TICKET BASED IDENTITY SYSTEM FOR DRM

Alapan Arnab and Andrew Hutchison

{aarnab, hutch}@cs.uct.ac.za
Data Networks Architectures Group
Department of Computer Science
University of Cape Town
Rondebosch, 7701
South Africa

ABSTRACT

One of the major stumbling blocks in achieving interoperability in DRM systems is due to the variety of different user authentication systems utilised by DRM systems. For example, in [6], the authors detailed how Microsoft's Rights Management System fails in fulfilling its requirements mainly because of a lack of its user identity system. The authors discussed how, because one DRM system cannot authenticate users from another DRM system, it cannot offer interoperability, even if they shared the same data formats. Furthermore, interoperability for user authentication in DRM systems is further hampered by the wide range of devices that need to support DRM enabled data, but do not necessarily offer the same features.

Decoupling of user identity from the main DRM system also reduces the chances of correlating users' access patterns of protected works. This improves the privacy of users of DRM systems, another major criticisms of current DRM systems. In this paper we discuss the requirements for user identity in a DRM system and then introduce a Kerberos like reusable ticket based user identity system. This system allows multiple systems to be authenticated by the use of time limited authentication tickets, without requiring online authentication. Tickets can be stored at a central controlling point, which is also responsible for acquiring tickets from authentication servers and redistributing tickets to the devices that need the tickets. In our experience, our approach fulfils all the requirements and is a more scalable and inter-operable approach when compared to existing DRM systems.

TICKET BASED IDENTITY SYSTEM FOR DRM

1 Introduction

User identity is a major problem in Digital Rights Management (DRM) systems, and is arguably the major stumbling block in interoperability. In an investigation of current media DRM systems [11] against a layered model detailed in [9], the authors concluded that none of the systems featured a user identity module. Similarly, in an investigation of three enterprise DRM systems, we concluded that none of the systems featured an interoperable identity system and in the case of Microsoft's RMS system, the tight integration of the identity system to the DRM system actively hindered a wider deployment of the system in enterprises [6].

Currently the major deployment of DRM systems is not on personal computers but on mobile phones. The Open Mobile Alliance released the OMA-DRM specifications in 2004, and some of these specifications have been deployed on mobile phones. Following the wider availability of DRM enabled phones, content publishers have made DRM enabled content available globally for mobile phones most notably by the Vodafonelive! service from Vodafone.

OMA-DRM 1 specifications make use of device authentication instead of user authentication for content [13]. Thus, any person with access to a device has access to the content but the purchaser of content cannot move content between devices they own even if the devices are of the same make and model. This is a major problem as mobile phone replacement rate is high and there is already high consumer demands for device portability [7].

Because authentication is a critical security primitive for DRM, alternatives to device authentication are required and user (or group of users) authentication is the obvious alternative. However, current user identity management systems have a number of problems with regards to DRM systems:

1. Device interoperability: Many embedded devices, like iPods, do not have the ability to perform user authentication because they lack essential input mechanisms.
2. Service interoperability: It should be theoretically possible for different DRM systems to make use of common DRM controllers[1]. Thus, there is a need to decouple authentication of users from the DRM controllers.
3. Online vs Offline Usage: Even in an increasingly connected world, there are many situations where offline usage of DRM protected works is desirable (or even necessary). Even new generation identity systems like Liberty Alliance do not cater for offline authentication.
4. Trusting End Users: Replication and distribution of digital data is cheap, fast and easy. Digital certificates in certificate based authentication mechanisms are usually easily accessible to the user, and thus can be easily replicated and distributed. Thus more than one user can easily make use of a digital certificate and thus compromise authentication. However more secure alternatives such as hardware or online only authentication creates a problem with portability.

