SECURE CONTENT MANAGEMENT IN AUTHORISED DOMAINS

S.A.F.A. van den Heuvel, W. Jonker, F.L.A.J. Kamperman, P.J. Lenoir

Philips Research, The Netherlands

ABSTRACT

Authorised Domains (AD) are introduced by DVB as a means to enable controlled electronic distribution of digital content. The main aim of an AD is to respect both the content provider's and consumer's interest, in the sense that the consumer is free to access and distribute content within the entire AD, while at the same time the rights of the content owners and service providers are covered by imposing strict import and export rules to prevent unlimited digital copying the content across domains. In this paper we present the requirements, an information model, and architecture for a specific AD realisation.

INTRODUCTION

Recent developments in content distribution technologies (i.e. Internet and removable media) make it much easier to exchange content than ever before. The rapid adoption by consumers shows that such technologies really address their needs. A side effect is that they also enable easy illegal copying and distribution of content. The content industry sees this latter development as a threat to their business and acts on it by lobbying for content protection technologies and legislation.

For the future we can expect that (wireless) networking between (portable) devices in the home and between homes will grow in importance, given the convenience it will bring to consumers for accessing services and content. Consumers eventually will require from connectivity technology that it enables access to their content on every device that they own, at any time that they want, and at any place that they like. That means for instance that they require access to their home audio collections from their car or from a portable audio player.

The current situation with respect to content protection systems is fragmented. Firstly, for each new interface technology and (physical) storage medium, a new protection system has to be developed and introduced into the market, e.g. (1, 2, 3). Secondly, the current copy protection technologies are mainly targeted to limiting content exchange between devices in the home. It is clear that such an approach is not suitable given the trend to connect all (portable) devices using wired or wireless connectivity technologies. It is also clear that the consumer wishes in this field cannot be denied and that digital connectivity technologies will arise anyhow, although these developments will increase the worries of the content industry.

In this paper we will present a technology in which we try to find an integrated content protection solution that serves both the interests of the content owners and the content consumers. The main concern of the content industry is to limit the uncontrolled distribution of illegally copied content, while the main concern of the consumer is to have uncomplicated access to the content of his choice.

These requirements come together in the concept of the authorised domain (AD), a controlled network environment inside which content can be relatively freely used, but which limits the crossing of content across its border. Every device that belongs to an authorised

domain can have access to the content in that domain. Within the domain, issues like replication of content and rights will be solved in such a way as to optimise the functioning of the network and the devices. The exchange of (copyrighted) content between ADs will be bound to strict rules. The AD concept is currently being discussed in standards bodies like DVB (4), TV-Anytime (5) and is being investigated by the industry (6).

In the following sections we will provide a list of requirements that then will be used to obtain a more formal definition for authorised domains. Based on this definition we will develop a functional specification and then come to architectural choices for an AD implementation. We end with conclusions.

DEFINITIONS AND REQUIREMENTS

In its CFP (7) the DVB-CPT[1] group has defined an AD as follows:

> A set of DVB-CPCM[2] compliant functional units, that controls the flow of content and the content format. The AD represents an environment of trust for the authorised use of copyrighted content. The authorised domain may consist of several, potentially disconnected, segments of a users home network. This includes the temporary connection of mobile devices. A virtual "connection" of network segments by portable media needs to be taken into account.

Important in this definition is the fact that within an AD content access is rather unrestricted, while content exchange between ADs is under strict control. In the definition, and also in this paper, authorised domains are centred around the user's house, although centring around other environments is possible as well. In the case that an authorised domain encompasses the user's home environment we call it a *Household Domain*.

Requirements

As mentioned before, the authorised domain concept tries to cover both the requirements from the consumers (and CE industry) and the content providers. We will therefore develop requirements from both points of view.

