Privacy Protection for Signed Media Files:
A Separation-of-Duty Approach to the Lightweight DRM (LWDRM) System

Rüdiger Grimm
Technische Universität Ilmenau
Am Eichicht 1
D-98693 Ilmenau
ruediger.grimm@tu-ilmenau.de

Patrick Aichroth
Fraunhofer Institute for Digital Media Technoilogy
Langewiesener Str. 22
D-98693 Ilmenau
ath@idmt.fraunhofer.de

ABSTRACT
The aim of strong digital rights management (DRM) is to enforce usage rules in end-user devices on behalf of content providers. Strong DRM is not well accepted by customers. Moreover, strong DRM is repeatedly circumvented and broken. Since Napster (and all its Peer-to-Peer follow-ups), the Internet is flooded with illegal digital content. We introduce the LWDRM technology as an alternative model. LWDRM relies on responsible behavior of customers. However, LWDRM contains a privacy problem, in that users sign media files which they wish to transfer freely from one place to the other. In this paper, we will explain the basic idea of the LWDRM technology and we will discuss the related privacy problem. We will show that there are methods to use LWDRM technology in compliance with privacy requirements of the users. A simple approach to harmonize LWDRM with privacy is separation-of-duty between certification authorities and content providers. Other, even more advanced models can be realized as well.

Categories and Subject Descriptors
K4.4 [**Computers and Society**]: Electronic Commerce – *Intellectual Property, Security.*

General Terms
Economics, Security, Human Factors, Legal Aspects.

Keywords
Virtual Goods, LWDRM, Light Weight Digital Rights Management, Privacy, Pseudonyms, Separation of Duty.

1. INTRODUCTION: The Problem of Digital Rights Enforcement
Thanks to modern compression techniques (e.g., MP3 from Fraunhofer IIS, standardized in the MPEG series) and increased bandwidth (the Internet and fast access even at home by DSL), the distribution of digital music, video and other media via the Internet has become affordable and easy. In fact, it has become simple enough to allow anyone to act as a distributor. This is exactly what happened with systems like Napster, Kazaa, Gnutella, Freenet and other file sharing systems.

Traditionally, publishers have a centralized view. Publishers assume that free usage of digital content out of their control would undermine their business models. Therefore music publishers rely on so-called strong Digital Rights Management (DRM) systems which control the usage of content [7,13]. The world of DRM technology consists of a huge set of mutually incompatible functions and formats, among which Microsoft (Windows Media Audio and Video), IBM (EMMS), Apple (FairPlay), and InterTrust (MPEG) are only a few among the best known. Also, there are many different digital rights languages, such as XrML (Xerox), ODRL (Australia), XCML (RealNetworks), or MPEG [8] which yield different mutually incompatible interpretation and enforcement functions. A good overview is given by [13]. However, the basic idea of strong DRM is always the same, and straight forward.

The enforcement of rights on digital content requires functions in the end-user devices which do the job: to control the usage of the content. A typical approach is given by the MPEG-21 standard IPMP – Intellectual property management and protection [7]. The rights holder specifies usage rules associated with the digital item he holds rights about, and encodes them within the digital item declaration which is, together with the content, part of the MPEG format of the media file. When downloaded to the user, so-called IPMP tools within the end-user device read and execute the usage rules associated to the downloaded content. Usage rules may restrict the replay environment by domain names, number or time intervals of replays, or combinations of those. The end-user device would not play a digital item if the rules would not allow so.

The main problem of digital rights enforcement by usage rules is that the content provider has an interest in the enforcement of the rules, but he has no power to do so. The power of enforcement is exclusively on the customer's side, who, however, has no interest in them. Customers are interested in free usage or, as cooperative economic partners, in fair usage. Usage rules normally disallow fair use. Therefore, users ignore usage rules. Many consumers circumvent usage restrictions, in that they consume and distribute digital music freely, that is, they use it illegally in the view of the publishers. Again, this is exactly what happened since Napster.

