DRM Interoperability and DLNA Devices

TOMAS SOMMAR

KTH Computer Science
and Communication

Master of Science Thesis
Stockholm, Sweden 2011

DRM Interoperability and DLNA Devices

T O M A S S O M M A R

Master's Thesis in Media Technology (30 ECTS credits)
at the School of Computer Science and Engineering
Royal Institute of Technology year 2011
Supervisor at CSC was Tommo Reti
Examiner was Nils Enlund

TRITA-CSC-E 2011:023
ISRN-KTH/CSC/E--11/023--SE
ISSN-1653-5715

Royal Institute of Technology
School of Computer Science and Communication

KTH CSC
SE-100 44 Stockholm, Sweden

URL: www.kth.se/csc

DRM Interoperability and DLNA Devices

Abstract

This degree project studies how both content owners' demand of content protection and users expectations of content portability can be met.

As content owners' demand of content protection when delivering premium content to end customers, service providers need to fulfill these requirements by implementing content protection systems. At the same time, end customers expect content to be portable across different devices and platforms. This degree project study of technology enabling Digital Rights Management (DRM) interoperability can be used to meet both content owners' and end customer's expectations. The degree project concludes that at this stage approaches proposed by a set of consortiums and organizations are still too immature for implementation by a single service provider. Furthermore, two content protection concepts, Link Protection and Authorized Domain (AD), have been evaluated. This degree project concludes that the AD is a stronger candidate for implementation due to the flexible business and user models, as well as the marked adoption the concept can deliver. In addition, three different DRM technologies that utilize the AD concept are evaluated against the amount of flexibility, platform independence, as well as market adoption the DRM technologies deliver. The degree project report suggests that the DRM technologies Microsoft PlayReady and Marlin are both strong competitors amongst these technologies.

Moreover, this degree project studies Digital Living Network Alliance (DLNA) technology and how such technology can be used to share and transfer content between devices in a home networked environment. Special interest is put into how DRM technologies utilizing the AD concept can be combined with DLNA technology. The degree project concludes that to create a union of these technologies, a DRM client supporting the current DRM system in the DLNA devices is needed.

DRM Interoperabilitet och DLNA Enheter

Sammanfattning

Då innehåll levereras till slutkunder i digital form har innehållsägarna strikta krav på att innehållet ska skyddas från otillbörligt användande. Samtidigt som innehållsägarna ställer detta kvar så vill kunderna kunna konsumera sitt innehåll på ett flertal olika terminaler och plattformar. För att kunna möta upp de båda viljorna har detta examensarbete studerat och utvärderat tekniker föreslagna av olika konsortiums och organisationer som möjliggör Digital Rights Management interoperabilitet. Examensarbetet kommer till slutsatsen att de föreslagna teknikerna ännu inte är mogna nog för en enskild tjänsteleverantör att implementera. Vidare har examensarbete studerat två olika koncept för skydd av innehåll: Link Protection och Authorized Domain (AD). Examensarbetet kommer till slutsatsen att AD konceptet är en starkare kandidat för implementering än Link Protection konceptet då AD konceptet erbjuder flexiblare affärs- och användarmodeller samt starkare marknads acceptans. Därtill så utvärderar examensarbetet tre olika DRM tekniker som implementerar AD konceptet. Slutsatsen dras att Microsoft PlayReady och Marlin båda är starka konkurrenter bland dessa tekniker.

Examensarbetet studerar även hur Digital Living Network Alliance (DLNA) teknik kan användas för att dela och överföra innehåll mellan olika enheter i det digitala hemmet. Intresse riktas mot hur DLNA teknik kan kombineras med DRM teknik som implementerar AD konceptet. Examensarbetet kommer till slutsatsen att en sådan kombination är möjlig, och för att uppnå en sådan kombination måste en DRM klient som stödjer det aktuella DRM systemet integreras i DLNA enheterna.

Foreword

I would like to thank TeliaSonera and the Royal Institute of Technology for letting me conduct this degree project as a part of their collaborative work in the Next Generation Media Project. I would also like to give special thanks to my supervisor at the Royal Institute of Technology, Mr. Tommo Reti, for his excellent advice and support during my work in this project.

Furthermore, I wish to thank Mrs. Annika Kilegran, Mr. Bruce Horowitz and Mr. Göran Edbom at TeliaSonera for their advice and support during my work at TeliaSonera.

Last, I wish to thank Mr. Joakim Svensson at the Royal Institute of Technology and TeliaSonera who persuaded me into applying for this degree project.

Table of contents

Table of abbreviations

Abbreviations	
Abbreviation	*Description*
AD	Authorized Domain
ADSL	Asymmetric Digital Subrsciber Line
API	Application Program Interface
CA	Conditional Access
CDN	Content Delivery Network
CE	Customer Electronics
CI+	Common Interface Plus
CIF	Coral Interoperability Framework
DECE	Digital Entertainment Content Ecosystem
DLNA	Digital Living Network Alliance
DMP	Digital Media Project
DReaM	DRM everywhere available
DRM	Digital Rights Management
DTCP-IP	Digital Transmission Content Protocol over IP
DVB	Digital Video Broadcasting
DVB CPCM	DVB Copy Protection and Copy Management
DVD	Digital Versitale Disc
HTTP	Hyper-Text Transport Protocol
IDP	Interoperable DRM Platform
IP	Internet Protocol
IPTV	Internet Protocol Television
JPEG	Joint Photographic Experts Group

Abbreviations	
Abbreviation	*Description*
LAN	Local Area Network
MP3	MPEG-1 Audio Layer 3
MPEG	Motion Pictures Exports Group
NEMO	Networked Environment for Media Orchestration
OIPF	Open Internet Protocol Forum
OMA	Open Mobile Alliance
OMA SCE	OMA Secure Content Exchange
OPERA	InterOPERAble DRM
PC	Personal Computer
PED	Personal Entertainment Domain
PVR	Personal Video Recorder
RGW	Residential Gateway
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SDK	Software Development Kit
SIM	Subscriber Identity Module
STB	Set Top Box
TS	Transport Stream
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VOD	Video on Demand
WMDRM	Windows Media Digital Rights Management
WMDRM-ND	WMDRM for Network Devices

Table 1: Abbreviations

Terminology

Content

A composition of intellectual property, e.g. feature films, music tracks, computer software, books etc.

Content owner

An entity that owns intellectual property rights of content.

Content producer

An entity that creates content. This role is often combined with content owner, and in some cases content provider.

Content provider

An entity that provides content to end users.

Copyright owner

The same as Content Owner

Device

Customer Electronics (CE) equipment with storing or playback capabilities. Typically a computer, cell phone, set-top box, game console or television set.

Digital Rights Management

Zhang Hua et al. defined DRM as: "a technology developed for protection against illegal distribution and usage of intellectual property and management of all participants' legal rights" [**1**]. This is the definition used in this report.

DRM protection

A DRM technology applied to some content. This is applied through the use of a DRM system that packages the content with the implemented DRM technology.

DRM system

An implementation of a DRM technology.

DRM technology

See Digital Rights Management.

End customer

The last entity in a value chain that acquires content in connection with a financial transaction.

End user

A person that acquires content to an end device. In contrast to the End customer, this person does not need to be involved in a financial transaction.

License

An authorization to use content under set permissions and limitations. When used in connection with DRM the license is an object accompanying either a piece of content or a bundle of content.

Piracy

The illegal act of distributing copyrighted content without prior allowances from the content owner.

Premium content

Content of supreme quality, normally provided and produced by a well-established content producer. Premium content differs from regular content in that premium content is not user generated.

Service provider

An entity that provides services such as internet connectivity, cellular network, and content providing services. Service providers with content providing services also act as a content provider.

Time-Shifting

A feature providing end users the ability to pause and/or skip forward and backward in broadcasted and/or live streamed content as well as store the content for future consumption.

User Model

A functionality enabling a use case scenario. For example, transferring and playing content from a PC to a Portable Device.

Figures

Tables

Chapter 1 Introduction

This chapter includes a problem description and a short background to the problem. It also discusses the purpose of the project, scope and intended audience.

1.1 Introduction

TeliaSonera is a telecommunications company operating in the Nordic countries, the Baltic States and in the growing markets of Eurasia. In the year of 2005, TeliaSonera announced their intent to start offering IPTV-services, an initiative that today has reached a broad customer base with over half a million paying customers.

One of the important changes in how TV is delivered to the end customer with IPTV is that IPTV is not as traditional TV broadcasting systems a one-way communication system. IPTV offers two-way communication, that is, the technology opens for the ability of the end customer to communicate back to the IPTV service. This, in turn, opens up for the possibility of a new range of services that may change the way in which end users consume media at the TV-set. Such services include Video-On-Demand (VOD) and Time-Shifting (TS) services. When providing premium content to end users content owners require the use of a content protection system to prevent that content is not used beyond what is specified in the license tied to the content [**2**]. Hence, TeliaSonera, as a service provider in the content delivery business, needs to implement a content protection system that live up to the standards set by content owners.

1.1.1 The IPTV Value Chain

TeliaSonera's IPTV service today include a VOD service, providing feature films and tv-shows from a range of production companies and TV-channels such as SF Anytime, Sveriges Television and TV4. The traverse of content, as suggested by the Open IPTV Forum [**3**], from creative process to end customer, is illustrated in Figure 1: The IPTV Value Chain:

Figure 1: The IPTV Value Chain

Content production

Produces content such as feature films, TV drama series, news, sport events, entertainment shows etc.

Content aggregation

Bundles content produced by the content producers into catalogs ready for delivery

Content delivery

Transports the bundled content to the end user (consumer)

Content Reconstitution

Converts content into a format that can be rendered by an end-user device, e.g. a STB.

The first step of the IPTV-value chain is as shown in figure x Content production. Production companies such as 20th Century Fox or HBO invests in and produces content such as feature films and television shows. This step is followed by Content aggregation, where stock of rights to the produced content is bought. Content aggregators can thus be viewed as a mediators between the Content production and the next part of the chain: Content delivery. As the name suggest Content delivery is the part where content is delivered to the end-users. The content deliverers transport the content from the content aggregator to the end-users. The last role in the IPTV value chain is content reconstitution. Content delivered to the end users is encoded and packaged in a way suitable for transport over the current medium, Content reconstitution is where delivered content is decoded and rendered to the end user. TeliaSonera plays the Content aggregation and content delivery roles in the IPTV value chain. As mentioned earlier, to minimize unwanted content proliferation, the production companies have rigid requirements on the use of copy prevention techniques, such as Conditional Access (CA) or DRM technologies, when providing content to end users [**2**]. Consequently, as a content aggregator, TeliaSonera must implement a robust CA or DRM system when offering content to end customers.

It could be argued that content aggregation and content delivery, could be cut out of the IPTV value chain, i.e. if the production companies developed their own service for content aggregation and delivery, hence letting the end customer acquiring content from them directly. However, other authors have previously noted that the acceptance of Digital Rights Management (DRM)

might benefit from a limited relationship between the production company, i.e. the content owner, and the end user [**4**] [**5**].

1.1.2 IPTV Environment

TeliaSonera's IPTV service is delivered to end users through the Internet connection of the end users home, either by ADSL or Ethernet. The content is carried by a MPEG2 transport stream to a set-top box (STB) located in the end users home. The signal is then delivered from the STB to the TV-set. The main entry point of content into the end users home is through a Residential Gateway (RGW). The RGW is a modem and router bundled into a single device. A much simplified view of how content enters the end users home is given in Figure 2: Streaming server to home-network architecture. This figure only focus on a small part of the architecture, i.e. the very last step where content traverses into the home. A more detailed description of TeliaSoneras IPTV architecture is given in 2.1.1.

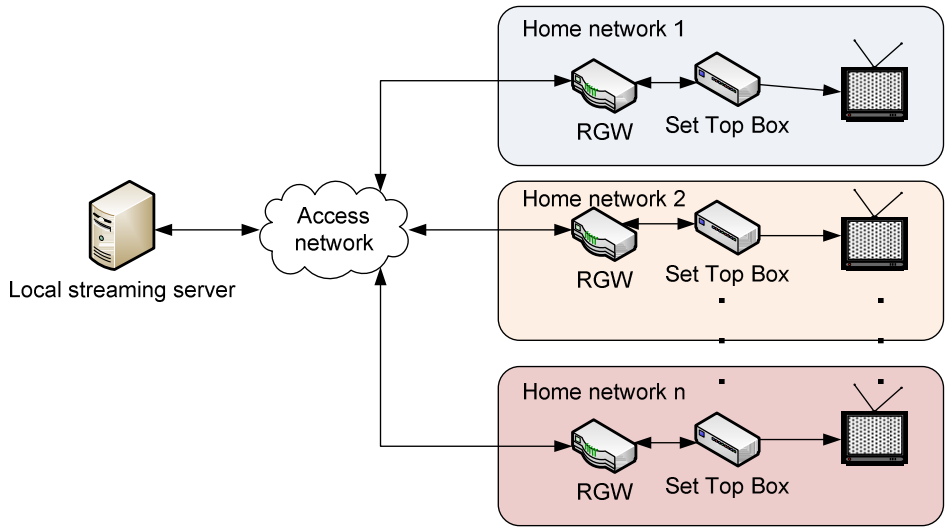

Figure 2: Streaming server to home-network architecture

1.2 Problem Statement

User behavior of digital media is changing in a rapidly fashion. People today tend to have several media devices in their home and users spend more and more time to consume digital media. At the same time as user behavior changes, many distributors of digital media protects their digital content from unauthorized copying and use by using various DRM technologies. The use of DRM protection and the ability to consume content on different devices presents some interesting interoperability problems.

The DRM interoperability problem has been recognized by many organizations such as the Digital Video Broadcasting project (DVB), the Digital Living Network Alliance (DLNA), the Open IPTV forum (OIPF), the Coral Consor-

tium and others. These organizations, among others, have published specifications and guidelines for interoperable DRM technologies.

TeliaSonera today offers IPTV services to customers via a set top box in the home and has a strong position at the Swedish market. These services include broadcasted television as well as Video on Demand (VOD). In order for TeliaSonera to be able to offer these IPTV services to be consumed on other Consumer Electronic (CE) devices than the set top box the DRM interoperability problem must be investigated. Since TeliaSonera has recognized DLNA technology as likely to be widely adopted in media consumption device, special interest is put in DLNA technology.

1.2.1 Use Cases

To further illustrate the problem statement of this report, three use cases are provided in this section. These use cases are meant to give a more thorough illustration of the problems described in this chapter.

Case 1 A PVR and a set-top box are connected to a RGW. Digital media is recorded to the PVR using a Digital Rights Management (DRM) technology implemented both in the PVR and the set-top box to protect the content from unauthorized use. With this configuration, how can content stored on the PVR be discovered by the set-top box? Furthermore, how can access be gained to this recorded digital content to offer playback functionality on the set-top box? In this scenario both the PVR and the set top-box shares the same DRM technology. This use case is illustrated in Figure 3: Project Use Case 1.

