Rights Management for User Content

György Kálmán and Josef Noll

1 Introduction

With the spread of always-online Internet connections, digital user content and upcoming tools or services for content sharing induced a change in user behaviour. Traditional user and provider roles are not separated any more. The end user is creating his content and sharing it over the network.

Rights management in the home area is composed from two, possibly disjunct problem areas. One is the management of content, which the user has been purchased from commercial sources, the other is the management of user-owned content.

User created content induces the need for a rights management solution, which keeps the user and his content in focus. Current solutions offer services only for industrial customers and are only dealing with the traditional consumer role of the user. The more active, content producing users need a tailor-made solution to handle their content. Such a solution will enable fine grained rights control over distributed material in an easy and secure way.

Social life over the internet is becoming more important, in an interconnected world, network presence – visibility and acknowledgement of other people – is a major driving force. A user may want to share pictures with his friends and family, with a society or just with one person. Currently, the user has a wide variety of possibilities to share content, but until now, no fine grained right management solution was designed with user needs in mind, and with support of home content.

György Kálmán
University of Oslo, UniK - University Graduate Center, Pb. 70, Kjeller, 2027 Norway, e-mail: gyorgy@unik.no

Josef Noll
University of Oslo, UniK - University Graduate Center, Pb. 70, Kjeller, 2027 Norway, e-mail: josef@unik.no

2 Background

The bigger user base results in the average knowledge of IT technologies is sinking. This raises the need for easy-to use systems, since this is not longer a matter convenience, but rather a limiting factor for success. Wide variety of terminals and extending range of user devices are requiring content adaptation (nearly the same user experience on different terminals) and integrated security methods (hard to set up public-key authentication or to type in 15 character passwords on a media player). For some purposes, it would be beneficial to use seamless authentication, like it is implemented for Wireless Application Protocol (WAP) services of the operator and selected third parties. Because no user interaction is needed it is recommended to use it in personalisation and content adaptation services[2]. If security is not critical, methods similar to cookies could be used, where after one successful authentication, the system is keeping the user logged in for a certain period. Alternatively, Single Sign On (SSO) solutions can be used, where after the user authenticates himself towards the SSO service, further authentication requests will be handled by the system.

Content adaptation has a growing importance in pervasive computing, since terminals with very different capabilities are used to access the same information sources. Beside the technical problems associated with conversion, the commercial content protection solutions usually do not provide a method for content transformations.

To provide good user experience, these incompatibilities may be hidden with deploying a DRM broker into the home network, which can cooperate with user devices and is able to distribute licenses in a secure and easy way. A central device for controlling a home network was introduced in the IST ePerSpace[3] project, which provides service discovery and content adaptation services for compatible devices. However, the ePerSpace solution lacks support for content management.

Although there are solutions for key distribution and license management, most of them are not optimized for the special circumstances in a home environment. Either the service is not user friendly (e.g. key directories of PGP) or use a third party pay service (e.g. VeriSign) and in general, are not designed for the constraints of the user environment: mobility, battery use, computational power and trustworthiness. Mobility can be addressed with secured transport protocols to provide secure and easy access to home content from the internet side.

Entertainment devices usually have limited computing capability, thus they might be supported through a specific network device which is able to carry out complex cryptographic operations and exchange the generated information with other parties using a secure and easy method. A solution to computational problems and trusted devices could be to deploy smartcard based authentication in the home environment[4].

In this paper we show a solution which can bridge the gap between the DRM solution shown in [5] and the smartcard based authentication architecture in [4] in order to enable cheap, easy and secure user authentication and personalisation services[10]. As an extension of the original concept, a new user scenario is shown,

where the user is sharing his own content to other users through his own home network and with the possibility of integrating external services (MySpace, FaceBook etc.).

As a new functionality, the concept of an interconnecting service is shown, which is using a (preferably) trusted entity for rights object generation. The objective is to provide a flexible solution, which can interoperate between the different service providers and make it possible for the user to select users of the different services from one interface and share content for them. The system then distributes the appropriate rights objects using the third party services or other solutions.

