Protection mechanisms for personal content

Øyvind Berget

Institute of Informatics

UNIK/University of Oslo

1 Introduction

The digitalising of the society have lead to a large scale sharing of pictures, video and other kind of content between people. The sharing is mainly based on trust between the sharer and the receiver of the content. One user can share his or her content if the trust in the receiver is large enough. The industry understood that it is not possible to base a product to earn money on trust of the consumer. Commercial products is not sold based on trust, but the industry tries to control the content sold with technological solutions. Digital Management Rights(DRM) is one such solution the industry has developed. A system to control personal digital content could be a way to increase the trust of sharing content in the personal domain. A system where it is possibilities to share and still control the private or personal content would greatly improve personal security. With a personal DRM system it is possible to revoke already shared content and to hinder a too wide spread sharing of certain content. This essay will discuss some of the key elements in systems that control content and how commercial DRM system is used and discuss some research in the area of content protecting systems as well.

2 Motivation

Several private films and pictures have been released on the Internet that probably the owner of the content would have liked undone. Today use of camera, mobile phones and other digital recording systems is used a lot, but the necessary control of the content is not in the mind of the recorder at all times. With an analogue camera it is necessary for the user to be sure of the portrait in the picture. The cost for every picture is quite high on analogue cameras. With a digital camera the cost of a picture is very low. Therefore a lot more pictures are captured. With a digital camera a user might take a picture to check out how it look. A picture stored at a camera costs quite little and is not always deleted. Perhaps this is luck for historians, but might have issues when it comes to privacy and the private space. There will also be a lot of private pictures that might be interesting for a lot of people, but it does not need to be spread to everyone. In a free society it must be allowed to have privacy. Still there is no solution on how to maintain this privacy in content for the public. DRM solutions might have some features that would help the public in controlling their content with both how content is spread and how it is used.

One scenario where private control over content could be advised is when users take pictures without being able to grasp every consequence that picture might have later on in life. With the content wide spread it could be difficult if not impossible to revoke these pictures. If content sharing is done through a DRM system, revocation of content is possible. Pictures or movies could be revoked years later as long as the pictures or movies are still controlled by the user. A little different scenario, but with many similarities is the scenario where it is possible to revoke private pictures. The pictures that were

shared of the Norwegian actor Kåre Conradi and his girlfriend through Internet in autumn 2006, was pictures the actor admitted he would have enjoyed if never have had been spread[1]. With a private DRM system he could have revoked the picture or quite possible the content would not have been possible to share in the first run.

Another scenario that is relevant in the context of controlling content is the sharing of community content. A group of people is on a trip together and some people is taking some pictures and not everyone. It would take a lot of time getting everyone to have all pictures taken so they agree on sharing the pictures that is taken. Sharing the pictures could be done through copies of the digital content. Still there might be some of the pictures, that some of the participants would enjoy, were not spread any further than to the people that was on the trip. A DRM system could control the spread of the content and could ensure that pictures was secure. Other scenarios could be imagined as well. Some things are done in a private frame and the control over this frame is not possible without a system to control private content.

There can be a lot of scenarios that systems controlling content for private people or communities could have a big role. DRM systems will, if it is implemented right, change the way people will share information, pictures and other content. Systems that allow such abilities can be implemented. This essay will look into several different approaches on how to have a system with some of the attributes that is necessary for protecting content. An aspect on a system controlling private content is: Who should control the system? A private household might be the solution but a systems protecting content could be something ISP or phone operators or another company offers for their consumers. Like a bank box in a bank. There are several factors that commercial industry cannot take into consideration, so there might be possibilities in private DRM systems that have not yet been seen in the commercial products existing today. One of these factors could be regarding privacy. A company cannot record every time a user plays a song that the user have bought. A private household system could record every time a user is watching another users content. Or an ISP or a phone company could record that this user is playing another users content, without knowing what that content is. Today, digital galleries exist, but they seldom have a fine grained DRM solution. Facebook for example, offers free gallery on their page, but you share all pictures or you share none. A more fine grained solution would allow for a more widespread sharing of pictures. Therefore a research in how DRM systems could effectively increase sharing, but protect the user of the system and give the user the possibility of regretting.

