Standardization of OMA DRM —Technologies for Handling Digital Content Distribution and Copyright Management—

OMA, a standardization organization dealing with mobile application technologies, has defined the OMA DRM specification for handling copyright management of digital content. OMA DRM can prevent illegal copy of digital content and also allows defining restrictions concerning usage of content (e.g., number of usages and expiration date) via mobile terminals. OMA DRM has various functions requested by content providers; it also has the super-distribution function for promoting content distributions that separate content and rights information. The OMA DRM version 2.0 specification was completed in July 2004, and it is now expected that a new form of providing content using this technology will be diffused.

Hidetoshi Ueno Masaomi Sumita Norihiro Ishikawa

1. Introduction

Unlike tangible goods such as industrial products and food products, digital content distinguish themselves by the fact that it is very easy to duplicate products of the same quality. The copyright law prohibits duplication of content without the permission of the creators can be obtained, but in reality, there are many cases where content are duplicated and used illegally. Properly protecting the copyright of content is extremely important for content creators and it's demand is strong as well. Considering these facts, the concept of Digital Rights Management (DRM), i.e., digital content copyright management technologies, has been attracting attention recently. At first, the focus of attention was on DRM technologies applied to music CDs, DVD movies, digital broadcast and similar media, but application of the DRM technology to mobile terminals is coming into the spotlight lately as well, as content provided to mobile terminals are becoming diversified and increasingly expensive.

From the background above, the Open Mobile Alliance (OMA), a standardization organization dealing with mobile application technologies, standardized the OMA DRM specification for mobile terminals. OMA DRM is intended to protect any content delivered to mobile terminals; it can prevent illegal copy of digital content and allows defining restrictions related to content usage (e.g., number of usages and expiration date). Moreover, OMA DRM has various functions requested by content providers; it also has the super-distribution function for promoting content distributions that separate content and right information.

There are two versions of OMA DRM: the simple OMA DRM version 1.0 (DRMv1.0), which is mainly targeted at inexpensive content, and the more sophisticated OMA DRM version 2.0 (DRMv2.0), which is mainly targeted at expensive content.

This article describes the standardization of OMA DRM and provides a technical overview of each version.

2. OMA DRM Version 1.0

OMA DRMv1.0, which is the first standardized DRM technology for mobile terminals, is targeted mainly at relatively inexpensive content such as wallpapers, ringtones and Java[*1] programs (from about tens to several hundreds of yen). OMA DRMv1.0 prescribes three DRM types, "Forward Lock," "Combined Delivery" and "Separate Delivery" (**Figure 1**), allowing each content provider to

[*1] Java is an object-oriented development environment for networks promoted by Sun Microsystems, USA.

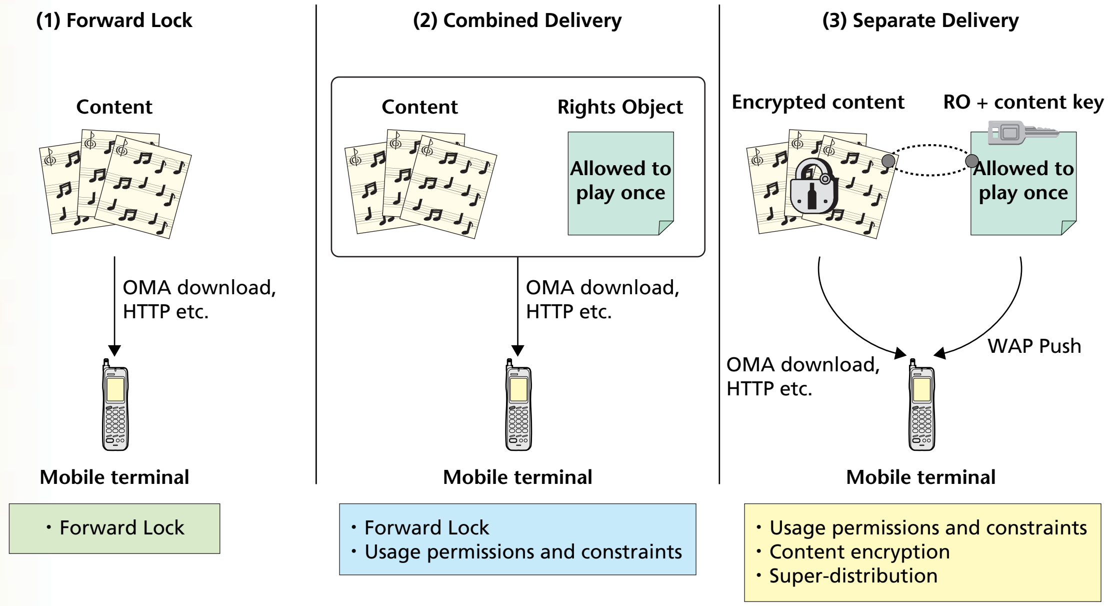
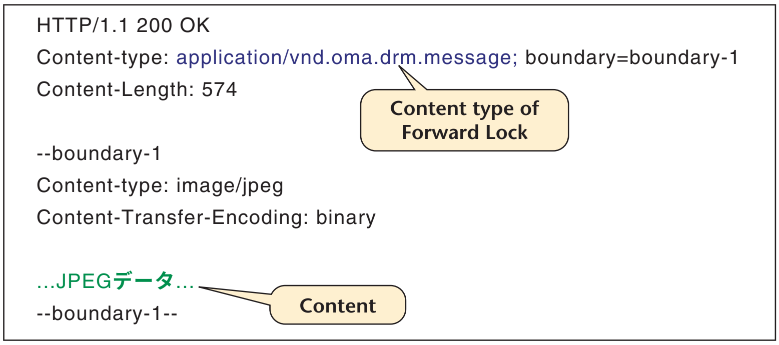