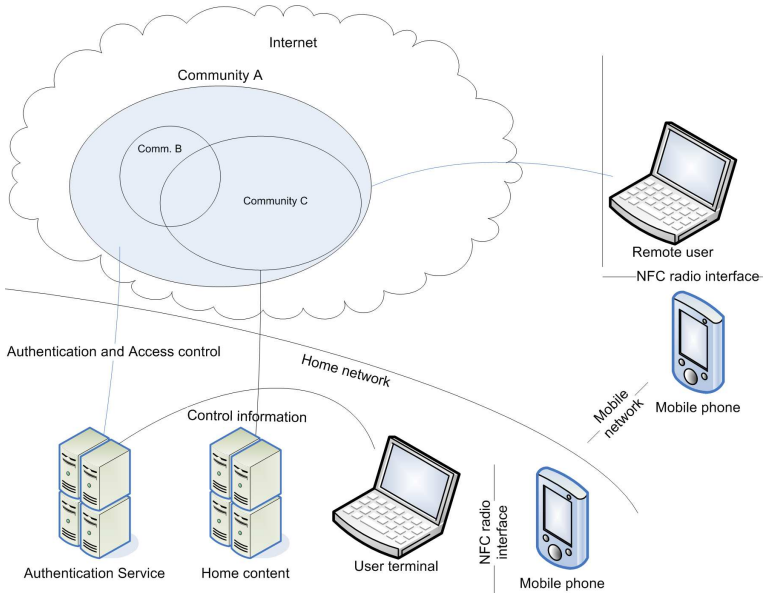

Fig. 1 Home network with access control and out-of-band key distribution

First, an overview is given about typical devices and their capabilities in a home network, then an overview about smartcards, their possible area of use and possible candidates for widespread use. A possible secure and widely available device, which can help to overcome the problematic deployment of a smartcard infrastructure, the mobile phone and its Subscriber Identity Module (SIM) capabilities are shown.

Two user scenarios are explained, where the first shows the typical case of commercial content distribution and the use of a DRM broker for a better user experience. The second shows the viewpoint of a content creator user, who wants to share his own content for his friends: photos from the last hiking trip for his friends, a video clip, where he is asking for advice from a workshop and sharing the unfiltered catalogue of his pictures within his family.

Possible solutions for these scenarios are shown and an evaluation of the proposed architecture is given and areas of further investigation described.

3 Devices in the home network

A home network can be composed of PCs, media players, mobile phones, storage units, STBs or other devices. Most of these devices are mobile and move between different networks. Wireless networks also made it easier to welcome guests on the home network.

The problems begin with securing access to a home network. Mostly there is no or just weak security applied on those, so they are wide open for malicious intruders. For example, lots of WLANs use no encryption at all or employ the compromised WEP standard. Networks with open access or even with WEP secured access open for malicious attacks on the user data from any place within the coverage of the wireless cell.

Setting up a secure network may be a hard task, since keys have to be transmitted and devices have to authenticate themselves. This may be done by using out of band key delivery methods (like using an USB stick or in an SMS via the mobile network), in case of automatic key delivery, only the communication is secured, but the client does not prove, that he is allowed to connect. Even if the user is able to do this process, convenience considerations might cause him to neglect security. Also, currently, the user may decide to grant access or not, but inside the network it is extremely rare to use some kind of additional access restriction. This means, that either no access is given or the guest can access practically all network resources.

While keeping secure access, content adaptation is becoming more important. In order to ensure good representation of content, profile management methods, such as UAprof[6] were introduced. This enables content creators to define content representation based on generic rules and the serving system can adapt these based on the transmitted terminal profiles.

Content stored in a home network may be also adapted to the different devices, to ensure good results (e.g. creating lower resolution video for a portable media player from a digital satellite stream). Content adaptation can be problematic, because current DRM solutions usually do not allow changes in the content. If a device could provide connection between the content providers rules and user needs, the adapted and legal content would be available on any user device. Such a device could act as an end entity for the content provider and hide the inner network of user devices.

4 Rights management

Since users are starting to create and share content with others, the home infrastructure has to support some kind of rights management. This includes not only storage of acquired licences from content provider companies, but taking care of own content. Home networks store a great deal of personal information which should be secured.

Based on various roles of a user in a certain context, a need to share with a specified group of users arise. This can be done by introducing community content

access, based on group authentication. A design with the end user in the focus is needed to enable secure and easy sharing of content over the internet. This means, that while preserving ease of use, the system has to use strong encryption, group authentication and efficient key management. Group authentication is essential to enable sharing between different user groups based on various properties, like friends, school classes or other interests.