Content providers and consumers treat each other as enemies with conflicting interests. This conflict blocks the development of a growing business on the Internet. We are looking for alternatives that overcome this paradoxical situation.

MM&Sec'04, September 20–21, 2004, Magdeburg, Germany.

The rest of the paper is organized as follows: In the next section 2 we will give an overview of two alternative protection models for rights on digital content, the Potato system, and the LWDRM technology. In section 3 we will describe the LWDRM technology in more detail. In section 4, we will explain the certification model of public keys which are used to verify signed content. In section 5 we will address the privacy problem of LWDRM. We introduce a separation-of-duty concept for the verification of user names, by separation of certification authorities from the content providers. In section 6 we will sketch more flexible identity management models, ranging from anonymous users to frequently changing user ids. Finally, in section 7 we will draw some conclusions, especially for further work to be done.

2. Alternative protection models: Potato and LWDRM

One radical approach, which gives the customers freedom to decide if they are willing to pay for digital products or not to pay, is the so-called Potato system, which we have introduced in [6, 11]. The Potato system introduces incentives to the users to pay. Users who pay are automatically integrated in a provision model. If a digital item (e.g., an MP3 file) which was paid for by customer Ginny, is transferred to Harry, and if Harry pays for this item as well, Ginny will receive a percentage provision of up to 35%. There are more incentives, such as better service and integration in a community. Therefore, the Potato system works well for communities who have strong feelings for the content, such as young fans of local music. Users are convinced to pay for digital content because they are interested in the advantage of payment. We will not discuss the Potato system in this paper.

Another alternative protection method of digital content is given by the "Lightweight Digital Rights Management (LWDRM)" technology, which we introduced in [9, 10]. In LWDRM, there are two file formats. One format is the so-called "local media file (LMF)" format, which binds a media file by hardware-driven keys to the very end-user device on which the file was downloaded. The LMF format is bound to a simple strong DRM rule, namely that this file may be consumed on this device freely, but it cannot be transferred outside of this device. If a user wishes to transfer the content to another device, for example within his private home network, he can transform the LMF to a so-called "signed media file (SMF)" by signing the content (in fact he signs and encrypts the file in one step, for details see below). The content may leave the end-user device within the SMF format and can be distributed freely. The user will not transfer the file illegally to places out of his reach, because it contains his signature, such that the file can be identified as illegal. Even worse, the illegal file can be traced back to the illegal source.

So far, we have sketched three fundamentally different approaches to the protection of rights on digital items. Approach number 1 is "strong DRM" which enforces rights: users cannot act illegally. Approach number 2 is the "Potato system" which encourages users into a provision model: users do not want to act illegally. Approach number 3 is the LWDRM technology by which users earn fair usage of digital items if they sign them: users do not dare to act illegally.

We will not discuss strong DRM or the Potato system any deeper. In this paper, we want to discuss the LWDRM approach. In particular we want to discuss the privacy problems of LWDRM. Of course, we do not want to break privacy of users. There is no need to. On the contrary, we will show that there are methods to keep illegal content from the network in full accordance with privacy requirements of the users. In this sense, the LWDRM technology protects both sides: illegal SMF content will no longer invade in mass portions the Internet, and their customers can use the content fairly, without fear to lose their privacy.

3. LWDRM and the Signed Media File

As said above, "Lightweight Digital Rights Management (LWDRM)" technology [9, 10] supports two file formats: the "local media file (LMF)" format, which binds a media file by hardware-driven keys to an end-user device, and the "signed media file (SMF)" format which (technically) allows the file to be transferred freely from the original end-user device through the electronic world. The user will not transfer the file illegally to places out of his reach, because it contains his signature. As a second line of defense, it contains also a watermark. By this means, the SMF format is related to the "responsibility" of the customer for the product he has purchased and which he wishes to consume freely by the fair-use principle.

