J. A. Onieva, et al., "Integration of non-repudiation services in mobile DRM scenarios", *Telecommunications Systems*, vol. 35, pp. 161-176, 2007.
NICS Lab. Publications: `https://www.nics.uma.es/publications`

Extending an OMA-based DRM Framework with Non-Repudiation Services*

Abstract - *Digital Rights Management (DRM) is an umbrella term for any of several arrangements which allows a vendor of content in electronic form to control the material and restrict its usage in various ways that can be specified by the vendor. These arrangements are provided through security techniques, mainly encryption, and the distribution, in a detached manner, of content and rights. This allows free access to the content by the consumers, but only those carrying the proper Right Object (RO) will be able to process such content. As a security service considered in different layers of the security framework defined by ITU X.805, almost all applications need to consider non-repudiation in the very beginning of their design. Unfortunately this has not been done so far in DRM specifications due to practical issues and the type of content distributed. We analyze this service for a DRM framework and provide a solution which allows the right objects acquisition to be undeniable.*

Keywords - *digital rights management, non-repudiation, secure electronic commerce, mobile applications.*

1 Digital Rights Management

The traditional industry for multimedia contents has used classical technologies for distribution and consumption. Nevertheless, with the introduction of digitalized multimedia and the use of telecommunication networks, content production and distribution has become easier and faster than ever before. These contents demand more protection from theft and prying eyes. This increasing need of content protection is driven by two trends. The first is mass piracy and theft of intellectual property and proprietary information. The second is that more "sensitive information" such as financial statement, medical records, and contracts are available in digital form and must be securely stored, shared, or distributed within and between organizations.

This is precisely the niche in which DRM comes out to offer us a solution. Technically, DRM is defined as a set of technologies and systems that can col-

*Part of the work has been published in [14].

lectively support the entire life cycle of contents (creation, manipulation, distribution and consumption) by preventing illegal copying, imposing fees, processing payments, tracking contents, and protecting each principal's right and profit. Summarizing, Digital Rights Management systems are the technological measures built into the hardware or software of any device for managing the relationships between users and protected expression [16].

The WIPO Copyright Treaty [4], recognized by at least 39 nations, refers to DRM as "technological measures" used to exercise rights and restrict unauthorized acts, and as the "copyright management information" needed to identify authors, rights holders and the terms of authorized use. So, DRM systems take three approaches to securing content. The first approach is "containment", the content is encrypted so that it can only be accessed by authorized users. The second is "marking," that consists on placing a watermark on content as a signal that the media is copy controlled. The third is "Separate Delivery", achieved by delivering the media and usage rights via separate channels, allowing a device to forward the content, but not the usage rights.

It is generally agreed that DRM involves different aspects: protection, such as copy protection or watermarking, information representation, e.g., metadata and rules, and the negotiation of the rights and agreements.

In order to improve the management of Rights in the Digital environment (Digital Rights), there is a need for a common language for DR representation. This kind of language is aimed to help building reliable networks where intellectual property rights can be managed in an open, global and adaptable form, so people can share, sell, buy, etc. content subject to DR, depending on their needs. A semantic approach seems a more flexible and efficient way of achieving these activities than a syntactic one.

Using metadata for referencing multimedia material is becoming more and more usual. This allows better ways of discovering and locating this material published in any kind of communication network. Several initiatives for establishing standards for metadata models are being carried out at the moment.

Currently, digital media commerce requires the integration of rights management systems with proprietary, often incompatible, back-end systems such as e-commerce management, customer relationship management, and asset management. In order to create interoperable digital commerce, including cross-system rights management, rights holders and retailers need a set of standard business rules to define the parameters of media usage - for example, establishing that a piece of content be viewed a certain number of times per payment. Rights expression languages (RELs) are a means of expressing the rights of a party to certain assets and serve as standardized exchange formats for rights expressions. There are many initiatives around the standardisation of DRM. Examples are ODRL, XMCL, XrML,

and DPRL .