The basic problem of home DRM is, that these systems usually rely on *compliant devices*. A device needs to meet certain requirements in order to get accepted by the system. Compliance raises a problem with the restricted and optimised nature of home devices. If individual authentication is used, public key operations need to be carried out, because mutual authentication is required between the DRM system and the terminal. This could be problematic for simple devices, like an MP3 player and resource consuming for a device like a PDA.

A DRM solution for home networks is proposed in [5], where creating device domains in the home environment is shown. This paper points out, that problems associated with the mobile environment (battery powered consumer devices in particular), and the possibility of reducing the number of expensive calculations. So, the use of a designated cryptographic device would be beneficial.

Content adaptation has a growing importance in pervasive computing, since terminals with very different capabilities are used to access the same information sources. Beside the technical problems associated with conversion, the commercial content protection solutions usually does not provide a method to make transformations without quality loss.

The use of group authentication can help to overcome the problems associated with content adaptation and personal content sharing. This solution fits much better to the general use of home devices, because in this scenario, a device has only to prove, that it is part of a group, which can be done by simple hash calculations for example.

After authenticating the devices, also securing of the transmission environment is advised. This could be done by negotiating symmetric session keys or calculating hash values for example.

It can not be assumed, that all devices have cryptographic hardware and tamper resistant hardware. This can be solved by adding a smartcard into the system.

5 Usage scenarios

In the introduction, two possible problem areas were shown.

Commercial Content The content is purchased from a commercial source, it is equipped with a DRM solution to enforce the owner's rules over the usage in the end user's system.

User Content The content is created by the user and shared over the internet. The local (home) infrastructure is playing a key role, no commercial DRM is available.

These problems can be framed into a user scenario, where possible problems and solutions can be shown. First, we will show a scenario for the commercial content. This one is more familiar and has more constraints.

5.1 Commercial Content

The main actors of this scenario are well-known:

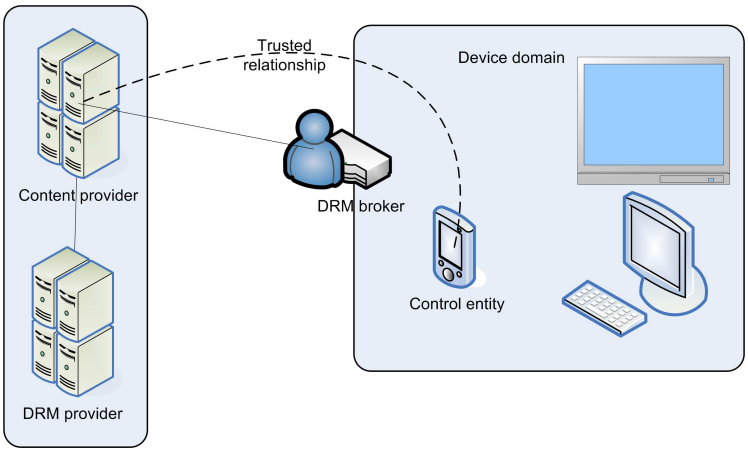

Fig. 2 User scenario with commercial content

Content provider The entity, which is making the content available for purchase for the end user. It represents the retailer. For easier presentation, the content creator/owner is represented by the retailer.

DRM provider A supporting entity, which delivers a software solution to ensure, that the content is used as it was defined by the Content provider.

End user The consumer, gets certain rights for the purchased content delegated by the Content provider and enforced by the DRM solution of the DRM provider

In this classical view, the user faces severe limitations. The lesser problems are for example, that in many countries, it is a customer right to create backups from content purchased (like backing up a CD) and the DRM solutions usually are not permitting to copy the content without quality loss.

The more important problem of compatibility arises, when the user is buying content from different providers and wants to use it on different devices. As the home networks are getting more complex, and digital media is being used in nearly all kinds of entertainment devices, the user faces problems with using legal content on various devices.

An example could be a song with Apple's FairPlay, where the song can be uploaded to an iPod, but cannot be converted to MP3 without quality loss. This means, that the user cannot play the song on a networked media player, a home theatre PC or a different mobile device. Also, it cannot be guaranteed, that the user will be able to play a piece of content, for example, 10 years after the purchase. Since he is not able to convert it without quality loss, a new standard can draw producer attention, and support may be stopped in years. The same problem arises, if the manufacturer of a specific device is shutting down and stopping support services. In a bad case, the user won't be able to enjoy the content after the (usually short) lifetime of the device.