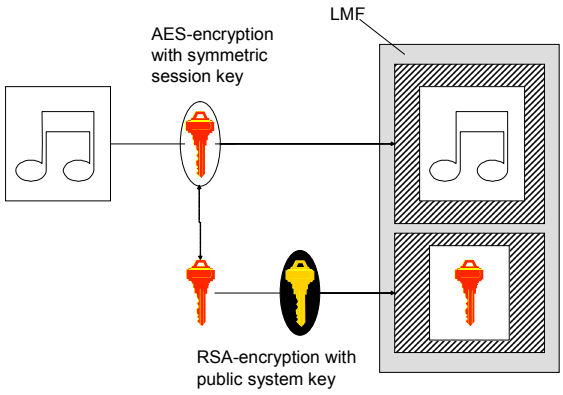

Figure 1: Local Media File (LMF) bound to consumer device by public system key

When a customer purchases content by download from a content provider (shop) he would receive a local media file (LMF) format bound to his target consumer device.

For the local binding of the content, LMF uses a hybrid approach: The content is symmetrically AES-encrypted using a randomly created session key, while the session key itself is asymmetrically RSA-encrypted using the public key of the target system. The session key (and therefore the content itself) can only be accessed by applying the corresponding private key, which is only available on the target system. The asymmetric RSA key pair is created using parameters of the target hardware system. Only the target system can derive the private key from its hardware parameters. The private key decrypts the session key, the session key will decrypt the content.

LMF cannot be transferred to other devices. In particular, LMF cannot be used on any other device, not even within the personal environment of its owner. LWDRM technology opens a gate to free

transfer. The user can release the content from its local binding, by transforming the LMF into a signed media file (SMF) format. However, this requires that the user accepts to sign the content with his personal identity. First the session key is decrypted using the private key of the target system which is available on the target system to which LMF is bound. Then, instead of encrypting the session key with the public system key, the session key is "signcrypted" using the private key of the user (not of the target system!), thus replacing the local binding with a binding to the user. The private user key is only available to the user, thus implying the non-repudiation of the personalization.

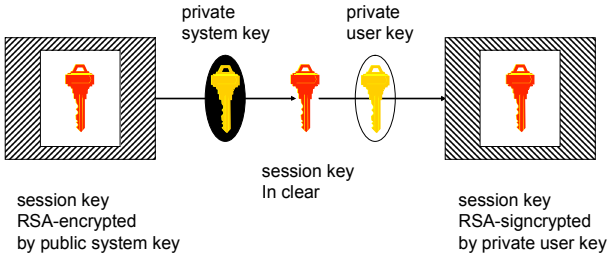

Figure 2: Releasing the session key from its local binding and rebinding it to the user

The resulting SMF contains: the watermarked and encrypted content, the corresponding signcrypted session key, the user's public key certificate, and a purchase receipt signed by the shop

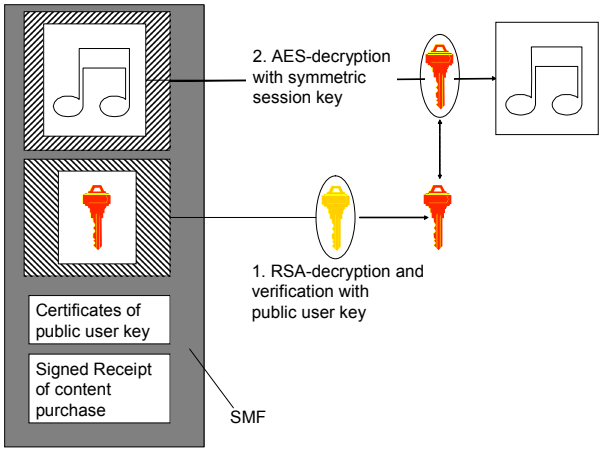

Figure 3: Signed Media File (SMF) bound to the user by his personal signature key: the symmetric session key is signcrypted by the user's private signature key; the receipt is signed by the content provider.

The accompanying certificate binds the user's public key to the user's name (see the following section 4 on certification of public keys). It allows for access to the content, and for the verification of the personalization at the same time: The certificate contains, among other things, the user's public key. For playback, this public user key is used to un-signcrypt the session key, which is again needed to decrypt the content. The step of un-signcrypting the session key includes verification of the personalization. Applying the public key of a user means that the very same user must have done the personalization, using his private user key, before.