Service interoperabity is also crucial for lower level DRM controllers (i.e. DRM controllers implemented in hardware or at the operating system level). Having user interaction for authentication (like password prompts) are simple for application level DRM controllers (as found in iTunes), but become increasingly complex to handle if the implementation of the DRM controller is at the operating system level or at the hardware level. In an earlier work [5], we discussed the use of *credential* tokens in DRM use licenses. In this paper, we extend the use of credentials as a generalised ticket based authentication mechanism for DRM.

[1] A DRM controller can be defined as the software or hardware engine that is responsible for enforcing the restrictions defined in a DRM use license.

Ticket based authentication systems are not new, but their potential application to DRM systems has not been explored. In this paper we describe a design for a ticket based authentication system and discuss how this approach overcomes the problems with current user authentication mechanisms detailed previously.

This paper is organised as follows; in section 2 we discuss work related to ticket based authentication and user identity management. We also position this paper in the broader context of our DRM project. We then discuss our reasons why identity systems need to be decoupled from DRM systems in section 3. This is followed by a description of our solution in 4 and our implementation experiences in section 5.

1.1 Security Assumptions

In our proposed solution, we assume that the user's DRM controller and the remote authentication servers are secure and trustworthy. However, the user of the device and the authentication daemon presented in this paper can be assumed to be untrustworthy.

2 Background and Related Work

Interoperability for DRM has often focused at the rights expression language (REL) level, which has been often identified as the core layer of DRM systems [9]. Most RELs have mechanisms to enable identity management of users, and both ODRL and XrML have generic syntax to cater for any identity management system.

Authentication in a DRM system usually occurs when the protected file is first accessed. In some designs, subsequent authentication steps take place when other rights are requested. User authentication requires the verification of the user's identity as prescribed in the protected work's use license. In systems such as Apple's iTunes, the user's identity is stored in a certificate and this certificate is matched to the work's license [1, 3]. In iTunes, this certificate is then locked onto the device thus prohibiting portability.

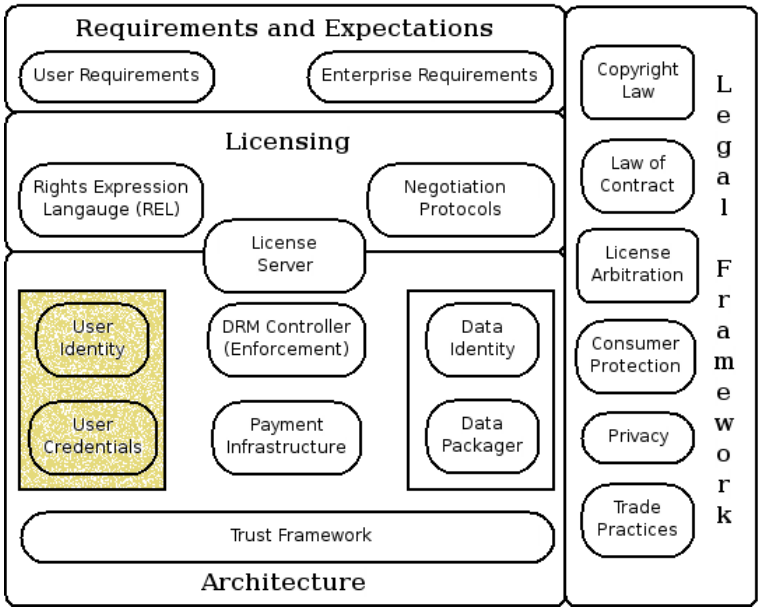

Figure 1: A componentised approach to DRM

The solution presented in this paper is part of a wider DRM system project we are involved in, which is outlined in figure 1. The solution was developed to provide non-interactive user authentication, without allowing for easy replication of certificates but allowing for device portability. The DRM controller in the project was implemented at the operating system kernel level, and the goal was to allow for enforcement of DRM licenses without the need for application support, as required by Microsoft's RMS system [6].

DRM systems do not necessarily have to use certificate based authentication for user identity. Microsoft's Rights Management Services (RMS) makes use of Microsoft Active Directory for authentication purposes. In RMS, users are authenticated once they have logged onto the machine using their active directory credentials. However, this approach is bound very tightly to the operating system and also limits its wider usage as discussed in [2, 6].