Content Access

From a consumer's point of view, unrestricted and uncomplicated access (including options for editing, storage, trick-play, etc.) to (legally) acquired content within the authorised domain should be possible. Furthermore, consumers require some form of content exchange between authorised domains, although they should understand that unlimited exchange is prohibited.

Device management

Consumers further require that they can manage the domain without hassle. This includes registration and deregistration of devices (stationary and portable devices, the car-stereo etc.). Moreover registration and deregistration should be possible without the requirement to be necessarily connected to another device or to have an on-line connection to some service provider, i.e. no back channel required.

---

[1] DVB technical module sub-group on copy protection technologies

[2] Copy Protection and Copy Management

The content owners desire an AD solution, which makes it impossible that the whole world converges to one AD; an AD should be centred on a household. Any user and device management system should at least enforce this domain limitation.

Content owners further desire compliancy of devices, i.e. devices obeying the rights, and mechanisms to revoke/renew hacked devices.

Rights Management

Consumers expect that they can add rights (and content) to the domain, but that they also can pass them along to others again. Rights include e.g. play rights, one-generation copy rights, etc.

The main concern of content providers is Internet redistribution. Therefore they require strong limitations on rights and content exchange between authorised domains.

It further is required that DRM and Pay-TV systems can distribute content to ADs and can connect to ADs. To achieve this we assume that the architecture of an AD DRM resembles existing DRM architectures, meaning that access to content is controlled by rights (8).

FUNCTIONAL SPECFICATION

In order to focus on the core elements (devices, media, rights (+content), and users) and not to make any implementation assumptions we refine the DVB-CPT definition to:

> *An Authorised Domain is an environment of (networked) devices, media, rights and users; in which users and devices handle content according to the rights.*

We mention networking as an option in this definition, to include devices that may not always be on, or even do not have a network interface at all (e.g. portables). We therefore abstract from the specific interconnection method of elements within the AD. Furthermore this definition does not define the environment of the Authorised Domain, e.g. is not limited to a household with a home network. The remainder of this paper, however, will focus on an AD in and around the user's house, the Household Domain.

Outline of the specification

In Figure 1 we present the AD information model in UML (9) notation. The model shows information objects and a selected number of operations, which are explained in Table 1. We only list the operations that govern membership of the AD. Note that we consider media as everything on which digital information can be stored. Devices can have built-in storage (media), e.g. a hard disk drive, or can employ removable media, such as optical discs. Note that the network itself is *not* considered to be a medium.

From the model in Figure 1 we can distinguish the following type of operations:

- User management operations: join and leave
- Device management operations: register and deregister
- Rights/content management operations: import and export of content and rights

This model can easily be extended on the relation between rights and operations and on operations on objects. Such an extension is, however, beyond the scope of this paper and will be further elaborated on in future work.
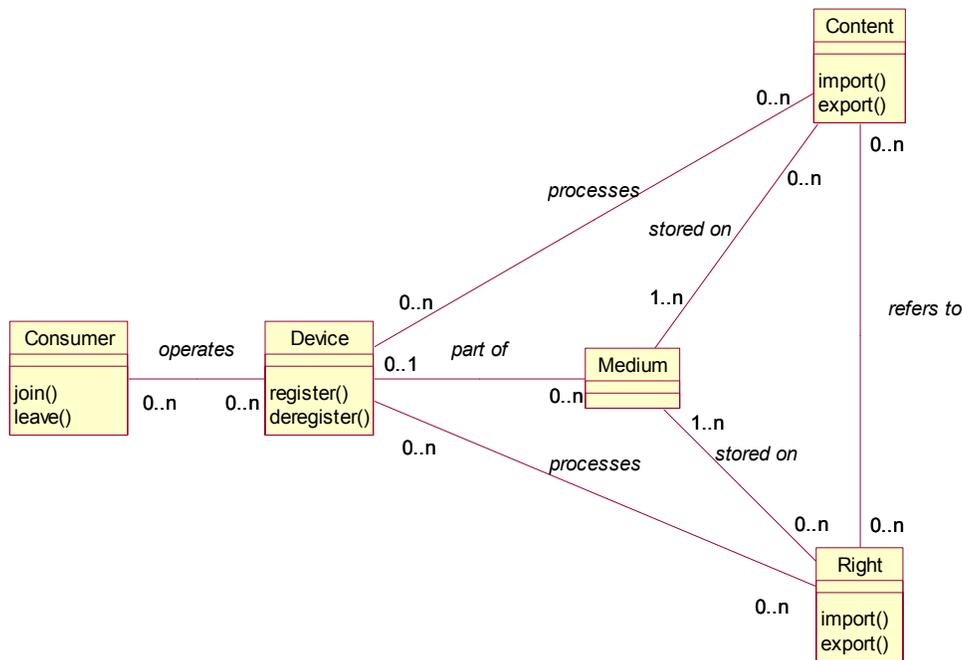
Figure 1 - Entities and their relationships in the Authorised Domain