The receipt is signed by the shop. It serves as a proof of purchase for the user, containing information about the transaction, a content id, user id, and the id of the shop. If the rights holder is willing to grant the permission, it can also carry information about whether the content may be shared with others ("free" vs. "private" content).

Thus, an SMF contains all information necessary to render that content. However, in consuming SMF the consumer verifies the content's ownership. We propose that SMF is an open format which is to be standardized. The essential parts of SMF such as receipt, certificate, and signcrypted session key, cannot be manipulated. It represents an idea that is very different from common DRM approaches, because it does not prevent the user from accessing the content in the first place.

4. Certification of public keys

Public keys are public, that is, everybody can use them to identify the signer of a digital item. A public key is a (large) number made for "decryption" of a cryptogram called "digital signature". Details on digital signatures and signcryption in particular can be found at [14, 17]. The naked public keys contain no information whatsoever about their owners. Public keys are linked to the owners of the related private keys by means of digital certificates. Some trusted "certification authority" states by a digital certificate: "this-and-this public key belongs to an owner of a private key who has that-and-that name". Digital certificates contain a public key, the name of the owner of the related private key, name and signature of the certifying authority, and other related information such as validity time intervals and algorithm identifiers. Two types of certificates have become common for practical use in the Internet, PGP and X.509 [12, 16]. The main difference between these two approaches is that PGP aims on a decentralized "web of trust" where everybody can certify everybody else, while X.509 aims on hierarchical certification trees. X.509 certification trees are better scalable and serve environments with hierarchical responsibility.

An X.509 public key certificate type:

```
Version
Serial Number
Certificate Signature Algorithm
Issuer (name of certification
       authority)
Validity
   Not Before
   Not After
Subject (name of certificate holder)
Subject Public Key Info
   Subject Public Key Algorithm
   Subject Public Key
Extensions (optional)
Certificate Signature Algorithm
Certificate Signature
```

Web browsers contain a certificate management area within the browser preferences, where users can enter and view the certificates accepted by their browser.

How could public-key certificates be used for LWDRM signcrypted SMFs? X.509 type certificates have the advantage of a simple hierarchy, and they serve the S/MIME message formats widely in common use [15]. We suggest a 2-layer model of one root certification authority and an open set of user certification authorities for customers and providers of digital products. For example, the music industry could agree on a root certification authority (root CA) which certifies an open set of user certification authorities (user CAs). Customers of music products who wish to create signed media files by signcryption with their private key are certified by user CAs.

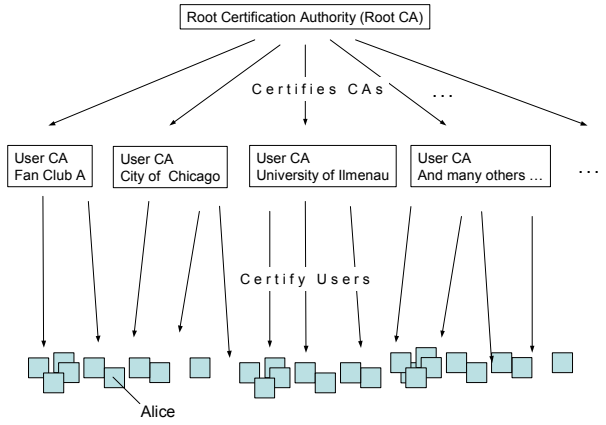

Figure 4: A 2-layer X.509 certification hierarchy

A customer signature would contain two certificates: the first certificate is the user certificate and links her name (Alice) to her public key and is signed by a user CA (Fan Club A); the second certificate is issued by the root CA and links the public key of Fan Club A to the name "Fan Club A". The public key of the root CA would be known to the whole music world.