Ticket based or credential based authentication is best known through the Kerberos authentication system [15]. In Kerberos, users authenticate themselves to ticket granting servers which issue time limited tickets to be used for accessing Kerberos enabled services. This idea has been further improved and integrated with the latest generation of identity management systems including Liberty Alliance.

The Liberty Alliance Federated Identity framework allows for a single user identity to be used to access different services from a variety of different service providers. The protocol for cross service authentication makes use of signed tickets from the main identity provider [8]. Unlike our proposed solution, however, tickets in the Liberty Alliance framework provide only one-time authentication (i.e. they are not re-usable), and do not necessarily provide any control over how long access is granted to the service. We feel that these features are necessary for authentication in a DRM scenario.

The use of tickets to control access to resources were discussed in [10] by Kim et al. They used tickets as an authorisation mechanism in Globus enabled grids. The scheme we present and its application to DRM systems share many similarities to the scheme discussed by Kim et al. However the scheme presented by Kim et al. does not make use of re-usable tickets, and focuses on providing fine grained access control to grid resources.

3 The Need to Decouple Authentication and DRM Controllers

In most current DRM systems, authentication of users is strongly coupled with the DRM system itself [6, 11] and some frameworks do not distinguish them as separate functions [9]. The main problem with this scenario is the lack of interoperability imposed by the strong coupling, as competing systems create their own authentication systems, and cannot cater for different authentication systems. In many instances the authentication systems themselves are proprietary, and thus even if new legislation forces systems to share data formats [4], they do not have any net effect as the rest of the system is not interoperable.

Strongly coupled systems which offer online authentication also mean that the rights holder has a complete knowledge of not only who has access to the protected data, but also when they are using the protected data. While this does not pose any problems for enterprise DRM systems (where this feature can be seen as a requirement [6]), usage in consumer DRM systems imply a massive privacy concern. Consumer DRM systems that communicate with rights holders without the knowledge of the consumer were exposed in [12], and the coupling of online authentication and the DRM controller makes it very easy to monitor consumer activity.

The decoupling of authentication from the control of the rights holders would therefore reduce the chance of correleation of when users access protected works. This is further enhanced if the authentication system is used for other activities such as instant messenger or email access. However, full correlation between exact time of access and the user is still possible if the data is available. The ticket identity solution we present here reduces the maximum correlation to a period of possible access as opposed to exact times, and thus, in our opinion a better approach.

4 Authentication Ticket System

In this section we outline our ticket authentication solution, including the system architecture and ticket design. We also look at the security considerations for our solutions, and compare our solution to Kerberos.

4.1 General Overview

Instead of fixed certificates, we propose, like Kerberos, the use of time limited tickets for user authentication in DRM. Depending on the nature of the protected data and maybe the user's profile, the lifetime of the ticket needs to be variable. For example, music being transferred to a portable media player will get a longer ticket (e.g. 1 month) than a ticket for a computer connected to the Internet (e.g. 2 weeks). Tickets themselves will not be renewable, and thus should a ticket be compromised, it would be useless after it expires. This concept provides a solution to all the problems described in section 1, although there is a trade-off between offline and online usage (online connectivity is still required to generate the tickets).

The authentication service needs to be trusted by the DRM system, and there are a number of different companies that can provide this service. These companies could be the equipment and component manufacturers (like Apple, Intel or Dell), network service providers (like AOL or Vodafone), content producers (like Sony or Universal), retailers (like Amazon.com) or third parties like Microsoft (through its Passport system) or Google (through its Jabber enabled user system). These services can also interoperate through federated identity management systems like Liberty Alliance.

