Willms Buhse and
Jan van der Meer

The Open Mobile Alliance Digital Rights Management

The Open Mobile Alliance (OMA) is an industry forum with nearly 400 members representing the entire mobile industry value chain, including the telecommunications, information technology, and content industries. The OMA focuses on developing market-driven, interoperable mobile service enablers for the rapidly converging communications, entertainment, and media worlds. OMA digital rights management (DRM) systems are important examples of such enablers. Although they have been developed for the mobile market, these systems assume network and bearer-agnostic delivery of the content over Internet protocol (IP). This assumption makes OMA DRM systems suitable for use in any environment where the content is delivered over IP, which is true of a very wide array of applications. In this article, we overview the OMA DRM systems, position them in the larger context of DRM work, and describe their most important features.

BACKGROUND

MOTIVATION

The mobile content market is expected to reach US$30 billion worldwide by 2008, with about 1 billion devices being released to the market every year. To keep up with this growth, new content delivery business models are evolving at fast rates. The success and profitability of these models depend upon the ability of the content and service providers to ensure a "trusted environment," with a secure end-to-end trust model and billing mechanism that prevents piracy and secures the rights to consume and distribute content. The basis for a secure distribution of digital content is a DRM system. The need for interoperability and, hence, for a standardized DRM system, has led to sustained work within the OMA, while outside the OMA some DRM standardization work was also conducted. Content services do not benefit from market fragmentation and require a strong, open DRM standard with wide adoption. Backed by its initial focus on mobile, the convergence of mobile services into home entertainment devices, and its suitability for use in nonmobile IP-based delivery channels to the home, the OMA DRM system has the potential of achieving this goal.

In response to an urgent market need for a relatively simple protection system for light media content (such as ring tones, screensavers, and music tracks), the world's first open DRM standard was released for mobile devices in the form of the OMA DRM 1.0 specification. As a next step, OMA DRM 2.0 was developed, with a focus on high-value premium content (such as music, audiovisual clips, movies, animated color screensavers, and games.) This standard allows operators, content providers, and consumers to take advantage of expanded device capabilities such as downloading and streaming of rich media content. OMA DRM 2.0 offers greater security and trust management, provides largely improved user convenience, and supports a wide variety of distribution and payment use cases, thereby opening up a new world of business opportunities for innovative services. Throughout this article we will briefly refer to OMA DRM 1.0 and focus primarily on OMA DRM 2.0.

OBJECTIVES

The objective of the OMA DRM systems is to provide standardized DRM solutions for content services across mobile networks, but in a network- and content-agnostic manner. These DRM systems can then be used for any content in a wide variety of environments, services, and devices.

ISSUING BODY AND SCHEDULE

The OMA was created in June 2002 through the consolidation of the Open Mobile Architecture initiative and the Wireless Application Protocol (WAP) Forum. As mentioned earlier, the OMA develops enablers, which are published in a two-step approach. When the technical development is finished, the specification is published as a candidate enabler, which serves as the basis for the first round of product implementations. Next, interoperability testing takes place and, if needed, refinements of the candidate enabler are performed. The enabler is considered mature as soon as interoperability is proven, at which time the specification is published as an approved enabler.

The OMA DRM 1.0 specification was published as a candidate enabler in November 2002 and as an approved enabler in September 2004. The OMA DRM 2.0 specification was published as a candidate enabler in February 2004 and (after extensive testing outlined in a later section) as an approved enabler in April 2006. The OMA DRM 2.0 tests have continued since then for the sole purpose of testing product implementations.

STRUCTURE OF THE STANDARD

The OMA DRM 2.0 specification consists of the DRM Requirements Document, the DRM Architecture Document, the DRM Content Format, the DRM Rights Expression Language (REL), and the (core) DRM specification. The DRM

1053-5888/07/$25.00©2007IEEE

Requirements Document contains informative use cases and a set of normative market and engineering requirements. The DRM Architecture Document describes the architecture of the OMA DRM 2.0 system. The DRM content format describes the secure file format(s) for download of OMA DRM 2.0-protected content and is based on the ISO base media file format (ISO 14496-12). Two formats are defined: the DRM content format (DCF) and packetized DCF (PDCF). With DCF, which is intended for discrete media such as ring tones, music tracks, and still pictures, the content in the file is encrypted as a single object, irrespective of its internal structure and layout. With PDCF, intended to protect continuous media such as audio and video, the content in the file is encrypted on a packet-by-packet basis. PDCF supports streaming and random access to the packetized content. Either no encryption can be used or the AES symmetric encryption method as defined by NIST, in Cipher Block Chaining mode or in Counter mode (AES_128_CBC or AES_128_CTR, respectively), can be used. The DRM REL is used to express the rights to consume OMA DRM 2.0 protected content. As for OMA DRM 1.0, OMA DRM 2.0 REL is based on the open digital rights language (ODRL). The (core) DRM specification defines the remaining elements of the OMA DRM 2.0 system such as: 1) the rights object acquisition protocol (ROAP) suite specifying the communication between a rights issuer (RI) and the DRM agent in a device, 2) the domain concept, allowing access to DRM content on a number of devices, and 3) a certificate revocation mechanism for RI and device certificates based on the online certificate status protocol (OCSP).