Certification path of a signed media file of Alice:

1. User certificate of Alice issued by user CA Fan Club A:

```
Version: 3
Serial Number: 2512
Certificate Signature Algorithm:
RSA with MD5 (PKCS#1)
Issuer: OU= Fan Club A; O=Music Online
        Magazine; C=De
Validity
   Not Before: 01.01.2004 06:00:00
   Not After:  02.01.2006 21:00:00
Subject: CN=Alice; OU= Online Service;
         O=City of Erlangen; C=De
Subject Public Key Info
   Subject Public Key Algorithm:
   RSA with MD5 (PKCS#1)
   Subject Public Key: 30 9d ...
Extensions (optional)
Certificate Signature Algorithm:
RSA with MD5 (PKCS#1)
Certificate Signature: b7 60 ...
```

2. Root certificate of user CA Fan Club A issued by root CA:

```
Version: 3
Serial Number: 4711
Certificate Signature Algorithm:
RSA with MD5 (PKCS#1)
Issuer: O=Root CA; C=De
Validity
   Not Before: 10.12.2003 15:36:36
   Not After:  29.11.2005 15:36:36
Subject: OU= Fan Club A; O=Music
         Online Magazine; C=De
Subject Public Key Info
   Subject Public Key Algorithm:
   RSA with MD5 (PKCS#1)
   Subject Public Key: ae 09 ...
Extensions (optional)
Certificate Signature Algorithm:
RSA with MD5 (PKCS#1)
Certificate Signature: 7f ca ...
```

We regard it as important, that the certification authorities are independent of the music providers. Moreover, we offer cross certificates to other certification environments. Any holder of a digital certificate is able to produce signed media files and become a free consumer in the sense of LWDRM regardless where he has received his certificate from, as long as his certification authority is cross-certified by any of our certification authorities. For simplicity and privacy reasons, however, any user who has no certificate of one of our certification authorities, would receive a certificate from one of our certification authorities automatically to make sure that he can act under a pseudonym. The details of our support for pseudonymous actions are outlined in the following section.

5. Privacy concern and separation of duty solution

LWDRM technology introduces source markings into media files in order to support business designers to tell legal from illegal content. This does not necessarily imply that illegal content is traced back to the source. Different policies may be in force. For example, illegal content can simply be removed instead. If there is suspicion of criminal energy, for example by re-sales of stolen media, sources may be traced, as usual in the real world.

Whatever policy is in force, LWDRM technology introduces user signatures into media files which may be transferred over the network. Therefore, there is always a privacy problem. Users must be aware, that they produce traces in the network which may be followed by others, authorized or unauthorized instances. Users have the right (and a strong demand) not to lay traces in the network. On the other hand, responsible behavior means that users can be accounted for their behavior. So, how can privacy and responsibility requirements be peacefully married? Note that this requirement holds regardless of the business and rights enforcement model.

It has been noted at many other places already, that digital rights management (DRM) is dangerous for privacy anyway, for example by the American "Electronic Privacy Information Center" [2]. We regard privacy as one of the main elements for user

acceptance of technology [5]. Therefore, we take privacy concerns very serious.

A simple way to hide traces of personal data is a separation-of-duty approach. The separation-of-duty principle, while being well established in the traditional commerce world, was first introduced into the IT security community by Clark and Wilson 1987 [1]. However, Clark and Wilson did not address privacy. In their "Integrity Model", well-formed transactions of sensible data should follow the "separation-of-duty" principle, in that they must be authorized by two different persons who are unlikely to collaborate against the system application environment. One reason for their well-behavior may be, as Clark and Wilson suggest, that they are from different social background. The Integrity Model has been both praised and criticized for the introduction of non-technical elements such as "unlikely to collaborate", "different social background". We believe that privacy is indeed a challenge which must be supported both by technological and organizational means. Separation of duty can be well applied for privacy protection.

The technological basis of separation-of-duty for signed media files is the separation of user names from pseudonyms to cover consumer actions in the LWDRM context. We call the pseudonyms "consumer identifiers".

A user of the Web who buys a digital product makes a contract with a content provider under her pseudonymous consumer id ("Alice"). The receipt included in the LMF contains the consumer id, not the (real) user name. When, later on, the user decides to signcrypt the content and thus creates an SMF, the signature certificate contains the consumer id, not the user name. Content providers as well as observers of SMFs will (normally) not know the user names, but only the pseudonymous consumer ids. They don't know who Alice is.