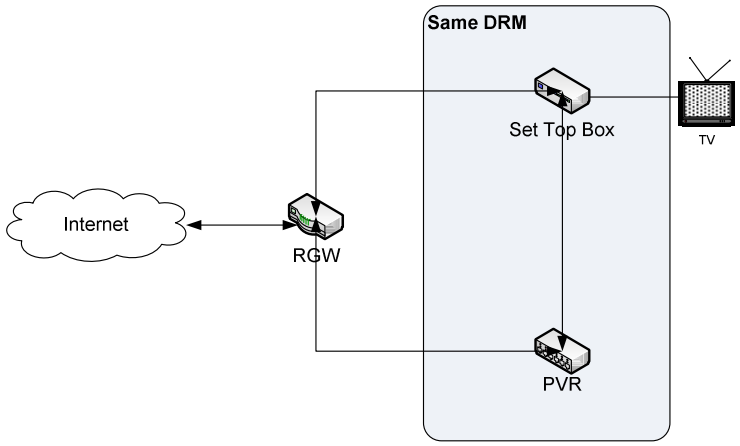

Figure 3: Project Use Case 1

Case 2 A PVR is connected to a RGW. Digital media is recorded and protected from unauthorized use by a DRM technology as in the first case. In this scenario a DLNA certified CE device is connected to the RGW, this device however does not support the DRM technology used by the PVR. Since the DRM technology is used only at one end, which is in the PVR, we cannot decode the digital content in the

DLNA device. The question that arises is: how can we decode the DRM protected content at the PVR end and then transmit it to the DLNA device, but still protecting the content from unauthorized use? The DLNA supposedly offers a solution for this situation called DLNA Link Protection. Can this be used as a way for transmitting the content to the DLNA device, and if so, how is this achieved? This use case is illustrated in Figure 4: Project Use Case 2.

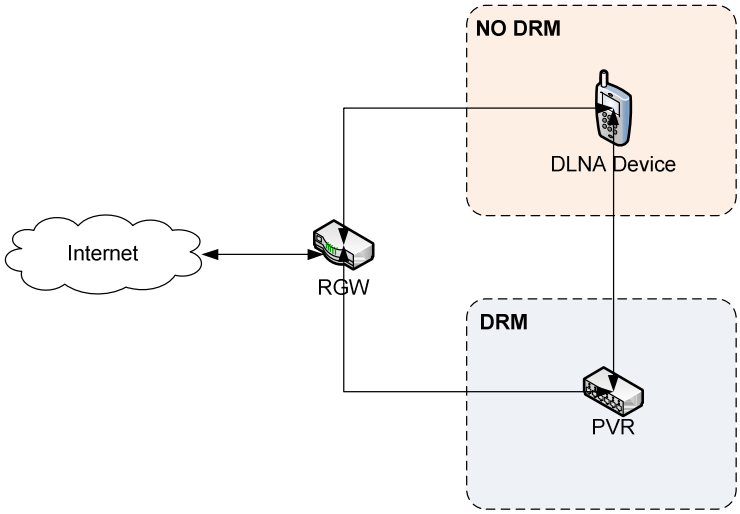

Figure 4: Project Use Case 2

Case 3 In this scenario a PVR and some other device, i.e. a Personal Computer (PC), is connected to a RGW. The PVR and the PC both supports a DRM technology, but not the same. Hence, different DRM technologies are used at each end. This raises the question: how can the PC discover and gain access to the DRM protected content in the PVR to offer playback functionality at the PC? Since different DRM technologies is used at both ends the protected contents DRM protection needs to be translated between two diverse DRM technologies. Furthermore, if the content is being decrypted in one end and encrypted at the other the content has to be protected from unauthorized use during transport. How can this functionality be achieved without compromising the contents protection from unauthorized use? This use case is illustrated in Figure 5: Project Use Case 3.

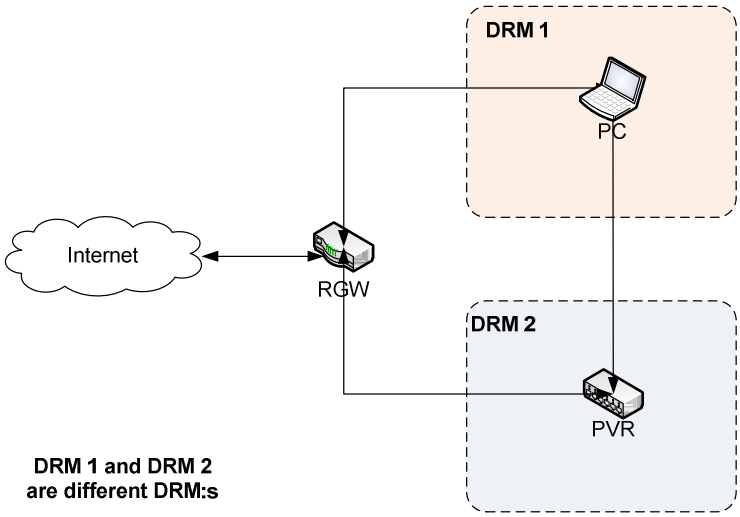

Figure 5: Project Use Case 3

This project will study the above three mentioned use cases, with the goal of providing a proposal for how the use cases can be realized.

1.2.2 Research Question

The ability to consume digital content over several different devices and at the same time protecting the content by using DRM consists of three main technical questions:

Interoperability

What frameworks for a multi-DRM environment exist, and how can such an environment be implemented?

Portability

How can DRM protection be used to protect content from illegal content proliferation while still maintaining content portability between CE devices in a digital home?

Flexibility

How can DRM protection be used while still satisfying user's expectation of flexible using rules?

Implementation

Based on the findings in the two questions above, how can a system for DRM interoperability between different CE devices be implemented, especially in the case of TeliaSonera?

1.3 Scope

As production companies require the use of DRM when distributing premium content to IPTV customers, IPTV operators need to conform to these requirements. At the same time, IPTV customers expect to be able to enjoy premium content at a range of various devices. Due to these mentioned facts, this project will study content protection implementation scenarios that can satisfy both the production companies and end users demand.

This project will not examine the possibility of circumventing any kind of DRM protection as a way of implementing an interoperable DRM platform, but instead how to consume DRM protected content under the limitations set by the DRM protection

Furthermore, this degree project will study the subject of content protection from a technical viewpoint. Thus, questions regarding juridical implications might be mentioned in the degree project report but are not pursued any further.

1.4 Methodology

The first phase of the work will consist of a preliminary study of the problem to get an overview of what work has been done by other organizations and what possible solutions are available today. This will provide an understanding of the research question and what are the main issues identified by other parties in this area. The work will continue with a study of TeliaSoneras IPTV architecture to identify requirements and criteria for a DRM interoperable system implemented in TeliaSoneras current IPTV solution. This work will mainly be carried out by conducting interviews with personnel at TeliaSonera with key-knowledge of the IPTV architecture, and studying material provided by TeliaSonera[1]. Based on the found criteria and requirements from these interviews, a set of existing interoperable DRM platforms, as well as current initiatives for DRM interoperability, will be studied and evaluated, with the goal of providing guidelines for TeliaSonera in the area of DRM interoperability.

Access to implemented DRM interoperable systems during this degree project is non-existent. As a result, it is hard to use a quantitative method to study the functionality of existing DRM interoperable systems. Furthermore, interviewing a large number of experts in the area of DRM interoperability is neither an option due to the lack of access to such expertise. As a consequence, the quality of these systems is instead estimated using a qualitative method. Throughout the degree project previous research in the area of DRM interope-

[1] TeliaSonera specific documents cannot be referenced.

rability will be thoroughly studied. Furthermore, available specifications for DRM interoperable systems will be studied with the aim of getting a solid understanding of the architecture and functionality of the systems. The gathered knowledge will provide a base for deciding however any of systems is applicable for use within the services provided by TeliaSonera.

To support in the development of valid results, a quantitative method will be used in combination with the qualitative analysis. Thus, a decision matrix (see 1.4.2) will be used to aid in the evaluation of the studied systems. The criteria and weights used in the decision matrix will be based upon the previous mentioned interviews with personnel at TeliaSonera. Consequently, the results of this degree project will in some extent be specifically developed to TeliaSonera's needs and requirements.

Furthermore, to strengthen the validity of the results, prototyping will be conducted in this degree project. Hence, a prototype for providing DRM interoperable functionality will be designed and developed. Results from the prototype implementation will be gathered and evaluated to demonstrate deliverability according to set requirements.

The following work tasks will be performed:

- Create an understanding of the DRM interoperability problem and why it needs to be solved.
- Provide a summary of previous work in the area.
- Develop a list of requirements for a DRM implementation within TeliaSonera's IPTV service.
- Study applicable content protection technology concepts.
- Evaluate existing applicable DRM solutions.
- Set up a reference application to demonstrate functionality of a content protection system.
- Evaluate current solutions and initiatives to the DRM interoperability problem

1.4.1 Reliability and Validity

As described in the previous section (1.4), distinct measurable values are hard to obtain in this degree project. To strengthen the validity of the results, a thoroughly literature study of previous research and proposed systems have been conducted. In addition, prototyping is applied during the degree project o further strengthen the validity of the results.

Since this degree project have been conducted with special consideration to TeliaSoneras needs and requirements, a high reliability of the results is harder to obtain. Moreover, the degree project has been conducted out of the view of

a service provider. Hence, it is possible that the results would vary if one instead would take on the view of other participants in the IPTV-value chain, or even broader, the content-to-consumer value chain.

1.4.2 The Decision Matrix

A decision matrix [**6**] (also referred to as the Pugh-matrix), is a tool to support decision making. Given a set of options and list of weighted criteria, each option is evaluated against the criteria. The decision matrix is used when a list of options must be narrowed down to only one choice. A typical situation for the use of a decision matrix is when given a set of possible solutions to a problem, only a single solution can be implemented.

The procedure for creating a decision matrix is as follows:

First, a list of relevant criteria for an optimal choice is identified. This list should only include criteria that are of great importance. Second, assign a relative weight to each criterion. This is done by distributing ten points among the different criteria. Now, an L-shaped matrix, with the criteria and their respective weights along one axis end the list of options along the other axis is drawn. The next step in the process is to establish a rating scale for each criterion, for example number one to five, where one is the lowest rating and five is the highest. Finally, multiply each options rating by the weight. With all the different options evaluated against the criterions the decision matrix can be used to provide a solid foundation for the choice of option. An example of a simple decision matrix is found below in Table 2: Example of a decision matrix used to calculate optimal choise of Friday night dinner.

Criteria	***Bouillabaisse***	*Meatballs*	*Weight*
Taste	5	4	5
Presentation	3	4	3
Originality	3	2	2

Table 2: Example of a decision matrix used to calculate optimal choise of Friday night dinner

The above example of a decision matrix shows that the Bouillabaisse scores 5x5+3x2+3x2 = 37 points, while the Meatballs score 4x5+4x3+2x2=36 points. Hence, the Bouillabaisse would be the better choice for Friday night dinner.

In this report the decision matrix is used as a tool for examining which platform for DRM interoperability is best suited for TeliaSonera's current IPTV solution and requirements. The set of DRM interoperability solutions is the list of options. The criterions are developed and presented in Chapter 3.

1.5 Contribution

The degree project contributions are, first, to study weaknesses and strengths of various content protection systems by reviewing documentation and specifications for such systems with regard to a few set criteria. This will in turn provide guidelines for TeliaSonera in the area of DRM interoperable platforms, as well as current initiatives taken by content production companies and device manufacturers.

Second, a prototype for consuming digital content stored locally at a Media Server using a DRM interoperable solution will be developed and evaluated. This contribution will illustrate how a DRM interoperable technology can be implemented.

1.6 Objective

The objective of this degree project is divided into three part objectives:

The first objective of the degree project is to investigate and propose a solution for how content protection can used while sharing content between different DLNA devices in a home network environment.

The second objective of the degree project is to prototype a solution for content sharing between different devices using a DRM technology that's interoperable between different devices.

Third, the degree project will evaluate and investigate previous and current approaches to interoperable content protection, and provide an overview of how the content and electronics industry is approaching interoperable content protection.

Chapter 2 Technology study

This chapter starts with a brief description of a general IPTV service architecture. Furthermore, various DRM concepts, as well as various approaches and initiatives with the aim of providing an interoperable DRM platform are examined.

2.1 General IPTV architecture

2.1.1 Architectural Overview

Bringing IPTV services to a large (and increasing) number of end users results in the need for a decentralized architecture. Hence, an IPTV service builds upon a distributed architecture depicted in Figure 6: General architectural overview of an IPTV service [**7**].

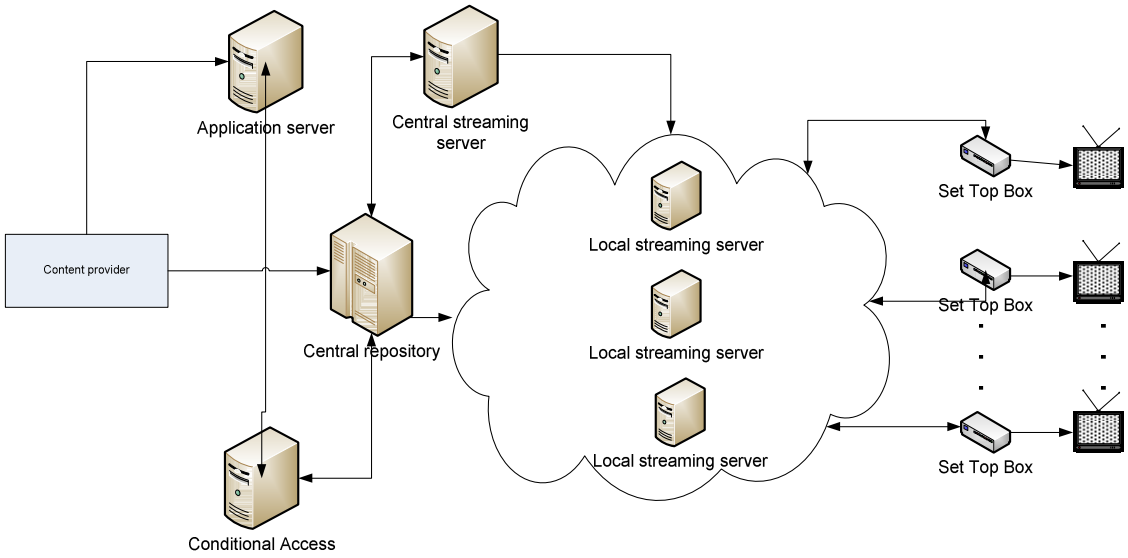

Figure 6: General architectural overview of an IPTV service

As shown in Figure 6: General architectural overview of an IPTV service, a general IPTV architecture consists of five main components: An application server, a central repository, a Conditional Access (CA) system, a set of local edge servers and set top boxes. Some components of the architectural overview are left out due to irrelevance to this report.

2.1.2 Component Description

This section contains brief descriptions of the different components in a general IPTV architecture.

Application server

The application server handles information about accounts, channels, VOD content; especially what channels and VOD content are available for a specific account.