DRM concerns many stakeholders such as authors and publishers, consumers, libraries, schools and educational institutes, infrastructure providers, hardware and software manufacturers, government or standard bodies. Therefore, any DRM related research must take into account both, the complexity and the various stakeholders. Moreover, it is necessary to find the balance between the appropriate security and the protection of consumer privacy.

Different techniques are used in DRM systems. There are techniques to identify original content such as hash codes in digital files, watermarks in images and hidden sound codes in music files, and encryption to secure communication and distribution. For instance, *Copy protection* schemes attempt to find ways, which limit the access to copyrighted material and/or inhibit the copy process itself. Examples of copy protection include encrypted digital TV broadcast, access controls to copyrighted software through the use of license servers and technical copy protection mechanisms on the media. On the other hand *Copyright protection* inserts copyright information into the digital object without a loss of quality. Whenever the copyright of a digital object is in question, this information is extracted to identify the rightful owner. It is also possible to encode the identity of the original buyer together with the identity of the copyright holder, which allows tracing of any unauthorized copies. The most prominent way of embedding information in multimedia data is the use of digital watermarking [17].

1.1 Mobile DRM

Mobile DRM (MDRM) is a set of actions, procedures, policies, product properties, and tools that can be used to manage rights in digital contents according to requirements over mobile networks. A MDRM System tries to establish a trusted computing environment and trusted infrastructure. This infrastructure supports the secure preparation and transmission of protected digital contents. Additionally it prevents the misuse of the protected digital contents. Therefore a MDRM System must prevent illegal acts on the protected content, but also on the associated rights. But it also has to be practical in terms of scalability, simplicity, implementation / operation cost and efficiency. This is sometimes a challenge that has to be met.

The hardness of the challenge of course depends on the type of contents. Depending on the content MDRM can be classified into different groups [19]:

- *Rich* MDRM: The content managed by the MDRM system is rich media, such as video, e-books, which can only be consumed by high-end mobile devices. Both cryptographic and watermarking technologies are needed for protecting the contents and controlling the usage.

- *Light* MDRM: The content managed by the MDRM system is light media, such as ring tones, images, music, which can be consumed by medium-end or low-end mobile devices, like older mobile phones, whose platform is close. Cryptographic protection may not be necessary. Watermarking can be used instead. The device handles enforced usage.

- *Minimal* MDRM: No digital contents are attached. The digital-right itself claims the holder's rights to be served. The typical examples are e-Tickets and e-Coupon. The digital rights just have to be saved in a secure mobile wallet.

In these systems, content and rights are distributed in a detached manner. This technique simplifies the download of content and its management. No protection of the content is needed, such that any user can download it. But, of course, in order to consume it, a user needs to access (purchase) the corresponding *digital right object*. Here, two possible approaches for rights management exist:

Centralized: A user needs to access the corresponding right from a central manager each time it wants to consume content. It is very effective against malicious users, but not so against malicious rights managers. Additionally, this approach suffers from scalability problems.

Distributed: A user maintains its rights and just makes use of them when needed. It overcomes the existing drawbacks of centralized systems, but nevertheless, in order to avoid illegal use of the rights, a tamper-resistant hardware or *Trusted Personal Device* (TPD) is needed (that locally manages the rights in a certified and tamper-proof way).

One of the main DRM services today is downloading digital contents from a service provider. This will definitely expand to mobile commerce. Protected contents, like films, music, ring tones, e-books, games, etc., are downloaded from the service provider to the mobile devices for consuming. The service provider obtains these contents from one or more content providers. In order to open the protected contents, the user needs to purchase a digital right from the service provider via mobile payment.

The right will be stored securely in his mobile device. With a correct digital right, the user can open DRM protected contents and consume the contents only with the help of the above said mobile device. The user can super-distribute the protected contents to other user's devices, what means peer-to-peer distribution among friends and communities. But similarly to the distributing user, these users will have to order digital rights for consuming the contents. The contents are

DRM protected using either cryptographic methods and/or digital watermarking, no matter how they are distributed.

