Controlled Sharing of Personal Content Using Digital Rights Management

Claudine Conrado, Milan Petkovic, Michiel van der Veen and Wytse van der Velde

Department of Information and System Security
Philips Research, High Tech Campus 34 MS61
5656 AE Eindhoven, The Netherlands
{claudine.conrado, milan.petkovic, michiel.van.der.veen}@philips.com
w.h.vandervelde@gmail.com

This paper describes a system which allows controlled distribution of personal digital content by users. The system extends an existing Digital Rights Management system for the protection of commercial copyrighted content by essentially allowing users to become content providers. This fact, however, makes the system vulnerable to illegal content distribution, i.e., distribution by users who do not own the content. To solve this problem a solution is proposed which involves the compulsory registration with a trusted authority of a user's personal content. During registration, the association between user identity and content is securely recorded by the authority, but users have the possibility to remain anonymous towards any other party. Moreover, in case the initial content identification fails and content is illegally registered, the authority can ensure user accountability.

Keywords: Digital Rights Management, content distribution, content protection, commercial content, personal content, security, privacy

ACM Classification: J.7 (Computers in Other Systems)

1. INTRODUCTION

Recent developments in digital technologies, along with increasingly interconnected high-speed networks and the decrease in prices for high-performance digital devices, have established digital content distribution as one of the fastest emerging activities nowadays. This trend of digital content distribution gives great opportunities for commercial content providers but also poses threats as digital content can be very easily illegally copied and distributed. Therefore, commercial content providers need technologies, accompanied by legislation, that can protect digital content from illegal use. Digital Rights Management (DRM) is a collection of technologies that provides content protection by enforcing the use of digital content according to granted rights. It enables content owners and content providers to protect their copyrights and maintain control over distribution of and access to content.

In parallel to the introduction of multimedia download services, there is also a clear increase in production of personal digital information by consumers including digital photos, home-video, text, and so on. This is inspired by the ever decreasing prices of digital cameras, camcorders, mobile phones, storage devices, as well as cheaper high-speed Internet. As a consequence, consumers have

Manuscript received: 12 April 2005
Communicating Editor: Julio Cesar Hernandez

to deal with an ever growing amount of personal digital data, alongside the downloaded commercial content. Some of this personal content might be highly confidential and in need of protection, therefore users may want to share it in a controlled way. This means that the content owner should be able to control the use of his content by other users with whom he shares it. For instance, the owner could specify rights such as play, play once and copy, which are enforced when those users access the content. More importantly, the owner could control further distribution of his content by preventing the users with whom he shares the content from spreading it further. However, in contrast to a lot of effort which has been put into the protection of copyrighted commercial content in a number of different DRM systems currently available, controlled sharing of personal content is often ignored.

In this paper, an approach to controlled sharing of personal content is described which reuses the concepts defined in DRM systems used by the commercial content owners. However, when personal content and commercial content are managed together in one system, the clear line between producers and consumers of content (or content providers and users) fades. Every user of the system is a potential content provider and is able to create and introduce new content into the system. As a consequence, numerous new issues arise such as the requirement that the security of the system should remain the same as before the introduction of personal content. This means that the system should prevent illegal distribution of commercial content as well as personal content. Further requirements are that content owners should be able to protect their privacy and the security of their content, even when jointly owning content. Therefore, while extending the DRM system to support controlled sharing of personal content, focus is put on preserving the system's security.

The remainder of the paper is organized as follows. In Section 2, the related work is reviewed. Section 3 discusses a solution that extends an existing DRM system for commercial content to support controlled sharing of personal content. In Section 4, a description of a method that prevents illegal sharing of commercial content and its security's aspects is given. Section 5 describes an extension of the system that enhances user privacy and allows private multiple ownership of the content. Finally, Section 6 draws conclusions.

2. RELATED WORK

Sharing of digital personal content, especially over the Internet, is nowadays widespread. For instance, P2P distribution networks have become one of the most used technologies for sharing content between people, which is attested by the popularity of applications such as KaZaa. However, these applications do not provide any control over the distribution of content and therefore allow illegal distribution of commercial content, in particular copyrighted music and movies.

