# Digital Rights Management Technology Using Profile Information and Use Authorization

*Masami Ueno*†, *Masakazu Kanbe, Toru Kobayashi, and Yoshitsugu Kondo*

**Abstract**

We describe a technique for satisfying both the copy control desired by content providers and the usability requirements of users. This technique works by controlling the use of content according to information about device ownership and relationships among users. It utilizes information about the service-providing equipment stored in an IC chip embedded in the equipment and user profile information stored in a smart card belonging to a user.

## 1. IC chips and the ubiquitous environment

Commuter train passes, credit cards, prepaid cards, and other such smart cards are becoming more common in our daily lives. In the future ubiquitous computing society, IC (integrated circuit) chips and IC tags will also be embedded in various machines that will exist all around us and provide convenient goods and services, in addition to the smart cards carried around by individuals. The IC chips embedded in machines will contain device profile information, and it will be possible to exchange machine and user profile information after mutual authentication by the user's smart card and the machine's IC chip. This profile information can be used to decide whether or not to provide a service to a user. It will also make it possible to vary the quality and type of service according to the user, facilitating personalized services. We use the term "use authorization" to cover the conditions for using services.

## 2. From ownership to use

These days, we get many services from machines or other devices that we own. For example, most people listen to music on their own audio player or stereo system and people who drive mostly use their own car. However, in the future, as more and more machines contain embedded IC chips, people will be able to obtain services at various different locations without owning the machines that provide them. We see this as a paradigm shift away from ownership toward the use of services (**Fig. 1**).

Assuming that these changes will apply to digital content such as music and video, we developed technology for managing content use rights based on profile information obtained from smart cards and from IC chips embedded in machines.

## 3. Problem analysis for content distribution

Currently, consumer-oriented content is mainly distributed via physical packaged media such as CDs (compact discs) and DVDs (digital versatile discs). However, the ease with which digital data can be copied has resulted in casual copying, such as the illegal creation of copies for friends and third parties, becoming a contagious problem. To counter this problem, content holders have recommended the introduction of CCCD (copy control CD) [1], which makes it difficult to rip the content of a CD using a personal computer. On the other hand, sales of content delivered over the network in unpackaged formats that employ digital rights management (DRM) [2] technology to prevent illegal copying are steadily increasing. However, CCCD technology and most

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
E-mail: ueno.masami@lab.ntt.co.jp

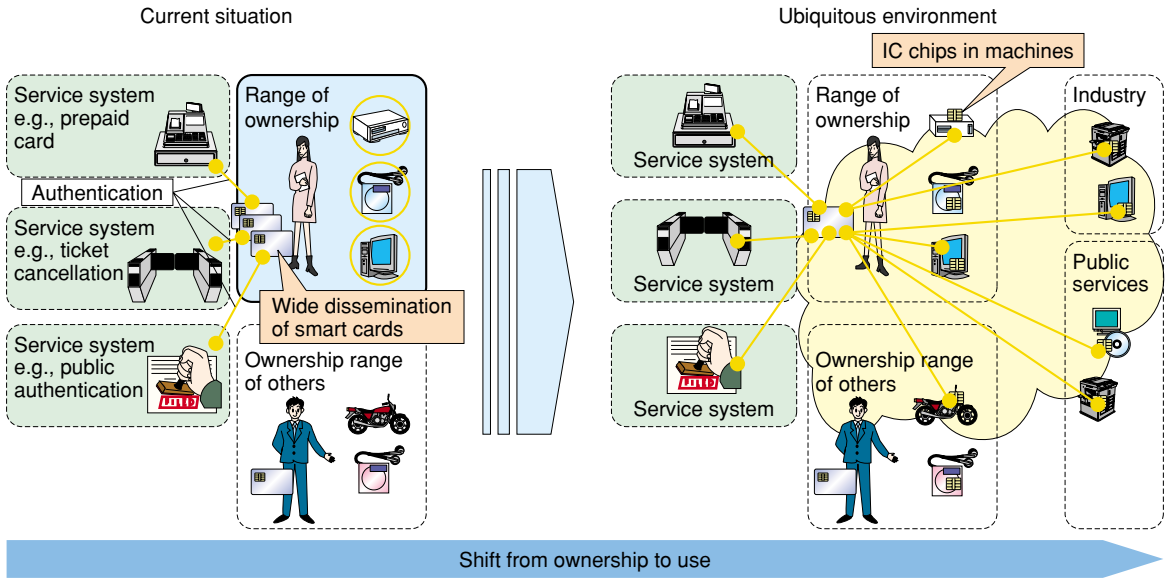


Fig. 1. Concept of the ubiquitous environment.