Our concept in this scenario introduces new entities into the system, and is using the capabilities of the current home networks. In order to enable a more flexible content use, the following entities are introduced:

Device domain A group of devices formed based on their relationship to the user, for example devices of a Personal Area Network (PAN) or devices of a home network (media players, HTPCs, MP3 players etc.).

Control entity A designated device, which controls a device domain, preferably on-line and equipped with easy-to-use user interface.

DRM broker A device, which plays the role of the end device for the Content provider and masks the internal devices while respecting the provider defined rules of content use.

The DRM broker can mask the internal network, so the user would be able to use the purchased content in any of his devices, irrespective of the provider of the content or the manufacturer of the device. This functionality can be integrated into

different devices based on the provider's preference or other requirements. A natural solution could be to include this service into the home gateway of the user (e.g. modem, router). Depending on the implementation, this can be done with the current devices.

While a license storage and distribution service certainly won't cause resource problems in an average router of an average home network, various problems arise with this solution.

The easier problem is to solve the additional resource needs of these services, like flash memory in the router and a bit more CPU power.

Harder problems are associated with the commercial requirements. For example, trustworthiness, license management and revocation[14]. At the moment, the SOHO routers or modems are not equipped with the necessary devices to provide safe endpoint services for commercial suppliers.

The problem of trustworthiness needs a trusted device in the home network. Since routers doesn't carry such a device, an other device has to be selected. In our scenario, this task is given to the SIM in the mobile phone. It provides secure storage, revocation capabilities and user identity management.

Certainly, the trusted device needs to add an internal DRM to the content delivered to local devices in order to keep rightful usage. This means, that the original DRM has to be removed and a new has to be installed on the content. The legal aspects of DRM handling are out of scope of this paper.

Possibility of manipulating DRM protected content depends on the content providers, this problem does not arise in the second scenario, where the user plays both the role of a content provider and a consumer.

5.2 User content

This scenario shows the upcoming situation of a user, who is sharing a piece of his own content to a friend. He is selecting the appropriate users on the user interface, where he has all of his contacts from the local address book, FaceBook or other online services, of the home right management service and the access keys are delivered to each of them. Content will be accessible through the user's own broadband internet connection or uploaded to a third party provider[12].

The actors in this scenario are more like a Peer-to-Peer (P2P) system, where every user can be a provider and vica-versa. In an explicit situation, the following actors are present:

User	Content consumer	Consumer of the content
	Content provider	Sharing his content to the Content consumer. He made the content accessible and selected the appropriate users.

Home Gateway A device, which is connected to both the LAN of the Content provider and to the internet. Has the possibility of granting access to content stored in the home network.

This minimal system is capable of sending out an access key to a remote user and letting access to local content[15]. But, there are several problem points: both the user's and the content provider's identities are only *assumed*[9]. Key delivery is done over the local internet connection and as such, possibly eavesdropped. The home gateway is getting access information on the LAN, which can be a problem source in certain situations (e.g. WEP secured Wireless LAN).

In order to create a more secure system, additional measures are required. New entities are introduced to ensure user identity and alternative delivery methods are included.

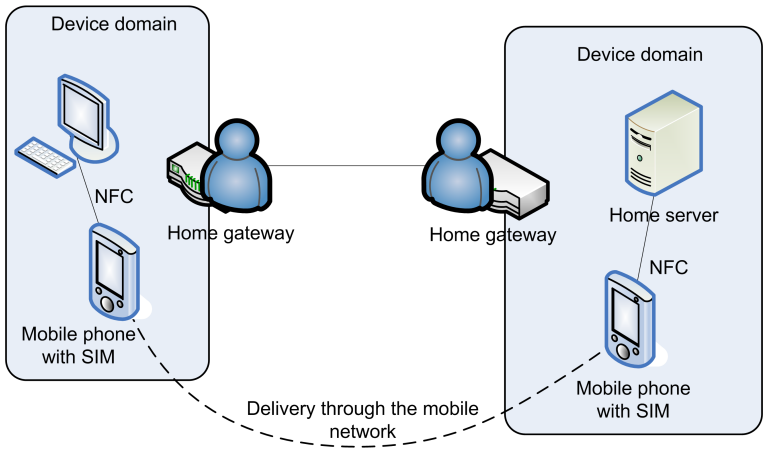

Fig. 3 Content sharing between users

SIM The Subscriber Identity Module of the user's mobile phone[11]