3 Background

A system protecting private content need to incorporate certain features to be able to its tasks. This chapter will look into some of the theory on how to accomplish this features. The formal way of looking at access control which is needed in this context will be the first subject. Then cryptographic features that might be used in such systems will be discussed followed by a description of some of the most common DRM systems on the market.

3.1 Access control

Usually when access to an object is discussed in a computer system the discussion is

either about Discretionary Access Control(DAC) or Mandatory Access Control(MAC). DAC is when an owner or someone with the right access to an object, sets all the attribute each subject have on that object. MAC on the other hand is when the system has a set of rules which determines the access to an object. Neither of these models describes the needs a system to control the spread of content. Content could be owned by others, but not changed or looked, at unless the originator agrees on it. This is what is recognized as Originator Controlled access control(ORCON)[2]. ORCON is a combination of DAC and MAC. Three rules is needed to understand what ORCON does[2].

1. The owner of an object cannot change the access controls of the object.
2. When an object is copied, the access control restrictions of that source are copied and bound to the target of copy.
3. The creator (originator) can alter the access control restrictions on a per-subject and per-object basis.

The first two rules implements MAC and the last rule is DAC. As we can see the originator is the one that control the access and not the owner of the object. Looking at DRM systems later in this essay it will be important to understand these rules for ORCON.

3.2 Cryptography

Cryptography was in the beginning used in governmental and military areas. After the introduction of information technology it has become a large research area within the information technology branch as well. Three different concepts of using cryptography is used and this chapter will briefly explain the purpose and usage of these concepts.

3.2.1 Symmetric cryptography

Symmetric cryptography have been used for thousands of years. The first knowledge of it is the cipher used by Caesar which is called Caesar cipher. The concept of this is to move the alphabet three places to the right. To decrypt the information the reader have to reverse the function and shift the alphabet three places to the left. This is very common example of symmetric key cryptography. We use the same key which in this example was the number three and use it to encrypt and to decrypt. In symmetric cryptography the sender and the receiver needs to know a shared secret. This secret is used as the key in the cryptography, but how the encryption and decryption is done does not have to be a secret. Modern cryptographic algorithms are much more complex than Caesar cipher. A common used algorithm today is the AES[3] which is an American standard for symmetric cryptography. The old standard which is still in some use is DES and variations of it. AES is accepted by the IETF as a standard as well.

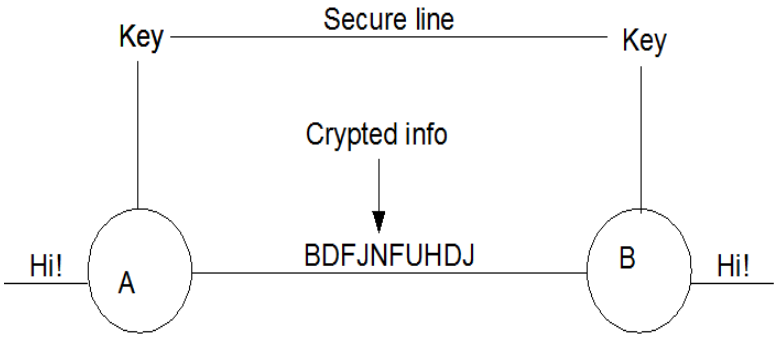

Illustration 1: Symmetric cryptographic system

3.2.2 Asymmetric cryptography

Asymmetric cryptography is a newer concept than the symmetric cryptography. It was first invented in the 1970's. It is based on the idea that if you have one key for encryption and another one to the decryption it would make the task of distributing keys much easier. To make this work the user will have to make a key pair. These keys are linked together mathematically, but it is a very difficult task to calculate one key from the other. The security is based on difficult mathematical problems that there is no known fast solution to. The user will name one of the keys for public and the other one for private. The user could then send out the public key to everyone and everything that are encrypted with that key can only be opened with the users private key. This way it is possible to secure the communication one way. Three men at MIT, Rivest, Shamir and Adleman figured this problem out in the mid 70's and made this possible. This encryption is named RSA after the inventors, but other algorithms exists as well. With the use of public and private key this algorithm could be used to sign information as well. Public Key Infrastructure(PKI) is a system that relays on asymmetric cryptography.