From the commercial content industry's point of view, illegal sharing of protected commercial content is one of the major downsides of the P2P technology. However, P2P networks do have the potential to provide an industry-compliant distribution model. The success of Apple's iTunes (iTunes, 2005) provides some evidence that there are possibilities of using copyright-compliant systems in a profitable way, provided that the incentives for using such a system are high enough. In the case of iTunes, these incentives are quality, availability and price of music.

Other proposals for providing such incentives have been presented, e.g., the Music2Share system (Kalker, Epema, Hartel, Lagendijk and van Steen, 2004). It uses quality control of music and combines this with relatively free usage conditions and an easy payment structure to make it interesting for users.

Another proposal by Grimm and Nützel (2002) combines the idea of DRM and P2P file sharing with the idea that a user who has paid for content can redistribute this content against payment.

Users that do not pay are unable to redistribute content, thus providing an incentive for payment.

In this paper, a different way to create an incentive is proposed: users of a commercial content protection system can utilize the same protection mechanisms which are used for commercial content also for their own personal content. In this way, the DRM system, instead of only restricting users, also helps those users by protecting their personal content. This presumably gives a much more positive image to DRM as a technology which can support and be in fact beneficial to users. Moreover, it gives an incentive to users to support the system and prevent that its security be compromised in any way.

3. A DRM SYSTEM FOR PERSONAL AND COMMERCIAL CONTENT

In this section, a DRM system for controlled distribution and usage of commercial as well as personal content is presented. The basics of the system, its components and settings are described in the next section, while Section 3.2 explains how the system is used for content protection and sharing.

3.1. System components and authorization hierarchy

The system is an extension of the DRM framework for protection of commercial content introduced by van den Heuvel, Jonker, Kamperman and Lenoir (2002). In the extended DRM system, users are able to protect and controllably share their personal content. This effectively means that the user who is the owner of the content takes over a role of content and license provider and therefore becomes involved in the content and license creation as well as content protection tasks. Considering personal content, owners will most likely be sharing content with other users, so the *person-based* DRM model (Conrado, Kamperman, Schrijen and Jonker, 2003), in which rights to access content are granted to persons rather than devices, is used as a basis for the presently described DRM system.

While describing the system, components and properties are highlighted which are relevant for the protection and sharing of personal content. Most of these system components are also part of the original DRM system for protection of commercial content and are described below:

i) *personalized smartcard:* a device used for user identification. The smartcard contains a private key which corresponds to the public key of the user. The public key is certified by some Trusted Third Party (TTP). Therefore, the TTP knows the link between the user's identity and his public key.

ii) *compliant device:* a device that behaves according to the DRM rules. It can identify a user by means of a personalized smartcard. The compliant devices provide a secure and robust computing platform for the DRM operations and offer a secure storage for keys and state information used in the system.

iii) *content container:* personal digital content is stored in encrypted form together with a unique content identifier (the "content container" abstraction) and can be retrieved from anywhere in the network.

iv) *Content Right:* a certificate issued by the content provider containing the content identifier, a content encryption key (CEK), the User Right Authority's public key and the content provider's signature. The Content Right is securely stored in the compliant device or securely obtained from a content provider.

v) *User Right:* a certificate issued by the User Right Authority authorizing a person to use content according to granted rights. It consists of content identifier, user identifier, rights expression and

