Privacy Rights Management for Mobile Phones

Silke Holtmanns, Frank Hartung

Ericsson Research, Ericsson Eurolab Deutschland GmbH
52134 Herzogenrath, Germany

Abstract. Recent progress in mobile phone technology enables the users to generate and store personal data, for example pictures taken with built-in digital cameras. This personal data can then be forwarded to other mobile devices. Currently, there are no mechanisms available that protect such user-generated content against unauthorized use and distribution, or that enforce the user privacy preferences. This paper presents a proposal for a mobile Privacy Rights Management system to protect the users privacy preferences for the generated content in a cost efficient manner by reusing existing Digital Rights Management functionalities.

1 Introduction and Use Cases

Mobile phone technology made rapid progress during the recent years. The latest generation of mobile phones has many new features and capabilities like

- Enhanced color displays
- Web and WAP browsing capabilities
- Download functionality and Java support
- In-built cameras
- MMS (Multimedia Messaging Service)
- Media players for audio and video rendering
- Mobile games

Further, many mobile phones do now support the download and rendering of media content and games protected by Digital Rights Management (DRM) mechanisms, for example according to the Open Mobile Alliance (OMA) DRM standards. DRM systems protect valuable content from intentional or accidental modification and duplication [2]. DRM systems are designed to prevent fraudulent use of the content delivered to the user by defining rights (permissions and restrictions), linking these rights to the content, and enforcing these rights on the trusted consuming devices, and preventing that the cleartext content can be extracted from the trusted logical zone. Content providers want to protect their content and deliver it only to the intended recipients, and within the trust boundaries of the DRM system. The transfer of the content is usually bound to conditions in form of a license agreement.

Holtmanns S. and Hartung F. (2004).
Privacy Rights Management for Mobile Phones.
In *Proceedings of the 3rd International Workshop on Wireless Information Systems*, pages 12-17
DOI: 10.5220/0002633800120017

A user generating content, for example taking pictures with her cameraphone, is in a similar position. This content shall be protected from unauthorized use by other parties, for example from unauthorized distribution or use for other purposes than intended by the originator. The privacy requirements a user poses to protect the privacy of her personal data are very similar to the requirements of a DRM system, but the roles of the entities are changed in a privacy rights management system. The user takes the role of the content provider, e.g. by taking a picture and distributing it in protected form. The general concept of utilizing DRM functionalities to protect the privacy of user data was presented in [1]. One large obstacle in providing privacy providing technology is that the implementation of the functionality is costly and does not create immediate business revenue for the implementing party. We describe an approach that reuses the existing mobile DRM infrastructure and DRM functionality implemented in mobile phones [2], and manages user privacy in a cost efficient and effective manner.

So far, there are no suitable mechanisms for user data protection on mobile devices in place. The Privacy Preference Platform (P3P) [3] does not integrate already deployed DRM functionalities and the design of P3P did not take the mobile aspects like latency, restricted memory, long round trip times into account. Therefore the current version of P3P is not optimized for the mobile environment and its mobile deployment would be very slow, since P3P has many message exchanges. However, mobile privacy protection will become an important issue in an environment where the user can generate personal content in an easy and fast manner e.g. taking a picture by using her camera phone.

The following three use cases shall illustrate situations where users wish to protect user-generated content.

- Family Stone spend their vacation in Spain and enjoy sun and beach. While being on the beach, the family members wear swimgear. The kids are playing in the sand. The mother takes many pictures with her camerphone. Some of these pictures are sent as digital postcards to grandmas, friends and colleagues. To avoid any accidental forwarding or reusing of these photos, they are protected by allowing print-out, but not forwarding, synchronization to a PC or modification. Postcards to friends shall be allowed to render for one month, postcards to relatives without time restriction.

- Catherine participates in a radio quiz. The radio station broadcasts a phone number to which SMS (Short Message Service) messages can be sent for participation. Using a form-fill function of her phone, Catherine sends an SMS containing her address and phone number to the radio station. She specifies the purpose of the processing into the data (purpose binding), defines a validity period, and a forward lock (only one forward allowed).

- Philipp decides to go to a cinema in the evening. He uses his mobile phone to order a ticket. He browses to the web page of his favorite local cinema, selects a movie, and the seat category. Since the film shows violence and is rated above 16 years only, he proves that he is over 16 by an age credential stored on his SIM (Subscriber Identity Module). He pays by using his mobile phone wallet. The data sent contains a purpose binding (purchase, date), but the actual purchase information (seat, film, etc) is handled separately. The wallet information is protected by a forward lock, modification protection, and validity period definition.