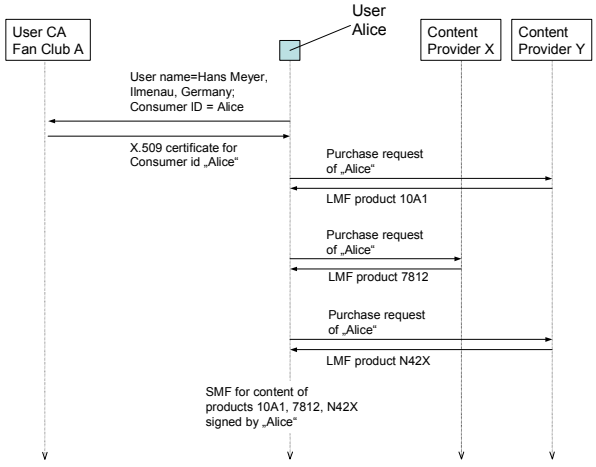

Figure 5: Separation of purchase data from user names

Nevertheless, communication between content providers and their customers is authentic, in that customers sign SSL authentication, as well as any contracts by their customer id, which is certified by an official certification authority. Whatever SMFs a customer creates she will sign under her customer id as well. The certification authorities do know the names of the users they certified pseudonymous public keys for, they keep maps of user names ("Hans Meyer from Ilmenau, Germany") on consumer ids ("Alice").

The separation-of-duty principle is satisfied by the separation of purchase data from user names: The content provider knows purchase data, but no user names. The certification authorities know user names, but no purchase data. In order to trace back a concrete purchase, or a concrete SMF, content provider and certification authority must collaborate in order to uncover the consumer id. Therefore it is essential, that these two instances are independent from one another.

The same kind of separation of duty is realized by the German electronic payment cards GeldKarte [4]. Banks can map bank account numbers to card ids; independent "evidence centers" can map card ids to payment data and initiate accumulated payments between banks (not between individual account numbers); and shops can map payment data to purchase data. In order to trace a purchase back to the real buyer, all three instances must collaborate.

In LWDRM, when illegal content is found in a file sharing system or elsewhere, the SMF reveals a signature and a responsible consumer id. It does not reveal the correspondent user name. A certification authority will not uncover the user name unless it is legally forced to. The standard behavior of the identification of illegal content is to delete the content, not to pursue the consumer. Consumers will only be pursued if there is serious suspicion of criminal activity.

How does a customer receive a pseudonymous certificate? The very first time when the user attempts to create an SMF from a legally purchased LMF, her LWDRM user tool will connect her with an LWDRM conformant user CA. Remember, that LMF is bound to one and only one end-user device by hardware driven keys and that the user needs to signcrypt the content when she wants to move the content to another place. Signcryption is part of the SMF format. If the user has already a certificate from another CA, the LWDRM conformant CA will simply accept this certificate and provide the user with a pseudonym (or accept a pseudonym suggested by the user, resp.). The user CA will issue a related LWDRM conformant user certificate with respect to this pseudonym. It will insert the mapping of the name of the original certificate's subject name to the new pseudonymous consumer id in its local list. If, however, the user does not already have another certificate, she would have to reveal her real name and affiliation or geographic belonging to the LWDRM conformant user CA. The user CA would then provide the user with a pseudonym and issue a related LWDRM conformant user certificate. At this point the user is authenticated and registered with her real name. The CA will insert the mapping of the name of the user to the new pseudonymous consumer id in its local list.

Now, the customer owns a digital certificate related to a pseudonymous customer id ("Alice") and is able to signcrypt any LMF content she wishes to convert to an SMF and transfer it to another place. Observers of the SMF will read the customer id both in the SMF, and in the receipt of the content provider: they will read "Alice", but they will not know who Alice is. The user CA either knows who Alice is, or has at least another subject name of Alice which is listed in another CA. Therefore, no unauthorised observer will be able to trace Alice to her real identity. In order to uncover her identity, one or more CAs must cooperate.