types of DRM technology are both more restrictive than conventional packaged media, so users have not warmly embraced them. This is one of the reasons that the sale of network-delivered content has not been successful in Japan. These restrictions limit:

1) Copying to other machines owned by the content purchaser besides the one whose ID was registered during the online purchase
2) Copying to machines other than those owned by the purchaser's family members
3) Making copies for personal use by the purchaser
4) Making copies for friends of the purchaser to be used on their equipment.

The fourth type of copying is prohibited by law, but it has been tolerated in the past because it has a promotional effect. Usage control by CCCD or DRM prevents copying, so it infringes on the scope of legal use. Permitting copying and allowing the use of copies on machines of the user and his/her family while preventing their use on a friend's machine or a third-party machine would be consistent with the scope of legal private use. This would result in usage control that is acceptable to both content holders and users. The current scope of usage control is compared with the ideal scope in **Table 1** and **Fig. 2**.

Table 1. Restrictions on use and control of usage rights.

| Target | User's registered machine | | | Other machines owned by the user | | | Family member's machine | | | Friend's machine | | | Other machine | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Use | Play | Copy | Transfer | Play | Copy | Transfer | Play | Copy | Transfer | Play | Copy | Transfer | Play | Copy | Transfer |
| Conventional packaged media (CD) | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● | ● | ● | ● | ● |
| CCCD | ○ | × | ○ | ○ | × | ○ | ○ | × | ○ | ○ | × | ○ | ○ | × | ○ |
| General DRM | ○ | △ | ○ | ○ | △ | ○ | ○ | △ | ○ | ○ | △ | ○ | ○ | △ | ○ |
| Ideal use control | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ▲ | ▲ | ▲ | ▲ | ▲ | ▲ |

Explanation of symbols
○ : Permitted for user
● : Available to the user, but not desired by the content holder
× : Not permitted to the user
△ : Use controlled by number of uses, number of machines, etc.
▲ : Can be controlled by the content holder
Range of use conventionally recognized as private use, but restricted by CCCD and DRM
Range of use that content holders most want to restrict