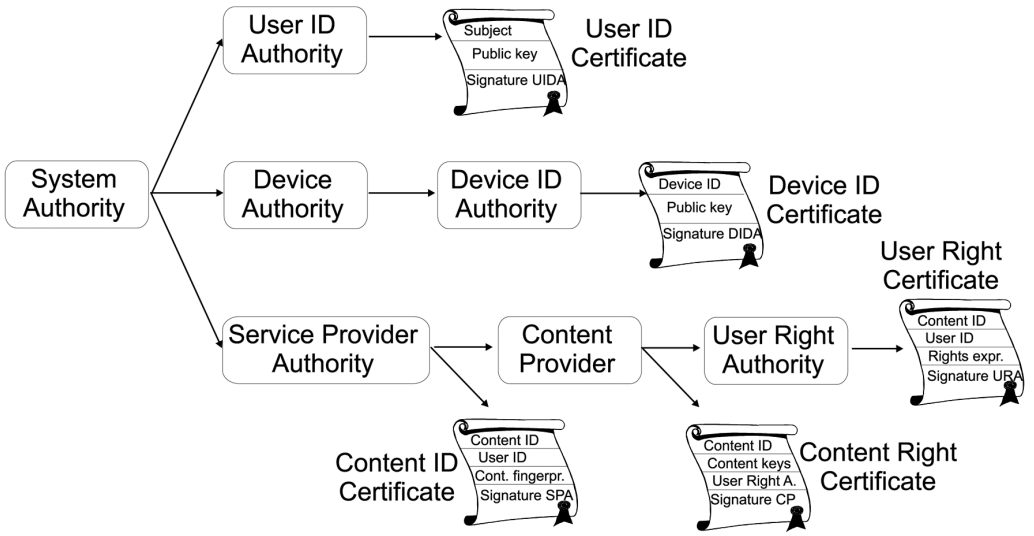


Figure 1: Certificate Authorization Hierarchy

the User Right Authority's signature. User Rights may reside anywhere in the system and are normally not stored in a secure way. Moreover, Content Right and User Right may be merged in one license (OMA-DRM, 2004).

vi) *Content ID Certificate:* a certificate that creates a secure link between content, its identifier and the content owner, who becomes also content provider. This certificate is needed for personal content, since the content provider may be any user in the system and needs, thus, to be explicitly linked to the content.

The certificates used in the system are issued by different authorities, which organize an authorization hierarchy depicted in Figure 1. The System Authority is the root of the hierarchy. Each compliant device has a built-in key of this authority. The Service Provider Authority (SPA) authorizes different content providers (users) by certifying their public keys and linking them with content items by means of the Content ID Certificate. Content providers are allowed to issue Content Rights. A Content Right contains in turn the public key of the User Right Authority. This construction allows content providers to delegate the issuing of User Rights. The User Right Authority issues User Rights for a certain piece of content. The Device Authority authorizes Device ID Authorities, e.g. device manufactures, to issue Device ID Certificates that give a unique identity to a device. The User ID Authority issues User ID Certificates. This certificate typically contains user identity information and a public key that identifies a user within the system.

3.2. Content protection and sharing

During the content protection and sharing procedures, a number of different transactions, schematically depicted in Figure 2, are performed within the system. The described transactions for content *protection* refer specifically to personal content: a user can act as a content provider, therefore this must be certified by means of the Content ID Certificate. The described transactions for content *sharing*, on the other hand, are essentially the same for both, personal and commercial

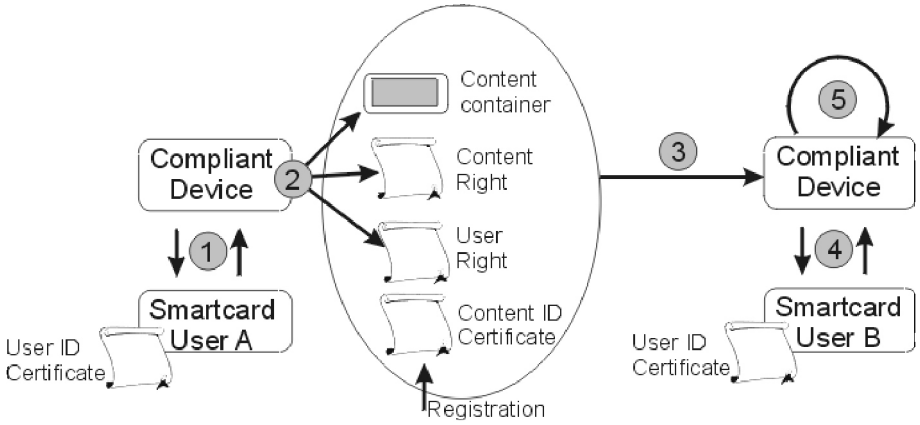


Figure 2: Representation of the various interactions in the DRM system

content, except that in the latter a (recognized) commercial content provider takes the role of the user. These transactions are described below, where references to the numbered links in Figure 2 are made at the appropriate points.