Figure 1 Delivery types of DRMv1.0

select and use the most suitable type for the given application.

2.1 Forward Lock

Forward Lock allows prohibiting forwarding content downloaded to a mobile terminal to external receivers (Fig. 1 (1)). Forward Lock has a mechanism that adds a special content type that prohibits forwarding of downloaded content. **Figure 2** shows a message example when it is instructed to prohibit forwarding a JPEG file downloaded via HTTP. A mobile terminal receiving this message prohibits forwarding the content to any external receivers; for instance, this JPEG file cannot be sent in an email to the user’s friends. Note that content can be downloaded by using OMA download [1], ensuring efficient download to the mobile terminals other than simply by using HTTP.



```
HTTP/1.1 200 OK
Content-type: application/vnd.oma.drm.message; boundary=boundary-1
Content-Length: 574

--boundary-1
Content-type: image/jpeg
Content-Transfer-Encoding: binary

...JPEGデータ...
--boundary-1--
```

Content type of Forward Lock
Content

Figure 2 Forward Lock

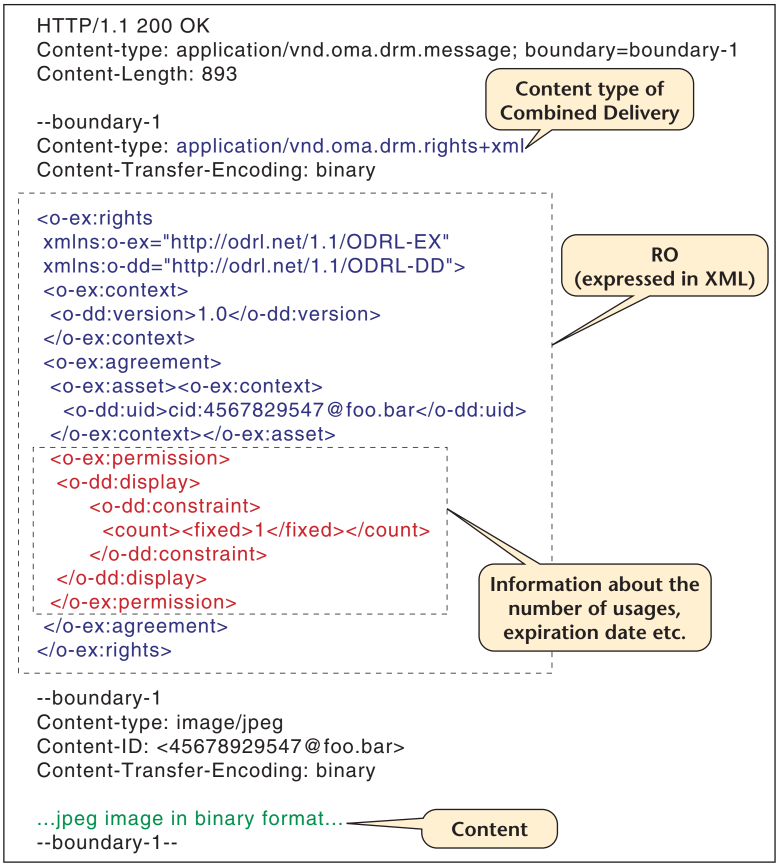
2.2 Combined Delivery

Combined Delivery can handle usage restrictions on content (e.g., number of usages and expiration date) in addition to the Forward Lock (Fig. 1 (2)). The information related to usage restriction of content is collected in a data structure called a Rights Object (RO) and expressed using eXtensible Markup Language (XML). OMA DRM describes ROs using Open Digital Rights Language (ODRL). ODRL is an extensible Rights Expression Language (REL), which allows describing usage permission and constraints of any kinds of content, agreements between rights holders and users etc. [2]. **Figure 3** shows an example of a Combined Delivery message where a RO restricts the number of times an image can be displayed. The mobile terminal receiving this message is not allowed to forward the content, but is allowed to display the content on the screen only once. Details of various permissions and restrictions that can be defined by REL are explained later in the chapter explaining OMA DRMv2.0.

