* method of the IPMP Services API, the OVM indicates to the plug-in to which content item access is requested. The OVM also indicates the nature of the access (e.g., rendering or copying) and the destination of the content. The content item is identified to the plug-in by a generic identification. This identification is used to refer to the content item in all communication between plug-in and OVM.
2. Using the *obtainContentRules* method, the plug-in subscribes to the ECM stream associated with the requested content item. The plug-in uses the content identification that was earlier provided by the OVM. Content encryption keys, and thus ECMs, may change frequently. This is why a subscription model is used. The OVM will filter the MPEG-2 TS in order to retrieve the ECMs.
3. Upon arrival of an ECM, the OVM will pass it to the plug-in using a call back function. The plug-in will process the ECM to obtain the content decryption key. This processing involves ECM decryption and authentication, and verification that an access right for the requested content exists. If not, it may be possible to acquire the access right, see Section 4.2. A dialog with the end-user may be required to confirm that an existing access right may be used (e.g., a password dialog to ensure parental guidance). The *sendMessageToUser* method can be used for this purpose. The IPMP Services API offer functions similar to a cryptographic API. If a CA system uses a smart card, the smart card will do most ECM processing. The plug-in will embed the ECM in a smart card command and interpret the smart card response. The plug-in may use the *sendAPDU* method to submit commands to the smart card, after the smart card communication has been set up.
4. After an ECM has been processed successfully, the content decryption key is known to the plug-in. The OVM implements a content decryption engine. After the decryption engine has been set up, the plug-in will submit the key to this engine using the *updateDecryptionKeys* method. This method also allows for synchronization of key changes.

4.2 Updating access rights

Before an end-user is allowed access to content, a corresponding access right shall be established. In a broadcast scenario the access rights are stored locally in the terminals, so that no contact between clients and service providers is required for clients that access services

for which they are already entitled. In smart card based systems, access rights are stored in the smart card.

The IPMP plug-in may use a point-to-point communication channel to contact the service provider. In addition it may communicate with the end-user through corresponding API calls. The IPMP plug-in may use these facilities to request new access rights from the service provider.

Alternatively, it is possible that the end-user contacts the service provider using means not defined by OPIMA. In that case, the service provider sends an EMM confirming the access right to the OPIMA peer either using the MPEG transport stream or using a point-to-point connection. The IPMP plug-in may ask the OVM to filter specific EMMs out of the MPEG stream, using the *obtainUserRules* method in the IPMP services API. In calling *obtainUserRules*, the plug-in passes to the OVM the user identification needed for filtering. Again, the OVM implements all functions specific for an MPEG-2 transport stream. Alternatively, the IPMP plug-in may wait for the service provider to open a point-to-point connection by calling the *addConnectionListener* method.

5. CONCLUSIONS

The OPIMA solution for interoperability between content protection systems and multimedia terminals is applicable in the application domain of digital TV. If applied, it will ensure a horizontal market for set-top boxes, integrated digital TVs, and other multimedia terminals that provide access to digital TV services protected by conditional access. This is of great benefit to consumers and facilitates the entrance into the market for new service providers.

OPIMA is a framework. Its application requires further specification, especially of the IPMP Services API. An example is the choice of a specific content encryption algorithm. Further specification is a task for application domains that choose to adopt OPIMA. The application domain has to identify the common elements (standards) followed by the content protection systems in that domain. DVB for example specifies how to embed ECMs and EMMs in the MPEG-2 transport stream. It also specifies a content encryption algorithm ('Common Scrambling Algorithm'). Note however that the management of access rights and clients is and remains proprietary for the content protection system. Smart card based systems can continue to use their existing smart cards.

An application domain using OPIMA has to introduce a certification authority in order to facilitate secure downloading of IPMP plug-ins into trusted multimedia terminals.

6. ACKNOWLEDGEMENT

OPIMA is an initiative of Leonardo Chiariglione (CSELT). The OPIMA specification 1.0 was finished in October 1999. Many people have participated in the OPIMA process, and their contributions are amply recognized.

7. REFERENCES

[1] "Functional model of a conditional access system", *EBU Technical Review*, pp. 64-77, Winter 1995.

[2] Guillou, L.C. and J.-L. Giachetti, "Encipherment and conditional access", *SMPTE Journal*, pp. 398-406, June 1994.

[3] Macq, B.M. and J.-J. Quisquater, "Cryptology for digital TV broadcasting", *Proceedings of the IEEE*, vol. 83, no. 6, pp. 944-957, June 1995.

[4] "Generic Coding of Moving Pictures and Associated Audio: Systems", *ISO/IEC 13818-1*, 1996

[5] "DVB; Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems", *European Telecommunications Standards Institute ETR 289*, 1996.

[6] "DVB SimulCrypt; Part 1: Head-end architecture and synchronization", *European Telecommunications Standards Institute TS 101 197-1*.

[7] "Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications", *CENELEC EN 50221*, 1996.

[8] "Point of Deployment Module Interface Specification", *Society of Cable Telecommunications Engineers, DVS 131*.

[9] Open Platform Initiative for Multimedia Access, "OPIMA Specification", version 1.0, *IEC/ITA*, 1999, downloadable form http://www.iec.ch/opima/

[10] "Identification cards – Integrated circuit(s) cards with contacts", *ISO 7816*, 1987.

[11] "The TLS Protocol Version 1.0", *IETF RFC 2246*, downloadable from http://www.ietf.org/