Right	A Right expresses what may be done with Content.
Device	A Device is equipment or hardware component with processing and/or storage capabilities that can perform operations on Content.
Content	Content is a digital item.
Medium	A Medium is a carrier on which content can be stored.
User	A user is a person who is able to operate devices.
processes	Processes refers to the actions performed by a device to perform operations on content which takes the rights into account.
Stored on	Stored on refers to the fact that content has to be kept somewhere.
operates	Operates refers to a person controlling a device according to the supplied user interface, e.g. by pressing buttons.
part of	Part of means that a single element may form a composite element together with other elements and performs a certain role there.
refers to	Refers to indicates that a right is linked to one or more content items and the rights associated with content can be described in zero or more right objects.

Table 1 - Explanation of information objects and operations for AD model.

ARCHITECTURE AND IMPLEMENTATION

As explained in the previous section, device, rights, and user management are the basic functions for Authorised Domain implementations. In this section, an architecture of the domain is defined based on these basic functions.

We will base our AD implementation on device and rights management, and not on user management. In practice the latter would imply the availability of easy, convenient, and acceptable ways of identifying users (persons) by devices, e.g. on the basis of biometric data. At this moment in time we consider this route too complicated and therefore we will not consider it any further.

Another important aspect concerning devices is device compliance, i.e. the effective enforcement of the content rights. This includes aspects such as robustness of device implementations, but also device revocation, and renewability. These last two aspects enable the system to restore compliance after a security breach, such as the leakage of cryptographic keys. We will not further elaborate on this function as a lot is already known in this field (2, 10) and we previously did assume that such functionality is in place.
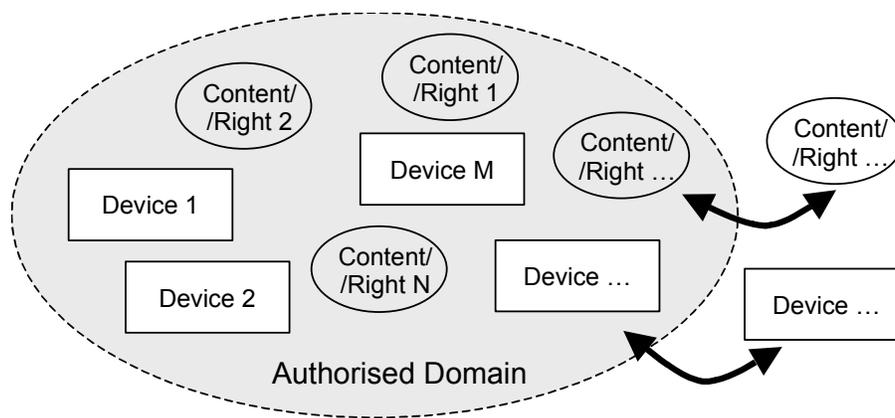

Figure 2 - Schematic representation of an authorised domain.