2.3 Separate Delivery

Separate Delivery realizes super-distribution by separating and delivering content and ROs independently of each other (Fig. 1 (3)). Super-distribution is a system where the user pays for certain ROs in exchange for allowing free duplication and re-distribution of content. In this mechanism, the content is encrypted and cannot be used unless the user obtains the appropriate content key included in the corresponding RO. Through super-distribution, it is possible to implement new services; for instance, users can forward encrypted content to friends via email, and the friends may then purchase the RO separately. As shown in **Figure 4**, encrypted content are converted to binary format according to the DRM Content Format (DCF). The DCF-encoded content contain the URL of the Rights Issuer (RI) that maintains the RO, and the mobile terminal requests delivery of the RO including the content key by accessing the URL of the RI. In OMA DRMv1.0, ROs and content keys are delivered without being encrypted; simple countermeasures against tapping are taken by using Wireless Application Protocol (WAP)[*2] Push [3] over the Short Message Service (SMS).

The OMA DRMv1.0 Candidate release[*3] was completed in November 2002, followed by announcement of mobile terminal and server products by many manufacturers. In addition, OMA completed interoperability tests and the Approved release specification was completed in June 2004 [3]. In the future, content delivery services based on the OMA DRMv1.0 specification are expected to come into widespread use.



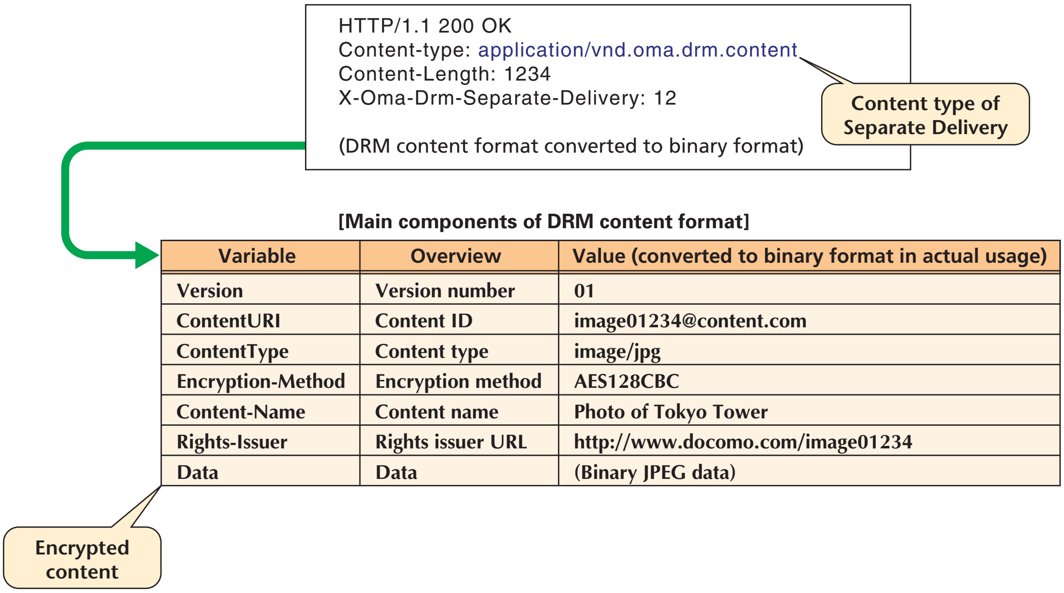
```
HTTP/1.1 200 OK
Content-type: application/vnd.oma.drm.message; boundary=boundary-1
Content-Length: 893

--boundary-1
Content-type: application/vnd.oma.drm.rights+xml
Content-Transfer-Encoding: binary

<o-ex:rights
 xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
 xmlns:o-dd="http://odrl.net/1.1/ODRL-DD">
 <o-ex:context>
  <o-dd:version>1.0</o-dd:version>
 </o-ex:context>
 <o-ex:agreement>
  <o-ex:asset><o-ex:context>
    <o-dd:uid>cid:4567829547@foo.bar</o-dd:uid>
  </o-ex:context></o-ex:asset>
  <o-ex:permission>
   <o-dd:display>
        <o-dd:constraint>
          <count><fixed>1</fixed></count>
        </o-dd:constraint>
   </o-dd:display>
  </o-ex:permission>
 </o-ex:agreement>
</o-ex:rights>

--boundary-1
Content-type: image/jpeg
Content-ID: <45678929547@foo.bar>
Content-Transfer-Encoding: binary

...jpeg image in binary format...
--boundary-1--
```

Content type of Combined Delivery
RO (expressed in XML)
Information about the number of usages, expiration date etc.
Content

Figure 3 Combined delivery (rights object)

[*2] The WAP Forum, which formulated the WAP standard specification, was integrated with various other organizations such as Wireless Village, SyncML Initiative, LIF etc. in June 2002, and OMA was inaugurated. The WAP specification can be referenced from OMA's open Web site (http://www.openmobilealliance.org).