With respect to the DR management approach, the selected approach should allow users to access content when no connection to a central server is possible and, at the same time, it should allow industry to introduce a minimum number of changes to the existing business platform for distributing multimedia content in a secure (and right-protected) manner. With the advent of cellular networks, the *distributed* approach allows the convergence of user and industry needs. Combining DRM solutions with mobile networks, users can access the digital rights by using their mobile phone as a TPD. Telecom operators can drive the users for accessing or purchasing digital rights as well as certifying the secure management of digital rights in the handset (see Figure 1).

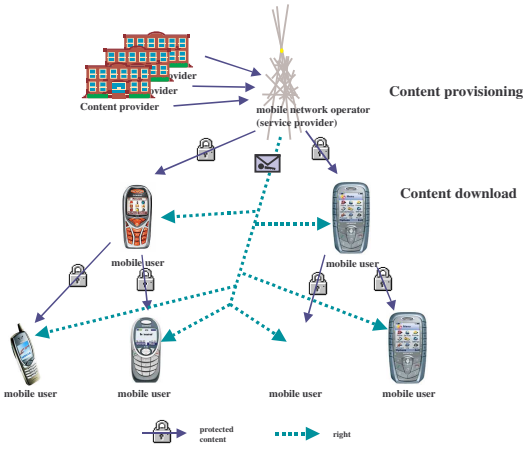

Figure 1: Content Distribution

Different standardisation organisations and initiatives coexist for MDRM. The *third Generation Partnership Project* [1] is a collaboration agreement between a number of standardisation organisations. It was established in December 1998. The main goal is to provide globally accepted and applicable technical specifications for third generation mobile communications (3G). 3GPP first planned to introduce a MDRM specification in their set of standards. A document manly containing requirements for enabling DRM was completed [18]. But in September 2002 the responsibility of 3GPP's MDRM standardisation word was transferred to the Open Mobile Alliance.

The *Open Mobile Alliance* [3] was founded in June 2002 by the Open Mobile Architecture Initiative and the WAP Forum. The main goal of OMA is to introduce

open standards and specifications based upon market and consumer requirements for the mobile industry. One of its specifications for the mobile industry is on MDRM. The OMA DRM 2.0 specification [15] introduces different methods for administering digital rights. One of then (and the most important for us) is *separate delivery*.

With the separate delivery method the content and the rights are delivered via separate channels to the mobile device. The content must be encrypted and converted into a special format, the DRM Content Format (DCF). A DCF object can only be accessed with the correct Content Encryption Key (CEK). This key is contained within the separately delivered right. With separate delivery the mobile device is allowed to forward the protected content, namely the DCF object, to other mobile devices. The rights containing the CEK can not be forwarded to other devices. To access the content the receiving device of a DCF object must request a new right containing the needed CEK. With this feature separate delivery enables the super-distribution of content.

Other initiatives are IPMP (Intellectual Property Management and Protection), from the Moving Picture Experts Group [2], integrated in standards MPEG-4, MPEG 7, and MPEG-21. The IPMP extension do not actually standardise complete DRM systems. They just standardise the DRM interface which can be used by other DRM applications. Table 1 compares some of the existing mobile or hybrid DRM systems [d2104, Yan01].

System	**Architecture**	**RDL**	**DRM Techniques**	**Comment**	**More Info**
NDS	mobile/ distributed	ODRL	Symmetric Encryption	OMA DRM 1.0 compliant	www.nds.com
InterTrust	hybrid/ distributed		AES, DSA, SHA-1	supports MPEG-4	www.intertrust.com
Content Guard	centralised/ hybrid	XrML	Digital Signature, Hash, Watermarking	no superdistribution	www.contentguard.com
Coremedia	distributed/ mobile	ODRL		OMA DRM 2.0 compliant	www.coremedia.com