When a user Alice wants to protect a personal content item, in order to be able later on to share it in a controlled way, she registers the content with the SPA (content registration is discussed in the next section) and obtains a Content ID Certificate. The certificate consists of the fields Content ID, User ID, Content Fingerprint and Signature SPA. The Content ID field refers to the content itself. The User ID field contains the public key of Alice, who is then considered the owner of the content (as well as content provider). The Content Fingerprint is a short "summary" of the multimedia content which can uniquely identify that content. It usually consists of robust features extracted from the content (see van der Veen, Lemma and Kalker, 2004). Finally, the Signature SPA is the digital signature of the SPA on the certificate. The next step in the content protection process is creation of the Content Right together with encryption of the content. Before allowing Alice to create a Content Right, a compliant device authenticates her (step 1 in Figure 1) and checks whether she is authorized to do so by inspecting the Content ID Certificate, which must contain Alice's ID (her public key). If so, the compliant device proceeds with the creation of the Content Right certificate (step 2 in Figure 1) by randomly choosing a symmetric key (CEK), which is used to encrypt the content, and placing the key in the certificate. Additional information in the Content Right certificate includes the Content ID and the public key of the User Right Authority. Typically, this authority will be the content owner Alice, but she may also create a Content Right for other users allowing them to sign User Rights (i.e. to share the content). Finally, Alice signs the Content Right.

If Alice wants to share such protected content item with another user Bob, she creates a User Right certificate that includes the public key of Bob and sends the secure content container together with the necessary certificates (User Right and Content ID Certificate) to Bob (step 3 in Figure 1). The Content Right certificate is also needed but it should be securely sent directly to the compliant device that will be handling the content access action with Bob, since that certificate has the CEK, which can be used to decrypt the content. When Bob wants to access the content, he must have a valid User ID Certificate. He authenticates to a compliant device using his smartcard (step 4 Figure 1) and presents the obtained certificates from Alice together with the secure content container. The

compliant device must check the validity of the certificates before allowing access to the content (step 5 Figure 1.). Moreover, the device will compare the User ID from the User Right with the User ID in the User ID Certificate. It also has to verify that all certificates are used for the content whose identifier is in the Content ID Certificate. To do so, the compliant device obtains the CEK from the Content Right certificate, decrypts the content, calculates the fingerprint of that content and finally matches the fingerprint of the content with the fingerprint in the Content ID Certificate. If the fingerprints do not match, the device will detect a content substitution attack, which means that the original encrypted content in the content container has been replaced with a different content, but assigned the same identifier. The device in this case will not allow Bob to access the content.

4. REGISTRATION OF PERSONAL CONTENT

Any content which is to be protected under a DRM system must be recognizable within that system. In the case of commercial content, typically each content item is assigned a unique content identifier within that specific DRM system. This assignment can be thought of as the registration of the content item in the DRM system.

The DRM system described in the previous section is used to protect both commercial and personal content. The assignment of a unique content identifier to every piece of content that enters the system is still necessary. However, as now every user can become a content provider and sign certificates in such a system, there is a danger regarding illegal distribution of commercial content. The problem exists because there are no explicit measures to prevent commercial content from being distributed as personal content by users of the DRM system. Without preventive measures, a malicious user who has obtained an illegal copy of commercial content is able to distribute that content within the DRM system as his own personal content.

A solution to the problem above is to introduce a secure registration procedure that not only assigns a unique identifier to content, but also verifies the identity of content by using fingerprint technology (van der Veen *et al*, 2004). The registration procedure as well as its security aspects are discussed below.

4.1. The Registration Steps

To introduce a new content item into the system, the user Alice has to follow a number of steps which are described below and shown in Figure 3.

Step 1: Alice imports to her compliant device a content item that she wants to introduce. The device calculates the fingerprint of the content item.

Step 2: The device provides the SPA with the fingerprint of the content item and the public key of Alice.

Step 3: The SPA matches the fingerprint of Alice's content against a database of fingerprints from known commercial content and already registered personal content.

Step 4: If there is a match the SPA refuses to register the content item. Otherwise, the SPA proceeds by generating a Content ID Certificate and a database entry, with a time stamp on it, linking Alice's ID to the content (i.e., to its fingerprint). This allows the SPA to prevent other users from trying to later on register Alice's content as their own. Optionally, a watermark identifier and a watermarking key (van der Veen *et al*, 2004) are also generated by the SPA to allow the possibility of "forensic tracking" outside the DRM system, as discussed below.

Step 5: The SPA sends the Content ID Certificate (and the watermark identifier and watermarking key in case watermarks are used) to the compliant device.