$Public\ key: e_K = 17$
$Private\ key: d_K = 2753$
$This\ is\ two\ keys\ which\ would\ work\ when\ n = 3233$
$Encrypt\ the\ number\ 123\ which\ could\ be\ representation\ of\ the\ alphabet.$
$C = 123^{17}\ mod\ 3233 = 885$
$M = 885^{2753}\ mod\ 3233 = 123$
$How\ numbers\ are\ picked\ is\ not\ something\ we\ go\ into\ here.$
$This\ is\ merly\ a\ proof\ too\ see\ that\ the\ keys\ are\ different.$

Example of asymmetric cryptography from article in wikipedia[4].

3.2.3 Hash

Hash functions uses one-way mathematical functions. It is hard to reproduce the original values when it is calculated. A hash function tries to turn information into a given size that can act as a fingerprint on that particular information. The function need to give same result with the same input. With an information fingerprint it is possible to check if it is the right information and that it is from the right source. A hash system could be created for incorporating keys to make difference in the same information, but it is not necessary to have an effective algorithm. An effective and good hash algorithm need to have two important traits. The first trait is that there should be very hard to reproduce the original

information from the hash. The other trait is that there should be difficult to find two blocks of information that hashes to the same value. Some quite common hash functions in use today is MD5, SHA-1 and SHA-2. A SHA-3 algorithm is expected to be developed to become a new standard in hash functions.

3.3 Existing DRM

Digital Rights Management (DRM) have been used for quite some time where there have been commercial interests. The motivation and design of these DRM systems have been to protect the a merchandise of some sort. An overview over three commonly used systems is given in this chapter.

3.3.1 Apple Inc. FairPlay

Apple Inc. have a DRM system which is incorporated into several of their products. They call their DRM system for FairPlay. QuickTime media player have FairPlay built in and it is built into iTunes, iPod and iPhone as well.

FairPlay is a DRM system that encrypts the media files[5]. The media files that are used uses the MPEG-4 Advanced Audio Coding (AAC) format. This format allows the use of DRM as an extension and it is an open standard. The songs sold in iTunes store is in AAC format with FairPlay. The system iTunes store handles is quite large. They sell music to a large number of customers and have an even larger number of songs to sell. This makes their system quite complex. It is designed to make sure the music is accessible to the customers, but still let Apple have control over the music. It is not possible to listen to music bought in iTunes store on other devices than the once that is allowed by Apple Inc.

To be able to buy music at iTunes store you have to have an account there. Then you have to authorize the computer you have to run the iTunes application. Each user can have 5 computers registered to them. When a user buys a song from the iTunes store the song is encrypted with a master key. This cryptographic key is then put into the AAC file. But this key is encrypted with a user key which iTunes makes on behalf of the user. This key sent to iTunes store and is stored there with the user name and it is stored in the iTunes application as well. This user key is not possible to read for the user. This way FairPlay do not need a connection to use the content it is protecting.

3.3.2 Windows Media DRM

Windows Media DRM is a DRM platform that protects media files[6]. Microsoft have made a set of components which all is considered to be Windows Media DRM. This platform consists of both software development kits and software to play and make media files. WMDRM can play at network and portable devices as well as computers.

WMDRM encrypts the information and stores the files in windows media format as .wma or .wmv. The encryption key used for the encryption of the media information is then stored in an encrypted license. This license is distributed separately from the media file. The media

file can be sent to other, downloaded through a server or burnt on a CD and many other ways. Still it can not be used unless it is authorized with the license for the file. This license can be obtained when the user gets the media file or it can send it the first time the content is played. It is possible to use the license to sell media or just control the use.