6. Privacy models for LWDRM

Separation of purchase data from real user names by pseudonyms (customer ids) which can only be uncovered by neutral user CAs is a simple method to protect the privacy of customers. This method is applied by the German electronic payment card GeldKarte [4], for example. However, this is only a first approach to privacy protection of users by introducing pseudonymous consumer ids. More refined models must be developed, such as changing ids and pseudonyms which are truly anonymous.

A more refined method is a method to change pseudonyms from time to time, or from content provider to content provider, or, even more radical, for every purchased product. This way, there would never be a visible trace of a user's products in the network, not even along his pseudonyms.

Another possibility is to refrain from links between customer ids and user names. Customer ids could be completely anonymous. In this case, nobody except the customer himself would be able to uncover his customer ids. Of course, illegal content could then never be traced back to their source without cooperation of the originators, who will most probably not be willing to cooperate. However, illegal content would be still identifiable as such. If a business model aims on the identification and removal of illegal content only, this anonymous approach is appropriate.

Further, like with credit cards, customers should have the chance to restrict their liability to a certain amount of money, or to a certain amount of products, or to a limited time period. There may be a general limitation by the business model of content providers, or by user CAs, or by a cooperative agreement between content providers and user CAs. Under such an agreement the customers' risk by errors or unwanted misbehavior with SMFs would not be out of control.

The business model of liability limits is well known and accepted by all credit card organizations. The limit is activated by revocation. This could also be done with SMFs. In the context of digital signatures revocation is an important issue anyway. Therefore, a revocation service must be included in the LWDRM application context. With respect to privacy, different models can be followed. For example, revocation deletes the relationship of a real user name to a pseudonymous customer id for the future, but not for the past. For a certain time period in the past, liability for misbehavior with this pseudonym could be limited. Another model could allow content providers to revoke customer ids which have become known to be used for illegal content distribution. It is a matter of further careful study, how fair revocation services can be realized, and also how revocation lists can be disseminated in the network. Revocation of revocation is also an issue, especially for the protection against attacks on reputation.

7. Conclusions

The protection of rights on digital content is not only a matter of technology. It is a matter of the way human beings produce, distribute, and consume content, i.e. a matter of business cooperation. It is important to save the rights of the publishers. In the same way, the users' interest must not be forgotten. It is the users who have the technological and economical power to decide on the success of the business models. Users wish to use the products they have purchased in a fair way. Responsibility of customers for their products is one vehicle to govern legal behavior. However, responsible behavior must never be on cost of privacy.

We believe that LWDRM technology can support both, responsible behavior of free customers, and their privacy. Customers of digital content are technically allowed to transfer their media files form one place to another, even across networks, if they signcrypt the content in a so-called "signed media file". In this paper we have introduced a simple separation-of-duty approach to privacy protection for LWDRM: In order to protect customers from unauthorized observation of their media consumption, they sign with pseudonyms, not with their real names. Observers of signed media files, as well as content providers will not be able to link the pseudonyms with the real user names. This mapping can only be done by neutral CAs, which are not observing media files.

There are more flexible privacy models for LWDRM which need to be substantiated. Identity management is one of the key words which stimulate studies in this direction, for example see the work of M. Hansen [3]. An important issue to be solved is the combination of revocation and privacy, both to protect users against wrong accusation, and content providers against malicious customers

8. ACKNOWLEDGMENTS

The LWDRM technology is developed jointly by colleagues of the Fraunhofer Institutes IIS, Erlangen, and IDMT, Ilmenau, as well as 4FO AG, Ilmenau [www.4friendsonly.com]. Among many others, Christian Neubauer, Karlheinz Brandenburg, and Jürgen Nützel play a leading role. The idea to utilize the separation-of-duty concept to overcome the privacy problem of LWDRM was developed on a summer excursion of our IDMT institute in the beautiful Thüringer Wald last summer, by all members of our research group, including especially Jens Hasselbach and Stefan Puchta. We are thankful that Marit Hansen (ULD Schleswig-Holstein) has offered to cooperate with criticism and ideas in order to improve and refine privacy models for the LWDRM application type.