Central Repository

The Central Repository is the main entry point for content provided by content providers. Briefly explained, the central repository is a fileserver where all content in the IPTV service is stored. All content stored at the central repository is encrypted by the Conditional Access (CA) system.

Conditional Access

Conditional Access (CA) is a content protection technology, requiring certain conditions to be met before the content can be consumed. A CA system encrypts all content that is uploaded to the central repository, and stores the decryption keys for the respective encrypted content. Before content can be consumed by an end user, access to the decryption keys has to be granted. If the user has the appropriate rights to consume the content, the CA system provides the user with the decryption key. The content can then be decrypted and consumed by the end user.

In the case of VOD content, the VOD files enter the CA system at preprocessor where the content is encrypted. After successful encryption, the VOD file is stored at a VOD server (the central repository). The corresponding keys are stored at a key storage facility. When a STB wants to access VOD content at the VOD server, the corresponding decryption key is downloaded from the key store. The decryption key is then used to decrypt the VOD content. Depending on the specific CA system, the decryption key can be stored at the set top box for up to twenty hours. Hence, if the set top box is rebooted, within the twenty hours, the decryption key does not need to be acquired again.

In the case of live broadcasted content IPTV distribution, content have to be encrypted in real time during broadcast. Thus, the broadcasted content enters a real-time encryption server. As in the previous case the corresponding is stored at a key store. When the STB tries to consume the broadcasted stream the content is decrypted with the decryption key provided by the key store.

Streaming servers (Local and Central)

Instead of having all STB's streaming from central streaming servers, which would imply a huge load on the central streaming server, the load can be ba-

lanced by the use of local streaming servers. When a user tries to access a VOD file a request is first sent to an application server. The application server replies with a URL to the geographical closest local server, and the central streaming server. If the requested VOD is not available at the local streaming server, the VOD is instead streamed from the central streaming server. This process is illustrated in Figure 7: VOD stream request.

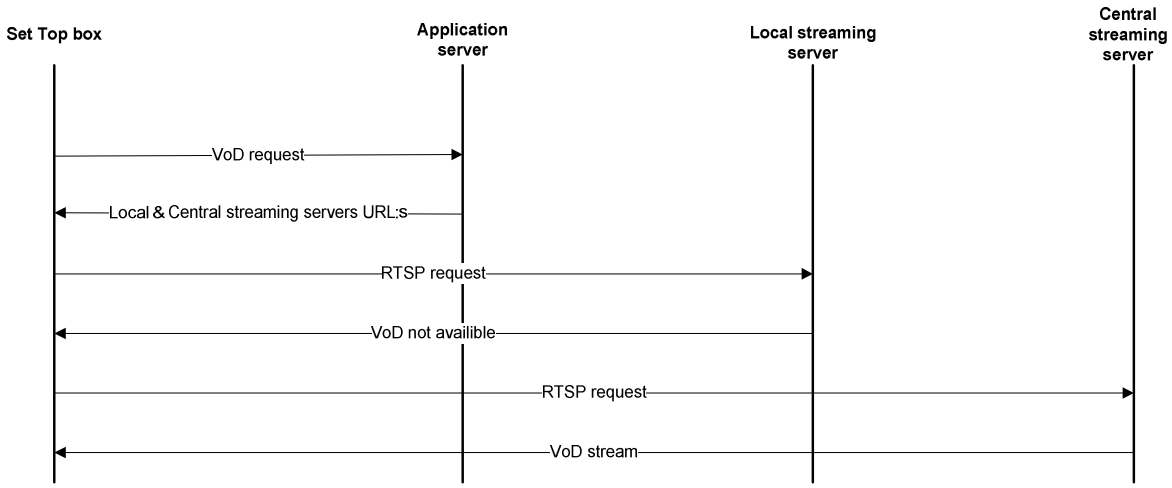

Figure 7: VOD stream request

Set top box

The set top box is the end device in the IPTV service architecture. The set top box presents a GUI on a TV set for the end user to interact with. Content is streamed in encrypted form to the set top box where the stream is buffered, decrypted (using keys provided by the CA system) and rendered for the TV.

To make STBs affordable, usually minimal hardware is contained within the STB. This implies that consideration to processing requirements has to be taken when software is developed and deployed at a STB.

2.2 A very brief introduction to cryptography

To assure that DRM protected content is used within the limitations set by the content license; a method for preventing direct access to the actual content has to be implemented. Most modern DRM systems implement this through the use of cryptography. Cryptography is briefly explained, the art of hiding information. When hiding data, the data is transformed in a way so that only parties with knowledge of one or more specific secrets can transform the text into an understandable form. The function of transforming data into unreadable data is called encryption, and the function of transforming it back into readable data is called decryption. Readable data is called plaintext, and encrypted data is called ciphertext. In modern cryptography, two components are needed to perform a encrypting or decrypting function: an algorithm and

one or more keys [**8**]. The algorithm takes the plaintext as input and uses the key to encrypt/decrypt the data. Cryptographic algorithms are categorized into two sets: symmetric and asymmetric algorithms. A symmetric algorithm uses the same key for both encryption and decryption. An asymmetric algorithm uses different keys for encryption and decryption. The asymmetric algorithm uses a public and a private key, where the public key can be distributed. The private key is kept hidden. Using asymmetric algorithms, one party can send a secret message to another party by encrypting the message using the other party's public key. Therefore prior to encryption the receivers public key need to be distributed to the sender. The algorithm for encryption is constructed in a way that only the other party with possession of the secret private key can decrypt the message. The main advantage with this kind of asymmetric algorithms is that the parties involved in secret communication do not need to physically exchange keys prior to communication, as opposed to symmetric cryptography where both parties have to agree on one single key prior to encryption and decryption.

The mathematical notion for symmetric cryptography is:

$$E_k(X) = Y, \textit{where k is the key, X is the plaintext and Y is the ciphtertext}$$

$$D_k(Y) = X, \textit{where k is the key, Y is the ciphertext and X is the plaintext}$$

The mathematical notion for asymmetric cryptography is:

$$E_{k_P}(X) = Y, \textit{where } k_P \textit{ is the public key, X is the plaintext and Y is the ciphtertext}$$

$$D_{k_q}(Y) = X, \textit{where } k_q \textit{ is the privatekey, Y is the ciphertext and X is the plaintext}$$

Symmetric algorithms are much faster than asymmetric algorithms, generally up to 1000 times faster [**8**]. As a consequence, when encrypting large amounts of data a symmetric algorithm is more effective. Asymmetric and symmetric algorithms are therefore used in combination. Using asymmetric algorithms, one party can encrypt a key and send it to another party. Now, both parties can use key with a symmetric algorithm since no other than the two can possibly have access to the key.

Modern DRM systems use the combination of asymmetric and symmetric algorithms. The content is encrypted with a symmetric algorithm and key, usually referred to as the content key. The content key is then encrypted with the receiving party's public key and sent to the receiver. Now, since the receiver is the only one in possession of the secret private key needed to decrypt the content key, nobody but the receiver will be able to decrypt the content.

When used in DRM systems, it is vital that the keys are hidden from the end user. This might seem counter intuitive, but if a dishonest end user gets hold of the keys he or she is able to decrypt the content and use it in ways not authorized by the accompanying license. Of course, the end device needs to have knowledge of the keys in order to decrypt and present the content. This is

implemented either through hardware or software implementations. These implementations have to be protected from dishonest end users with the intent of breaking the DRM system. This will not be studied any further in this degree project since it is out of scope.

2.3 Definition of Digital Rights Management Interoperability

To gain a better understanding of the term interoperability, an understanding of the term compatibility is useful. Compatibility, in a technical sense, is defined as the capability for different components of a system to be used together without special modification or adaption [**9**]. Interoperability extends the definition of compatibility to the ability of diverse hardware or software from different vendors to communicate and to seamless exchange functionality [**10**].

The definition of DRM interoperability differs between different roles in the chain of distribution [**9**]. For the consumer, DRM interoperability could be seen as the possibility to have different devices and use them with different content services. For the content producer or content aggregator DRM interoperability can signify that producer or aggregator is not locked in to one distribution channel. For the device manufacturer DRM interoperability is the ability for the manufacturer's devices to be used with different content services.

In this report, DRM interoperability will be defined as by Petkovic, et al. [**10**] , the ability for devices that implement diverse DRM technologies to share and consume content between the devices in a seamless manner.

2.4 Previous Work

2.4.1 Digital Rights Management Concepts

In the paper Identity-Based DRM: Personal Entertainment Domain, Paul Koster et al. suggests three state-of-the-art DRM concepts [**11**]: Device-Based DRM with tethered devices, device-based AD and Person-based DRM: Device-Based DRM with tethered devices, Device-based AD and Person-based DRM.

Device-Based Digital Rights Management with tethered devices

This concept builds upon the use of tethered devices. A tethered device is an end-point device that can act upon its own behalf. Content is strictly bound to one device from where it can be transferred to a finite set of other devices, under some defined rules, see Figure 8: Device-Based DRM with tethered devices. Such rules typically includes that the content can't be further transferred to any other device. The tethered devices can receive content from a

finite set of devices. An example of tethered devices concept is the Windows Media Player using Windows Media DRM.

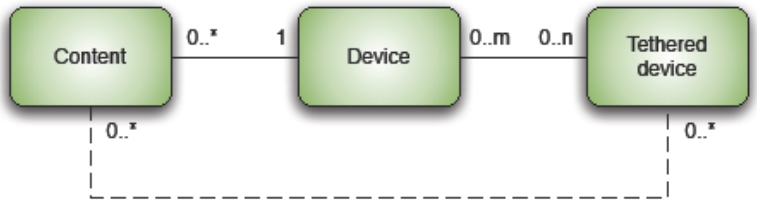

Figure 8: Device-Based DRM with tethered devices

Device-based DRM fulfills its purpose as a copy preventing technology since the content is transferred to tethered devices under strict limitations of how the content can be used. However, device-based DRM brings poor user experience to the customer due to the different rules and conditions for the main device and the tethered device. Furthermore, there is a lack of availability since content can't be consumed at another place by distributing over a network, instead of carrying devices.

Device-based Authorized Domain

In the previous concept described (Device-Based Digital Rights Management with tethered devices) content is stringently bound to devices. As a result, content can't be transferred between devices, which bring poor availability and usability to the consumers. In the Device-based AD concept content is bound to an AD instead of a device. The Digital Video Broadcasting Project (DVB) defines an AD as: *"a set of DVB CPCM compliant devices, which are owned, rented or otherwise controlled by members of a single household"* [**12**]. In a broader sense there are nonetheless any reasons to define the term to only include DVB CPCM compliant devices, since the concept is adopted in other DRM systems [**13**] [**14**], as well as current DRM initiatives [**15**]. The general idea of the AD is to let content flow freely between devices belonging to the domain, while still restricting content transactions between different AD's. The basic principle behind the AD is to instead of binding content to a device the content is instead bound to an AD, see Figure 9: Device-based AD. Devices bound to the AD can consume content bound to same AD. This approach enables users to access content on devices within the same AD, while still satisfying the content owners demand on prevention of illegal content distribution. A requirement from the content owners is that an AD is centered on a household, and obviously that it is impossible for an AD to grow to include all devices and content available in the world [**16**].

Figure 9: Device-based AD

The device-based AD approach provides good availability of protected content among the devices belonging to the AD. However, multiple users binding content to the same domain poses for possible future problems. These problems are apparent in a scenario of a user who want to take his or her content and devices with them outside of the AD, e.g. in the case of a divorce or children moving out.

Person-based Digital Rights Management

The Person-based DRM (see Figure 10: Person-based DRM) is an alternative concept where content instead of being bound to a device or AD is bound to a user. After the user is authenticated access to content is granted for the length of the authentication session. In this concept the user has the central role instead of a device or AD. This implies that content is available to a user on any device after successful user authentication.

Figure 10: Person-based DRM

This concept provides god availability of content since content can be accessed on any device after successful user authentication. Illegal distribution of content is also prevented due to the user authentication requirement. However, the user re-authentication process is a tiresome task which might irritate users. A more serious drawback of the Person-based DRM concept is the need of an authentication infrastructure that can be accessed by a wide variety of devices. Username and password authentication alone is unlikely to be sufficient for authentication since it is easily shared among users, and hard to support when the device lacks an online connection.

Personal Entertainment Domain

In this concept content is bound to a specific user, in addition to being accessible on a domain of devices, and furthermore, temporarily accessible on other devices. Hence, this concept can be described as a combination of the Device-based AD concept and the Person-based DRM concept, see Figure 11:Personal entertainment domain. This concept allows members of a household to share content by accessing content on devices bound to a user's domain, while still

demonstrating clear ownership of content, which facilitates changing social relationships. Furthermore, since content can be temporarily accessible on devices not bound to the same domain, the availability of content is increased.

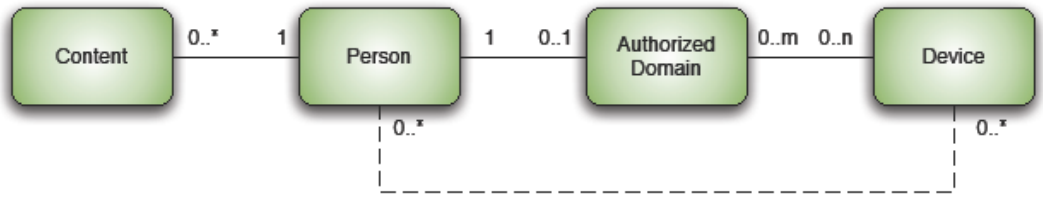

Figure 11:Personal entertainment domain

As in the case of person-based DRM, the need of an authentication infrastructure that can be accessed on a wide variety of devices might be a complication. However, since an alternative way to access content is provided, this complication is, in this concept, less significant.

2.4.2 Approaches to Digital Rights Management Interoperability

One of the earliest published papers in the area of DRM interoperability is "The long march to DRM interoperability" [**17**]. This paper has been widely referenced in related research regarding DRM interoperability. The authors suggest three different approaches to DRM interoperability:

Full Format interoperability

This approach requires all device manufacturers and content providers in the value chain to use the same DRM protection. An example is the Digital Versatile Disc (DVD) where all participants in the value chain use the same data representation and DRM protection. Hence, the end users do not experience any churn related to DRM in the DVD market. There are obvious gains with full format interoperability, such as ease of producing content, building mass market applications, and development of devices. On the other hand, developing industry standards is a long process. Adoption demands a large number of companies in the industry to accept and adapt to the standard. Also, approach is vulnerable to security breaches since a single attack at the system can compromise all simultaneously.

Connected interoperability

The connected interoperability relies upon the expectation that all devices have an internet connection and use online services that solve interoperability problems in a transparent way. Different DRM protections can coexist, and interoperability is reached by the use of translations ore bridges. However, this implies that the devices have an online connection part of the time. Using connected interoperability different parties can use different DRM protections, but still providing a sense of interoperability to the end users. However, when

content crosses the boundaries between different DRM protections the rights might be "downgraded" to the least possible amounts of rights supported by both the DRM protections, due to technical, as well as business reasons.