[*3] The OMA specification release schedule for individual application constituent technologies (enablers) is divided into three phases: the Candidate release, a level where prototypes can be implemented, the Approved release, which reflects the results of mutual connection tests to the Candidate version, and the Interoperable release, for which end-to-end mutual connection tests have been completed for multiple enablers.



```
HTTP/1.1 200 OK
Content-type: application/vnd.oma.drm.content
Content-Length: 1234
X-Oma-Drm-Separate-Delivery: 12

(DRM content format converted to binary format)
```

[Main components of DRM content format]

Variable	Overview	Value (converted to binary format in actual usage)
Version	Version number	01
ContentURI	Content ID	image01234@content.com
ContentType	Content type	image/jpg
Encryption-Method	Encryption method	AES128CBC
Content-Name	Content name	Photo of Tokyo Tower
Rights-Issuer	Rights issuer URL	http://www.docomo.com/image01234
Data	Data	(Binary JPEG data)

Figure 4 Separate delivery message (encrypted content format)

3. OMA DRM Version 2.0

OMA DRMv1.0 was mainly designed to handle delivery of inexpensive content, so its security functions were not sufficient for more serious use; for example, ROs and content keys were transmitted as plain text. After the OMA DRMv1.0 specification was completed, services that delivers relatively expensive content such as music, images, games etc. to mobile terminals started to be provided, and there was a need for a DRM system designed to handle such content efficiently. Moreover, it became necessary to be able to handle new usage cases such as support for other terminals than mobile terminals (e.g., PCs and music players) as well as coordination with DRM systems other than OMA DRM. To deal with these issues, development of the OMA DRMv2.0 specification, which expands the features of OMA DRMv1.0, was started and the OMA DRMv2.0 Candidate release was completed in July 2004 [5].

In OMA DRMv2.0, advanced security functions based on the Public Key Infrastructure (PKI) were implemented in order to prevent problems such as tapping and spoofing, and the following upgraded function were implemented.

1) Enhancement of Information Related to Content Usage Permissions and Constraints

The information related to content usage permissions and constraints described in the ROs was upgraded.

2) Domain Functions

Several functions are now provided so that, for instance, music content can be shared between mobile terminals and other terminals such as PCs, enabling the users to share content among multiple terminals within the limits of personal usage.

3) Support for Non-connection Terminals

As part of the domain-related functions, use of content is now allowed in unconnected devices (e.g., music players), which do not have functions to communicate directly with a server.

4) Preview Functions

Preview functions were implemented to allow content usage for a certain period of time without billing, for example, to allow listening to parts of music content before buying.

5) Support for Streaming Delivery

Content that are delivered by streaming, such as live sports broadcasts delivery, are now supported. The supported delivery formats include not only unicast but also streaming delivery via multicast/broadcast.

6) Export to Other DRM Systems

A mechanism for exporting content and ROs from OMA DRM to other DRM systems is now provided; this means that, for instance, music content acquired by OMA DRM can be used in devices supporting a DRM system other than OMA DRM (e.g., music players conforming to Content Protection for Recordable Media (CPRM)[*4]).

OMA established a official liaison relationship with various organizations deeply involved with the regulation of music delivery, such as the Recording Industry Association of America (RIAA), as well as the 3rd Generation Partnership Project (3GPP) in order to upgrade the functions above, making effort to support wider range of usage cases by exchanging opinions with these organizations during the requirement formulation phase. Since OMA DRMv2.0 is designed for the purpose of upgrading several functions listed above, interconnection with OMA DRMv1.0 is not possible.

3.1 OMA DRMv2.0 Architecture

In OMA DRMv2.0, the functions of content providers are logically divided into two types according to their nature: Content Issuers (CI) which maintain content, and Rights Issuers (RI) which manage ROs related to content (**Figure 5**). It is possible to operate the CI and RI on the same device.

3.2 Procedure for Obtaining Content According to OMA DRMv2.0

In OMA DRMv2.0, content and ROs are separated as in Separate Delivery of OMA DRMv1.0, so that a configuration allowing super-distribution of content can be achieved. The following explains the details of basic download and super-distribution, which are the basic procedures in acquiring content according to the OMA DRMv2.0 specification.