2 Privacy Rights Management

The Privacy Rights Management (PRM) system proposed uses DRM functionalities to protect the personal content generated by the user of the mobile phone. The privacy of personal user data is protected in mobile devices through a PRM module or PRM agent. The PRM agent shares and re-uses some functionality available today from the DRM agent, but mainly adds complementary functionality. The proposed PRM proposal includes PRM agent and server architecture in several variations, a new interface to a trusted rights server, and extensions to the Rights Expression Language (REL).

The task of the PRM agent is to encapsulate and package user data, to specify usage rights/permissions, and to protect the content using cryptographic means, i.e., confidentiality protection and integrity protection. The protection can be done on the device. Alternatively, if the device does not have the capability to encrypt, the protection can also be delegated to a trusted server. The content is protected by encryption with a Content Encryption Key (CEK). The corresponding decryption key (if symmetric cryptography is used, the CEK itself) and the usage rights are combined into a rights object (RO).

Our approach is different from the classical server-client DRM model, where the source of protected data is a content provider, not an individual end user, and where packaging and protection of content is done on a computationally strong server at the content provider, not on an end user device.

2.1 Architectures for Privacy Rights Management

We assume that content is generated or stored on a mobile device. Such content can for example be pictures taken with a built/in or attached camera, audio clips recorded with a microphone, text typed in by the user, data received from the users home PC and so on. The user wants to securely forward the content to another user's mobile device, and have control how the other user can consume and forward the content. For that purpose the PRM agent is invoked from the user. Thus, the content needs to be protected, and usage rights need to be specified. Specification of usage rights is done using a standard REL, possibly with some new PRM extensions, that provide permissions and restrictions for example:

- Restriction by purpose binding of the content, e.g. binding to the terms of a payment contract
- Restriction of the validity period (time to live)
- Forward lock for distribution
- Restriction of copying and synchronization e.g. only allowed to copy to one other device
- Permission to print

Usually, the rights are at least integrity protected as to prevent unauthorized modification, they may also be encrypted. To provide interoperability the REL rights and extensions outlined above are usually encoded using XML. The rights need to be bound to an object, e.g. by a reference or by putting them together in a common container or envelope. The required functionalities to protect the content can be supported by the SIM (Subscriber Identity Module) or Wireless Identity Module (WIM), e.g. by offering encryption and signature functionality. The privacy description needs then to be recognized by the receiving device, which would be the privacy enforcement point. This is a crucial point; both sending and receiving mobile devices need to support these mechanisms. Today some mobile devices already enforce DRM rights specified by the content providers, and then enforcement of PRM rules would therefore be a similar task.

Depending on the functionality available in the device, several architectures for PRM are conceivable. If DRM functionality shall be re-used, the PRM architecture needs to be compatible with, or an extension of, the DRM architecture. The architecture also depends on whether a mobile device is authorized to issue rights; in mobile DRM systems it may be that rights issuers need to be registered and authorized, and it is not feasible to authorize all mobile phones. In these cases, it is possible to delegate some of the functionality to a server that is authorized to issue rights in the DRM trust system. The following mobile PRM architecture variations are for example possible, depending on the available functionality on the device:

A. All PRM functionality on device

If the device is authorized to issue rights objects to another DRM device, all steps can be executed on the sending device. Protection of the content is done on device A with a content encryption key (CEK), and a rights object (RO) for the receiving device B is generated on device A. The device A sends B the RO consisting of the rights and the CEK which is encrypted e.g. with the public key of B. This assumes that B has sent its public DRM certificate, containing its public DRM key, to A. It should be noted that the role of a rights issuer is a very sensitive one. The issuing of rights needs to be supported by strong security mechanisms and strong authentication requirements.

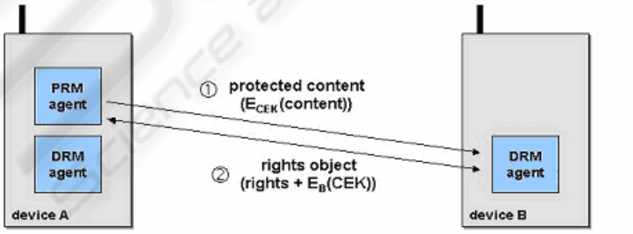

Fig. 1. PRM with content protection/encryption and RO generation done on device A

B. Encryption and rights specification on device, rights issued from server

The second possibility is that the protection of the content is done on device A, and usage rights are specified on the sending device as well. However, A is not authorized to issue a rights object in the DRM trust system to B. Thus, the CEK and the rights description are sent to a PRM server, which is authorized to issue rights objects to DRM capable devices. The device A sends the content that is protected by encrypting it with the CEK to device B. The PRM server generates a RO for the receiving device B (by encrypting the CEK with the public DRM key of B), and sends it to device B.