Configuration driven interoperability

This approach builds upon the ability for devices and software's to download components needed to gain new functionality needed to support new formats and DRM protections. This is ideally made in such a transparent way that the user do not even notice that any dynamic configuration takes place. With configuration driven interoperability online access can be minimized to when new components are downloaded to the device. On the other hand, configuration driven interoperability depends on the possibility to install an arbitrary number of components and configurations at the device. This may be a cumbersome requirement for small CE devices.

These three approaches illustrate three possible scenarios for an interoperable DRM platform. To this date, *configuration driven interoperability* is investigated by the Motion Pictures Experts Group [MPEG] [**18**], but not widely undertaken by other groups, companies or consortiums. The *connected interoperability* approach has been investigated by the Coral Consortium, who has released specifications for such a platform. The most common approach undertaken by companies and consortiums is *full format interoperability* [**19**]. However, none of the various approaches to full format interoperability has yet been widely adopted by the industry.

2.4.3 Translation

Another approach to reach a DRM interoperable environment in a home network is to translate the content from the origin DRM system to the appropriate DRM system for the receiving device. Reihaneh, et al. [**18**] suggests three architectures for such an approach:

Translation services

Translation services make use of a third party server, acting as an intermediary between two devices implementing separate DRM systems. The intermediary translates the content from the first DRM into to the DRM implemented by the receiving device. This approach is also investigated by Schmidt, et al. [**20**], whom also argues that the intermediary between the content owner and the end user can weaken the tension around DRM.

Terminal translation

Terminal translation makes use of import and export functionalities built in to the devices. Either, a device can export DRM protected

content into another DRM system used by a receiving device, or the receiving device can translate the content during import, from the origin DRM system into the DRM system implemented in the receiving device.

Pre-Export

Pre-export build upon the idea that when a device acquires content from a content provider, contracts for both the acquiring device DRM system as well as other DRM systems the content might be exported to is provided with the content. The contracts can be used to repackage the acquired content into a DRM system supported by another receiving device. This requires the content provider to have knowledge of what DRM systems the content may be exported to. Furthermore, there is an increasing demand on the amount of storage capacity on the acquiring device. An advantage is that the amount of computation capacity on the exporting and importing device during transfer decreases, without the need of a third party translation service.

A possible problem with translation between DRM systems is the existence of rights in licenses belonging to different DRM systems that can't be directly mapped between the systems [**18**]. This might imply that rights might be downgraded when content is translated between different DRM systems.

Other issues when translating between DRM systems are economic and legal issues [**18**]. For example, some DRM vendors might not want to enter into translating agreements. Furthermore, if a DRM system is compromised and protected content is illegally proliferated across the internet content owners might want to hold the content provider liable for the losses, even if the content DRM system used by the content provider is not the one compromised.

2.5 State of the Art Digital Rights Management Technologies

Do this date, several organizations have developed DRM systems that promote the ability to move and consume DRM protected content between different devices. These systems hope to augment the consumers acceptance of DRM by reducing the experienced churn when consuming protected content across a users complete set of devices.

2.5.1 The Open Mobile Alliance

The Open Mobile Alliance (OMA) was formed in 2002 to facilitate collaboration between over two hundred companies including mobile operators, device manufacturers, network suppliers as well as content and service providers. The

OMA delivers specifications that provide interoperability between different devices, operators, networks and service providers [**21**].

OMA has developed a DRM system for protection of content delivered to mobile devices, called OMA DRM. Two versions of OMA DRM exist today. OMA DRM 1.0 [**22**] is a basic DRM standard without support for any strong protection of content, where OMA DRM 2.0 [**23**] makes use of encryption to protect content. An extension to OMA DRM called OMA Secure Content Exchange (OMA SCE) [**24**] enables OMA DRM protected content to be moved and consumed across an end customer's domain of devices, including other devices than mobile devices. That is, OMA SCE makes use of the AD DRM concept previously described in 2.4.1. Furthermore, the OMA SCE enables content to be temporarily consumed at devices in near proximity to the device containing the protected content, even if the devices in the near proximity is not in the end users domain of devices.

To facilitate DRM interoperability, OMA SCE extends the functionality in OMA DRM to include import and export functionality to enable translation into other DRM systems.

2.5.2 Marlin

The Marlin Developer community was founded in 2005 by Intertrust, Panasonic, Philips, Samsung and Sony. It provides an end-to-end digital rights management toolkit, consisting of specifications as well as Sample Implementation Kits (SDK's) to develop a complete DRM system [**25**]

Marlin resembles the PED concept described in 2.4.1, and has a clear objective to let the user be in control of acquired content [**26**]. The rights management in Marlin is based on the Octopus DRM engine [**27**], where usage models are built upon a graph model. The graph includes nodes and links, where node objects are used to represent entities such as users, authorized domains, devices and content where the links between nodes represent relationships. The right to consume Marlin protected content is evaluated by determining if the content node is reachable by the user node [**27**].

One of Marlin's advantages is the flexible user models. These include the ability to:

- Give acquired content to somebody else.
- Associate content with another AD, as would be desirable in the case of a child moving out of the house or in the sad event of a divorce.
- Leverage temporary authorization to allow access to content at a device that is not member of the user's device.

The above three user models are all very desirable for a DRM system that aims at meeting end users expectations of content portability, as well as rare among current state-of-the-art DRM systems.

The main components of a Marlin DRM system is depicted below in Figure 12: Marlin DRM architecture.

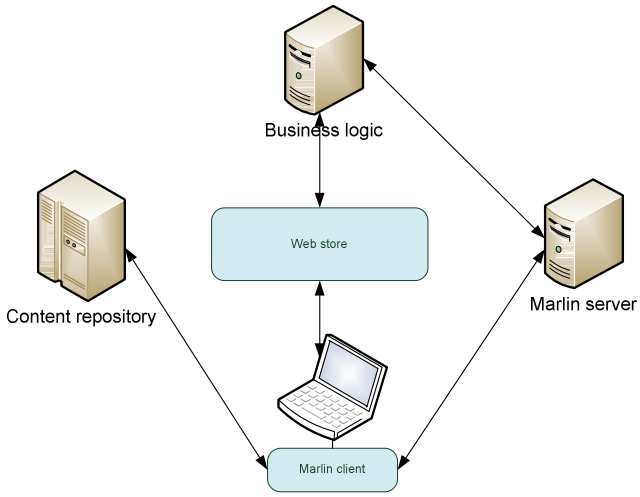

Figure 12: Marlin DRM architecture

2.5.3 Microsoft PlayReady

To meet customer's demand of content portability, Microsoft advanced their Windows Media DRM (WMDRM) into a new DRM system called Microsoft PlayReady. The biggest improvement is the adoption of the AD concept. In PlayReady, content is strictly bound to a device **or** a AD . PlayReady offers content portability as well as flexible user models. In addition, PlayReady DRM protected content can be consumed using a Microsoft Silverlight client [**28**]. A Silverlight client is installed and executed within the end users web browser, thus simplifying the DRM client installation process which previously has been experienced as a cumbersome process. Today the current Silverlight client supports very limited user models, including lack of support for offline content, the AD concept, and H.264 support.

Microsoft PlayReady is available for deployment by three SDK's, including a Server SDK, a PC Client SDK and a Portable Devices SDK. In addition, a SDK for Silverlight DRM development is available [**14**].

The main components of a Marlin DRM system is depicted below in Figure 13: Microsoft PlayReady DRM architecture.

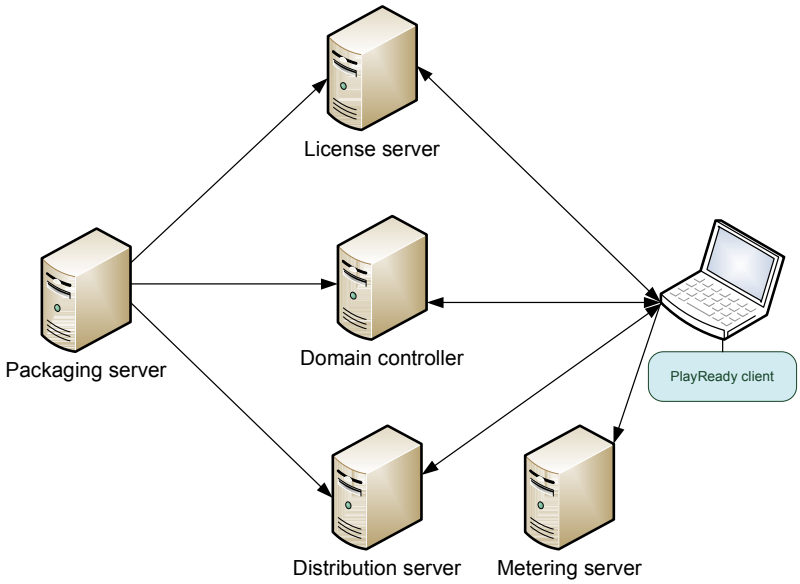

Figure 13: Microsoft PlayReady DRM architecture

2.5.4 Summary

A list of features presented by the above mentioned DRM technologies are presented in the tables below. The list is not exhaustive, but still captures the main features of the mentioned systems.

Platforms and export capabilities

Feature	*Marlin*	*PlayReady*	*OMA DRM*
Windows	√	√	√
Mac OSX	√	√	√
Linux	√	√	√
WMDRM-ND compatible	×	√	×

Table 3: Platforms and export capabilites for Marlin, PlayReady and OMA DRM 2.0

Usage rules

Feature	*Marlin*	*PlayReady*	*OMA DRM*
Supports multiple devices	√	√	√
Embedded licenses	√	√	√
Separate licenses	√	√	√
Device-bound licenses	√	√	√
Person-bound licenses	√	×	×
Domain-bound licenses	×	√	√
Time-bound licenses (e.g. rental)	√	√	√
Pay-per-view / counted plays	√	×	√
Subscriptions	√	√	√

Table 4: Usage rules capabilities in Marlin, PlayReady and OMA DRM 2.0

File formats, codecs and transport mechanisms

Feature	*Marlin*	*PlayReady*	*OMA DRM*
H.264	√	√	×[2]
MPEG2	√	×[3]	×[4]
Download	√	√	√
Progressive download	-[5]	√	√
Streaming	√	√	√
Live streaming	√	(√)[6]	×[7]
Smooth streaming	×	(√)[8]	×

Table 5: File formats, codecs and transports mechanisms in Marlin, PlayReady and OMA DRM 2.0

Additional features

Feature	*Marlin*	*PlayReady*	*OMA DRM*
Documentation	√	×	√
Watermarking	×	×	×[9]
Authentication	×	×	×
Payment infrastructure	×	×	×
Web-browser plug-in client	×	√	×
Offline support	√	√	√
Metering	√	√	√
Availible SDK's	√	√	√, (6)

Table 6: Additional features of Marlin, PlayReady and OMA DRM 2.0

It is easy to see that the features offered three DRM systems are in many ways the same. Table 7: Differing features of Marlin, PlayReady and OMA DRM 2.0 lists the above features where the DRM systems differs.

[2] Not covered in the OMA DRM 2.0 specification

[3] Support will be added in SilverLight 3

[4] Not covered in the OMA DRM 2.0 specification

[5] No public information is available from Marlin Developer Community.

[6] Requires third-party components.

[7] Not covered in the OMA DRM 2.0 specification.

[8] Through SilverLight PlayReady client.

[9] Not covered in the OMA DRM 2.0 specification.

Feature	*Marlin*	*PlayReady*	*OMA DRM*
WMDRM-ND compatible	×	√	×
H.264	√	√	×[10]
MPEG2	√	×	×[11]
Live streaming	√	(√)	×
Smooth streaming	×	(√)	×
Web-browser plug-in client	×	√	×

Table 7: Differing features of Marlin, PlayReady and OMA DRM 2.0

The main differences between the three DRM systems can be summarized as follows:

- Due to the OMArlin specication, OMA and Marlin can import and export content both ways.
- PlayReady is the only WMDRM for Network Devices (WMDRM-ND) compatible system.
- In Marlin content is bound to a person that in turn is bound to a domain of devices (see PED concept described in 2.4.1), where both PlayReady and OMA binds contend directly to a domain of devices.
- The content to person binding opens up for temporary authorization and content-to-domain re-registration in Marlin.
- Marlin supports targeted user rules.
- No public information regarding live streaming capabilities in OMA DRM 2.0 could be found, thus there is no guarantee that OMA DRM 2.0 supports live streaming.
- PlayReady is the only DRM system with support for smooth streaming[12].
- PlayReady is the only DRM system that has a finished web-based DRM client implementation.

[10] Not covered in the OMA DRM 2.0 specification

[11] Not covered in the OMA DRM 2.0 specification

[12] Smooth streaming is a streaming technology where the transfer rate automatically adapts to available bandwidth while streaming. Read more on: http://www.iis.net/extensions/SmoothStreaming .

2.6 Digital Rights Management Interoperability Activities

To date several organizations are working on various frameworks to promote a DRM interoperable environment. These organizations include, among others, the Coral Consortium, the Digital Media Project, The Digital Video Broadcasting project and Sun Microsystems. These organizations are either single companies, or coalitions of companies that all have recognized the problems in the area of DRM interoperability, and thus have decided to co-work in order to reach a suitable solution for all parties involved.

2.6.1 OPERA

OPERA is a project owned by the European Institute for Research and Strategic Studies in Telecommunications GmBH [**29**], also referred to as Eurescom. Eurescom is a private organization for research and development in European Telecommunications [**30**].

The OPERA project [**31**] specifies an open DRM architecture to enable interoperability between different DRM systems. The goal is to achieve a user based content registration system that will integrate with already available DRM systems. The architecture provides two main features:

- A usage license is independent of the underlying DRM system.
- The usage license is bound to a user.

OPERA includes a license management system. This management system is added on top of the each DRM systems own license management system. The license management system assigns content to a user registered within the OPERA system. Secure authentication of the user is built upon the idea that authentication is provided through a Telecom provider and the users Secure Identity Module (SIM) card. Hence, a user authenticates to the system by the use of his/her cell phone.

The usage rules of content is built upon the least common denominating license model that OPERA has recognized among various DRM systems, that is, the "play once" license. Each time a user tries to play licensed content a single "play once" license is delivered by the underlying DRM system.

2.6.2 MPEG-21

In the specifications for MPEG-21, MPEG provides specifications for protection and management of multimedia content [**32**]. This includes standardized interfaces between Intellectual Property Management and Protection (IPMP) tools. MPEG-21 does not standardize IPMP itself, but instead standardizes the interfaces to provide flexibility between various IPMP systems. When a device tries to consume protected content it determines what IPMP tool is

required to consume the content. The DRM interoperability issue is solved by searching for and installing the proper DRM tool when needed [**19**]. The approach to DRM interoperability undertaken by the MPEG falls in to the category of configuration driven interoperability [**18**].