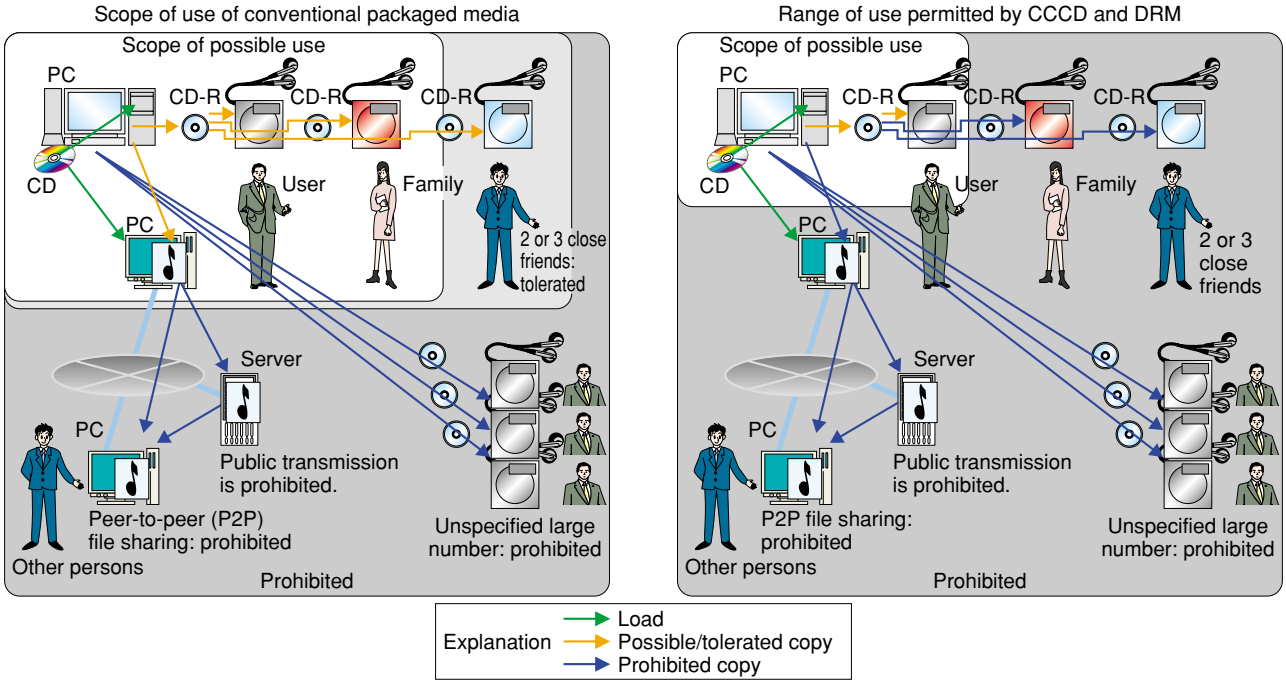


Fig. 2. Changes in the scope of use permitted by CCCD and DRM technology.

## 4. Usage control by smart cards and IC chips

Ideal usage control should:

1) Enable control that can prohibit content piracy (i.e., prevents the use of copies on the equipment of other persons)
2) Allow use in principle within the scope of private use
3) Enable content-holder-based control of restricted use on the equipment of friends, etc.

From these requirements, we conclude that the technically required functional elements to be provided by the smart card possessed by the user and the IC chip embedded in the machine can be summarized as follows. Functions are needed to implement user authentication, machine authentication, the ownership relationship between machine and user, the family relationship between users, and the friendship relationship between users. Storing this attribute information in either the smart card or IC chip (with a master copy stored on a server) allows the implementation of usage control. Furthermore, incorporating conventional DRM technology to implement usage control based on time, number of uses, number of copies, etc. is also desirable.

## 5. Implementation concept

The execution method is shown in **Fig. 3**. To implement a system that can provide the kind of control described above, we chose to use the signed user pro-

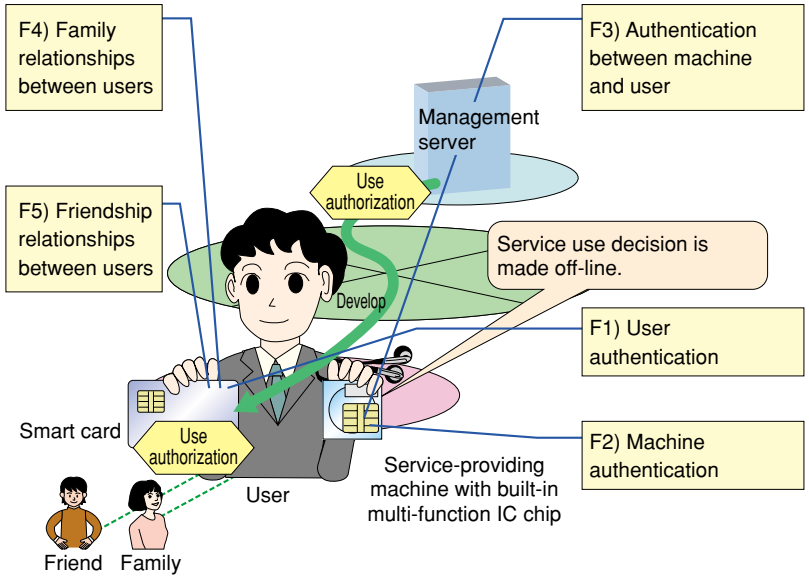


Fig. 3. Overview of the system.

file information stored in the smart card as the means of user authentication (F1). Similarly, signed machine profile information is stored in a multi-function IC chip installed in the machine that provides the service maintains the machine profile information, allowing machine authentication (F2). The ownership relationship between machine and user (F3), the family relationship between users (F4), and the friendship relationship between users (F5) are recorded in the server and the mutual ID information used for machine and user authentication is maintained as a list within the smart card or chip. In that way, the relationship information can be managed locally. Therefore, although the smart card and service-providing machine must be online when the relationship is registered, the more frequently performed service execution decision processing can subsequently be done off-line, thus improving convenience.