Table 1: Existing MDRM Systems

After reviewing the existing products and initiatives, the UBISEC[1] consortium analyzed the common requirements and identified shared weaknesses to be overcome. Mobility is considered in the way that the client device for managing digital rights is a secure mobile device, which could in particular be a smart card. The secure mobile device is keeping the rights to execute protected content and connects (via an appropriate connection) to a MNO which in turn obtains the desired rights from a Rights Issuer and forwards them to the secure mobile device. The fundamental concept is to keep the rights (together with their permissions and constraints) on the secure mobile device. The right may not be forwarded to other devices (as opposed to other proposals, which allows under certain circumstances to transfer rights to other devices). In contrast, protected content can be distributed without any restrictions, as no one is able to consume the protected content without the correct decryption key, anyway.

Anonymous purchase of rights is supported, as the Content Provider and Rights Issuer do not require privacy details of consumers. Consumer billing is performed through MNO to whom the consumer is subscribed. Contracts between network operators, rights issuers, and content providers have to regulate payments for content usage, but this is not in the scope of our specification.

Taking all this into account, we modified a platform based on the OMA DRM specification 2.0 for the distributed rights management. The modified scheme proposed in the European project UbiSEC enables a more secure framework for charging on the digital rights acquisition by the consumer, taking into account important issues as anonymity and efficiency (see Figure 2).

In this architecture the user browses and downloads the desired content. The Content Provider supplies reference to the corresponding Right Object. Using this reference, the consumer will make use of his TPD for accessing the Right Object once he gets price and usage information. This basic use case can be seen in Figure 3.

In our scheme, the distribution of the RO to the user through a *Mobile Network Operator* (MNO) comes out as a final important step on the fair distribution of digital content (see Figure 4). The MNO participation in this process is one of main changes introduced to the OMA specification. Detaching the user and the RI in the right acquisition process, we do not only instantiate the billing service provider but also introduce anonymity and push forward a required property (and often ignored): **non-repudiation**.

[1] Ubiquitous Networks with a Secure Provision of Services, Access, and Content Delivery (FP6-2002-IST-1-506926)