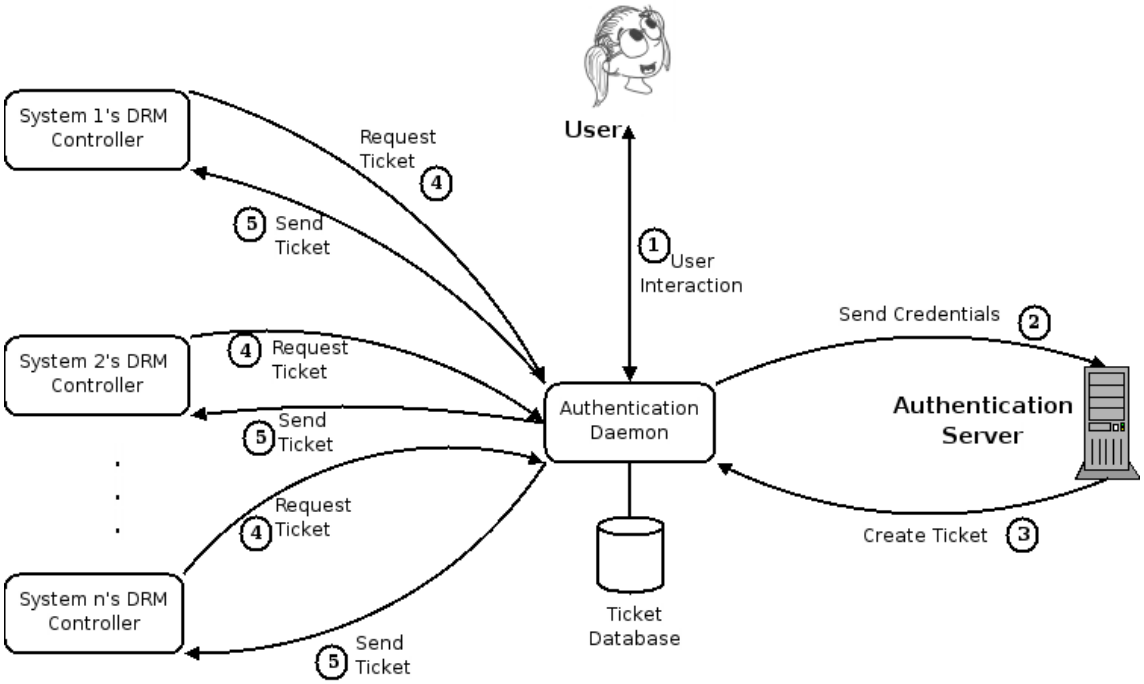

Figure 2: Authentication Ticketing System

An overview of the complete system is shown in figure 2. The user only needs to interact with the authentication daemon, and can enter details such as authentication server, username, password and the target device identifiers (1). The authentication daemon interacts with the authentication server and maintains a database of valid authentication tickets (2/3). Depending on the authentication service itself, the password can either be sent over an encrypted session channel, or sent as a hash with the username. The aim of the ticket service is to attempt to integrate different authentication services under one authorisation ticket service.

When a DRM daemon needs to authenticate a user, it asks the authentication daemon for a ticket corresponding to some user (4), and then authenticates the user itself when it receives the ticket (5). Thus, the DRM controller is still ultimately responsible for granting access to data. If the user has multiple devices (or systems), (s)he does not need multiple authentication devices. Instead, other devices (or systems) can interact with the main authentication daemon to acquire tickets. Thus, mobile devices like iPods can acquire their tickets when they are being charged or being synchronised.

If a requested ticket is not found, the user remains unauthenticated until the user acquires a ticket. While this does imply restricted access if the system is offline, it also ensures that access is granted only with access to valid tickets with the minimum intervention from the user.

4.2 Ticket Design

The general ticket solution does not solve the problem of replicated certificates (i.e. tickets themselves being distributed to attackers). Thus there needs to be a mechanism to restrict a ticket to a set of particular devices. If there is no such information, it is assumed that the ticket is valid for any device. However, this should not require the device itself making the request for tickets. There are a number of mechanisms that could be used to identify devices, and this is not explored in this paper.