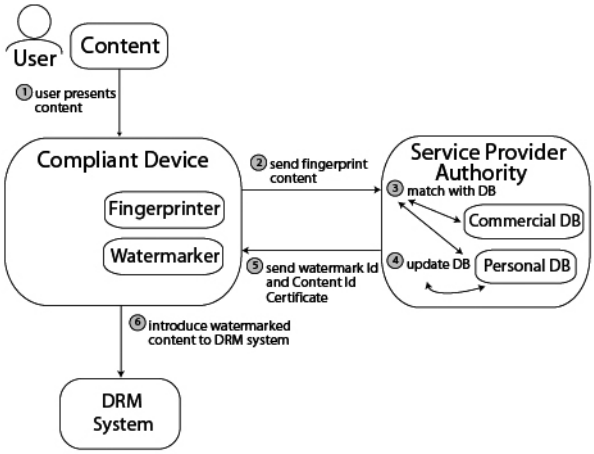


Figure 3: The Registration Phase

Step 6: Finally, all the necessary certificates are created so as to make the content suitable for distribution using the DRM system. When watermarks are used, the compliant device also watermarks the content with the watermark ID using the watermarking key.

4.2. Security Analysis

The threat model used for the present security analysis is as follows. A casual-copying model is assumed as described by Felten (2003). This means that the security of the system is not concerned with widespread copying and distribution by organized groups of criminals, but with small-scale and disorganized copying amongst small groups of ordinary users. The security of the system tries to frustrate and create barriers for would-be infringers. In the threat model, it is assumed that if the barriers for illegal distribution are high enough and there is an incentive for users to behave in accordance with the system, then most of the users will behave in such a way. Therefore, if only a few users manage to distribute illegal content within the system, the system itself does not fail regarding the threat model. With such a threat model in mind, specific system security aspects are discussed below.

Fingerprint Check and DRM Infrastructure. The goal of fingerprint identification at the beginning of the registration procedure is to prevent malicious users from registering commercial and pre-registered personal content as their personal content. It is assumed that the SPA has a database with the fingerprints of all existing commercial content as well as pre-registered personal content. In a more realistic setting, the SPA may use a distributed system in which the query to match a given fingerprint is forwarded to other parties with their databases. The management of such databases is, however, outside the scope of this paper.

After the fingerprint check has been performed, content is rejected in case a match is found, otherwise it is accepted for registration in the system. However, the fingerprint identification may fail, for instance, if the checked fingerprint databases are incomplete and therefore unable to recognize all registered content, or if the malicious user manages to tamper with the content and changes its fingerprint so that it cannot be recognized. In the latter case, however, the robustness of

the fingerprint should be sufficient to substantially degrade the quality of the changed content. In any of these cases, the consequence of fingerprint identification failure is that content is successfully and illegally registered and can be distributed within the DRM system as belonging to the malicious user.

The very infrastructure of the DRM system, however, can be used as a mechanism against illegal registration of content. This infrastructure is based on digital certificates issued by competent authorities, as depicted in Figure 1. In order for a registered content item to be distributed within the DRM system, certificates must be issued and presented to compliant devices for verification. In particular, a Content ID Certificate is issued by the SPA which contains the User ID (public key) of the content introducer. Moreover, this public key can also be used to check signatures on Content Rights and possibly User Rights. Therefore, if illegal content is detected within the DRM system, the original content introducer can be found via his public key and the corresponding User ID Certificate.

Watermark Extraction. A further measure which can be used to increase the system's security is the use of watermarks. During the registration phase, the content may be optionally watermarked by the compliant device with a watermark ID which is created and sent to the device by the SPA. This acts as a pointer to a user's ID in the SPA's database. The primary aim of such a watermark is to serve as a "stamp" of ownership which the content item carries wherever it goes. Therefore, in case of a dispute, for instance, over content ownership, it can always be determined by means of the watermark.

The watermark also allows the possibility of the so-called "forensic tracking" outside the DRM system. This covers the situation in which illegal content has been introduced into the DRM system by a malicious user and has been, later on, brought outside the DRM system. In this case, the infrastructure of the DRM system can no longer be used to identify the malicious user. Moreover, tampering with the content may lead to changes in its fingerprint in a way that it can no longer be recognized. By means of the watermark ID, however, the malicious user's identity can be recovered from the SPA's database.