9. REFERENCES

[1] D. D. Clark; D. R. Wilson: A Comparison of Commercial and Military Security Policies. Proceedings of the 1987 IEEE Symposium on Security and Privacy, Oakland, California. Computer Society Press of the IEEE, Washington D.C., 1987, 184-194.

[2] EPIC: DRM Anti-Consumer, Threatens Privacy, Free Speech, Fair Use. In comments to the Department of Commerce Technology Administration workshop on Digital Rights Management (DRM), see the EPIC DRM Page www.epic.org/privacy/drm/tadrmcomments7.17.02.html (July 18, 2002)

[3] Sebastian Clauß, Marit Köhntopp: Identity Managements and Its Support of Multilateral Security; in: Computer Networks 37 (2001), Special Issue on Electronic Business Systems; Elsevier, North-Holland 2001; 205-219. See also http://marit.koehntopp.de/pub/idmanage/index.html

[4] GeldKarte: Interface Specification for the EC Card with Chip (in German language). Bankverlag, Postfach 300191, 50771 Köln.

[5] Grimm, R.; Roßnagel, A.: Can P3P help to protect privacy worldwide? Proceedings of the ACM International Workshop on Multimedia and Security, November 4, 2000. Los Angeles,

California, pp 157-161. A short version of this paper is available from http://www.w3.org/P3P/

[6] Grimm, R.; Nützel, J.: Digital Rights Management, Security and Business Models. ACM Multimedia and Security Workshop. Dec 6, 2002, Juan le Pins, France. http://www1.acm.org/sigs/sigmm/MM2002/

[7] ISO/IEC JTC 1/SC 29/WG11: Coding of Moving Pictures and Audio: Requirements for MPEG-21 IPMP, Final Draft, München, March 2004, 28 pages.

[8] ISO/IEC IS 21000-5, Rights Expression Language, July 2003 (FDIS, N5839).

[9] Neubauer, Ch.; Pickel, J.; Brandenburg, K.; Siebenhaar, F.: Aspekte des Rechtemanagements für digitale Güter, 22. Tonmeistertagung, Hannover, November 2002, VDT.

[10] Neubauer, Ch.; Brandenburg, K.; Siebenhaar, F.: Technical Aspects of Digital Rights Management Systems, In 113th AES-Convention, Los Angeles, October 2002. Convention Paper 5688.

[11] Nützel, J.; Grimm, R.: Potato System and Signed Media Format - an Alternative Approach to Online Music Business, Wedelmusic 2003 Conference, Leeds, United Kingdom, 14th - 17th September 2003, p. 23 – 26.

[12] OpenPGP Message Format. Internet Standard RFC 2440 by J. Callas, L. Donnerhacke, H. Finney and R. Thayer. Nov 1998, 65 pages, http://www.ietf.org/rfc/rfc2440.txt. See also the OpenPGP Alliance home page http://www.openpgp.org/

[13] Rosenblatt, B.; Trippe, B.; Mooney; S.: Digital Rights Management – Business and Technology. M&T Books, Hungry Minds Inc., New York, 2002, 288 pages.

[14] Schneier, B.: Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd Ed. Wiley & Sons, Chichester 1996, 758 pages.

[15] S/MIME Version 3 Message Specification. Internet Standard RFC 2633 by B. Ramsdell (Ed.), June 1999, 32 pages. http://www.ietf.org/rfc/rfc2633.txt

[16] ISO/IEC 9594, ITU X.500 (1988/92): Information technology – Open Systems Interconnection – The Directory 1993(E). Contains: X.509 – The Authentication Framework.

[17] Zheng, Y.: Digital Signcryption or How to Achieve "Cost(Signature&Encryption) << Cost(Signature) + Cost(Encryption)", Advances in Cryptology – CRYPTO '97, Springer, LNCS 1294, p. 16 ff.