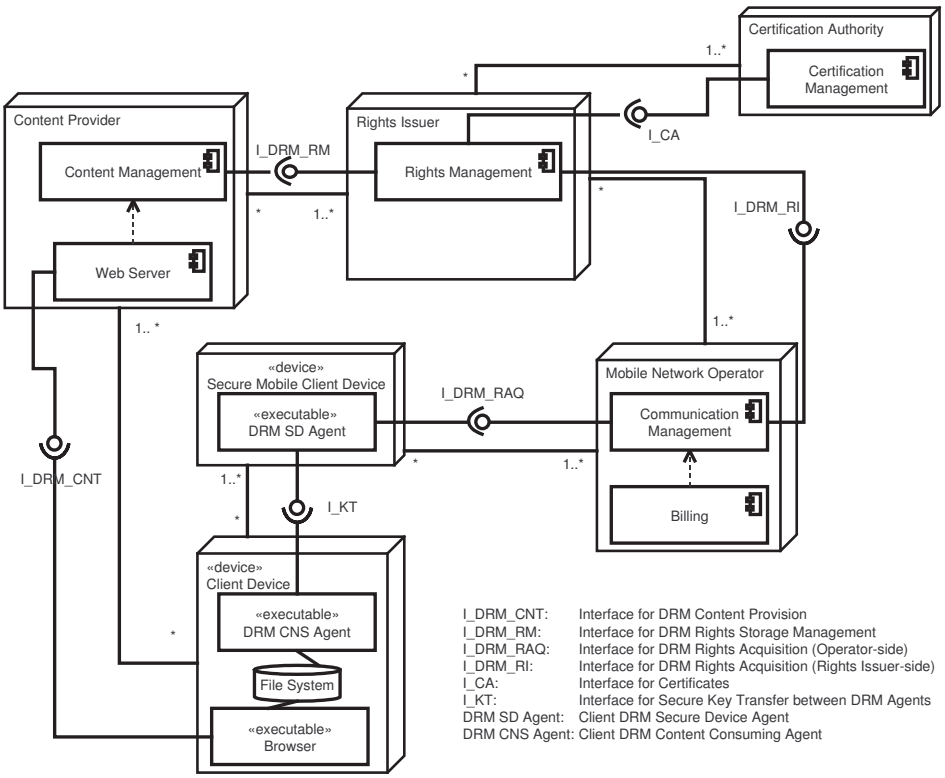

Figure 2: UBISEC DRM Architecture

2 Non-Repudiation in DRM Architectures

As a security service considered in different layers of the security framework defined by ITU X.805 [8], almost all applications need to consider non-repudiation in the very beginning of their design. Unfortunately, this has not been done so far in DRM specifications due to practical issues and the type of content distributed. In this section, the analysis of this service for a DRM framework allows us to provide a solution which enables the right objects acquisition to be undeniable.

2.1 Non-repudiation: A Security Service

Repudiation is one of the fundamental security threats existing in paper-based and electronic environments. Dispute of transactions is a common issue in the business world. Transacting parties want to seek a fair settlement of disputes, which brings

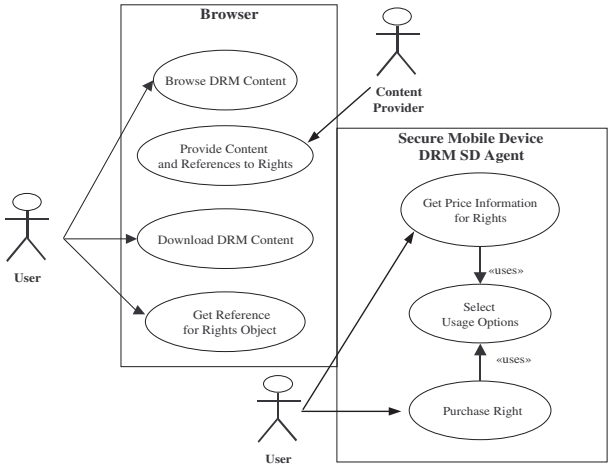

Figure 3: DRM

the need of non-repudiation services in their transactions. The motivation for non-repudiation services is not just the possibility that communicating parties may try to cheat each other. It is also the fact that no system is perfect, and that different and unexpected circumstances can arise in which two parties end up with different views of something that happened. Network failures during the protocol run is a representative example.

We define a *basic transaction* as the transferring of a message M (e.g. electronic goods, electronic cash or electronic contracts) from user A to user B, and represent this event with the following flow: $A \rightarrow B : M$. Thus, typical disputes that may arise in a basic transaction with a deadline T could be

- A claims that it has sent M to B while B denies having received it;
- B claims that it received M from A while A denies sending it;
- A claims that it sent M before T while B denies receiving it before T.

Non-repudiation must ensure that no party involved in a protocol can deny having participated in a part or the whole of the protocol. Therefore, a non-repudiation protocol must generate cryptographic evidence to support dispute resolution. In a typical non-repudiation protocol, a *trusted third party* (TTP) helps entities to accomplish their goals. Non-repudiation is especially important in electronic commerce to protect customers and merchants. It must not be possible for the merchant to claim that he sent the electronic goods when he did not. In the same way, it must not be possible for the customer to deny having received the goods.