The tickets could make use of a XML file, but with the absence of a tree structure, it could also be expressed as a flat file. Since XML processing is more expensive, we are in favour of a flat file description. The proposed file format is given in figure 3.

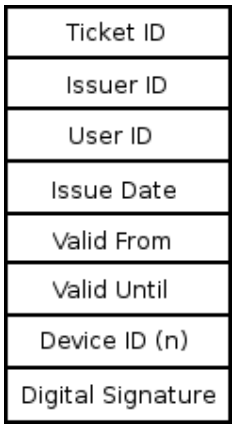

Figure 3: Proposed ticket format

4.2.1 X.509 Certificate and Kerberos Similarities

There are many similarities between the functions of a digital certificate and an authentication ticket and except for the device identifiers, an authentication ticket can be considered to be a subset of X.509 certificates and does follow most of the recommendations in the ISO Authentication Framework [14]. Data confidentiality is not a requirement for the authentication tickets, but ticket integrity is crucial. In this respect, this ticket format differs from Kerberos tickets [15].

Unlike Kerberos, the tickets are generated for use by the client for a specific device. Thus, replay attacks that are possible on Kerberos 4 and 5 [14] are not applicable on this scheme. However, attacks based on clock differences on client machines will still succeed.

Apart from a different ticket structure, our service is also more lightweight when compared to Kerberos. Unlike Kerberos, which utilises an encrypted messages at all but one steps, our system requires only the first communication between the daemon and the authentication service to be secured. Furthermore, there is only one device that needs online connectivity to function, as opposed to every device as required by Kerberos. We believe that our system is easier to adapt for current authentication systems, allows better scalability and is better for a wider range of devices when compared to Kerberos.

4.2.2 Credentials Usage

The ticket presented in figure 3 could also be used as a credential ticket. The *User ID* field should contain the credential value instead of the user's id. This format would thus also be able to restrict a credential from being

redistributed to other devices.

4.3 Security Consideration

4.3.1 Chain of Trust

The DRM controller needs to keep a list of authentication servers it trusts, and will thus limit the number of authentication servers that can be used with the system. If the DRM controller receives a ticket that it cannot recognise, it marks it as an invalid ticket, and refuses access to the protected work. Because the authentication daemon is a system that acquires tickets for usage and not the actual authentication of the user, a rogue authentication daemon cannot influence the decision of a DRM controller. Thus, the authentication daemon can remain untrusted without compromising the security of the system.

Rogue authentication daemons however can still pose other problems as they can be used to harvest usernames and passwords from unsuspecting users; which could then be used to acquire tickets. This would be an indirect attack on the system, but is no different to phishing attacks on current authentication systems.

4.3.2 Secure Storage

Secure storage of tickets is not strictly required as long as ticket integrity can be assured. Because tickets are limited to devices and period of validity, replication of tickets do not pose any problems. Systems do however need to keep a public key chain of trusted authentication systems, which needs to be secure.

4.3.3 Ticket Confidentaility, Integrity and Non Repudiation

Except for privacy concerns, ticket confidentiality is not a requirement for the system. However, ticket integrity is of paramount importance, and as long as the private keys of the authetication servers are not compromised, the integrity and non-repudiation of the tickets are assured.

5 Implementation Experience

An authentication system as described in this paper has been implemented and tested with a kernel level DRM controller. The DRM controller was a GNU-Linux kernel module, and thus did not offer any user interaction possibilities. The authentication daemon was part of a larger application daemon set that managed use licenses and authentication tickets. The daemon and the kernel communicated via device files. To keep processing costs as low as possible, a flat file format was used for the ticket.

When a user requested access to a DRM enabled file, the kernel requested the daemon for an authentication ticket and use license. Once the daemon located the required detail, it sent the information to the kernel, which could then make a decision on whether to grant access. The interaction was fast enough not to cause any apparent delays to the user.