1) Basic Download

In the basic download procedure, encrypted content

[*4] Copyright protection technology used in the DVD standard.

and ROs are acquired directly from a content provider. For instance, the case where a user makes a payment (acquisition of RO) immediately after downloading music content and uses the content is an example of basic download. The mobile terminal first acquires the encrypted content according to the DCF for OMA DRMv2.0 using the OMA download etc. (Fig. 5 (1)). At this point, if the CI and RI are implemented in separate devices, a separate procedure for sharing the content key between them will be necessary (Fig. 5 (2)). Next, the mobile terminal acquires the RO (including the content key) from the RI in order to start using the content (Fig. 5 (3)). OMA DRMv2.0 prescribes the RO Acquisition Protocol (ROAP) for acquiring the RO; encryption as a countermeasure against tapping of ROs and mutual authentication between the mobile terminal and RI as a countermeasure against spoofing.

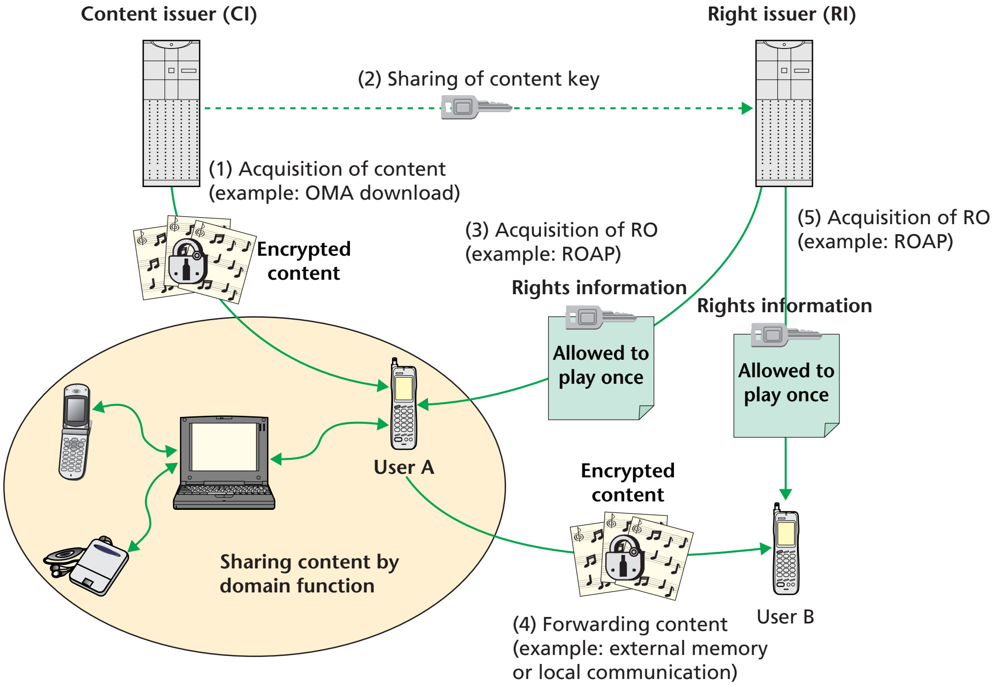


Figure 5 Architecture of OMA DRMv2.0

2) Super-Distribution

Content are encrypted based on the DCF, and can thus duplicate and forward it freely. For example, a case where a user forwards his favorite music content to a friend using external storage and local communication (e.g., Bluetooth[*5]) can be considered (Fig. 5 (4)). If the friend wants to listen to the music content later, s/he can acquire the RO from the Rights Issuer and pay the necessary fee (Fig. 5 (5)). ROAP is used for acquisition of ROs in super-distribution as well, in the same way as for the basic download.

In OMA DRMv2.0, both the basic download and super-distribution can be combined with the preview functions. Users can preview content by acquiring ROs for preview before acquiring normal ROs.