Illegal content in this context may be (i) *commercial content,* which typically is not originally watermarked but has its ownership certified by other means, and (ii) *other user's registered personal content,* which will in this case include an additional watermark ID pointing to the original owner's ID (and therefore with an earlier time stamp on it). In either of these cases, ownership had been established prior to the registration performed by the malicious user, so malicious behaviour, i.e. the illegal registration of content, can be proved.

Forensic tracking outside the DRM system is performed with participation of the SPA (for the watermark extraction and database check) as well as participation of the User ID Authority (which knows the real identity of the user whose public key is in the SPA's database).

5. PRIVATE AND CONTROLLED OWNERSHIP SHARING

In order to register a content item, the user has to authenticate with the SPA, so he is not (and should not be) anonymous towards the SPA. However, he does not need to identify himself to any other party in the system. In particular, a user may require that he cannot be linked to a given content (anonymous publishing) nor linked to other users for whom he creates User Rights. Moreover, a user may require that all his content items cannot be linked to one another and to his identity. These are user privacy requirements which can be fulfilled by means of content registration with user pseudonyms. Additionally, if a different pseudonym is used for each different piece of registered content, unlinkability of content items can also be achieved.

A further requirement is that shared ownership of personal content amongst multiple users be possible. For instance, a family vacation movie in principle belongs to the group of family members. In this case, the whole group participates in the registration of the content and therefore acquires all rights implied by content ownership. It is important to notice that *ownership sharing*, which is established at the registration phase and addressed in this section, is distinct from the *sharing of the content itself*, which is performed via the DRM system as described in Section 3.2. The rights implied by content ownership include, e.g., access to the decrypted content as well as the power to determine who can distribute the content as User Right Authority. But as personal content is likely to contain private information about its owners, an additional privacy requirement is that further sharing of ownership with outsiders (who would then acquire owners' rights) be jointly decided by all owners. This requirement aims to limit the dissemination of personal content in a large and uncontrollable scale since, via a content ownership sharing chain, the content may get out of the control of the DRM system.

5.1. Registering Content with Controlled Anonymity

Pseudonyms generated from a user's public key can be easily obtained from the SPA in the following way. Assuming that the public/private key pair is built according to the Diffie-Hellman key agreement, let x be the user's private key and $h=g^x$ be the corresponding public key, where g is a group generator (for further details see Menezes, van Oorschot and Vanstone, 1997). To generate a pseudonym h', the SPA generates a random value a and computes the new public key $h'=h^a$ whose corresponding private key is $x'=xa$. The value a is then *securely* sent to the user, so that he is able to calculate his new key pair (x', h'), with no other party learning his pseudonym.

Content can now be registered under the user's pseudonym h', which no party (except the SPA) can link to the original public key h. For any new piece of content, a new pseudonym can be generated in the same way and used for registration. When ownership of a given content is shared between N owners, the procedure above is repeated for all owners. Upon registration, all owners i (where $i \in \{1, 2,\ldots, N\}$) obtain from the SPA distinct pseudonyms which are unlinkable to one another, to the owners' real identities and to further pseudonyms the owners may get. The registration procedure proceeds as described in the previous section with a few modifications. After content fingerprint checking, the SPA generates random values a_i and computes the pseudonyms $h_i'=h_i^{a_i}$. Each value a_i is sent to (and only to) owner i. The Content ID Certificate now comprises a unique content identifier, the content fingerprint and the new pseudonyms h_i' of each registered owner. This certificate serves also to ensure that all the pseudonyms h_i' are constructed in the correct way. Moreover, information stored in the SPA's database now must include the original identifiers h_i as well as the generated random values a_i for each of the owners.

Because the SPA stores the values h_i and a_i for all owners of a given content, any pseudonym and/or any content can be traced back to any of the owners' real identities. This provides revocable anonymity which is important to provide accountability in the system. For instance, illegal import of content into the DRM system can be traced back to the culprits, even if they are normally anonymous in the system.

5.2. Controlled Ownership Sharing

A further privacy issue is how to control the further sharing of ownership. This sharing should be allowed only if jointly decided by all owners (in which case the registration process is carried out again with an extra owner added to the data). Sharing, however, may happen without the approval of all owners. This can happen via the disclosure by one of the owners, say i (the "leaker"), to an

outsider of the pseudonymous private key x_i'. With this key, the outsider has all rights of the leaker in the DRM system. And since the outsider does not learn anything about the leaker's *original* private key x_i (given that x_i' is randomly related to x_i), a deterrent mechanism is needed to stop such potential leakers. Such a mechanism is described below.