The system achieved a high degree of portability as any protected file could be accessed if an appropriate license and authentication ticket was secured. Because of a separation of authentication and licensing, accurate tracking of usage was not possible, achieving our privacy goals.

Initially, we implemented a standard X.509 certificate authentication for the DRM controller. The ticket approach is a more secure and comprehensive approach and we have replaced the certificate authentication completely with the ticket based approach.

The one problem we did encounter was the fact that most authentication systems, including open systems such as Jabber and closed systems such as Novell Netware, do not have any support for ticketing (we implemented our own authentication system). In the remaining part of this paper, we present a crude solution to this problem.

5.1 Ticket Gateway

While tickets could be issued directly from the authentication service, most current authentication systems do not support such a mechanism. Thus, we also propose the use of a ticket gateway server. This server accepts user authentication details, and forwards the information to the authentication service. If the user is authenticated, the gateway would then issue a ticket to the user. This approach has a major benefit – DRM controllers need to implement only one standard ticket identity format, but at the same time can cater for any user identity system. The system with a ticket gateway is shown in figure 4.

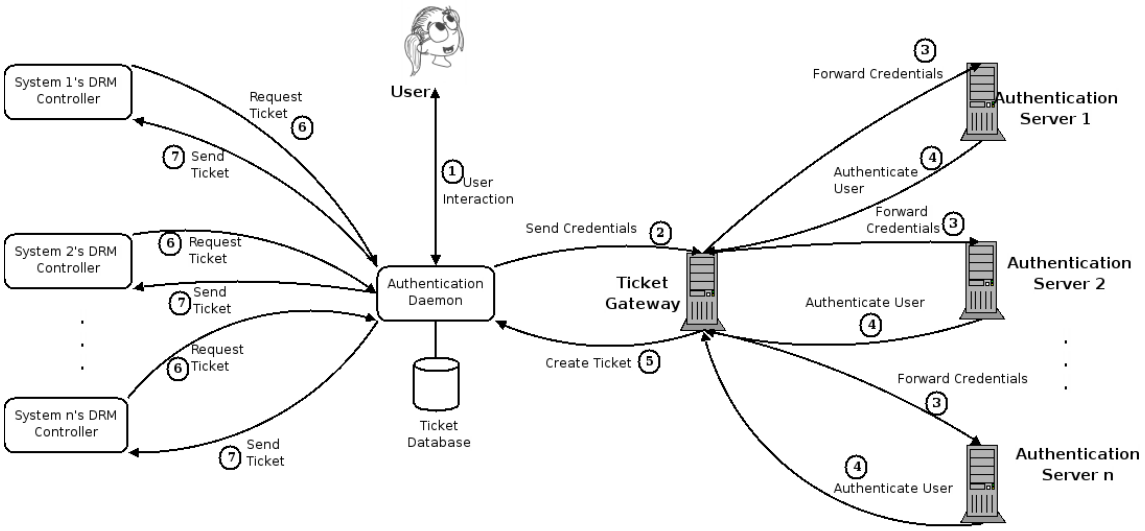

Figure 4: Authentication Ticketing System with a Ticket Gateway

However, this approach does pose its own security problems. Different identity management systems make use of different security standards. Furthermore, many systems submit passwords as a hash (as opposed to the actual text), making any conversion between incoming and outgoing formats virtually impossible. For a gateway solution to work, the gateway needs to get the “plain text” version of the username and the password, which creates a major security risk, if implemented incorrectly.

A ticket gateway could still make sense for a closed environment which has a multitude of different identity systems.

6 Conclusion

User authentication is a major component of DRM systems, not all DRM systems can support complicated authentication mechanisms, and many devices do not feature user interfaces supporting password authentication. X.509 certificate authentication is a possibility but have two major problems – long validity periods and easy replication. Current authentication ticket systems such as Kerberos are engineered for single usage and require online connectivity to operate.