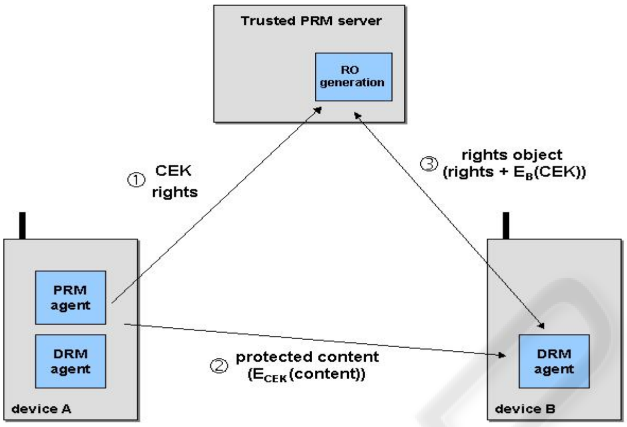

Fig. 2. PRM with content protection/encryption done on device A, RO generation done on PRM server

C. Specification of rights on device, encryption done and rights issued from server

The third options that the unprotected content and the description of the rights are sent to a PRM server (possibly over a secured link e.g. using IPSec). Thus, most tasks are now delegated to the server, except the specification of the usage rights (on device A) to be enforced on device B. The content protection is done on the server by encrypting the content with a server-generated key CEK, and the PRM server also generates ROs for devices A and B, where the CEK is encrypted using the public keys of A, resp. B. The rights objects are sent to A and B. Also, the protected content is sent to A. A may then forward the protected content to B, or the server directly send the protected content to B.

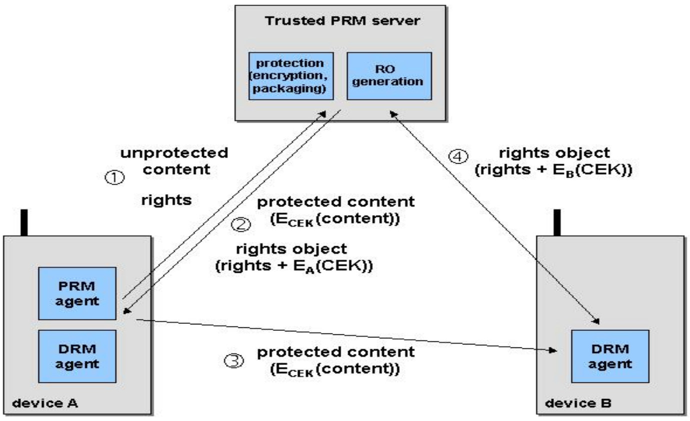
Trusted PRM server
protection (encryption, packaging)
RO generation
① unprotected content
rights
② protected content (E_{CEK}(content))
rights object (rights + E_A(CEK))
④ rights object (rights + E_B(CEK))
PRM agent
DRM agent
device A
③ protected content (E_{CEK}(content))
DRM agent
device B

Fig. 3. PRM with content protection/encryption and RO generation done on PRM server

In all three cases, device B finally receives the protected content and a rights object that gives access to the content, but also contains usage rights for the content. The DRM agent on device B then enforces those rights, such that the content can be consumed on device B in accordance with the privacy and usage rights specified on device A. Thus, A has control over the use of its content.

3 Summary

The introduction of MMS, camera phones and mobile wallets increased the privacy problems for the mobile environment substantially. Users want to assure that their data, e.g. photos, are only used in accordance to the intentions the user had. Especially an always-present camera with the "threat" of easy sending and forwarding is a serious privacy risk. Privacy concerns might lead to a slow adoption or failure of new technology. The proposed privacy rights management system can be one solution to protect user content in an efficient and affordable manner. A user can define usage and privacy rights governing the distributed content, The receiving device(s) can only use the content in accordance to the defined rights. By re-using DRM functionality in the devices, the additional functionality required is minimized.

4 References

1. Larry Korba, Steve Kenny "Towards Meeting the Privacy Challenge: Adapting DRM", http://crypto.stanford.edu/DRM2002/KorbaKennyDRM20021.pdf
2. Open Mobile Alliance, Digital Rights Management Specification Version 1, http://www.openmobilealliance.org/
3. W3C Platform for Privacy Preferences, http://www.w3.org/P3P/