3.3 Sharing Content using the Domain Function

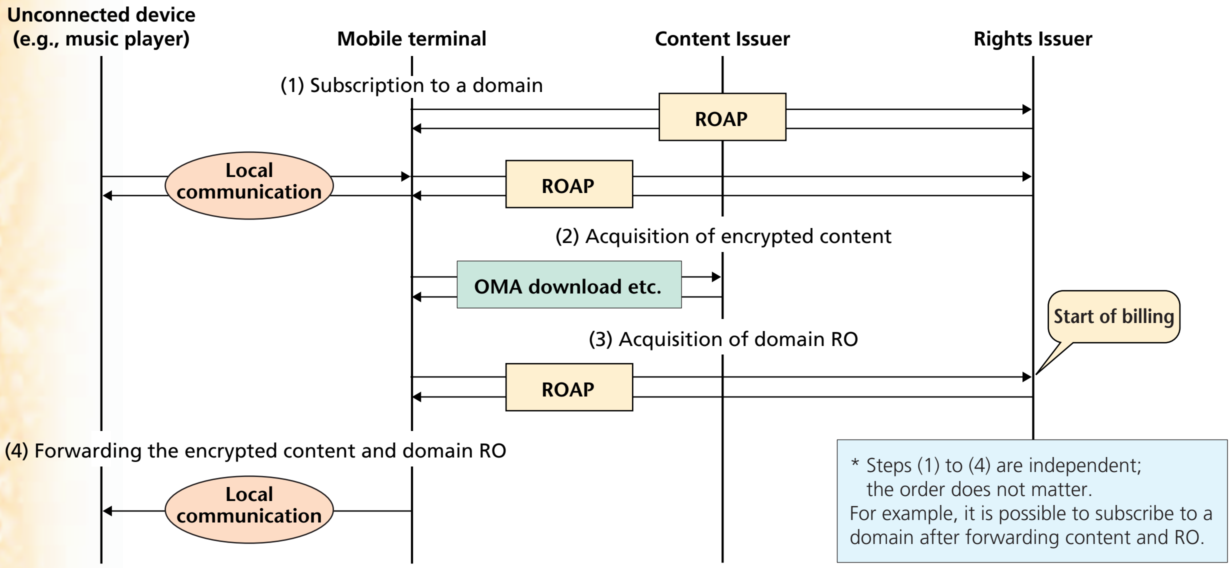
The domain function is one of the features of OMA DRMv2.0 that allows the sharing of content among mobile terminals and other terminals such as PCs within the limits of personal usage. The RI maintains domain ROs to be shared within a domain and manages mobile terminals subscribing to the domain. Issuance of ROs for the domain and exchange of messages involved in subscribing to and unsubscribing from the domain are performed using ROAP.

Figure 6 shows an example of using the procedure for sharing content within a domain. In this example, a mobile terminal and an unconnected device (e.g., a music player) without functions to communicate directly with a server share a content within the same domain. Each terminal acquires necessary information such as the domain key to be shared within the domain via the domain subscription procedure (Fig. 6 (1)). The unconnected device uses local communication such as a cable or Bluetooth to access the RI via the mobile terminal with a function to communicate with the server. After that, the mobile terminal acquires the content (Fig. 6 (2)) and domain RO (Fig. 6 (3)) and forwards them to the unconnected device, and share the content (Fig. 6 (4)). If the mobile terminal sharing content is equipped with a function to communicate with a server, it can access the RI directly and acquire various types of data.

3.4 ROAP

ROAP is a protocol used between mobile terminals and RIs

[*5] Bluetooth: Registered trademark of Bluetooth SIG, Inc. in the USA.


Unconnected device (e.g., music player)
Mobile terminal
Content Issuer
Rights Issuer
(1) Subscription to a domain
ROAP
Local communication
ROAP
(2) Acquisition of encrypted content
OMA download etc.
Start of billing
(3) Acquisition of domain RO
ROAP
(4) Forwarding the encrypted content and domain RO
Local communication

* Steps (1) to (4) are independent; the order does not matter. For example, it is possible to subscribe to a domain after forwarding content and RO.

Figure 6 Procedure for sharing content within a domain

that provides various functions related to security, including transmission of ROs, PKI based mutual authentication between the mobile terminal and RI, data confidentiality, time synchronization and revocation management of digital certification. ROAP is described in XML; XML Encryption is used for data confidentiality and the XML Signature is used for mutual authentication. Various proven algorithms are used for data confidentiality and authentication, such as RSA and Secure Hash Algorithm 1 (SHA-1).

3.5 Rights Object (RO)

ROs of DRMv2.0 are expressed using ODRL in the same way as for DRMv1.0, as shown in Fig. 3. ROs include usage permissions and constraint of content (**Table 1**). The usage permission information specifies how particular content can be used, such as playing, displaying, executing or printing. Information about usage constraint specifies the number of times particular content can be used and the expiration date of the content. Moreover, if the export function is used, ROs are used to specify restriction for other DRM systems at the exporting destination.

3.6 DRM Content Format (DCF)

OMA DRMv2.0 prescribes the following two types of content formats in order to handle encrypted file- and streaming-type content.

DCF is converted to binary format in the same say as for DRMv1.0 as shown in Fig. 4. In OMA DRMv2.0, however, the format has been changed based on the ISO Base Media File Format [6] and more information elements are added (**Table 2**). The DCF data includes the URL of the RI (RightsIssuerURL), allowing a mobile terminal to acquire a RO by accessing this URL.

The Packetized DCF (PDCF) is used for streaming content and continuous content such as movies played over an extended period of time. PDCF adopts the Packet-switched Streaming Service (PSS) format [7] prescribed by 3GPP, and is configured to include information corresponding to the DRM common area in Table 2.