2.6.3 Digital Media Project

The Digital Media Project (DMP) [**33**] is a non-profit Association that has recognized the need of an interoperable DRM platform to meet the needs of both the content producers and end customers. The DMP has defined *primitive functions* as a *function* embedded in more than one *function*, where *function* is defined as any action implemented with DMP-specific technologies. These *functions* are obtained by breaking down *functions* performed when parties in the value chain interact in business transactions. The general idea is that *functions* may undergo big changes as the business models are altered over time, but the *primitive functions* will in general remain constant. The DMP approaches DRM interoperability by providing specification for tools that enables the *primitive functions*. The set of tools specified by the DMP is called Interoperable DRM Platform (IDP), and is one of the first specifications that build on the MPEG-21 standard [**34**]. The IDP is, as the name suggests, the foundation in the DMP's interoperable DRM platform. However, just like MPEG-21 and Coral, the DMP does not provide a DRM system standard, but instead specifies how to achieve DRM interoperability between disperse DRM systems.

The DMP Reference Software provides a normative reference software implementation of the DMP specification. This software is under development in *the Chillout project* [**35**].

2.6.4 Networked Environment for Media Orchestration

Networked Environment for Media Orchestration, abbreviated NEMO, is Intertrust's reference technology for interoperability between dispersing DRM systems [**36**]. NEMO provides a Service Oriented Architecture (SOA) for secure dynamic communication between disperse DRM systems. Various DRM systems can request operations from other DRM systems through services provided by NEMO, without any knowledge of the inner workings of the other DRM system. The basic idea is that NEMO should be to DRM systems what TCP/IP is to computer network communication [**37**]. NEMO is a core technology used by both the Coral Consortium and Marlin.

2.6.5 Coral Consortium

The Coral Consortium is a cross-industry group of companies consisting of content providers, service providers and device manufacturers that focuses on creating an open technology framework for interoperable content distribution channels that use different DRM systems.

The Coral Consortium has developed specifications called Coral Interoperability Framework (CIF), designed to provide interoperability between disparate DRM systems [**38**]. This will provide the ability for users to move premium content between different devices that implement different DRM systems.

The CIF architecture bridges differences in trust management between different DRM systems. Each Coral compliant device has a unique certified identity used to establish trust with other Coral compliant systems. Each device or system is certified for one or more roles defined by the CIF. The combination of unique certified identities and certified roles ensures that devices and systems developed by different manufacturers implementing different DRM systems can establish trusted communication. Each role in the CIF architecture may be required to expose one or more standardized interfaces to other coral compliant systems that implement other coral roles. This ensures that different parties can interact independent of their implementers.

In online mode, the CIF provides the ability for customers to reacquire content in a DRM format supported by other devices than the device it was originally acquired on. In offline mode, the CIF can function by the help of local instantiations of Coral roles that allow consumer to transform the contents DRM in to a form suitable for other devices.

Briefly explained, DRM interoperability is provided by Coral Consortium by the use of rights tokens [**10**]. A rights token is a DRM system independent uniform usage license. In a Coral Consortium ecosystem, each time a purchase occurs, a rights token is sent to a rights token service. If a device B implementing DRM B now wishes to consume content from device A implementing DRM A, device B acquires the content and the appurtenant rights token. Device B then contacts a rights mediator role. The rights mediator role now performs an identity check and contacts the rights token service with the corresponding rights token provided by Device B. Next the rights mediator contacts a DRM system B with a request for a DRM system B license, which is if allowed, transferred to device B.

Content can be translated by either decrypting content at the source device, sending the content to the sink device over a secure channel and then reencrypted into correct format at device B, or re-downloaded from a service provider that uses DRM system B.

2.6.6 The Digital Video Broadcasting project

The Digital Video Broadcasting (DVB) project is a consortium of broadcasters, device manufacturers, network operators, software developers and regulatory bodies. The consortium develops open technical standards for global delivery of digital television and data services [**39**].

The DVB systems have been widely adopted around the world and new members continue to join every year. The DVB has recognized the move towards

convergence between different delivery systems, broadcast and point-to-point. Therefore the DVB is currently working on creating an interoperable world of converged systems.

The Copy Protection Technologies (CPT) group is a sub-group of the DVB with the aim of developing a specification for Copy Protection and Copy Management (CPCM). The CPT group has worked on a CPCM system that will provide interoperable end-to-end copy prevention in a home network environment that will be able to interface with existing proprietary copy prevention systems.

DVB-CPCM leverages the AD concept previously described in 2.4.1. Content can be delivered to the consumer using various methods such as broadcast, the internet, mobile delivery, packaged media etc.

A CPCM System consists of AD's, CPCM compliant devices and CPCM content. When content enters the CPCM system the content becomes CPCM-content, and is then managed and protected within the CPCM-system. CPCM-content leaves the system by either consumption of the content or when exported to another system.

A CPCM compliant device is any device that implements CPCM functionality. The CPCM device may embed non-CPCM functionality, but this functionality can have no access to CPCM content.

The DVB-CPCM specification consists of eleven published documents. Two documents with guidelines for implementers will be published at a future date. During a presentation by the DVB in the late spring of 2009, the DVB informed that the DVB-CPCM system is not yet ready for implementation. The DVB-CPCM system is expected to be implemented within a few years.

2.6.7 Digital Rights Management Everywhere Available

Digital Rights Management everywhere available is normally referred to by its abbreviation "DReaM". Project DReaM [**40**] is a Sun Labs initiative to develop an open standards DRM solution, based on Suns participation in the Opera project [**41**] (see 2.6.1). Dream will be able to integrate any proprietary solutions that the market demands to provide interoperability that meets the demand of the end customers [**42**]. Two main goals of project DReaM is to develop a solution for distribution of content that focus on authentication of network identity instead of device authentication, and to provide an open environment where creators, content owners, network operators, device manufacturers and consumers can work together to solve technical obstacles associated with DRM [**43**].

Due to no activity in Project DReaM for six months, the project was reviewed and archived in August 2008 [**40**].

2.7 The Open IPTV Forum

The Open IPTV Forum (OIPF) was created in 2007 by its founding members Ericsson, France Telecom, Nokia Siemens, Panasonic Corporation, Philips, Samsung Electronics, Sony Corporation and Telecom Italia. The OIPF was created to provide an IPTV solution with a "plug and play" user experience. Such a solution inherently requires advanced technology which is likely to be eased by the adoption of open standards. The goal of the OIPF is to through collaborated efforts develop such standards [**44**]. TeliaSonera is today an active member of the OIPF.

Currently the OIPF suggest two approaches to content protection: a terminal-centric approach using Marlin (see 2.5.2) technology and a gateway-centric approach using either DTCP-IP or CI+ [**45**].

The terminal-centric approach is an end-to-end content protection system, where the terminal is the end device, and the content provider is at the other end. The approach builds upon the idea that content is provided to the end device protected by a DRM common to all end devices.

The gateway-centric approach builds upon a gateway service in the home network that removes the DRM protection, and then transmits the content to a consuming end device using a link protection technique, such as DTCP-IP.

2.8 The Digital Living Network Alliance

The Digital Living Network Alliance (DLNA) was formed in 2003 when several companies agreed that they would be able to provide better products to customers if their products where compatible across the branded boundaries. The DLNA provides interoperability guidelines for devices working in a home networked environment. The basic idea is that content stored at a device should be easily accessible for consumption on another device; even if the devices are developed by different device manufacturers [**46**]. E.g., utilizing DLNA certified technology, a TV-show recorded at a DLNA certified PVR located in a family's living room can be watched on a DLNA certified TV-set located in a bedroom.

Another important point in DLNA is that devices is connected either through an Ethernet interface or a WIFI network instead of a device-specific interface, and installation and configuration procedures completed by the end user is to be minimal. A DLNA certified device is supposed to be compatible with other DLNA certified devices out-of-the box.

The DLNA guidelines [**47**] does not specify any new technology, but is instead built upon a set of existing technologies. The combined technologies are presented below in Figure 14: DLNA layers.

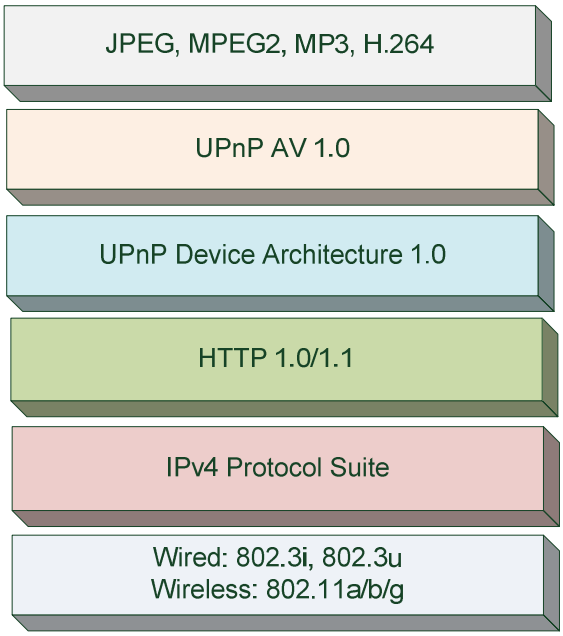

Figure 14: DLNA layers

DLNA utilizes Ethernet or Wi-Fi interfaces together with the IPv4 protocol and UPnP for peer-to-peer communication. The guidelines specify HTTP as a mandatory protocol for media transport as well as RTP as an optional protocol. A set of devices types grouped into device classes (see Figure 15: DLNA Device Classes) is specified along with mandatory capabilities for each device type. Furthermore, the guidelines specify how the capabilities are to be conveyed as well as mandatory and optional file format support for each device type.

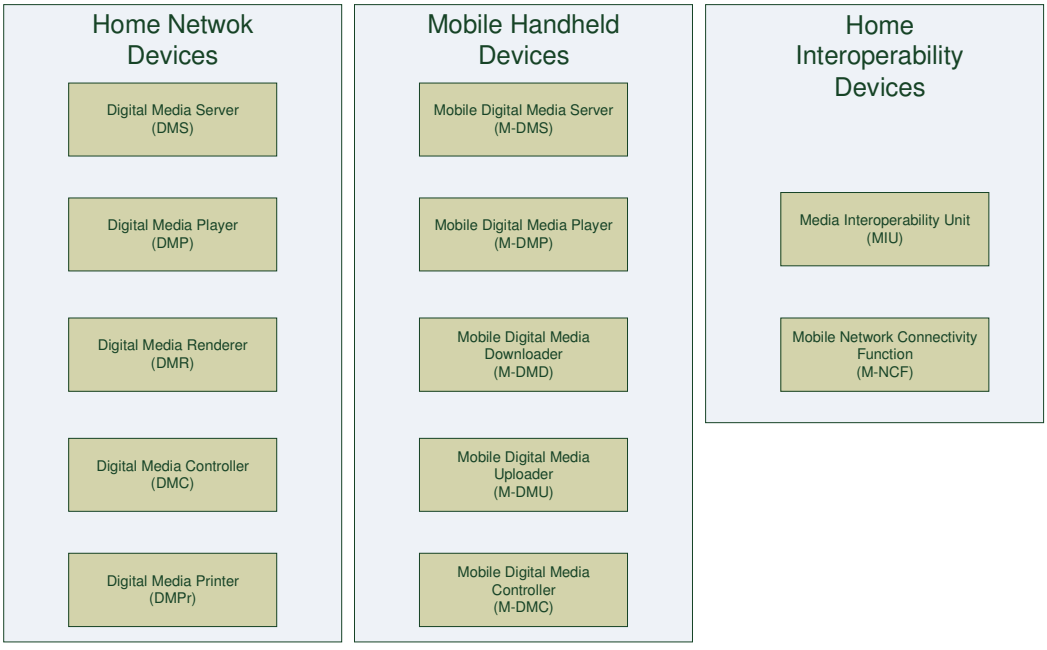

Figure 15: DLNA Device Classes divided into categories

A **Digital Media Server (DMS)** is used to store, expose, and distribute content.

A **Digital Media Player (DMP)** is used to find content exposed by a DMS and play that content locally.

A **Digital Media Renderer (DMR)** is used to playback received content after setup from another device.

A **Digital Media Controller (DMC)** is used to find content exposed by a DMS, and set up the connection and playback between the DMS and a DMR with matching capabilities.

A **Digital Media Printer (DMPr)** is used to print images.

A **Mobile Digital Media Server (M-DMS)** is a the mobile equivalent of a DMS.

A **Mobile Digital Media Player (M-DMP)** is the mobile equivalent of a DMP.

A **Mobile Digital Media Uploader (M-DMU)** is used to send content to a M-DMS with upload capabilities.

A **Mobile Digital Media Downloader (M-DMD)** is used to find, download and play content exposed by a M-DMS.

A **Mobile Digital Media Controller (M-DMC)** is used to find content exposed by a M-DMS, and set up the connection and playback between the M-DMS and a DMR with matching capabilities.

The Home Network Device (HND) category and the Mobile Handheld Device (MHD) category are very much alike, for example is the M-DMP the mobile handheld device counterpart to the DMP of the home networked devices. Even if they are very much alike, they differ in the network connectivity and the media format layer. To bridge these differences, the DLNA guidelines specify the Home Interoperability Device category.

A **Mobile Network Connectivity Function (M-NCF)** is used to bridge the network connectivity functionality between the HND category and the MHD category.

A **Mobile Interoperability Unit (MIU)** is used to translate content between required media formats for the HND category and the MHD category.

The combination of the devices classes divided into device categories along with the HID devices a complete interoperable device environment is created.

2.8.1 Digital Living Network Alliance and Content Protection

A DLNA certified device will likely implement some DRM technology to enable consumption of premium content. However, as several different DRM technologies exist and different devices might implement different DRM technologies, the device interoperability the DLNA certification was intended to

provide is, in the case of premium content consumption, very limited. Thus, DLNA has recognized DRM interoperability as a core part of the content protection guidelines work within the DLNA [**48**].

Because of the complexity regarding DRM interoperability, the DLNA decided to put effort in providing guidelines for link protection technologies. DLNA Networked Interoperability Guidelines Expanded, published October 2006, included DLNA Link Protection. DLNA Link Protection is used to protect content when transferred from a source device, for example a DMS, to a sink device such as a DMR.

DLNA specified Digital Control Protocol over IP (DTCP-IP) as a mandatory Link Protection scheme used in DLNA Link Protection. In addition, Windows Media DRM for Network Devices (WMDRM-ND) was specified as an optional Link Protection scheme. This does not imply that an implementer of DLNA Link Protection may implement WMDRM-ND instead of DTCP-IP, but that WMDRM-ND can be implemented in addition to DTCP-IP. Any device that supports DLNA Link Protection must be able to transfer one of the media formats specified by the DLNA utilizing DTCP-IP.

It is worth to notice that Link Protection is not equivalent to DRM. When using Link Protection, DRM protected content stored at a source device is decrypted and re-encrypted before being transferred to the consuming sink device, where the content is decrypted before consumption. Such technology is provided through the DTCP-IP protocol.