Mobile phone Provides a user interface for access key management and alternate delivery network

NFC Near Field Communication (NFC) interface for very short range transmissions, for example WLAN access setup, access control data exchange between the mobile phone and the home gateway

With the inclusion of the mobile phone, our network is now capable of delivering keys through the mobile network (the keys won't pass through the local internet uplink) and has a trusted device, which is can hold access information in safe storage. As an addition, this phone is capable of generating access control objects (keys, certificates) with internal, tamper resistant routines and is capable of delivering them to local devices and remote devices as well.

The last major addition is, that the mobile phone can represent the user in a limited, but better-than-nothing way. The mobile phone is a personal device, and it can be assumed with a good probability, that if the user knows the PIN of the phone and the access key was delivered to the good number, the actual human being reading the information is the one, who the owner wanted to select.

Out-of-band key delivery would be possible with other solutions, for example using Bluetooth for short range exchange or a USB stick, which can be carried around. The mobile phone provides a more pleasant alternative, since it has a separate network connection, a user interface, which is common for the user and the possibility of revocation[13].

So, for example the owner can select his girlfriend's FaceBook user and grant access to a flickr picture with the key delivered via the mobile network and the access information delivered via the FaceBook messaging service. The mobile phone will generate a key, then it will send it to the girlfriend's mobile number, then the user puts the phone close to his laptop, where the right management client is sending the access information (e.g. URL) to the designated user account on FaceBook and uploads the DRM protected picture to flickr, which is only accessible for the girlfriend.

6 Authentication and Encryption

In both scenarios, security is playing a key role. The content needs to be protected against eavesdroppers or other attacks.

Most devices do not have extensive encryption capabilities and a secure infrastructure, they may rely on external units, like a smartcard. A smartcard is tamper resistant, which can support complex encryption functions and provide them to compatible devices.

In [4] a smartcard is shown, which implements the Extensible Authentication Protocol (EAP) stack in hardware thus providing high security on a widespread protocol family for WLAN authentication.

While these hardware elements provide good security capabilities, it can be problematic to add those to all the devices in the home network. Besides the costs to equip every single node with a smartcard reader, compatibility issues and additional battery powered devices for certain hardware will make the smartcard solution difficult.

To keep the advantage of a tamper resistant cryptography device and keep costs low, we propose to use the mobile phone's SIM to calculate and the phone hardware to distribute keys for devices.

The phone is becoming a permanent part of the user's personal area. In many cases the handset is already part of the user's identity, because of it's communication services, look and important the role in social connections. Users are taking care of it, since a phone holds a great deal of social and personal information.

According to [7] it could be possible to use the SIM as a fully featured smartcard as the SIM is capable of storing keys and providing cryptographic functions for third party services, not only for mobile providers.

While the phone is capable of generating a key, the problem of key delivery still remains. If the user has to connect the phone via USB or Bluetooth, it can be problematic, since Bluetooth needs pairing and USB is not supported by a considerable amount of devices.

To solve this problem, we propose to use NFC technology to transmit encryption keys between devices. NFC is a short range communication technology based on RFID, but with more limited range and the possibility of using active devices on both sides. An NFC reader adds only a small cost overhead to devices, does not need to be powered continuously and provides contactless transfers for very limited ranges.

Through the mobile phone, the user has full control over the identification process either based on the location e.g. putting the phone close to the reader or on knowledge e.g. typing in a PIN when requested by the remote service.

A key problem is the correct selection of the identifier to be used in a transaction. This can be done either by profiles or by asking the user to allow access to the data, requested by the service.

The public key of the phone represents the root trust in the system. The key pair can be placed to the SIM either by the mobile provider or other, verifiable source, to ensure correct user identity association.

If the private key of the SIM gets compromised, the identifier can be revoked by the identity provider and the user can get a new key without losing access to the services. The remote revocation and user control makes the SIM an ideal device for making payments and gaining access to services.