3.7 OMA DRMv2.0 Related Trends

The OMA DRMv2.0 Candidate release was completed in July 2004 [5], and it has already been put into practical use as several manufacturers announced commercialization etc. OMA DRMv2.0 handles many use cases, and it is capable of providing sophisticated security functions including use of PKI. On the other hand, it requires advanced technologies for the operation on the RI side, which hinders diffusion. This is a real and significant issue for small-scale content providers, and it requires use of operation agents for RI. Moreover, implementation of mobile terminals and server devices is complex and may cause compatibility issues in connections involving products from different vendors. For these reasons, several of the companies that promoted the standardization of OMA

DRMv2.0 established the Content Management License Administrator (CMLA). CMLA is an organization dedicated to deal with licensing related to OMA DRMv2.0 and authorizing products and content providers, as well as promoting of diffusion of OMA DRMv2.0 by dealing with the practical aspects not covered by the specification.

4. OMA Download

This chapter explains the OMA download, which can be used to download content to mobile terminals. The OMA download procedure was standardized at the same time as OMA DRMv1.0 and designed to be used for downloading of any kinds of content by referencing the Mobile Information Device Profile for the J2ME Platform (Java MIDP) [8] [1].

Figure 7 shows the communication procedure used in the OMA download. A mobile terminal, upon finding a content via browsing etc. (Fig. 7 (1)), obtains a Download Descriptor (DD), which contains meta information about the content (Fig. 7 (2)). The DD contains information about the content size (size), content type (type) and content URL (objectURI) etc., allowing the user to judge whether or not to actually download the content based on the information (**Figure 8**). If the user decides to download the content based on the information in the DD, the actual downloading of the content is then performed (Fig. 7 (3)). Next, the mobile terminal sends an installation notification (Install-Notify) to the server in order to notify that installation is completed (e.g., when the content are passed to an appropriate application) (Fig. 7 (4)). In other words, the OMA download adds various functions to the simple download method specified by HTTP and makes it possible to provide an efficient download method for mobile terminals, among other things by allowing obtaining meta information before actually downloading content.

Table 1 Information element defined by REL

			DRMv1	DRMv2
Permission: Permission of how content can be used				
play		Play (audio/midi, video/quicktime etc.)	○	○
display		Display (image/jpg etc.)	○	○
execute		Execution (java games etc.)	○	○
print		Printing hard copy (image/jpg, text/plain etc.)	○	○
export		Export to other DRM systems	–	○
Constraint: Constraint of consumption of content				
count		Number of times	○	○
count-dial		Specification of the number of seconds counted as one time (e.g., it is counted as one time when the content is used for 30 seconds)	–	○
datatime		Date and time	○	○
	start	Start time	○	○
	stop	End time	○	○
interval		Effective period from start of usage	○	○
accumulated		Absolute effective period (e.g., one week from obtaining content)	–	○
individual		Specification of certain mobile terminals that can use the content	–	○
system		Specification of DRM systems of export destination	–	○

5. Conclusion

OMA DRM not only specifies functions for copyright management of content that are important for content creators, but it also realizes vari-

Table 2 Example of information elements in DCF

Area	Variable	Description	Example of value
Discrete Media Header box	ContentType	Content type	image/jpg
Common headers box	EncryptionMethod	Encryption method	0x0001 (AES_128_CBC)
Common headers box	ContentID	Content ID	w08087sdf80@ri.docomo.com
Common headers box	RightsIssuerURL	URL of RI	http://ri.docomo.com/
Common headers box	Silent Header	Whether or not to acquire ROs without inquiring the user about permission	on-demand
Common headers box	Preview Header	URL of RO for preview	http://ri.docomo.com/pre/a1.html
Common headers box	ContentURL	URL of content	http://ci.docomo.com/pic/mtfuji.jpg
Free space box	Rights Object	Area used when including RO in DCF (used when sharing data within a domain etc.)	(RO converted to binary format)
User data box	Title	Content title	A hundred sceneries of Japan
User data box	Description	Explanation of content	Photo of Mt. Fuji