## 6. XACML policy description

To describe the use conditions, we chose XACML (extensible access control markup language) [3], a policy description language for controlling access to various resources that is being standardized by OASIS (Organization for the Advancement of Structured Information Standards). Because XACML takes into consideration universality as well as flexibility and expansibility in describing conditions, it allows conditions concerning various kinds of user operations on digital content and other objects to be described in a consistent format. If a digital signature is attached to use authorization descriptions written in XACML, then the signed descriptions can be managed as an object that represents use authorization.

## 7. Experimental system

We constructed an experimental system to evaluate this technology (**Fig. 4**). The system includes a use authorization management server that issues and revokes use authorization, an ownership management server that manages user and owned machine relationships, a use authorization platform that operates within the service-providing machine, a user profile application for managing use authorization and various kinds of user attribute information stored on smart cards and multi-function IC chips, and service applications that provide services to the user by using the other system components. The system design is premised on user, machine, and service-dependent information being different managed objects; they are managed by separate applications on the smart card and multi-function IC chip. The applications on the smart card and multi-function IC chip communicate with the machine providing the service and a server system that issues use authorization, etc. over public-key-based secure communication paths to prevent forgery of information. Because no product for mounting the multi-function IC chip exists yet, we ran simulations with two smart cards (one for machine authentication and one for user authentica-

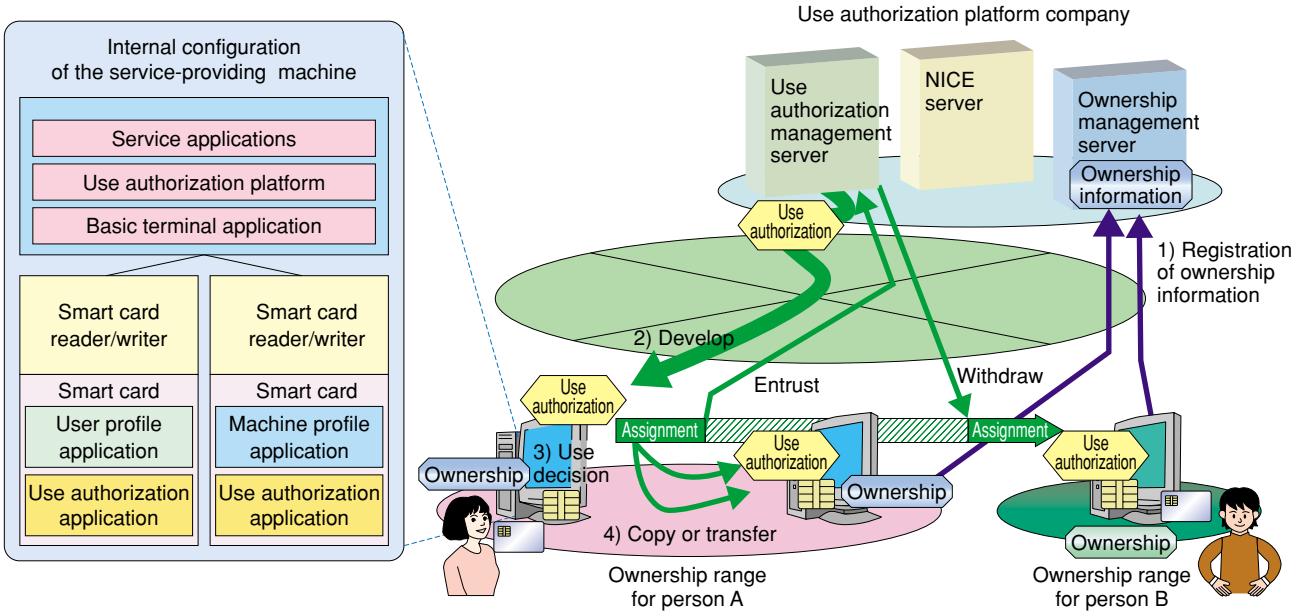


Fig. 4. Configuration of the experimental system.

tion) connected to a terminal (notebook personal computer) running the service application, which acted as the service-providing machine. To construct a trusted system, applications must be downloaded to the smart card safely. Therefore, we used NICE (network-based smart card environment), a smart card operation management platform developed by NTT [4], for downloading the respective management applications to the smart cards.