7 Service Architecture

We propose to incorporate the device domain management capabilities and the EAP capable smartcard functions. The EAP family is used for easier cooperation with current network authentication technologies.

With using the SIM's cryptographic functions[7], we build a device domain, and distribute these keys through the NFC interface.

The constraints, the system has to face are

- continuous network connectivity cannot be assumed between the members of the domain,
- there are no secure clocks in the system,
- no cryptographic hardware is available in the devices,
- key management must be efficient even for large number of devices.

The CPU power of current smartphones makes possible the use of public key operations and so act as a proxy between the provider and the user devices. The provider can be either the DRM broker on the home network or external content providers.

The DRM broker handles rights associated to local and user created content outside the home network. This entity certifies approved devices and revokes expired or compromised ones. No global device identification key is proposed because the phone can deal with the domain's internal right management issues.

This lowers the resource needs at commercial right management providers and also keeps user privacy on a higher level, because he does not have to disclose, what kind of devices he is using. With a DRM broker and an always online phone in the system, we can also extend the proposed systems functionality to physical media, like DVD-s since the networked media played is connected to the broker, which is accessible for example through any mobile IP service.

If a new device is added to the domain, a request is shown on the display of the phone and requires response from the user. This ensures, that access is only granted, if the remote party gets a correct key and in addition, the user confirms his will to permit access. This can be requested once or any other period, based on user preferences.

We recommend the use of NFC interface for distributing keys out of band. With this short range transfer method it is possible to allow the phone to negotiate or generate an authentication and encryption key for the user device, and send it to the mobile device, where no expensive cryptographic methods are needed.

The loss of the mobile phone does not compromise the system's security, since the SIM can be disabled remotely (if the intruder wants to generate a new key, they have to connect to the network). After getting a replacement, the existing keys of the domain will be revoked and the user has to distribute them again.

Usability of the proposed system depends mainly on the easiness and security of key distribution. In the demo system we use either NFC technology to deliver keys to local devices or the mobile network for remote users.

Local key delivery can be accomplished with NFC, because it has very limited range and is convenient for the users, just to put the phone close to the device they want to exchange a key with.

To enable remote access to home content, it is possible to send the access key out of band, via the mobile network to the remote user's phone, where he can use the NFC interface to download the key to the terminal, he wants to use for content access.

One of the key factors of a user centric system is to enable the safe and easy delivery of keys to other users. In order to demonstrate the usefulness of the mobile phone in this task, we created a prototype system, which enables key exchange via

NFC or delivery via SMS to an other phone. The other phone can also forward the key for the remote user's terminal. In both ways, the key is delivered out-of-band, which provides better security, as access control information is not transmitted through the network, where the content is accessible.

8 Future work

The current prototype is using the SmartMX chip instead of the SIM for key storage, which limits the possible range of devices. This is a technological limit, which is in the process of being resolved. Nodes need to be equipped with NFC readers to enable key transfer with this technology. NFC readers are not usual in the home environment. The security of the system depends on the tamper resistance of cryptographic functions on user devices.

Our proposal shows an improvement over the original idea of [5] by using the possibilities of the mobile phone and the inclusion of a DRM broker, which act as a gateway between different DRM solutions and acts like a home agent for the user's right entities. A possible drawback of using the SIM is that the mobile providers usually do not allow access to the SIM in order to ensure correct functionality of the network.

The authors want to point out, that by using the SIM as secure storage and executing signature and session key generation routines over the SIM (which would be included by the operator on the EAP capable SIM) does not interfere with any networking function of the phone while keeping the advantage of being a widespread device which lowers the introduction costs.

Storage may be also limited, but since an encryption key (for example the master key for adding domain members) can be quite short, well under one kilobyte, even current SIM capacities seem to be enough, but also, high capacity SIMs are already on the horizon[8].

NFC technology is just entering the contactless market, so additional tests are required to test its security against various attacks.

By default, it is a hard problem to ensure a user's identity. As shown in [9], a typical Identity Management system has three types of trust models:

pairwise the two entities have direct connection,
brokered the two entities are reachable via a network of direct connections,
community for common agreements.