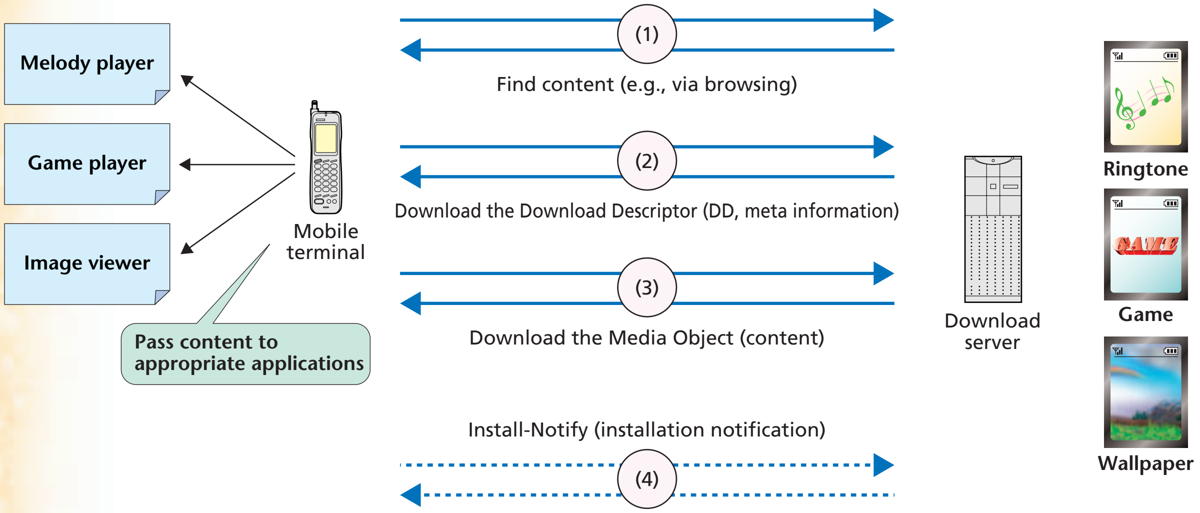
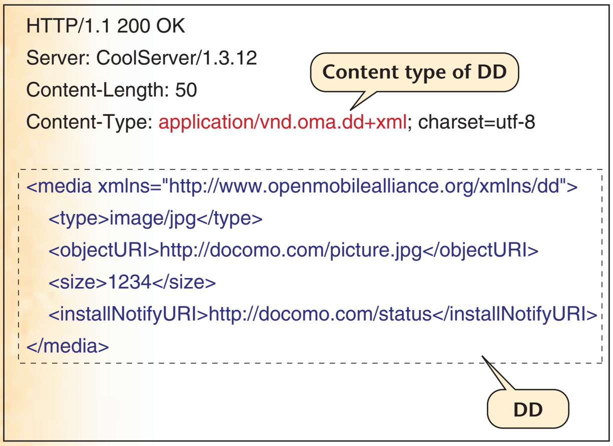

Melody player
Game player
Image viewer
Mobile terminal
Pass content to appropriate applications
(1)
Find content (e.g., via browsing)
(2)
Download the Download Descriptor (DD, meta information)
(3)
Download the Media Object (content)
Install-Notify (installation notification)
(4)
Download server
Ringtone
GAME
Game
Wallpaper

Figure 7 Communication procedure of OMA download



```
HTTP/1.1 200 OK
Server: CoolServer/1.3.12
Content-Length: 50
Content-Type: application/vnd.oma.dd+xml; charset=utf-8

<media xmlns="http://www.openmobilealliance.org/xmlns/dd">
   <type>image/jpg</type>
   <objectURI>http://docomo.com/picture.jpg</objectURI>
   <size>1234</size>
   <installNotifyURI>http://docomo.com/status</installNotifyURI>
</media>
```

Content type of DD
DD

Figure 8 DD (download descriptor) acquisition

ous usage cases including domain function, preview function and streaming delivery. The super-distribution function of OMA DRM, in particular, allows distribution of content without going through mobile communication networks and has the effects of reducing waiting time and cost for users in downloading large-volume content. Moreover, for network operators, it has been proven effective as a way of reducing the amount of communication in mobile communication networks. Content providers can also expect increased profits as content are provided effectively by the use of the super-distribution function. The basic concept of super-distribution has not come into widespread use yet, although it was proposed as long ago as in 1983 [9]; it is worth paying attention to, however, as it is a technology that is likely to undergo a major breakthrough in terms of usage in the future considering the current conditions where various environments, including network infrastructure, mobile terminals, content and users, are being upgraded.

References

[1] Open Mobile Alliance: "OMA Download Enabler Release," Approved Version 1.0, OMA-DL-V1_0-20040625-A, www.openmobilealliance.org. Jun.2004.

[2] The Open Digital Rights Language Initiative: "Open Digital Rights Language (ODRL)," Version1.1, Aug. 2004.

[3] WAP Forum: "WAP Push Architectural Overview," WAP-250-PushArchOverview-20010703-a, www.openmobilealliance.org. Jul.2001.

[4] Open Mobile Alliance: "OMA Digital Rights Management Enabler Release," Approved Version 1.0, OMA-DRM-V1_0-20040615-A, www.openmobilealliance.org. Jun. 2004.

[5] Open Mobile Alliance: "OMA Digital Rights Management Enabler Release," Candidate Version 2.0, OMA-DRM-V2_0-20040715-C, www.openmobilealliance.org. Jun. 2004.

[6] International Organization for Standardization: "Information technology-Coding of audio-visual objects-Part 12: ISO Base Media File Format," ISO/IEC 14496-12, 2003.

[7] The Third Generation Partnership Project: "Transparent end-to-end Packet-switched Streaming Service (PSS); File Format," 3GPP TS 26.244, Sep. 2004.

[8] Java Community Process: "Mobile Information Device Profile (MIDP)," JSR-118, Nov. 2002.

[9] Ryouichi Mori: "The Software Service," Journal of JECC, No.3, pp.16–26, 1983 (in Japanese).