2.8.2 Digital Transmission Content Protocol over IP

Digital Transmission Content Protocol over IP (DTCP-IP) was created by its five founding companies: Hitachi, Intel, Panasonic, Sony and Toshiba, usually referred to as the "5C" [**49**]. DTCP-IP protects content by Advanced Encryption Standard (AES) encryption with a 128 bit content key during transfer. Content keys are exchanged after a secure channel has been established using public-key cryptography. Authentication of devices is performed utilizing a device certificate issued by the Digital Transmission Licensing Administrator (DTLA) [**50**]. The content stream contains a Copy Control Indicator (CCI) that indicates usage rules of the content. Four different usage rules are supported: Copy-never, Copy-once, No-more-copies, and Copy-Freely.

To ensure that content is not transferred over long distances; DTCP-IP includes localization functionality. This prevents packets to do more than 3 "hops", and the roundtrip time for a packet may not exceed 8 milliseconds. This ensures that devices within a home network may transfer content over DTCP-IP since the only intermediate entity is likely a router, thus the number of hops is less than three and the roundtrip time of 8 ms should be more than enough.

Chapter 3 Technology evaluation

This chapter will describe relevant criteria for evaluation of DRM systems applicable for TeliaSoneras IPTV environment. These DRM systems are then evaluated with respect to the described criteria.

3.1 Evaluation of Digital Rights Management Interoperability Activities

Chapter 2 studied a few activities working on a solution on DRM interoperability. These activities include: OPERA, Coral, DReaM, DVB-CPCM and the DMP. These activities will be evaluated against a set of criteria that have special importance for TeliaSonera's position in the field of DRM interoperability, using a slightly modified version of the decision matrix described in 1.4.2.

3.1.1 Criteria

The bellow criterion was developed through interviews with personnel at TeliaSonera with extensive experience in developing and integrating software in TeliaSonera's IPTV system.

Proof of concept

If a system is to be implemented and integrated into the TeliaSonera IPTV system, for TeliaSonera as an operator it is of vital importance that the system can deliver the expected functionality.

Available SDK's

Developing a whole system for DRM interoperability "from bottom up" is a very exhaustive project for TeliaSonera. Consequently, it is important that well documented SDK's exist to aid in the implementation process.

Market adoption

As TeliaSonera are dependent on other parties in the IPTV-value chain (see 1.1.1) it is important that the system in hand has a wide market adoption. Furthermore, the market adoption of the system is the ultimate proof of concept.

3.1.2 Execution

The evaluation of DRM interoperability activities will be conducted by the use of a simple checklist, where each DRM interoperability activity is checked against each criterion. The √-sign signifies existence and the ×-sign signifies absence.

Criteria/Proposal	*OPERA*	*DReaM*	*The DMP*	*Coral*	*DVB-CPCM*	*NEMO*
Proof of concept	×	×	×	×	×	×
Available SDK's	×	×	×	×	×	×
Market adoption	×	×	×	×	×	×

Table 8 Checklist for DRM interoperability activities

3.1.3 Results

As sad as it might seem, Table 8 Checklist for DRM interoperability activities shows that the proposals fail on all of the given criteria. However, this does not imply that the proposed systems would not be functional. Rather, it suggests that at this time neither of them is yet ripe enough to be implemented by a single company such as TeliaSonera.

3.2 Proposed Concepts

For an implementation in TeliaSoneras IPTV environment two candidate concepts for DRM interoperability have been chosen. This two candidates are described in the below sections.

Implement the Authorized Domain

This concept would imply implementing an AD DRM concept, earlier described in this section 2.4.1. Various technologies for such a DRM concept exists today e.g., OMA DRM [**13**] and Microsoft PlayReady [**14**], with more technologies to come, such as DVB-CPCM [**12**]. Furthermore, an additional system implementing the AD concept is Marlin [**51**], that on top of implementing the AD DRM concept, could be categorized as an implementation of the earlier described Personal Entertainment Domain DRM [**26**].

Link Protection

Link Protection technologies aim to secure digital content from unauthorized exploitation by securing content during the transmission between devices implementing the same link protection technology. The devices can consume or store the content under set permissions. The current state of the art technology for link protection is the Digital transmission content protocol (DTCP). DTCP [**50**] can be used over various digital interfaces, such as IEEE 1394 (FireWire), Bluetooth, USB, MOST, and IP networks (DTCP-IP). Content protection systems can output content through DTCP if allowed by the content protection system. For example, DTCP-IP is a permitted export entity from WMDRM [**52**]. Hence, a device with a DTCP-IP implementation may output WMDRM protected content to another DTCP-IP compliant device using DTCP-IP.

Link protection enables devices that implement DTCP to consume DRM protected content without supporting the specific DRM system. The prerequisite is that both the transmitting and receiving device implements DTCP. Consequently, DTCP can be used as an enabler for interoperability between devices that not share the same DRM systems. On the other hand, using DTCP as a content protection scheme still requires an implementation of DTCP in all compliant devices.

3.2.1 Criteria

An obvious difference between the proposed concepts are that where the first concept translates from an origin content protection scheme into a Link Protection scheme such as DTCP, the second is a complete end-to-end DRM system. It is worth to note that the Link Protection concept still requires the content to be protected by a content protection scheme, e.g. a DRM or CA system, when distributing content to the first receiving or consuming device. Hence, adopting the Link Protection concept still requires implementation of a second content protection scheme, if not already present. As TeliaSonera currently use a CA system (see 2.1), a possible solution would be translating the current CA protection into DTCP. However, it is worth noticing possible legal implications of such a solution, previously mentioned in section 2.4.3. This being noted, evaluation of the two concepts will be based on the three following criterion (next page):

Flexibility

The amount of flexibility provided by user models supported by the content protection scheme.

Implementation effort

Estimated number of components (e.g. license servers, packaging servers, device clients) needed in order to implement the content protection scheme.

Market adoption

Estimated adoption among service providers and device manufacturers at the current market.

3.2.2 Execution

The evaluation is conducted using a decision matrix (see 1.4.2). 10-points have been distributed over the different criterions weight. Each criterion is then rated on a 5 point scale. Each criteria rating is then multiplied by the corresponding criterion weight.

Criteria/Proposal	*Link Protection*	*AD-concept*	*Weight*
Flexibility	1	4	3
Implementation effort	4	2	2
Market adoption	1	3	5
Total:	16	31	

Table 9: Decision matrix for concept evaluation

3.2.3 Results

Table 9: Decision matrix for concept evaluation shows that the AD-concept scores 31 points, while the Link Protection concept scores 16 points. The quite large difference in scored points between the two concepts mostly depend upon the lack of user models as well as the earlier mentioned (see 2.4.3) possible loss of rights when translating from the origin content protection scheme into a Link Protection scheme. Furthermore, the apparent lack of devices implementing Link Protection schemes such as DLNA Link Protection or DTCP-IP reduces the points scored by Link Protection. The AD-concept, on the other hand, brings flexible user models by leveraging the domain concept, as well as market adoption through service providers adopting DRM systems that utilize the AD-concept.

The results clearly favor the AD-concept.

3.3 DRM Evaluation

Chapter 2 studied the features of three state of the art DRM systems that utilize the AD concept. This section will evaluate the strengths and weaknesses of these DRM systems.

3.3.1 Criteria

In contrast to the study of concepts, this evaluation will rate actual deliverable DRM systems for implementation. As one of the main goals is to distribute content to more platforms than the TV-set, it is important to look at what platforms the DRM system is applicable to. Furthermore, as described in section 3.2.1, both flexibility and market adoption is of great concern. Thus, the DRM systems will be evaluated against three criterions: flexibility, platform independence and marked adoption.

Flexibility

The amount of flexibility provided by user models supported by the content protection scheme.

Platform independence

This criterion signifies how independent the DRM system is from the underlying platform, that is to say, what platforms are available for implementation (Windows, Mac OS X, Linux, etc.).

Market adoption

Estimated adoption among service providers and device manufacturers at the current market.

3.3.2 Exectution

The evaluation is conducted using a decision matrix (see 1.4.2). 10-points have been distributed over the different criteria weight. Each criterion is then rated on a 5 point scale. Each criteria rating is then multiplied by the corresponding criterion weight.

Criteria	*Marlin*	*PlayReady*	*OMA DRM*	*Weight*
Flexibility	5	3	3	3
Platform independence	3	4	2	3
Market adoption	2	4	3	4
Total:	32	37	24	

Table 10: Decision matrix for DRM system evaluation

3.3.3 Results

Table 10: Decision matrix for DRM system evaluation shows that Marlin scores 32 points, PlayReady scores 37 points and OMA DRM scores 27 points.

It is clear that Marlin offer very flexible using models and thus scores very high on flexibility, whereas PlayReady and OMA DRM scores less due to less flexible user models. This is mainly due to Marlins resemblance to the earlier described PED concept, where the domain is centered on a person instead of a set of devices. However, where Marlin offer flexibility, PlayReady instead offer platform independence and marked adoption. Both Marlin and PlayReady offer platform independent SDK's in the ANSI C programming language. In addition, PlayReady offer a web-browser DRM client through the Silverlight plug-in. This implies that PlayReady protected content can be consumed on any computer with the Silverlight plug-in, available today for both Mac and PC. Hence, the service provider does not necessarily have to develop a DRM client for each platform themselves. OMA DRM is developed by the Open Mobile Alliance (OMA), who does not provide any SDK's. These have to be licensed through a third party vendor such as Cloakware or Coremedia.

In terms of market adoption, there is a strong case for Microsoft. This is mainly due to the success of WMDRM, which have been widely adopted by service providers. Since PlayReady is the further development of WMDRM, there is a good chance that PlayReady will have the same success. To this date, Marlin has reached short marked adoption with only a few presented implementers. PlayReady, on the other hand, has gained a bigger market acceptance; mainly through the use of the Silverlight plug-in. OMA DRM 1.0 enjoyed an apparent acceptance from cell-phone manufacturers such as Nokia and SonyEricsson. OMA DRM 2.0 has not reached the same success, even though it has been implemented in some mobile devices. However, OMA DRM is mainly targeted at portable devices and especially cell-phones, whereas both Marlin and PlayReady is targeted at both portable devices and more stationary devices such as PC's, TV-sets, and game consoles.

Chapter 4 Implementation

This chapter describes how a use case that utilizes an AD concept can be realized with an implementation of a DRM client player.

4.1 Introduction

Chapter 3 concluded that the AD DRM concept is a stronger candidate for implementation than the Link Protection concept. As a consequence, a prototype for demonstrating AD DRM functionality is to be developed. The biggest enhancement from previous DRM systems is the introduction of the AD concept. Hence, for this implementation, the main focus is to evaluate the functionality of this concept.

A general AD based DRM system consist of server as well as client components. This implementation will focus on the client part of the DRM system, and hence will rely on server components supplied by a DRM system provider.

4.1.1 Use case

Two or more PC's is to be registered the same AD, denoted **Domain C**. The first PC, denoted **PC A** downloads and plays a piece of content. This piece of content is later transferred to the second PC, denoted **PC B**. To test that the content can be consumed offline[13], PC B 's internet connection is cut. **PC B** tries to play the content.

Expected results: **PC B** plays the content without any license acquisition process.

4.1.2 Execution

The implementation is dependent on a license server, a domain controller, a metering server, a packaging server and the client player. Developing the server components is likely to be an exhausting task, thus, for this implementation, the server components are provided by a DRM system provider. The

[13] Without internet connectivity.

DRM client communicates with server functionality utilizing SOAP requests and responses over HTTP, see Figure 16: DRM system component architecture.

Content protected by the DRM system is supplied by the DRM system provider, with various licenses for testing purposes attached to the packaged content which is used in the implementation.

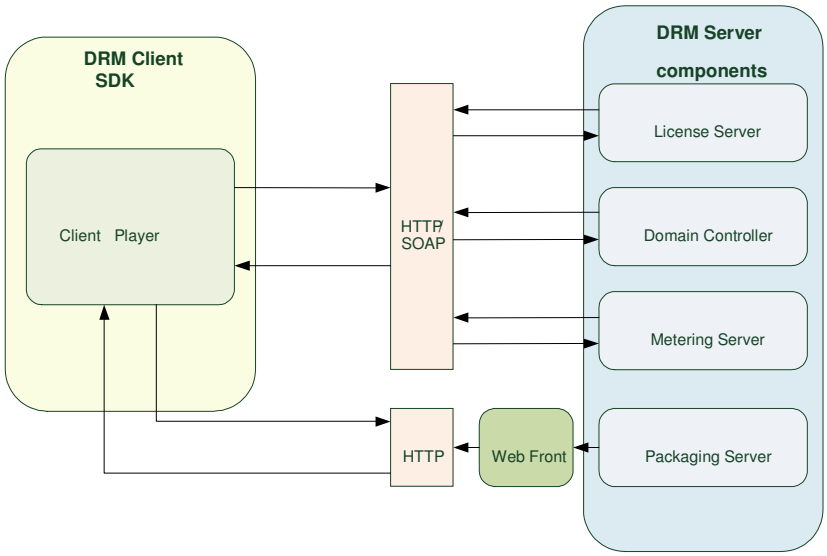

Figure 16: DRM system component architecture

The execution involves the following steps:

1. A reference DRM client player is installed on two separate PC's, denoted PC A and PC B.
2. Both PC's joins downloads an audio content file bound to AD C from a test content repository.
3. By playing the audio file downloaded in step 2, both PC's try to join AD C. If join is successful, both PC's are now in AD C.
4. PC A downloads a video content file bound to AD C from a test content repository.
5. PC A plays the content.
6. PC B is internet connection is closed.
7. The video content file stored at PC A is transferred to PC B by utilizing a USB memory stick[14].
8. PC B tries to play the video content file. If playback succeeds, PC B has played a DRM protected content file without acquiring any license from a license server. Playback is thus supported through the AD C membership.

[14] The video content file can be transported to PC B by any method, for example with a DVD or a Local Area Network.

4.2 Results

By executing the steps described under 4.1.2, the outcome was positive. The second PC (PC B) played back the content without any internet connection. Thus, playback was supported through the AD membership. This shows that the domain concept offered by the AD DRM system functions as expected.

4.3 Combining Digital Living Network Alliance technology and Authorized Domain Digital Rights Management

Since DLNA technology provides a generic method to share content between devices, special interest is put into the interaction between DRM packaged content and DLNA Media Servers, as well as DLNA Media Players/Media Renderers. The combination of the two technologies could possibly create an environment where premium content protected by DRM could be easily shared and consumed among devices within the same AD. To realize such a combination three main technical gaps have to be filled in: the exposure of DRM packaged content in the DLNA Media Server and discovery as well as consumption at the DLNA Media Player/Media Renderer.

To expose DRM packaged content at a DLNA Media Server, it is vital that the content header of the DRM packaged file is not encrypted, and thus can expose metadata about a specific file to the DLNA Media Server. At the other end, the DLNA Media Player/Media Renderer need to implement DRM client functionality to be able to render transferred content.

To test sharing of DRM protected content utilizing DLNA technology, two separate PC's was connected through a Local Area Network (LAN). The first PC, denoted **PC A**, acted as a DLNA Media Server by utilizing an out-of-the-box software. DRM protected content bound to an **AD W** was stored at the file repository of the DLNA Media Server on **PC A**. The DRM protected content stored at the DLNA Media Server is to be consumed by a DLNA Media Player at **PC B**.