The system shown in the second scenario is fully operational with the minimal entity implementation, where a PGP-like web of trust solution could provide limited identity management (community model) and better-then-nothing security for personal content. The inclusion of the mobile phone offers an easy solution for providing a more secure and easy way for user content management and the possibility of the more exact identity management models (pairwise and brokered).

Future work will focus on implementing a home right management system, where the mobile phone will play the role of a trusted cryptographic device.

9 Conclusion

This paper provides an architecture of rights management for home content. While current solutions are device centric, our solution supports both an I-centric and a community centric approach. Two user scenarios are shown, where commercial and personal right management problems are elaborated. With the focus on the user created content, problems and possible solutions for various security requirements are shown.

We have shown that the mobile phone with the SIM card has the potential to provide strong encryption services, being applicable for securing home content. Key generation and distribution are the main functions of the phone, supported by the capability to interconnect devices in the home network. It may also be used to enable access to guests and store device profiles for content adaptation.

Because the phone is practically always online, update and revocation of profiles or keys can be done remotely and nearly instantly. The SIM is trusted by mobile providers and can be the tamper resistant device, which the user needs for building an I-centric rights management infrastructure.

In an always online environment, with networks holding more and more personal information, the user has to be able to control access to his own content.

References

1. Broy, M.: Software engineering — from auxiliary to key technologies. In: Broy, M., Dener, E. (eds.) Software Pioneers, pp. 10-13. Springer, Heidelberg (2002)
2. Chowdhury, M. M. Rahman and Noll J.: Service interaction through role based identity. In: Proceedings of WWRF 17, Heidelberg (2006)
3. IST ePerSpace: Towards the era of personal services at home and everywhere. http://www.ist-eperspace.org/ Cited 10 Oct 2007
4. Pujolle, G., Urien, P., Loutrel M.: A smartcard for authentication in WLANs. In: Proceedings of the 2003 IFIP/ACM Latin America conference on Towards a Latin American agenda for network research, Available via ACM. http://portal.acm.org/citation.cfm?id=1035662.1035673 Cited 10 Oct 2007
5. Bogdan C. Popescu et al.: A DRM Security Architecture for Home Networks. In: Proceedings of the 4th ACM workshop on Digital rights management (2006)
6. WAP Forum: UAProf specification. Available online. http://www.openmobilealliance.org/tech/affiliates/wap/wap-248-uaprof-20011020-a.pdf Cited 10 Oct 2007
7. ETSI: TS 102 350 V7.0.0 Smart cards, Identity Files and Procedures on a UIC. In:ETSI Technical Specification, ETSI (2005)
8. M-Systems: M-Systems and Microelectronica Announce Plan for 1 Gigabyte SIM Cards by End of 2006. In:Press Release, 3GSM World Congress, Barcelona, Feb. 15 (2006)

9. Bhargav-Spantzel, A., Squicciarini, A., Bertino, E.: Trust Negotiation in Identity Management. IEEE Security and Privacy Magazine. **Marc/April**, 55–63 (2007)
10. Heikkila, F.: Encryption: Security Considerations for Portable Media Devices. IEEE Security and Privacy Magazine. **July/August**, 22–27 (2007)
11. Tarkoma, S., Prehofer, C.: Composable Mediation for Security-Aware Mobile Services. IEEE Communications Magazine. **July**, 58–65 (2007)
12. Dusparoc, I., Dahlem, D., Dowling, J.: Flexible Application Rights Management in a Pervasive Environment. In: Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service, 2005., Available via ACM.
http://portal.acm.org/citation.cfm?id=1048928.1049593 Cited 10 Oct 2007
13. Merabti, M., Llewellyin-Jones, D.: Digital Rights Management in Ubiquitous Computing. In: IEEE MultiMedia Magazine, Available via ACM.
http://portal.acm.org/citation.cfm?id=1130720.1130816 Cited 10 Oct 2007
14. Abbadi, I. M., Mitchell, C. J.: Digital rights management using a mobile phone. In: ACM International Conference Proceeding Series; Vol. 258, Available via ACM.
http://portal.acm.org/citation.cfm?id=1282138 Cited 10 Oct 2007
15. Geambasu, R. et al: Homeviews: peer-to-peer middleware for personal data sharing applications. In: Proceedings of the 2007 ACM SIGMOD international conference on Management of data, Available via ACM.
http://portal.acm.org/citation.cfm?id=1247508 Cited 10 Oct 2007