DIGITAL RIGHTS MANAGEMENT AS A SERVICE
Developing Towards an Internet Service for Desktop and Mobile Users

Shih-Fang Chang
Industrial Technology Research Institute, 195 Sec. 4 Chung-Hsing Rd., Chutung, Hsinchu 310, Taiwan

Keywords: Digital Rights Management, Software as a service, Platform as a service, Web 2.0, Web Service.

Abstract: In November 2002 the Open Mobile Alliance starts to work out standard protection mechanism on digital content, so-called digital rights management (DRM). Then the OMA DRM 1.0 and 2.0 were approved in June 2004 and March 2006. Lots of industries and companies not only use the technology to protect their own media content, but also make sure the content should be revealed and retrieved in reasonable and secure manner. However, the cost and the availability for operating and integrating the technology would be very huge. Therefore, the proposed system is named DRMaaS that redesign the scenarios, those traditionally DRM technology has, with concept of Software as a Service (SaaS). In addition, we preserve the feasible feature to conjunct with other optional functionalities, like storage service and certification service. The proposed system is a work in progress towards an internet service for both desktop and mobile applications.

1 INTRODUCTION

For the past decade, the main technology used in digital content and copyright protection is DRM, the digital rights management. The DRM system aim at protecting ownership and copyright of electronic content by restricting what actions an authorized recipient may take with respect to that content. It is a most common research direction and application field when projecting the environment to be the versatile heterogeneous network.

The transmission requirement of DRM would perfectly fulfilled by the advantages of the network that for example, a client device with heterogeneous network accessibility can utilize wired broadband to carry heavy and encrypted multimedia data and retrieve authorization of the content via a more closed and secure cellular network. Recently, in addition to the already in place wired high speed xDSL and cable network infrastructure, the wireless network technologies also elevate themselves with a more competitive bandwidth, e.g. WiFi, WiMax, 3G, 3.5G. This grants more possibilities for newer DRM technical and service models.

In August 2003 Dhamija and Wallenberg had illustrated and evaluated the existing and potential DRM frameworks at that time. They pointed out several aspects to identify what a good DRM solution should have, and described that there are many tradeoffs to establish and operate such a complicated system. Besides, they have made conclusions that a successful technical solution would be in combination with models where the incentives to circumvent are limited, and the motives to cheat will depend on the price per copy of digital works and the restriction that are placed on usage. Therefore, a flexible and low-cost system with privacy and efficiency issues considered will be optimistic.

In 1999 Bennett brought he concept of “software as a service” (SaaS). SaaS could provide flexible environment which supports software solutions to grow easily and rapidly. Based on the concept of SaaS, an open platform of digital content and copyright protection service is described within this research.

The proposed system tends to develop a platform system considering the needs of content providers, service providers and end users, and architects the system as a service-oriented solution. It defines consistent interfaces for technical solutions and an integral services’ mechanism for different roles. The new approach would be more secure and effective than conventional client-server approaches, and bring more opportunities for independent solution providers and low-budget content service providers.

Chang S. (2009).
DIGITAL RIGHTS MANAGEMENT AS A SERVICE - Developing Towards an Internet Service for Desktop and Mobile Users.
In *Proceedings of the International Conference on Wireless Information Networks and Systems*, pages 176-179
DOI: 10.5220/0002230401760179

2 RELATED WORKS

We briefly review two related works, “Digital Rights Management (DRM)” and “Software as a Service (SaaS)”. Digital rights management is a technology used in digital content and copyright protection. Software as a service is a model of software deployment where an application is licensed for use as a service provided to customers on demand.

We employ DRM into the architecture of SaaS to expand the scenarios for fast and easy usage, and to increase interest to people. In the followings we will only describe the functions and architecture of these two works.

2.1 Digital Rights Management

Digital rights management (DRM) refers to access control technologies those are used by copyright holders, publishers, and hardware manufacturers to limit usage of digital media or devices. It enables the publisher to control what can and cannot be done with a single instance. For example, a publisher can limit the number of viewings, number of copies, or which devices the media can be transferred to. Digital rights management is widely being used by companies such as Sony, Apple Inc., Microsoft and the BBC.

The Open Mobile Alliance (OMA) pronounced the OMA DRM 1.0 which was started in November 2002 and approved in June 2004. It is basic DRM standard without strong protection. There are three main methods within the standard, Forward Lock, Combined Delivery (combined rights object and media object), and Separate Delivery (separated rights object with encrypted media object). Forward lock prevents the user from forwarding content such as ringtones and wallpapers on their phone.

Later, the OMA also pronounced the OMA DRM 2.0 which was started in July 2004 and approved in March 2006. It is the extension of the OMA DRM 1.0 separate delivery mechanism. Each participating device in OMA DRM 2.0 has an individual DRM PKI certificate with a public key, and the corresponding private key. Each Rights Object (RO) is individually protected for one receiving device by encrypting it with the device public key. The RO in turn contains the key that is used to decrypt the media object. Delivery of Rights Objects requires a registration with the Rights Issuer (RI, the entity distributing Rights Objects). During this registration, the device certificate is usually validated against a device blacklist by means of an “Online Certificate Status Protocol (OCSP)” verification. Thus, devices known to be hacked can be excluded once they try to register with an RI and receive new ROs for content access.