The SPA is set up such that it will reveal the value a_i (of any of the owners i) to any party who comes to it and proves knowledge of the private key x_i' corresponding to the pseudonym h_i'. The party may do so completely anonymously. The idea behind this is that only one of the two, the owner i himself or an outsider who received the private key x_i' from owner i, is able to authenticate with pseudonym h_i'. In the first case, there are no consequences since owner i should in fact know a_i. He may need to ask this value in case, e.g., he looses it. In this case, he *must* authenticate with his original public key h_i, in order to prove that the request is legitimate. The second case, however, has major implications since the outsider is able to learn the leaker's original private key by calculating $x_i = x_i'/a_i$. Given that the outsider may considerably profit from the knowledge of x_i, with no liabilities on his part, he is likely to do so. A further implication of the outsider's action is the fact that the SPA is immediately notified that owner i has leaked his private key to an outsider. The SPA can then warn the other owners about the fact and, furthermore, can tell them who the leaker was.

6. CONCLUSION

This paper presents and discusses a system for the protection of users' privacy when sharing personal digital content with other users. The system allows the controlled sharing of personal content, which is achieved by means of an extension of a DRM system originally devised to protect commercial content. The idea behind extending an existing DRM system to protect both types of content is twofold. First, the whole infrastructure (e.g., compliant devices and certificate authorities) of the existing system, which is already in place, can be re-used for personal content. Second, the use of a DRM system for protecting personal content is thought to create for users a more positive view of DRM in general, and this can contribute to the acceptance by users of controlled distribution of commercial content.

The original DRM system involves an authorization hierarchy implemented by means of competent authorities that create and sign digital certificates. This authorization hierarchy is modified in the extended DRM system to accommodate the fact that consumers can now be content providers as well. For this reason, a new digital certificate (i.e., a "certificate of ownership") is introduced which establishes a secure link between a user and his personal content.

The fact that consumers become content providers has security implications as well. Consumers are now able to control the usage of their personal content in the system, but this also opens the door for potential misuse of commercial content (e.g., its illegal introduction in the system as personal content). To prevent such a threat, the extended DRM system requires that users register their content with a competent authority, at which point they obtain the certificate of ownership and may have their content marked with their identity, but only after the identity of the content itself has been checked and the content certified as new.

The extended DRM system can provide further user privacy by providing users with the possibility of private ownership of content with private and controlled multiple ownership. This means that users are able to register their personal content under pseudonyms, with unlinkability of pseudonyms also supported (i.e., a unique pseudonym per content item). Moreover, multiple users may own a content item, with their privacy protected in two ways: (i) pseudonyms, a different one for each user, can be used for content registration, and (ii) transfer of ownership of their content must be decided jointly by all owners.

Privacy of content ownership can be achieved as described above, except towards the registration authority which always keeps a record of the original user identifier and all the content registered under the corresponding pseudonyms. This is done in order to enforce accountability in the system but may be seen as a downside of the system. This lack of privacy can be alleviated by means of a mechanism of *distribution of trust*. In this case, the original user identifier can be replaced by temporary identifiers which are then used by the registration authority. The temporary identifiers are, in their turn, generated by another trusted third party which must then (to enforce accountability) keep a record of the user's real identity. As long as the authorities do not collude, the association between users and their personal content is not known by any of the parties in the system. Of course, trust can be further distributed to diminish the possibility of collusions between authorities.

While the mechanism described above would increase users' privacy, it would also make the technological solution more complex, certainly from the architectural point of view. This trade-off between system's privacy provision and system's complexity is encountered often, mainly in systems with the strong requirement that security levels be preserved after addition of privacy enhancements. This is certainly the case for the original system considered, i.e., a DRM system for the protection of commercial content. Its extension to protect personal content, as well as further extensions to provide user's privacy, must include mechanisms to ensure user accountability, otherwise commercial content providers will certainly object to such extensions. Therefore, privacy protection has limitations in such systems. This means that it is unrealistic for any user, specially the user who values the freedom of anonymous publishing above the right to claim content ownership, to expect completely anonymity in the system.

REFERENCES

CONRADO, C., KAMPERMAN, F., SCHRIJEN, G.J. and JONKER, W. (2003): Privacy in an identity-based DRM System. *Proceedings of the 14th International Workshop on Databases and Expert Systems Applications*, Prague, Czech Republic.