The DLNA Media Server recognized the media container and was thus able to access the metadata stored in the file header, hence the file was exposed by the DLNA Media Server. The conclusion drawn is that to enable content exposure it is vital that the DLNA Media Server supports the container type, and that the file header is not encrypted by the DRM system.

For the DLNA Media Player to discover the protected file exposed by the DLNA Media Server, the DLNA Media Player must as well support the container type. Furthermore, for the DLNA Media Player to be able to decrypt

and render DRM protected content stored at the DLNA Media Server, the DLNA Media Player must implement DRM client functionality.

As of today, no DLNA Media Player implementing the AD DRM system used in this prototype have been found. As a consequence, for testing such functionality an implementation of a DLNA Media Player integrating the AD DRM must be realized.

If the above mentioned implementation is realized, to enable playback from a DLNA Media Server capable of exposing DRM protected content to a DLNA Media Player that integrates the DRM technology, the DLNA Media Player must be joined into the same AD as the DLNA Media Server. Furthermore, the protected content need to be licensed to the same AD as the above mentioned DLNA devices.

4.4 Further work

The prototype implementation described in the above sections is limited to a AD of two PC's[15] consuming content licensed to the same AD. This implementation can be further extended to include for example portable devices. Furthermore, this implementation has only dealt with the DRM client using test server components provided by a DRM system provider along with prepackaged content provided by a test content repository. In that sense, the implementation has only tested functionality in the DRM client. The implementation could be further expanded to include server components. Such work could contribute with knowledge such as:

- How can authorized domains be managed? Especially, how is a closed AD created and how can the domain controller be integrated with underlying business logic?
- How is content bound to a AD? How are licenses created and issued in such cases?
- How can underlying business logic be used to transfer content from one AD to a second AD? How can licenses issued to AD bound content be removed?
- How is a time-bound AD created, and what business models could such authorized domains realize?
- What business models can emerge by leveraging the Autorized Domain concept?
- How can AD management (join/leave) be implemented at portable devices with special concern to usability?

The prototype implementation could be further expanded to include portable devices. The development of a reference player for portable devices would con-

[15] Tests with additional PC's have been conducted.

tribute with knowledge regarding how content can be shared between portable devices within the same AD, as well as how domains can be managed on portable devices.

Chapter 5 Discussion and Conclusions

This chapter discusses a few relevant topics in the area of content protection and DRM interoperability. It reconnects with use cases described in Chapter 1 and concludes the work presented in this report.

5.1 Current industry initiatives

This project has studied some current initiatives undertaken to achieve a DRM interoperable content ecosystem. While many of these have presented innovative ideas and proposals for DRM interoperability, little market adoption is yet to be seen. What the future holds for initiatives such as OPERA, The DMP, DReaM, Coral, etc. is hard to tell. It is likely that the success of the initiatives lies in the support from the content industry. OPERA, The DMP and DReaM seems to lack this support. It is also worth noticing that the project DReaM is now filed as inactive, and neither is there any recent activity to be seen in the OPERA project. The work in the DMP is still ongoing, but the above mentioned lack of support from the content industry indicates that success might be remote. Coral, on the other hand, is supported by big companies in the content industry such as Twentieth Century Fox Film Corp and NBC Universal, Inc. As a consequence, it is easy to suggest that Coral is a technology that is more likely to have greater market adoption in the future. However, since no large scale reference implementations of Coral exist, no proof of concept is to be found.

The lack of reference implementations of the various approaches further complicates evaluation of the mentioned approaches. These factors boils down to the simple conclusion that the current approaches are not yet ripe for a large scale implementation. Furthermore, for TeliaSonera in the role of content delivery and content aggregator (see 1.1.1), it is vital that an implemented technology for DRM interoperability has a broad market acceptance. As a consequence, one could draw the conclusion that it is too early for TeliaSonera to invest in an implementation of any of the above mentioned approaches.

In the near future, bringing premium content to other devices in a home networked environment than the TV-set will most likely be dependent a content protection system such as DRM due to the current requirements from the content industry. In turn, the success of a content protection scheme such as DRM is dependent on customer acceptance of the DRM system. Such acceptance is in turn dependent on the ability to consume the protected content over the whole range of devices that the end customer owns. At a market where diverse DRM systems are implemented into the CE devices by different device manufacturers, the need of interoperability between these DRM systems is apparent. The need for consumer acceptance of DRM, in combination with the need to provide customers with better content services to battle piracy is likely to push the development towards a DRM interoperable content ecosystem. This is apparent when looking at the ongoing collaboration between different organizations, such as the ongoing work in the DECE.

5.2 Digital Entertainment Content Ecosystem

In September 2008, a consortium of Hollywood content providers, CE device manufacturers, software companies and service providers announced their intent to develop a DRM interoperable content ecosystem that would allow consumers to buy digital media almost anywhere and play them at any type of device [**53**]. The consortium called Digital Entertainment Content Ecosystem (DECE) is led by Sony Pictures and involves big name players such as Warner Brothers, Fox, Paramount, NBC Universal, Comcast, Philips, Toshiba, Intel, Microsoft, Best Buy and many more.

Mitch Singer, President of the DECE, states that DVD is the most successful digital distribution medium yet, and the reason is because the DVD is built upon open standards. When a consumer buys a DVD at for example Wal-Mart, that consumer knows it will be consumable on a DVD player from Philips. When digital content is sold over the internet today, it will only play at a specific type of player. For example, a feature film purchased from iTunes is only consumable on an Apple iPod, a feature film purchased from Zune Market is only consumable on a Microsoft Zune player, a feature film purchased from PlayStation Store is only playable on a Sony PlayStation 3 or PSP. Mitch Singer further states, quote: “If DVD rolled out this way, people would think we’re crazy” [**54**].

The DECE anticipates that removing the dependence of device market penetration is crucial to facilitate development of new content services. When launching a new content service today, the service is dependent on the devices that can consume the provided content. For example, when Microsoft launched their Zune content service, they were limited to a very small market share of Zune devices. If a service provider can reach all kinds of devices, the service is not longer dependent on the marked share of a specific device. The

same goes for device manufacturers. The market penetration of a new device is dependent on what content services are accessible to the device. The DECE intend to remove the dependencies between content service and devices in both directions. To remove these dependencies, the DECE introduces the concept of a "Rights Locker". A rights locker is a service, where every purchase of digital content is registered along with a license and the identity of the customer. The basic idea is that when a consumer purchases some content from a content provider to device A, this transaction is registered in the Rights Locker. Hence, there is a proof of license ownership stored in the Rights Locker. If the same consumer now wishes to consume the content at Device B that implements a different DRM system, Device B requests the content from content provider that uses Device B's DRM system. This content provider verifies the ownership by contacting the Rights Locker. If a proof of license ownership exists, the content provider now transfers the content with appropriate DRM protection to Device B. The content is now consumable at Device B. A reasonable question to ask is why a service provider would transfer content to a device if it was not part of any financial transaction. The DECE believes that the above described device independence will be a sufficient incentive to do so.

The DECE embraces the AD concept, but sees a problem in the AD being administered by individual service providers. If one service provider, e.g. TeliaSonera, administers a customer's authorized domains, this implies that consumers are locked in to this service provider. To solve this problem, the DECE wants to separate the service provider and the authorized domains. When separating the service provider and AD, the DECE also want to embrace the service provider's freedom on choice of DRM technology. As a consequence, the DECE will not promote one single DRM technology, but will instead provide an ecosystem where different DRM technologies can interoperate, thus letting the service provider to implement the DRM system of their own choice.

The DECE has not officially announced what DRM systems will be approved for use within the DECE. It is however easy to speculate in the possibility of PlayReady and Marlin becoming approved DRM systems in the DECE, since Microsoft is an active participant in the DECE, as well as the fact that the DECE is led by Sony Pictures, who also is the founder of Marlin. The SVP of Sony is also a member of the management committee of the DECE, Co-Chairman of the management committee of the Marlin Developer Community, and Director of the Coral Consortium. Furthermore, The SVP of Sony is also the president of the DLNA Corporation. Such an influential person on the board of both the DECE and the DLNA opens up for a possible collaboration between the DLNA and the DECE. Such collaboration could result in DLNA specifying DECE as a framework for devices to comply with in future releases of DLNA guidelines.

Today, Apple Inc. is one of the biggest players in the field of digital media distribution and enjoys a huge market share on downloadable digital music

and film. Noticeably, Apple Inc. is not present in the DECE. Some voices claim that the DECE is an industry collaboration to overturn Apple Inc.'s dominance. However, president of DECE Mitch Singer, stated in an interview that the DECE's mission is not to replace Apple Inc. and that Apple Inc. has been invited to join [**55**]. However, so far there have been no sign of Apple intending to do so.

The DECE is not history's first attempt to create and interoperable DRM content ecosystem (see 2.6), and thus it is questionable however this consortium will succeed in its mission when so many others seem to have failed. It is possible that Apples dominance in digital music pressures the industry toward a solution by the possibility of getting as big a market share on digital movies as on music. Furthermore, the ongoing large-scale piracy of digital content might be another incentive for the industry to come to a joint solution. These two mentioned factors could be big enough motivators for different players in the industry to reach a common solution on DRM interoperability.

5.3 Proposal for Use Case Realization

Chapter 1 described three different use cases that would be studied in this project. All three use cases share the same common denominator in that they approach content protection while still providing content portability in some sense.

The first use case (Use case 1) described a scenario where two separate devices shared the same DRM technology implementation. The question was how content could be transferred and consumed at the second device. Previous DRM technologies have prevented such usage of protected content which has resulted in a "content-device lock-in" situation where content could only be consumed at one, usually the origin content acquiring, device. Such situations have created tension between content providers and consumers, since consumers expect to consume their premium content at several different devices. Chapter 2 described a set of DRM systems that utilized an AD-concept (see 2.4.1), which allows for devices that are bound to the same AD to share and consume content independent of which device that originally acquired the content. Such an AD-based DRM system can enable a scenario as described in Use case 1.

The second use case described a scenario where the one device implemented a DRM system and the other did not. Consuming the content at a device that does not implement the DRM system while still preventing unauthorized use of the content poses the following logical problem:

Most DRM systems use cryptography (see 2.2) to prevent content from unauthorized use. To decrypt the content two pieces of information is crucial: the algorithm used to encrypt the content and a key. Hence, to consume the con-

tent the device that does not implement the DRM system needs both an algorithm for decryption as well as a key. This implies that some kind of content protection scheme needs to be implemented at both devices. Link Protection (see 2.8.1 and 2.8.2) was described under Chapter 2, a content protection scheme where the DRM is removed at a transmitting device, re-encrypted and then transmitted to the consuming device. Such a content protection scheme still requires an implementation in both ends, but at least removes the requirement of both devices implementing the same DRM system. Using such a content protection scheme as Link Protection do not fully enables the scenario described in Use case 2, but with consideration to the logical problem described above it is a solution that partly fulfills the described scenario.

Use case 3 described a scenario where two devices implement disparate DRM technologies. A user wishes to transfer content from the first device to the second device for consumption. This scenario was studied in Chapter 2, where previous research in this area as well as current activities for achieving DRM interoperability were studied. An evaluation of current approaches was conducted in Chapter 3, where it was concluded that the current activities lacks both proof of concept and market adoption. Thus, for TeliaSonera it would be precarious to invest in the development of such technology. Chapter 4 discussed ongoing work in the relatively young consortium called DECE where Coral technology is allegedly used [**53**]. If the DECE succeeds in its mission to bring an interoperable DRM content ecosystem, it is likely that Coral technology will be used for DRM translation. At this time, the various approaches proposed systems for DRM interoperability is not yet ripe enough to be implemented by a single actor in the IPTV-value chain. Hence, at this time it is very hard to realize the described use case.

5.4 Further work

As mentioned in Chapter 1 under 1.3 Scope, this degree project have studied the subject of content protection from a technical viewpoint. As noted in a few sections of the degree project report, the area of DRM and DRM are surrounded by legal questions that could be further investigated. These questions include (next page):

- How can agreements for translations between disparate DRM technologies be constructed? Who is liable in the event of a breach?
- If a set of end users share devices and content bound to one AD, who is the legal owner of acquired AD-bound content?
- What rights do end customers have with regard to user models for purchased content? E.g., if an end customer purchases content with specific rules set in the license, what guarantees can the user be sure to enjoy with persistence?

Chapter 2 briefly touched on the subject of security in DRM systems see (2.2). This degree project has not studied the security of either previously discussed DRM systems or DRM interoperability approaches. This is a subject that could be further explored.

The relative new concept to DRM is the introduction of the AD. As mentioned earlier in 2.4.1, an open question is how to handle situations when users of an AD wishes to leave the AD, e.g. in case of a divorce or children moving out. These situations will need to be handled, and thus a valid question to pursue further is how to manage authorized domains, especially how authorized domains can be spitted and how content can be transferred between authorized domains.

Another aspect of the AD concept is the business models the concept can enable. A trivial business model could be to sell content with a persistent play license bound to the AD. Since some authorized domains (dependent on DRM technology vendor) can be time-bound, open, or restricted to a specific set of end users due to authorization, the concept is likely to enable new types of business models previously not explored. Proposals for such business models could be developed and evaluated. This would provide valuable guidelines for emerging service operators at the digital content market.

Chapter 4 presented how the presented prototype implementation could be further explored. Especially, prototyping server components of an AD DRM system would add a lot of value to this work. Furthermore, integrating an AD DRM client into a DLNA Media Player/Media Renderer could demonstrate how DRM protected content could be seamlessly shared between devices in a home networked environment.

5.5 The Future of Digital Rights Management

Over the past years, DRM has been a subject surrounded by a lot of controversy. A common statement by opponents to DRM is that “DRM is dead”. This statement is usually backed by the opinion that DRM prevents fair use which repels customers from purchasing DRM protected content, combined with the statement that all content protection schemes are breakable due to the blow reasoning:

To prevent unauthorized access to plaintext content, DRM systems use some sort of cryptographic scheme to hide plaintext content from dishonest users. As mentioned in 2.2, to decrypt any data (content) both the decrypting algorithm and key has to be present. Thus, the key used for decryption need to be present in the end users device. As the key is present, even if craftily hidden, it is very hard to protect the key from a user with enough determination and skill. If a dishonest user accesses the key and thus can decrypt the content, it might not take long before the content is subject to widespread piracy. Now, as the argument follows: why would an end user bother with purchasing content DRM protected if the same content is accessible through piracy?

Moreover, opponents to DRM further bring the argument that an unbreakable DRM technology is provable impossible due to a flaw referred to as "the analogue hole". The analogue hole means that DRM protected content inevitably has to be presented in plaintext at the last step of the presentation process. That is to say, when playing a DRM protected feature film on a computer screen, the content has to be in plaintext at the monitor. Since the content is in plaintext at the monitor, the content is now accessible in analogue. Hence, even if it is impossible to break the protection and digitally acquire the content in the device, it is always possible to shoot the screen of the device. In other words, it is very hard to prevent a dishonest user from setting up a tripod and digital video camera in front of the screen during playback. This problem have been recognized, and there are ongoing research in how watermarking could be used as a way of discourage dishonest users from piracy [**56**]. The basic idea is to use watermarking to uniquely identify the buyer, and then use this information to identify the source of the piracy.