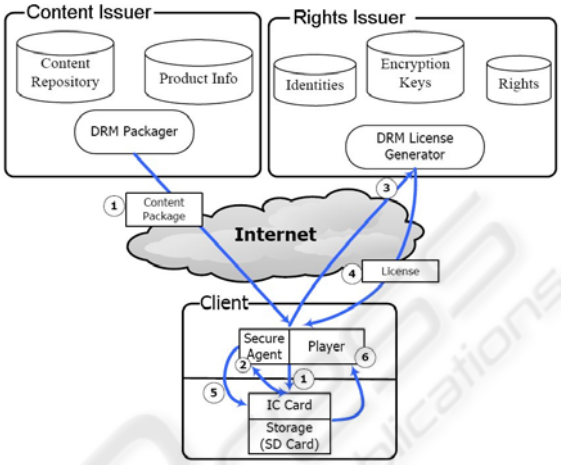

Figure 1: The structure of OMA DRM.

Since 2006, OMA has been working on DRM 2.0.1 and 2.1, and on new features such as SRM (Secure Removable Media) and SCE (Secure Content Exchange). It seems that DRM is the most common use for media protection; however, it’s extremely growing cost and preparation for system initial always let companies cowardly to invest and integrate. These drawbacks devalue DRM in practice, despite how remarkable it is.

2.2 Software as a Service

The concept of “software as a service” started to circulate prior to 1999 and was considered to be “gaining acceptance in the marketplace” in Bennett et al., 1999 paper on “Service Based Software”.

SaaS is generally associated with business software and is typically thought of as a low-cost way for businesses to obtain rights to use software as needed versus licensing all devices with all applications. It enables the benefits of commercially licensed use without the associated complexity and potential high initial cost of equipping every device with the applications that are only used when needed.

Using SaaS can also conceivably reduce the up-front expense of software purchases, through less costly, on-demand pricing from hosting service providers. The key characteristics of SaaS software include:

i. Network-based access to, and management of, commercially available software;

ii. Activities that are managed from central locations rather than at each customer's site, enabling customers to access applications remotely via the web;

iii. Application delivery that typically is closer to a one-to-many model than to a one-to-one model, including architecture, pricing, partnering, and management characteristics;

iv. Centralized feature updating, which obviates the need for downloadable patches and upgrades;

v. Often used in a larger network of communicating software, either as part of a mash-up or as a plug-in to a platform as a service. Service oriented architecture (SOA) is naturally more complex than traditional models of software deployment.

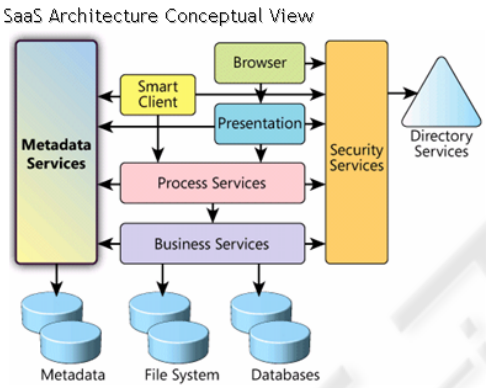

Figure 2: The architecture conceptual view of SaaS.

In the traditional world of software platforms, the cost of the first copy of the platform was enormous, often requiring companies to invest hundreds of millions before they could offer the platform to their very first customer. So, to lighten the heavy burden in using the software or services, the SaaS would be a fast and flexible model for general software developing.

3 THE PROPOSED SYSTEM

The proposed DRMaaS is based on the structure of OMA DRM technology, and extends the usage and behaviours with the philosophy of SaaS. It is implemented and presented as web native interface which allows content issuers, service providers, and end users may easily to follow their own scenario and achieve the flows and functionalities needed.

Like the typical digital rights management solutions, DRMaaS has the same main roles and scenarios. The content issuers generate the digital media content, while the service providers publishing the content which is authorized by content issuers. Thus, the end users purchase and download the protected content and suitable access rights, and then play or view it. Users of the platform may play as different main roles, content issuers, service providers, and end users, at the same time with the same interface.

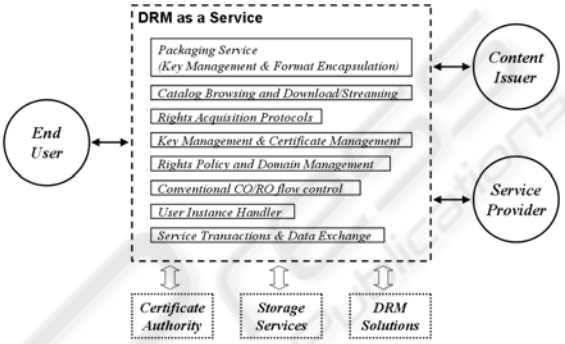

Figure 3: The architecture conceptual view of DRMaaS.