License server is needed to get licenses online. This server do Microsoft call a clearing house. The clearing house it self do not have the media file, but the license and with the right authorisation it can pass the license on to the user. The clearing house can revoke a service for a player as well.

3.3.3 Open Mobile Alliance DRM

OMA have members in every aspect of the mobile industry. Member examples are Nokia, a mobile phone manufacturer, Ericsson, telephone system manufacturer, Vodafone, who is a mobile phone operator and IT companies like Sun and IBM[7]. The OMA DRM purpose is to make a DRM solution for the mobile phone content provider. Typical use is for ringtones and wallpapers on mobile phone. It is independent on the media format.

OMA DRM exists in two versions. Version 1.0 can be used in three modes[8]. Forward lock which protect the content from being copied. Combined delivery has the same feature as forward lock, but could have other features like one-time use and time limit use. Separate delivery allows the encrypted content to be forwarded without the user rights because the rights are not integrated in the media file. Separate delivery have also the features as combined delivery have, but uses encrypted content.

Version 2.0 uses another system based on PKI. There all content are encrypted with a public key. The corresponding private key is in a Rights Object(RO) that will be issued from Rights Issuer(RI) when the RO is registered at the RI. In this version it is possible to not authorise information in devices in case of hacking content and other reasons. In this DRM solution there is also possible to share content between OMA DRM v2.0 enabled devices that is together in a domain. This domain is made by the RI as well.

4 Discussion

DRM have been researched in quite some areas and will probably in the future play an important role in how content will be distributed. The definition on DRM is not definitive, but regarding the ORCON we can put some rules into what we expect from a DRM system. Arguments that a proprietary format is some kind of DRM could be made, but it's not what is mean in this essay. This chapter will look at DRM as a solution for certain problems discuss how they differ in aspects.

4.1 Privacy

DRM have been a subject for commercial use for a long time. But there have been proposals to use DRM to protect peoples privacy[9]. The European Union have a quite strict legislation on how to handle private information. In a digital world where everything

can be copied and retransmitted and the possibilities that when information is out there is no way to regain control over the information. Therefore it is a great challenge to solve this problem. It is suggested that there should be possible to use a generic DRM system to cope with the challenges the privacy directive gives. The system suggested divides the system into three participants. First the “data subject” is the person which the information is concerning. The second is the “data controller” which handles the information about the data subject. Finally the “data processor” is the one part that offers services for the information.

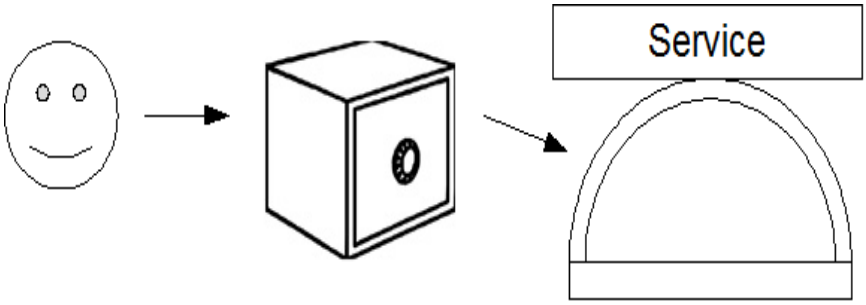

Illustration 2: Subject stores info at controller which offers it through processor

The data controller have databases about rights, the subject and the processors. This way the trust in the system first and foremost have to be at the data controller. With a server containing the controller it could be considered as a trusted third party. Some DRM systems protecting commercial products may have the possibilities, that they can be used to monitor the usage of the product. When a system is protecting private information, this is suddenly a positive possibility for the consumer. It is possible to watch when a users private information is used by tracking it in the data controller.