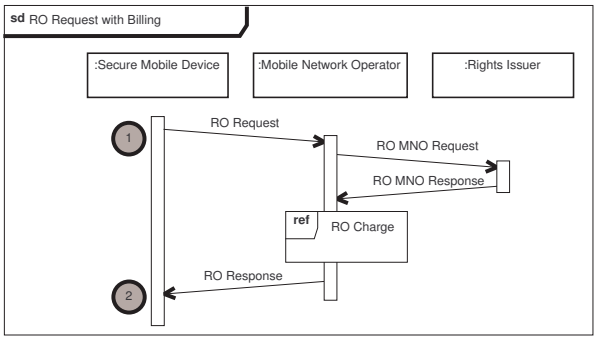

Figure 4: Right Object Acquisition

Non-repudiation can be considered as an extended *fair exchange* problem in which non-repudiability is made an integral requirement of the exchange (in general it is not required). Exchange of one data item for another between mutually distrusted parties is usually the difficult part of an electronic transaction. We can find various instances of the general exchange problem in different types of commercial activities: a purchase, contract signing, certified mail or, more generally, in any barter conducted by means of digital networks. An exchange is said to be *fair* if at the end of the exchange, either each player receives the item it expects or neither player receives any additional information about the others item. For instance, in payment protocols, fair exchange can ensure that a customer receives a digital good from a vendor if and only if the vendor receives payment from the customer.

For any non-repudiation service, evidence processed is a crucial object. There are different activities at each phase of processing. The non-repudiation policy defines the behavior of these activities. Finally, the eventual success of non-repudiation depends upon technical and legal supports. In order to achieve a non-repudiation service, some common phases have to appear in the protocol:

Service request - One or more parties involved must somehow agree, prior to its origination and delivery, to utilize non-repudiation services and to generate the necessary evidence for a non-repudiation service.

Evidence generation - Depending on the non-repudiation service being provided and the non-repudiation protocol being used, evidence could be generated by the originator, the recipient, or the trusted third party. The elements of non-repudiation evidence and the algorithms used for evidence generation

are determined by the non-repudiation policy in effect and service request phase. Namely, evidence can be generated using secure envelopes or digital signatures. The latter is more widely employed. A digital signature basically links a message with its originator, and also maintains the integrity of the message.

Evidence transfer - The evidence generator must transfer the evidence to the party who may ultimately need to use it. The principal participants may utilize trusted third parties to receive evidence.

Evidence verification and storage - Newly received evidence should be verified to gain confidence that the supplied evidence will indeed be adequate in the event of a dispute arising. The verification procedure is closely related to the mechanism of evidence generation. As the loss of evidence could result in the loss of future possible dispute resolution, the verified evidence needs to be stored safely. The duration of storage will be defined in the non-repudiation policy in effect.

Dispute resolution - This phase will not be activated unless disputes related to a transaction arise. When a dispute arises, an adjudicator will be invoked to settle the dispute according to the non-repudiation evidence provided by the disputing parties. The evidence required for dispute resolution and the means which the adjudicator will use to resolve a dispute are determined by the non-repudiation policy in effect.

A non-repudiation protocol generates at least the following important evidence for the participating entities:

Evidence of origin. This evidence is generated by the originator (perhaps with the assistance of a TTP) for a particular message and intended to the recipient, such that the originator cannot deny having sent that message.

Evidence of receipt. This evidence is generated by the recipient (perhaps with the assistance of a TTP) for a received message and intended to the originator, such that the recipient cannot deny having received that particular message from the originator.

In a typical two-party non-repudiation service, we identify several requirements, some of which could be optional, depending on the application the non-repudiation service is running over:

Fairness. A non-repudiation protocol provides fairness if neither party can gain an advantage by quitting prematurely or otherwise misbehaving during a protocol. At the end of the protocol either the sender gets evidence of receipt and the recipient receives a message as well as evidence of origin for that message or none of them gets any valuable item.

Timeliness. A non-repudiation protocol provides timeliness if any of the participating entities has the ability to reach the end of the protocol in a finite amount of time without loss of fairness.

Confidentiality. A non-repudiation protocol provides confidentiality if none but the intended parties can get access to the (plaintext) message sent during the non-repudiation protocol.

Several solutions to fair non-repudiation have been developed [11]. Some of them use a TTP which plays the role of a delivery agent between the participating entities. The major disadvantage of this approach is the communication bottleneck created at the TTP. Nevertheless, Zhou and Gollmann presented a protocol [20] where the TTP intervenes during each execution as a "low weight notary" rather than as a delivery agent. Other solutions use an off-line TTP, assuming that participating entities have no malicious intentions and the TTP does not need to be involved unless there is an error in the protocol execution. This is called an *optimistic approach*. There are also solutions that completely eliminate the TTP's involvement. However, they need a strong requirement: all involved parties must have the same computational power in *gradual exchange* protocols, or fairness depends on the number of protocol rounds in *probabilistic* protocols.