We will develop the architecture with the help of the model in Figure 2, which is derived from a subset of the model in Figure 1. In Figure 2 the dashed line represents the boundaries of the authorised domain. A number of devices and rights/content reside inside the domain. The figure further shows that rights can be imported and exported from the domain, and that devices can be registered and deregistered.

Architectural considerations

AD device and rights management can be implemented either centralised or decentralised (i.e. distributed). A centralized solution can be either local, i.e. at home, or remote at e.g. a service provider. Given the requirement that the solution should also work without an external connection we will abandon remote centralized solutions. This leaves us with local centralised and local distributed solutions.

Given the requirements that the solution must work for portable devices, which are mostly off-line, centralised rights management is not useful. This implies that rights management should be done in a distributed way (portable device should be able to carry content and rights!). On the other hand we need a solution for changing rights that can best be handled in a central way.

Concerning device management we can remark that both centralised and distributed solutions can be used depending on the requirements. Strict device management is required to prevent that "the whole world" can join into a single authorised domain. As an initial approach it seems logical to handle this in some centralised way.

The considerations above lead us to Figure 3, representing the devices in an authorised domain. As can be seen from the figure, typically one device will perform AD device management (ADDM), while all devices will perform rights management (RM), i.e. are able to (securely) store rights.
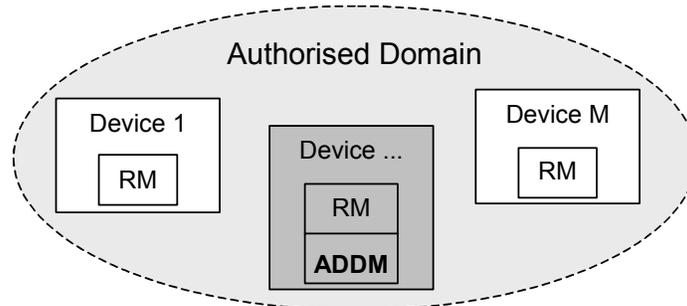

Figure 3 - Central ADDM and distributed RM.

AD device management

AD device management (ADDM) involves three types of actions:

- Device identification: Is a device part of a certain authorised domain?

- Device registration: Add a device to an authorised domain.

- Device deregistration: Remove a device from an authorised domain.

For device identification two methods are possible:

1. Common (secret) key (used to encrypt rights): The domain is comprised of devices possessing the same secret key

2. Common (secret) identifier (rights are protected by rights lockers in devices): devices possessing the same identifier comprise the domain.

Device (de)registration is done by the central ADDM. This device will first check if the conditions for (de)registering devices are fulfilled and subsequently perform the necessary actions.

During device registration, the device to be registered will obtain the AD key or identifier, if all conditions are fulfilled. The minimum required conditions are that the device is compliant and that the domain size stays within certain limitations. These conditions will be enforced by the ADDM.

During device deregistration the AD key or identifier in the device will be deleted. Furthermore, the device may contain some rights from the AD. A decision has to be taken on how to handle these rights, e.g. delete, take along, and leave. This will be explained below.

AD rights management

AD rights management involves three types of actions:

- AD rights identification: To which domain belongs a right?

- Import of rights in to the AD: Add a right to a domain.

- Export of rights from the AD: Delete/transfer a right from a domain.

Rights identification may operate in different ways:

1. A common AD key may encrypt the rights in the domain (Only devices that posses the common key can use the content key in the right).

2. A right is implicitly bound to the domain, i.e. once entered it cannot leave the domain. It is protected by devices and on secure interfaces.

The differences between method 1 and 2 relate to rights protection within the domain. In method 1, the rights are encrypted and only devices within the same domain having the same domain key can access the right. This allows the right to be stored on unprotected media. In method 2, the communication between domain devices needs to be secure and the rights are then only available within this secure communication framework. In this case, rights are only encrypted when transmitted and special care has to be taken when storing and processing the rights by devices.