There are certain aspects of the privacy DRM solution which is difficult. The first of these subjects is the creation of data or asset as it may be called. The difficult part is to make sure that the information is linked to the right user. A secure way of authentication is needed. There should be a possibility for a user to correct information as well, but the user should not be able to change any information at will. A policy on what is allowed is necessary. This will have to remember what kind of permit a user have agreed on as well. A well organised policy will not allow a user to trick the system by committing a request then to revoke the information at once. Policy on information management in general is important in such a system. What is the usage of the asset and history on what the user have agreed on is what is considered most important in this information management policy.

In large there are quite some useful elements in how a DRM system can be of use to protect privacy. Still there are some areas where this area is not so clear. A central “privacy bank” with personal information could be safe, but the “privacy bank” must be controlled by someone as well. Therefore some information that the user is not allowed to change could be put in a government DRM server for private information, but other kinds of information should be controlled by the user or someone the user have control over. For example encrypted information at an ISP and then information which is stored somewhere can open that information for the user. Then the information have backup and is protected, but not controlled by the ISP.

4.2 Protecting content within home environment

Systems to control already purchased content in homes have been an area of research for years. The protection of movies in DVD's was a function that worked fine for around three years. After a descrambling technique was discovered DVD's could be copied, but a lot of research and effort is done to protect content in other ways. Some of that research looking for protection of commercial content in homes will be discussed in this chapter.

4.2.1 DVB-CPCM

Copy Protection Content Management(CPCM) of the Digital Video Broadcast consortium is a DRM solution[10]. This solution is based on a system where content could be copied and played by CPCM enabled devices. The DRM system have several features which is described through information that is stored in the the Usage State Information(USI) that belongs to the content[11]. Some of these information is how to play the content, could the content be copied or could the content be copied but played only at one spot at the time. It could also be put information that says that the content is not playable after a certain time.

This system is not in production in any way, but it have an idea that the system should be device independent. As long as the device do what is expected of it in CPCM matters it is CPCM compatible. It does not require a certain way to be transferred either, so it is not concerned about technology. So new technology can be incorporated. The devices in a household are typically whats considered an Authorized Domain(AD). Within the AD it is allowed to transfer data between devices if the USI have the right flags set. A device could only be in one AD. One of the key ideas is that the AD should be autonomous. It does not need a third party registration although it is not describe it will never come to that. The content is sent into the AD and could be distributed there, but the USI should have the control over the content.

This system is described in a standard from DVB consortium and could be very interesting to look into. It is not very specific in many areas, but it have a lot of ideas on how to implement a DRM system in house. This system is meant for commercial use and therefore does not have a revocation plan of one particular content, but rather revocation of devices. When some content have arrived into the CPCM system it will be able to be there until deleted or the timestamp of the content exist and passes.

4.2.2 Home DRM architecture

Some researches have looked specifically in to the AD concept from the ideas of DVB consortiums CPCM system[12]. They have looked at on-line content distribution and does not take into consideration pre-packed content like CDs and DVDs. These researchers add some important constrains to the devices. These constraints are as following:

- No continuous connection between devices is needed.
- There are no tamper resistant clocks in devices.
- Devices will probably not have encryption acceleration hardware.

- There should be possible to revoke devices from AD if their counterfeit or false.

These constrains imply that there should be as little public key encryption as possible because it is very processor demanding. Symmetric cryptographic algorithms could be as secure and easier for the processors. Therefore the system will emphasis symmetric cryptography for communication between devices. The algorithm that is suggested is the 128 bit AES. The constrains will also imply that the content is stored distributed as well since the there is no continuous connection.

Some of the devices in a domain have certain roles. The AD Manager(ADM) is a role one and only one of the devices have. Many devices may have the ability of being the ADM, but only one in the AD is active and every device in the AD need to be registered in this device. It is the ADM function to revoke falsified or illegal devices as well as voluntarily revocation of a device. Content Manager(CM) is another role in the system. These are the points where content arrive into the AD. Several content providers may choose different devices or CM and that is why there is a possible to have many CM's in an AD. One device may have several roles and it does not limit the device.