Previous work on non-repudiation in the literature was mostly focused on the two-party scenario. There has been some work with participation of several entities in related topics like *fair exchange*, where multiple entities exchange items among themselves without loss of fairness [7, 5, 6, 9]. Markowitch and Kremer extended the two-party non-repudiation scenario to allow one originator to send the same message to multiple recipients in a single protocol run [10, 12], whereas Onieva et al. extended this scenario for sending different messages to multiple recipients. The work done in this paper is based in [13], which presents a semi-trusted intermediary for multi-party non-repudiation, which helps final entities to collect, verify, and store evidence in electronic transactions. All of them are theoretical studies. Using those basic construction elements, we have designed a protocol that is integrated into our DRM framework. It uses an intermediary and allows fair exchange of evidence in the RO acquisition phase[2].

[2] Although the requests and responses are XML signed in the DRM specification, this does not ensure fair exchange of items and thus it does not provide a complete non-repudiation service.

2.2 Non-repudiation in the UBISEC DRM Architecture

Since the rights acquisition process means an exchange of money (or other valuable item) for rights via a mobile payment, evidence of the exchange needs to be generated, such that, if any dispute arises among the parties, they will be able to demonstrate their participation in the DRM scenario. Even though the proposed architecture strongly relies on trusted third parties (MNO and RI), non-repudiation issues on content distribution have to be considered, without having an impact on all the above mentioned properties.

Considering the user as the customer which receives content and rights in order to be able to consume such content, non-repudiation is a valuable service for the customer in the last phase when it has to access the Right Issuer (through the Mobile Network Operator) to get the RO in exchange for the payment. (The MNO charges the user for the RO value in its monthly bill.)

Even though the MNO and the RI are considered trusted entities, there can be several difficulties in the process (e.g., a network failure or loss of data) which can end up in disputes among the parties. Such possible disputes could be as follows.

1. The MNO charges the user for the RO it did not purchase or receive. (It could also occur that the amount of money charged does not coincide with the one expected by the user.)
2. The user receives a corrupted RO while already having paid for it.
3. The user denies having sent a request (RORequest) for purchasing the RO.
4. The MNO denies having received a request from the user.
5. Similar disputes between the MNO and the RI.

From this list, the non-repudiation of origin and non-repudiation of receipt services have to be provided between the user and the MNO and between the MNO and the RI, thus establishing a logical non-repudiation channel between the user and the RI.

Nevertheless, collecting, verifying and storing evidence about the digital right purchase might be operationally undesirable. On the other hand, *intermediary* entities are useful in such scenarios to help final entities to carry out their protocol exchanges. It is thus clear that this philosophy matches or MDRM approach in which the Mobile Network Operator serves as an intermediary entity, and users have direct access to the MNO and implicitly place certain degree of trust on it.

The rest of this paper is organized as follows.. TBM

3 Conclusions

As the technology evolves, content downloading will be an inexpensive operation. In order to protect Intellectual Property Rights, distributed DRM appears as a very good approach. Furthermore, DRM frameworks will be enriched by the implementation of security services from the very beginning. Non-repudiation is one of them.

We have designed a non-repudiation protocol for a DRM platform that takes into account all participants in the acquisition of rights, namely, the user, the Mobile Network Operator and the Rights Issuer, thus providing all of them with sufficient evidence to be used in case a dispute arises.

The implementation of the protocol is briefly sketched. It is designed such as to integrate with the Mobile DRM framework we are modifying from the OMA DRM standard. We are still in a test phase, and the necessary API has not been deployed yet. This is the main field in which we plan to continue our work.