Rights import is only allowed when the rights format is compliant to the rights supported by the domain and was allowed to be "exported" from its origin (typically a DRM or pay-TV system). Export of a right may only occur when it is allowed by the right. The correct handling of a right will be ensured by the compliance of the devices handling that right.

Given the considerations above we present an AD architecture that is build upon the idea that we can recognize two types of rights: Authorised Domain (AD) rights and Cross Authorised Domain (XAD) rights. The purpose of XAD rights is to transfer rights to and from an authorised domain. AD rights are for use within the authorised domain only and are derived from the XAD right. Initially XAD rights originate from the rights owner. If an XAD right is imported in to an authorised domain, AD rights can be derived from this right. AD rights may be multiplied at will in the domain, but they may never leave the domain. The XAD right will be used to control inter domain communication. For ease of management reasons only one copy of the XAD right is allowed. However, if XAD rights leave the domain, the derived AD rights must be deleted. This can be accomplished (best effort) by sending a AD-right revocation message from the device that stored the exported XAD right.

We will describe the difference between XAD and AD rights by means of an example. Assume that content with the XAD right (CopyOneGeneration+Play) is imported into the domain AD0. The derived AD right will be (Play), which may be distributed to all devices within the domain. As "copy" rights are considered to be inter-domain actions (replication within the AD is not restricted!) AD rights will not contain such rights.

When the XAD right (+content) is copied to domain AD1, the AD1 XAD right will be changed into (Play). The XAD right of AD0 will remain (CopyOneGeneration+Play). Both domains will have the AD right (Play), which may be distributed freely within each domain. In case the original XAD right was (CopyOnce), the XAD rights in both AD0 and AD1 would have to be changed into (Play).

Rules of operation

In the architecture as described above, the AD is governed by the following rules concerning rights:

- Only XAD rights may enter or leave an AD (if allowed by the XAD right of course), AD rights never may leave.

- Only one copy of any XAD right may exist in the domain for rights management reasons (counting mechanisms, i.e. limited number of copies, can now easily be taken care of),

- For devices leaving the domain this means: AD rights on such a device must be deleted, while XAD rights may travel along with the device (or can remain in the original domain, depending on the user's preference). If the XAD right leaves the domain the corresponding derived AD rights must be deleted.

CONCLUSIONS

We have presented an information model and outline of an architecture for Authorised Domains, where we focussed on the core functionality of ADs. An important contribution of our architecture is the clear separation between AD device and AD rights management. In addition, we explicitly distinguish between AD and Cross-AD (XAD) rights to control the content import and export between ADs. We are currently working on an implementation of the architecture in order to validate our design decisions. For this implementation we use a collection of different usage scenarios in which content is manipulated in different ways within and between ADs.

REFERENCES

1. Eskicioglu, A. M. , Delp, E.j. *An overview of multimedia content protection in consumer electronics devices*. Signal Processing: Image Communication, Elsevier, 2001.

2. DTCP, http://www.dtcp.com/.

3. CPRM, http://www.4centity.com/.

4. DVB, http://www.dvb.org/.

5. TV-Anytime Forum, http://www.tv-anytime.org/.

6. SmartRight, http://www.thomson-multimedia.com/.

7. DVB technical module sub-group on Copy Protection Technologies. *Call for Proposals for Content Protection & Copy Management technologies*. TM2549, DVB-CPT rev. 1.1, 5 July 2001.

8. Kamperman, F.L.A.J., Heuvel, S.A.F.A. van den, Verberkt, M.H., 2001. *Digital Rights Management in Home Networks*. Proceedings of the International Broadcasting Convention (IBC), September 2001. pp. 70-77.

9. Grady Booch, James Rumbaugh, Ivar Jacobson. *The Unified Modelling Language User Guide*. Addison Wesley, 1999.

10. ITU-T Recommendation X.509. *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*, 1995.

ACKNOWLEDGEMENTS