Every device that is manufactured will have a Global Device Identification(GDI) with a private/public key pair that are implemented in a certificate. When every device have a unique ID it is possible to revoke a device if it have violated the rules given in the AD system. It is possible to revoke CM's as well. When content providers want to send content it will control the device with the revocation list. This is a very clever way of assuring that the content that is asked for arrives at known and authorized CM.

This system have many of the features necessary from the DVB consortium. A lot of consideration is taken into the system as mathematical problems of cryptography and such. Still there is some problem with this system when it comes to detail and discrete control over content. A whole family will still be a part of one domain. When such points arise there might be som borderline issues that is not considered. For example a children of a divorced couple will have difficulty with its devices on which domain do they contain. Also content at work versus content at home it will be necessary with several authentication devices. Therefore when a system is device orientated the personal identity has to be more specified as long as only one device can be in only one domain.

4.2.3 Identity based DRM: Personal Entertainment Domain

Authorized Domains are in large device oriented. Both the the system discussed in last chapter and the DVB's solution is based on a devices with trust to each other. Another approach is the Personal Entertainment Domain(PED)[13]. PED-DRM have an approach where a single person also is the domain. Both a set of devices and a set of content are bound to the domain which is controlled by a single person. The system divides devices into permanent devices and temporary devices. In permanent devices content can be access without authorisation. That will make it convenient and make it possible to share content between family members. Temporary devices will have to have an authorisation before accessing content. Each device may be connected to several domains. A personal device is used for authorisation if that is necessary. This device could be a mobile phone or a some kind of smartcard. A wireless authentication would give the best solution, because it would be easiest for the user.

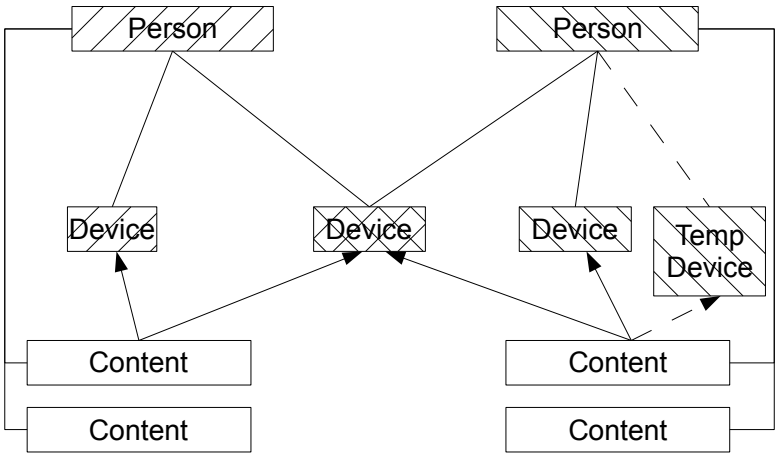

Illustration 3: PED DRM system

This DRM system would be able to handle many kind of challenges. One of the very interesting thoughts are the ones that allow a user to temporary access home content through other devices like hotel television. The user will be able to temporary access content that is stored home or in the office if both the device is connected through the Internet. Playstation 3(PS3) and Playstation Portable(PSP) have a very simliar function in a new update[14]. PSP can hook up to the PS3 and play content which is stored on the PS3. Another feature of PED-DRM is that if a family have devices they share, everyone in the family can use the content stored. There is other features as well, but in general the consumers of content should have control over what they buy, but the content providers will be able to block content if it is hacked.

The PED-DRM system have a challenge in how to manage the system. The suggestion how this could be done is that every user and device have a private/public key pair. These keys are used for authentication purposes. Domains make a certificate consisting of each device and the one user. These certificates describe the domain and when devices are synchronized updates are done. Updates mean revocation and authorisation information in this setting. The system trust these certificates so much that the content is not encrypted as a standard, but it is not ruled out. Still there is a final amount of devices a certificate can contain. But a certificate to manage the domain is a clever idea.