Acknowledgement

The work described here was partially funded by the FP6-2002-IST-1 project UBISEC, contract number 506926 which successfully ended at the beginning of 2006. The first author has been funded by the Consejeria de Innovacion, Ciencia y Empresa (Junta de Andalucia) under the III Andalusian Research Plan, and the fourth author has been funded by the Ministry of Education and Science of Spain under the Programa Nacional de Formacion de Profesorado Universitario.

References

[1] http://www.3gpp.org/.

[2] http://www.chiariglione.org/mpeg/.

[3] http://www.openmobilealliance.org.

[4] http://www.wipo.int/treaties/en/ip/wct/index.html.

[5] M. Franklin and G. Tsudik. Secure group barter: Multi-party fair exchange with semi-trusted neutral parties. In *Proceedings of Financial Cryptography 1998*, volume 1465 of *Lecture Notes in Computer Science*, pages 90–102. Springer, Feb. 1998.

[6] N. González-Deleito and O. Markowitch. An optimistic multi-party fair exchange protocol with reduced trust requirements. In *Proceedings of the 4th International Conference on Information Security and Cryptology*, volume 2288 of *Lecture Notes in Computer Science*, pages 258–267. Springer-Verlag, Dec. 2001.

[7] N. González-Deleito and O. Markowitch. Exclusion-freeness in multi-party exchange protocols. In *Lecture Notes in Computer Sciences*, pages 200–209. 5th In-

ternational Conference on Information Security (ISC 2002), Springer-Verlag, Oct. 2002.

[8] ITU-T. *Security architecture for systems providing end to end communications*, October 2003.

[9] J. Khill, I.and Kim, I. Han, and J. Ryou. Multi-party fair exchange protocol using ring architecture model. *Computers & Security*, 20(5):422–439, 2001.

[10] S. Kremer and O. Markowitch. A multi-party non-repudiation protocol. In *Proceedings of SEC 2000: 15th International Conference on Information Security*, pages 271–280. IFIP World Computer Congress, August 2000.

[11] S. Kremer, O. Markowitch, and J. Zhou. An intensive survey of fair non-repudiation protocols. *Computer Communications*, 25(17):1606–1621, Nov. 2002.

[12] O. Markowitch and S. Kremer. A multi-party optimistic non-repudiation protocol. In *Proceedings of 3rd International Conference on Information Security and Cryptology*, volume 2015 of *LNCS*, pages 109–122. Springer-Verlag, December 2000.

[13] J. A. Onieva, J. Zhou, M. Carbonell, and J. Lopez. Intermediary non-repudiation protocols. In *Proceedings of 2003 IEEE Fifth Conference on Electronic Commerce*, pages 207–214, June 2003.

[14] J. A. Onieva, J. Zhou, J. Lopez, and R. Roman. Extending an OMA-based DRM framework with non-repudiation services. In *Fifth IEEE Symposium on Signal Processing and Information Technology*, pages 472–477. IEEE, 2005.

[15] Open Mobile Alliance. *DRM Specification*, 2 edition, 2006.

[16] P. Plaza, J. L. Gonzales, M. Lacoste, D. Stern, F. Bormann, C. Zoth, J. Tacken, J. Lopez, J. Onieva, M. Soriano, J. Forne, A. Marin, F. Almenarez, J. Görlich, H.-J. Eikerling, W. Müller, and R. Schäfer. Mobile security: Requirements and state of the art analysis. Technical Report D2.1, UBISEC Consortium, 2004.

[17] J. Seitz. *Digital watermarking for digital media*. Hershey, PA : Information Science Pub., 2005.

[18] T. S. G. Services and S. Aspects. 3gpp s1-01 1197. ts 22.242. Technical report, 3rd Generation Partnership Project, Nov. 2001. V6.2.0.

[19] Z. Yan. Mobile digital rights management. In L. Staffans and T. Virtanen, editors, *T-110.501 Seminar on Network Security*. Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, 2001.

[20] J. Zhou and D. Gollmann. A fair non-repudiation protocol. In *Proceedings of IEEE Symposium on Security and Privacy*, pages 55–61. IEEE Computer Society Press, May 1996.