The content issuers may upload their own media content online, edit the related metadata, like ID3 tag, and then authorize it to service providers. The authorization means that content issuers allow specified or not specified service providers to deal with the content. The service providers may decide using which kind of DRM protection, adjust the parameters, like the number of viewings, number of copies, total time or expire date of viewings, etc, and publish the content at last.

Once the content was published, the content will be queued to encrypt with the settings gave by individual service provider. Then the end users may browse and find it in the content list through the web native interface. The content may with different offers that indicate service providers could use to provide kinds of programs for consumption. According to the information revealed by service providers, they can check it and to see if the content is what they want. When they decide to download one among the content listed, what they needed is only to have a single click. Thus both the content file and access rights document will be downloaded simultaneously to end users as long as the payment is made and confirmed. Finally, the end users use the DRM client, which is reachable and downloadable from DRMaaS, to view or play the content according to the access rights.

DRMaaS treats DRM solutions as part of configuration which can be easily substituted and

replaceable. It uses the application programming interface (API) which is based on http or https protocol with the "JavaScript Object Notation (JSON)" or the "Extensible Markup Language (XML)" format to communicate with service providers and achieve the goal. The service providers can choose for using which kind of DRM mechanism supported before publishing the content. Currently, we only support the standard of OMA DRM 1.0 and OMA DRM 2.0, while Windows Media DRM (WMDRM) is still underway.

Besides above, the DRMaaS still keep the flexibility and capability in conjunction with supporting services extensively, like storage service and certification service. It use the storage service to enforce the capability of storing digital media content, and use the certification service to verify the users' identity and certificate used to encrypt and decrypt the media content. The communication between DRMaaS and all other supporting services is also through individual APIs. Simply transmission with json or xml format data, both sides of DRMaaS and supporting services may capable to maintain the system states and exchange corresponding information.

4 CONCLUSIONS

The DRM technologies and solutions have been followed and practiced for years. However, the prevalence in many ways seems not to satisfy DRM solution providers. Most people know the important of the technology and have the will to experience it, but feel the gap between the technology and the reality. With the proposed system, DRMaaS, the significant benefit would be reducing the threshold to enjoying the world of digital rights management. People who want protect their content but less experienced in security or computer science, will be still easy to use the system without numerous parameters and troubling settings.

DRMaaS implements the most familiar scenarios among digital rights management solutions among content issuers, service providers, and end users. It basically doesn't break any behaviour that the traditional DRM technology has, but extends the possibility in growing of digital rights management solutions. However, we think DRMaaS is not suitable for all the services that DRM used for. To conjunct with DRMaaS, DRM solutions need to develop extra appropriate API to maintain the original behaviours. Thus, the close systems or the complicated solutions of DRM may result in a burden. Furthermore, the privacy and trust issues also perplex the model. Normally it will lead to be driven the service by government eventually.

There are some future works based on DRMaaS that require continuous efforts. Since the system is base on web technologies, the adjustment in appearance and embellishment on handset model is underway. We also study the improvement of the storage management, like connecting within the environment of cloud computing. By the mechanism of it, the proposed system may spread out rapidly, and reduce the response time obviously for operations. In the long run we will try to enhance DRMaaS with architecture of cloud computing.

REFERENCES

Bennett, K., Layzell, P., *Budgen*, D., Brereton, P., Macaulay, L., Munro, M., 1999. Service-Based Software: The Future for Flexible Software. Service Based Software.

Brereton, P., Budgen, D., Bennett, K., Munro, M., Layzell, P., Macaulay, L., Griffiths, D., Stannett, C., 1999. The Future of Software: Defining the Research Agenda. In *Comm. ACM, Vol.42, No.12, December 1999.*

Chong, F., Carraro, G., 2006. Architecture Strategies for Catching the Long Tail. *http://msdn.microsoft.com/en-us/library/aa479069.aspx*

Coyle, K., 2003. The Technology of Rights: Digital Rights Management. *http://www.kcoyle.net/drm_basics.pdf*

Dhamija, R., Wallenberg, F., 2003. A Framework for Evaluating Digital Rights Management Proposals. In *Proceedings of the First International Mobile IPR Workshop: Rights Management of Information Products on the Mobile Internet, August 2003.*

Ghosh, S., 2008. Essential decisions before choosing a good Platform-as-a-Service. *http://wolfpaas.blogspot.com/2008/10/essential-decisions-for-choosing-good.html*

Hoch, F., Kerr, M., Griffith, A., 2001. Strategic Backgrounder: Software as a Service. *http://www.siia.net/estore/ssb-01.pdf*

Ianella, R., 2001. Digital Rights Management (DRM) Architectures. In *D-Lib Magazine*, Vol. 7 (6).

Open Mobile Alliance Ltd., 2008. Architecture Document of OMA Digital Rights Management V2.0.2. *http://www.openmobilealliance.org/Technical/release_program/drm_v2_0.aspx*

Shah, D., 2007. force.com: The Perils of Platform As A Service. *http://onstartups.com/home/tabid/3339/bid/2421/force-com-The-Perils-of-Platform-As-A-Service.aspx*

Stefik, M., 1997. Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing. In *Berkeley Technology Law Journal*, Vol. 12 (1).