The PED-DRM system have shifted the orientation on the system from devices over to the user. Still there is many constraints on the system that limit the user experience. The temporary devices could be difficult regarding privacy. Users may share content like picture or videos and the temporary device might not be as good as it seems. The idea of not controlling the devices might be troublesome.

5 Conclusion

There exist a lot of research in the area of protecting content. Most of the research is done for commercial use. The industry sees that a lot of digital content is copied and mass distributed over peer-to-peer networks and download sites. Stoping the spread using technological systems together with judicial means have been a popular yet not successful way. Still we can see that Apples FairPlay is cracked, but it is still very popular because of

the features and the popularity of iPod and iTunes. So even when a system is cracked it might continue in production. Commercial use of DRM systems would probably be a focus area in research. The use of digital content and the needs for protecting it from being copied unauthorized will probably increase. Therefore it will be important to look at the industry in how DRM systems could evolve in the future. The problem of the commercial system and looking at them is that they could be closed from public view. But the basic idea is still possible to render.

Home DRM systems does not take into consideration that companies can be misusing the user. When a system is put from the industry into the home of the user. The industry can look at what kind of content that particular user is looking for. It can actually monitor everything that system is doing. This way the industry can get user information that could control what the user actually would look at. When systems are designed, it should be very clear that this is not going to be possible. Still when systems are proprietary it could be difficult to control this.

With systems trying to control privacy through DRM solution it could be very nice feature to actually be able to look at what companies are looking up of information regarding the user. This is not something that have been done, but could give the user it's right for privacy. The problem with this privacy system is to control what information should the user control and what is controlled by the government. Location and controlling the content server could be a problem as well.

A system for controlling private content would have other preferences than the both commercial systems and privacy systems. Still this is the areas where there is research on DRM systems. Protecting of personal content through the use of DRM systems would have a whole other set of both constrains and markets. Research in the establishment of trust between users and the physical sharing of content would needed to be done. The force the sharer of content may have on the content might give problems regarding, privacy or not effective force and then not a good system. A system protecting personal content would give the sharer an effective mean to get back the control over the private space.

6 References

[1] vg.no, “Private bilder spres på nettet”, http://www.vg.no/pub/vgart.hbs?artid=135588

[2] M. Bishop, “Originator Controlled Access Control”, Computer Security Art and Science

[3] NIST, FIPS PUB 197, http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[4] Wikipedia, “RSA”, http://en.wikipedia.org/wiki/Rsa

[5] RoughlyDrafted, “How FairPlay Works: Apple's iTunes DRM Dilemma”, http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351C60-A4E5-4764-A083-FF8610E66A46.html

[6] Microsoft, “Windows Media DRM FAQ”, http://www.microsoft.com/windows/windowsmedia/forpros/drm/faq.aspx

[7] Wikipedia, “OMA DRM”, http://en.wikipedia.org/wiki/OMA_DRM

[8] Nokia, “OMA DRM-related questions”, http://www.forum.nokia.com/document/Forum_Nokia_Technical_Library/contents/FNTL/OMA_DRM_related_questions.htm

[9] L. Korba and S. Kenny, “Towards Meeting the Privacy Challenge: Adapting DRM”, Springer

[10] Wikipedia, “DVB-CPCM”, http://en.wikipedia.org/wiki/DVB-CPCM

[11] DVB, “DVB Document A094 Rev. 1”, www.dvb.org

[12] Popescu, Crispo, Tanenbaum, Kampermann, “A DRM security architecture for home networks”, Proc. 4th ACM Workshop on Digital Rights Management

[13] Koster, Kampermann, Lenoir, Vrielink, “Identity Based DRM: Personal Entertainment Domain”, Springer

[14] Sony, “Oppdaterte funksjoner (ver 2.00)”, http://no.playstation.com/help-support/ps3/guides/detail/item85149/Oppdaterte-funksjoner-(ver-2-00)/

[4] Wikipedia, “RSA”, http://en.wikipedia.org/wiki/Rsa