In this paper we have presented a ticketing solution, based on the principles of X.509 certificates and Kerberos, that overcome these problems. We have discussed its security features and requirements and discussed our implementation experiences in a live DRM system. In our opinion, the solution is simple, lightweight, scalable and secure.

7 Acknowledgements

We would like to acknowledge the input and contributions of our fellow members of our research group, Marlon Paulse and Duncan Bennett who have contributed immensely in the implementation of the system.

This work is partially supported through grants from the UCT Council and the National Research Foundation (NRF) of South Africa. Any opinions, findings, and conclusions or recommendations expressed in this paper/report are those of the author(s) and do not necessarily reflect the views of UCT, the NRF or the trustees of the UCT Council.

References

[1] Playfair.
URL: http://playfair.sourceforge.net/.

[2] Technical overview of windows rights management services for windows server 2003. White paper, Microsoft, 2003.

[3] New Tool Cracks Apple's Fairplay DRM. *Slashdot* (2004).
URL: http://apple.slashdot.org/comments.pl?sid=102992.

[4] Online music makes up for cd sales losses: survey. *Reuters.com* (2006-03-27). Online, last accessed: 2006-04-23.

[5] ARNAB, A., AND HUTCHISON, A. Fairer usage contracts for DRM. In *Proceedings of the fifth ACM Workshop on Digital Rights Management, Co-Located with ACM CCS 2005, Alexandria, Virginia, USA* (2005), R. Safavi-Naini and M. Yung, Eds., ACM, pp. 1 – 7.

[6] ARNAB, A., AND HUTCHISON, A. Requirement Analysis of Enterprise DRM Systems. In *Proceedings of Information Security South Africa (ISSA) Conference 2005, Johannesburg, South Africa* (2005).

[7] DUFFT, N., STIEHLER, A., VOGELEY, D., AND WICHMANN, T. Digital music usage and drm – results from an european consumer survey. Report, INDICARE Project, 2005.

[8] GROSS, T., AND PFITZMANN, B. Proving a WS-Federation passive requestor profile. In *Proceedings of the 2004 ACM Workshop on Secure Web Services (SWS), Co-Located with ACM CCS 2005, Fairfax, Virginia, USA* (2004), ACM.

[9] JAMKHEDKAR, P. A., AND HEILEMAN, G. L. DRM as a Layered System. In *Proceedings of the Fourth ACM Workshop on Digital Rights Management* (2004), A. Kiayias and M. Yung, Eds., ACM, pp. 11 – 21.

[10] KIM, B. J., HONG, S. J., AND KIM, J. Ticket-based fine-grained authorization service in the dynamic VO environment. In *Proceedings of the 2004 ACM Workshop on Secure Web Services (SWS), Co-Located with ACM CCS 2005, Fairfax, Virginia, USA* (2004), ACM.

[11] MICHIELS, S., VERSLYPE, K., JOOSEN, W., AND DECKER, B. D. Towards a software architecture for DRM. In *Proceedings of the fifth ACM Workshop on Digital Rights Management, Co-Located with ACM CCS 2005, Alexandria, Virginia, USA* (2005), R. Safavi-Naini and M. Yung, Eds., ACM, pp. 65 – 74.

[12] MULLIGAN, D., HAN, J., AND BURSTEIN, A. How DRM Based Content Delivery Systems Disrupt Expectations of "Personal Use". In *Proceedings of the 2003 ACM workshop on Digital Rights Management* (2003), ACM, pp. 77–89.
URL: http://doi.acm.org/10.1145/947380.947391.

[13] OPEN MOBILE ALLIANCE (OMA). Digital rights management. Approved Version 15 Jun 2004 – OMA-Download-DRM-V1_0-20040615-A, 2004.

[14] SCHNEIER, B. *Applied Cryptography*, second ed. John Wiley & Sons, 1996.

[15] STALLINGS, W. *Network Security Essentials – Applications and Standards*, international second ed. Prentice Hall, 2003.