## 8. Evaluation results and future work

We used the experimental system to test the feasibility of control based on separate control policies for the use of digital content on the machine owned by the user, a family member's machine, a friend's machine, and a third-party machine. This technology also allows content to be used free of copying and playback restrictions for promotional purposes. It is also possible to limit use to machines owned by the user and his/her family. Use can even be further restricted to only the purchaser, in the same way as content provided under the current DRM. We found that the system had sufficient functionality, but the performance was inadequate. The prototype was implemented with an IC chip having low processing capability for public-key-encrypted communication, so there is a margin for improvement in terms of speed. In future work, we intend to develop this technology further and improve its speed.

## References


[1] Recording Industry Association of Japan, "Concerning Copy Control," http://www.riaj.or.jp/all_info/cccd/ (in Japanese).

[2] The Berkeley Center for Law and Technology and the Berkeley Technology Law Journal, "DRM Conference Resources," http://www.law.berkeley.edu/institutes/bclt/drm/resources.html

[3] XACML 1.0 Specification Set (Feb. 18, 2003): OASIS Standard as of Feb. 6, 2003, http://www.oasis-open.org/committees/xacml

[4] S. Yamamoto, R. Toji, S. Hirata, and E. Niwano, "IC card information distribution platform: NICE," NTT Technical Journal, Vol. 13, No. 12, pp. 14-18, 2001 (in Japanese).



**Masami Ueno**
Senior Research Engineer, Ubiquitous Computing Project, NTT Information Sharing Platform Laboratories.
He received the B.E. and M.E. degrees in computer science from Yamanashi University, Kofu, Yamanashi in 1991 and 1993, respectively. In 1993, he joined the Software Laboratories, NTT, Tokyo, Japan. He has been engaged in requirement engineering and development of a billing platform and digital rights management system. Since March 2003, he has been engaged in R&D of a ubiquitous computing network architecture. He is a member of the Information Processing Society of Japan (IPSJ).



**Masakazu Kanbe**
Ubiquitous Computing Project, NTT Information Sharing Platform Laboratories.
He received the B.A. and M.A. in cognitive psychology from Waseda University, Tokyo in 1994 and 1997, respectively. He joined NTT in 1997. He has been engaged in the development of computer-supported collaborative learning, knowledge management systems, and smart card platform systems. His research interests include man-machine interaction and a human-centered service architecture. He is currently engaged in research on a ubiquitous computing architecture. He is a member of the Association for Computing Machinery, the Institute of Electronics, Information and Communication Engineers (IEICE), and IPSJ.



**Toru Kobayashi**
Senior Research Engineer, Supervisor, Ubiquitous Computing Project, NTT Information Sharing Platform Laboratories.
He received the B.E. and M.E. degrees in mechanical engineering from Tohoku University, Sendai, Miyagi in 1985 and 1987, respectively. In 1987, he joined the Software Laboratories. Almost all of his experience is in R&D of software development environments including groupware tools and software development management. Since August 2003, he has been engaged in R&D of a ubiquitous computing network architecture. He is a member of IEICE and the Japan Society of Information and Systems.



**Yoshitsugu Kondo**
Senior Research Engineer, Supervisor, Group Leader, Ubiquitous Computing Project, NTT Information Sharing Platform Laboratories.
He received the B.E. and Ph.D. degrees in computer science from Yamanashi University, Kofu, Yamanashi in 1983 and 1996, respectively. In 1983, he joined Nippon Telegraph and Telephone Public Corporation (now NTT), Tokyo, Japan. He has been engaged in the development of intelligent network systems, distributed computing systems, and specification description languages. Since 2003, he has been engaged in R&D of a ubiquitous computing network architecture. He is a member of IEICE Processing Society and IEEE.