Given that the argument that all DRM systems can be broken, it is doubtful that is a sufficient argument for content owners to not promote DRM. A reasonable question to ask when discussing the future of DRM is: what is at stakes for the content owners? A study by the International Intellectual Property Alliance (IIPA) estimates that the copyright industries contributed 792,2 billion dollars, or about 7,75 %, of the U.S 2001 gross domestic product [**57**]. Hence, one could easily argue a lot is at stakes for the content owners. As a consequence, content owners are likely to promote that their content is protected from illegal proliferation due to piracy.

In January 2009, Apple Inc. announced their intent to remove DRM from their iTunes store. Some voices in the debate argue that this move from Apple indicate that the content industry is starting to loosen its strict requirements on DRM and that we are moving into a DRM free era. However, it is worth to notice, this move was only related to music. Feature films and TV-shows are still DRM protected at the iTunes store. This might be because of the huge budgets involved when producing such content. For example, the feature film Transformers 2 had a budget of 200 million dollars [**58**]. With such a big of an investment, it is likely that the production company is very concerned about

their return of investment, and as a consequence is likely to require DRM protection when sold at the iTunes store.

Content providers have always viewed piracy as a serious problem and with the huge increase in internet bandwidth during the last few years, content providers are even more concerned. In her book Digital Rights Management – Protecting and Monetizing Content, Professor Joan Van Tassel summarizes three options content providers are currently taking [**57**]:

Do nothing and accept that content on the internet is to be free and seek revenue from other sources such as advertising.

Fight back by **establishing new legal and regulatory environments** to defeat piracy. Provide legal ways of fighting pirates and provide for strong enforcement of such laws.

Protect and monetize the content by utilizing DRM to allow content providers to gain control of how their content is used.

To this date, content providers have taken all three paths. With services such as Hulu, Spotify and the Swedish TV4 Play content providers deliver content free of charge with recurring advertisements during playback. Recent regulatory laws such as the IPRED and HADOPI laws as well as the Pirate Bay-trial prove that content owners are using legal means to fight piracy. In addition, big investments are still being made into DRM technologies as well as ongoing work in consortiums like the Coral Consortium and DECE.

It is impossible to tell however DRM in its current form will be used in the future. History has shown that technological paradigm shifts in the media industry result in a period of time when business models are not properly adapted to the new technology. Eventually, business models have been adapted to the new technology. By looking at the history, it is likely that the current paradigm shift we are currently experiencing will result in new business models. With that in mind, it is likely that some kind of mechanism for guaranteeing revenues to copyright holders will eventually be in place. It is today impossible to tell however DRM in its current form will be used in the future. However, current investments in DRM technology and the present requirements on DRM from content owners indicate that for now, DRM is here to stay as a way of controlling how content is used by end users.

5.6 Conclusion

This degree project has studied DRM with special interest to DRM interoperability. This is an area that has been previously studied by several organizations, and several different approaches have been proposed. In this degree project, the approaches have been studied from a service provider's viewpoint with the aim of finding an implementable solution. Unfortunately, a conclusion drawn is that the approaches so far only consist of a set of specifications with-

out any actual implementations. Hence, no de facto standard is to be found. The vast implication of this conclusion is that at this stage, it is too early for a single service provider to implement a DRM interoperable content ecosystem. With this conclusion drawn, two content protection concepts that aim at bringing content portability across device boundaries have been studied and evaluated. This resulted in the conclusion that content portability of protected content can be obtained by implementing a DRM system that utilize the AD concept. Today, DRM technologies that utilize this concept exist. Three of these DRM technologies have been evaluated. A list of capabilities was developed to ease the evaluation of the three technologies with respect to platform independence, flexibility and market adoption. The evaluation concluded that a DRM technology from Microsoft called Microsoft PlayReady is a strong competitor as it brings apparent marked adoption and fairly flexible user models. Marlin is another strong competitor that brings very flexible user models but has a weaker market adoption. A previous version of OMA DRM has been a strong competitor on the cellular phone market. However, their newer OMA DRM 2.0 that in contrast with their previous OMA DRM 1.0 utilizes the AD concept has not enjoyed the same market adoption.

The evaluation of an AD DRM system presented in Chapter 4 demonstrates that utilizing the AD concept, content bound to the same AD can be consumed in offline mode by a DRM system client bound the same AD, even if the DRM system client was not the original acquirer of the DRM protected content. This shows that content portability and content protection can indeed be combined. Furthermore, the combination of DLNA technology and AD DRM technology was studied. The aim was to set up an environment where content can be easily shared and transported between DLNA devices using DLNA technology. However, to achieve such an environment it was concluded that the DLNA Media Player devices need to implement an AD DRM client. Unfortunately, due to time restrictions such an implementation could not be realized within this degree project. A conclusion drawn is that enabling such a combination of DLNA technology and AD DRM requires a bigger implementation effort than what could be fitted into the time restrictions of a degree project.

This degree project suggests that at this stage technology for DRM interoperability is still immature and should not be implemented. To fulfill customer's expectations of content portability and flexibility while at the same time meeting content owners demand of content protection, DRM systems utilizing an AD model is the best option.

Bibliography

References

[1] Chen Chunxiao, Zhao Li, Yang Shiqiang, Zhou Lizhu Zhang Hua, "Content Protection for IPTV-current state of the art and challanges," , Beijing, China, 2006.

[2] Gerard O'Driscoll, *Next Generation IPTV Services and Technology*. New Jersey: John Wiley & Sons, 2008.

[3] Open IPTV Forum, Functional Architecture, December 08, 2008.

[4] J.Han, A.J. Burstein D.K. Mulligan, "How DRM-based content delivery systems disrupts expectations of "personal use"," *Proceedings of the 2003 ACM workshop on Digital Rights Management*, pp. 77-89, October 2003.

[5] John S. Erickson, "Fair Use, DRM, and Trusted Computing," *Communications of the ACM 46*, no. no.4, pp. 34-39, 2003.

[6] Second Edition, ASQ Quality Press, 2004, pages 219-223 Excerpted from Nancy R. Tague's The Quality Toolbox. ASQ. [Online]. http://www.asq.org/learn-about-quality/decision-making-tools/overview/decision-matrix.html

[7] Tom Newberry Joseph Weber, *IPTV crash course.*, 2007.

[8] Bruce Schneier, *Applied Cryptography, second edition.*: John Wiley & Sons, 1996.

[9] High Level Group on Digital Rights Management, "Final Report," 2004.

[10] Milan Petkovic and Willem (Eds.) Jonker, *Security, Privacy, and Trust in Modern Data Management.*, 2007.

[11] Frank Kamperman, Peter Lenoir, Koen Vrielink Paul Koster, "Identity-Based DRM: Personal Entertainment Domain," *Transactions on Data Hiding and Multimedia Security I*, 2006.

[12] DVB, Part1: CPCM Abbreviations, Definitions and Terms, 2008.

[13] Open Mobile Alliance, DRM Architecture: Approved Version 2.0, 2006.

[14] Microsoft Corporation, Microsoft PlayReady Content Access Technology

White Paper, 2008.

[15] (2008, August) ars technica. [Online]. http://arstechnica.com/old/content/2008/08/open-market-video-drm-aims-to-let-1000-retailers-bloom.ars

[16] W. Jonker, F.L.A.J. Kamperman, P.J. Lenoir S.A.F.A van den Heuvel, "Secure Content Management in Authorized Domains," The Netherlands,.

[17] Jack Lacy, Michael Mackay, Steve Mitchell Rob H. Koenen, "The Long March to Interoperable Digital Rights Management," *Proceedings of the IEEE*, vol. 92, no. 6, 2004.

[18] Nicholas Paul Sheppard, Takeyuki Uehara Reihaneh Safavi-Naini, "Import/Export in Digital Rights Management," *Proceedings of the 4th ACM workshop on Digital rights management*, 2004.

[19] Ki Song Yoon Seong Oun Hwang, "Interoperable DRM Framework for Multiple Devices Environment," *ETRI Journal*, vol. 30, no. 4, August 2008.

[20] O. Tafreschi, and R. Wolf A. U. Schmidt, "Interoperability challenges for DRM systems," *In IFIP/GI Workshop on Virtual Goods*, 2004.

[21] Open Mobile Alliance. Open Mobile Alliance. [Online]. http://www.openmobilealliance.org/AboutOMA/Default.aspx

[22] Open Mobile Alliance, Digital Rights Management - Approved Version 1.0, 2004.

[23] Open Mobile Alliance, DRM Specification - Approved Version 2.0.2, Jul 23, 2008.

[24] Open Mobile Alliance, Enabler Release Definition for Secure Content Exchange - Candidate Version 1.0, Dec 09, 2008.

[25] Marlin Developer Community. Marlin. [Online]. http://www.marlin-community.com/technology

[26] Frank L. A. J. Kamperman, Lukasz Szostek, and Wouter Baks, "Marlin Common Domain: Authorized Domains in Marlin technology," *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*, Jan 2007.

[27] Community, Marlin Developer, The Role of Octopus in Marlin, 2006.

[28] Microsoft Corporation, Using Silverlight™ DRM, Powered by

PlayReady®, with Windows Media® DRM Content, 2008.

[29] Susan Wegner. Eurescom. [Online]. http://www.eurescom.de/message/messagesep2003/Open_DRM_architecture.asp

[30] Eurescom. Eurescom. [Online]. http://www.eurescom.de/Aboutus/profile.asp

[31] Eurescom, "OPERA - Interoperability of Digital Rights Management (DRM) Technologies," 2003.

[32] MPEG, ISO/IEC TR 21000-1:2004(E), 2004.

[33] Leonardo Chiariglione. IDP-3 walkthrough. [Online]. http://www.dmpf.org/documents/walkthrough_in_idp-3.htm

[34] Bill Rosenblatt. (2005, May) DRM Watch. [Online]. http://www.drmwatch.com/special/article.php/3502806

[35] Chillout. [Online]. http://chillout2.dmpf.org/wordpress/

[36] David P. Maher William B. Bradley, "The NEMO P2P Service Orchestration Framework," *Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04) - Track 9 - Volume 9*, 2004.

[37] Intertrust. (2009, September) Reference Technology. [Online]. http://www.intertrust.com/main/research/reference.html

[38] Gerard O'Driscoll, *Next Generation IPTV Services and Technologies.* Chicester: Wiley-Blackwell (an imprint of John Wiley & Sons Ltd), 2008.

[39] DVB. History of the DVB project. [Online]. http://www.dvb.org/about_dvb/history/

[40] java.net. [Online]. https://dream.dev.java.net/

[41] David H. Ramirez, *IPTV Security: Protecting High-Value Digital Contents.*, 2008.

[42] Tom Jacobs, and Vishy Swaminathan Gerard Fernando, Project Dream An Architectual Overview, September 2005.

[43] Sun Microsystems. Sun Microsystems. [Online]. http://research.sun.com/projects/dashboard.php?id=67

[44] The Open IPTV Forum. (2009, Mar) Open IPTV Forum. [Online]. http://www.openiptvforum.org/aboutus.html

[45] Open IPTV Forum, Volume 7 – Authentication, Content Protection and Service Protection v1.0, 2009.

[46] Digital Living Network Alliance, DLNA Overview and Vision Whitepaper, 2007.

[47] Digital Living Network Alliance, DLNA Networked Device Interoperability Guidelines Expanded, October 2006.

[48] Digital Living Network Alliance. (2009, September) Digital Rights Management and Content Protection. [Online]. http://www.dlna.org/industry/why_dlna/key_components/drm/

[49] Digital Transmission Licensing Administrator, Digital Transmission Content Protection (DTCP) - Technical and Licensing Overview, 2009.

[50] Digital Transmission Licensing Administrator. Digital Transmission Licensing Administrator. [Online]. http://www.dtcp.com/

[51] Marlin Developer Community. Marlin Developer Community. [Online]. http://www.marlin-community.com/develop/downloads/white_papers

[52] Microsoft Corporation. (2006, Dec) Compliance Rules for WMDRM Export - Appendix A.

[53] Bill Rosenblatt. (2008, September) DRM Watch. [Online]. http://www.drmwatch.com/drmtech/article.php/3772546

[54] Mitch Singer. TechCrunch. [Online]. http://www.techcrunch.com/wp-content/uploads/2008/08/singer.pdf

[55] Gina Keating. (2008, September) Reuters. [Online]. http://www.reuters.com/article/technologyNews/idUSN1234778920080912

[56] P., Steinebach, M., Diener, K. Wolf, "Complementing DRM with digital watermarking: Mark, search, retrieve," *Online Information Review*, vol. 31, no. 1, pp. 10-21, 2007.

[57] J. Van Tassel, *Digital Rights Management - Protecting and Monetizing Content.*: Focal Press, 2006.

[58] Mali Elfman. ScreenCrave. [Online]. http://screencrave.com/2009-06-29/box-office-transformers/

Appendices

Appendicle: Feature description

Authentication

The DRM system embeds an authentication system

Available SDK's

The DRM vendor have deliverable SDK's for the DRM system implementation.

Device-bound licenses

Licenses bound to a specific device is supported.

Documentation

Documentation is available in advance to purchase.

Domain-bound licenses

Licenses bound to an AD is supported**.**

Download

The DRM technology can protect content downloaded and stored at a device locally.

Embedded licenses

Licenses can be embedded into the contents file header.

H.264

H.264 encoded content can be protected by the DRM technology.

Live streaming

Content can be DRM protected during live streaming to clients.

Metering

Content usage can be metered for statistical use, revenue distribution and/or billing.

MPEG2

MPEG2 encoded content can be protected by the DRM technology.

Offline support

Offline consumption of content is supported.

Payment infrastructure

The DRM system embeds a payment infrastructure.

Pay-per-view / counted plays

The DRM system can set a value representing the number of allowed playbacks in the content license.

Person-bound licenses

The DRM technology support issuing of content licenses bound to a personal identity.

Progressive download

The DRM technology supports decryption of content during progressive download.

Separate licenses

Licenses can be delivered separate from the actual content file.

Smooth streaming

The DRM technology have built in support for Microsoft Smooth Streaming.

Streaming

Protected content can be streamed during playback at a DRM client.

Subscriptions

Subscription based business models are supported.

Supports multiple devices

The DRM technology is applicable for several device types and is not applicable only to a specific device brand (e.g. Apple or Sony).

Time bound licenses

Licenses can be set to be valid between specific time limits.

Watermarking

Content can be embedded with an invisible watermark which enables content to be traced to the original acquirer.

Web-browser plug-in client

The DRM technology offers an out-of-the-box web-browser plug-in DRM client.

TRITA-CSC-E 2011:023
ISRN-KTH/CSC/E--11/023-SE
ISSN-1653-5715

www.kth.se