FELTEN, E.W. (2003): DRM, and the first rule of security analysis. *Freedom to Tinker.* http://www.freedom-to-tinker.com/archives/000317.html. Accessed 12 May 2005.

GRIMM, R. and NUTZEL, J. (2002): A friendly peer-to-peer file sharing system with profit but without copy protection. In *Innovative Internet Computing Systems* 2346:133-142, Lecture Notes in Computer Science, Springer-Verlag.

ITUNES (2005): iPod+iTunes for Mac and Windows. http://www.apple.com/itunes. Accessed 12-May-2005.

KALKER, T., EPEMA, D.H.J., HARTEL, P.H., LAGENDIJK, R.L. and VAN STEEN, M. (2004): Music2Share - Copyright-Compliant Music Sharing in P2P Systems. *Proceedings of the IEEE* 92(6).

MENEZES, A.J., VAN OORSCHOT, P.C. and VANSTONE, S.A. (1997): *Handbook of Applied Cryptography*. CRC Press.

OMA-DRM (2004): Specifications: DRM Specification V2.0. *Open Mobile Alliance*. http://www.openmobilealliance.org/release_program/drm_archive.html. Accessed 12 May 2005.

VAN DEN HEUVEL, S.A.F.A., JONKER, W., KAMPERMAN, F.L.A.J. and LENOIR, P.J. (2002): Secure content management in authorised domains. *IBC 2002*.

VAN DER VEEN, M., LEMMA, A. and KALKER, T. (2004): Watermarking and fingerprinting for electronic music delivery system. *SPIE 2004*, San Jose, USA.

BIOGRAPHICAL NOTES

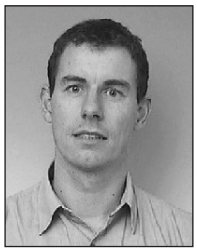
Claudine Conrado

Claudine Conrado obtained her PhD degree in 1993 in theoretical non-linear physics from the Niels Bohr Institute in Copenhagen, Denmark. Further, she worked on environmental-related research at Imperial College, London, UK, looking at multi-component and multi-phase systems. She joined Philips Research in Eindhoven, The Netherlands, in 1999 to work on adaptive algorithms for home systems. Currently she is working at the Information and System Security Department of Philips Research on Privacy Enhancing

Technologies. Her areas of interest include privacy and security in electronic interactions and ubiquitous systems, in particular in digital content distribution systems and healthcare applications.

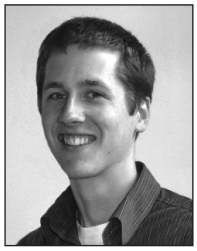
Milan Petkovic

Milan Petkovic is a senior scientist in the Information and System Security department at the Philips Research in the Netherlands. Before joining Philips Research, he was a research assistant in the department of Computer Science at the University of Twente, the Netherlands, and a teaching assistant in the Faculty of Electrical Engineering at the University of Niš, Yugoslavia. Dr Petkovic received his Dipl-Ing. and MSc degrees in Computer Science from University of Niš, and his PhD degree in Computer Science from University of Twente. Among his research interests are information security, secure content management, privacy protection, multimedia information retrieval, and database systems. His publication records include a book on Content-Based Video Retrieval, as well as a number of book chapters and research articles. He was invited to talk at various international conferences and workshops on the topics of his research interests.



Michiel van der Veen

In 1996 Michiel van der Veen received his MSc in physics (with honours) from Utrecht University. He then lived for a period of four years in Zurich, Switzerland where he obtained his PhD degree from the ETH-Swiss Federal Institute of Technology. In January 2000 he joined Philips Research Eindhoven and since then worked on projects related to Information Security, Privacy, Digital Watermarking and Biometrics. In these fields, he published over 30 scientific papers and filed more than 20 patent applications.



Wytse H.
van der Velde

Wytse H. van der Velde has been a student at the University of Twente, Enschede, the Netherlands since 1998 and is close to receiving his MS degree in Computer Science. From 2004 to 2005 he was a member of the Information and System Security research group at Philips Research in Eindhoven. There he has done research for his thesis in the fields of privacy in ambient intelligence and content sharing in DRM systems. His other research interests include distributed systems and computer architectures.