TECHNOLOGY

FUNCTIONALITIES

OMA DRM 1.0 is a simple protection system for single media objects (such as a ring tone or a music track) and supports three basic functionalities: 1) *forward lock* to prevent an unprotected media object from leaving the device, 2) *combined delivery* for distributing a protected media object jointly with the rights to consume it, and 3) *separate delivery* for separate distribution of a protected media object and the rights to consume it. In particular, separate delivery allows users to legitimately forward a protected media object to other users, such as their friends and family. Recipients cannot consume the protected content until they have requested the rights to consume it from the RI. This innovative marketing concept, called *superdistribution*, uses peer-to-peer data transfer to its advantage rather than positioning it as a threat. The rights associated with superdistributed content enable revenue collection to be independent of how the digital goods were distributed.

OMA DRM RESOURCES

The Standard

- OMA DRM 1.0: http://www.openmobilealliance.org/release_program/drm_v1_0.html
- OMA DRM 2.0: http://www.openmobilealliance.org/release_program/drm_v2_0.html

Tutorials, Overviews, Books

- E. Becker, W. Buhse, D. Günnewig, and N. Rump, Digital Rights Management—Technological, Economic, Legal and Political Aspects. (An 800 page compendium from 60 different authors on DRM.) Berlin: Springer-Verlag, 2003.

Resources for further developments

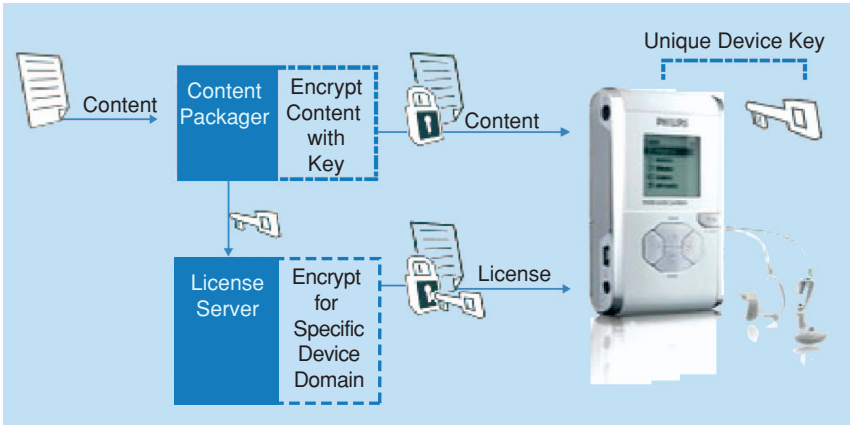
- Group in charge of the OMA DRM system: BAC-DLDRM; DLDRM portal accessible (for OMA members) via the OMA site: http://www.openmobilealliance.org/
- Email discussion list (for OMA members): OMA-DLDRM@mail.openmobilealliance.org
- OMA DRM 2.0 client conformance test tool (only for OMA members): http://www.openmobilealliance.org/testfest/ and http://www.openmobilealliance. org/testfest/IOP-DRM20-TestFest.html
- OMA DRM interoperability testing (for non-OMA members): info@coremedia.com

The main focus of OMA DRM 2.0 is on mobile content services. However, from a user convenience perspective, it is very desirable that the protected content be consumed not only on mobile phones but also on other user devices. User convenience is a major condition for consumer acceptance of a DRM system. Therefore, OMA DRM 2.0 introduces the concept of so-called *domains*. Equivalent to the user experience with CDs and DVDs, OMA DRM 2.0 enables sharing of protected content between OMA DRM 2.0-compliant devices within the home by creating a domain that contains all these devices. The devices may belong to the same user or to other users within that domain, such as family members or friends.

In OMA DRM 2.0, the creation of domains and the sharing of content within a domain are controlled by the RI. When the user buys a new device, that device can be added to the personal domain by sending a registration request to the RI, upon receipt of which the RI sends the device and domain keys to the new device as appropriate. The domain concept allows various use cases, such as 1) automatic content synchronization between the devices within a domain after downloading new "domain content" on one of the devices within said domain, whereby new content becomes available on all devices within that domain; 2) usage of domain content on "unconnected devices" (for example, a portable media player without connection to the wireless network and without Internet browsing capabilities, but with a Bluetooth interface that is used to convey the protected content and associated rights); and 3) automatic download of video at different resolutions (for example, if a video clip is downloaded to a mobile phone for use within a domain, and if the RI knows that the domain also contains a set-top-box (STB) that requires a higher-quality video than the mobile phone, then the RI can send a message that the video clip is also available for download at higher video resolution for use on the STB).

OMA DRM 2.0 distributes protected content in encrypted form using a content key. By means of an access license

carried in a rights object (RO), users can obtain the rights to consume the content either on a specific device or within a specific domain. The access license contains the content key and is encrypted for use by the specific target device or domain by means of the unique device or domain key, respectively. The OMA DRM 2.0 agent on the device decrypts the access license by means of the device or domain key, retrieves the content key from the access license, and decrypts the content during its consumption, as illustrated in Figure 1.

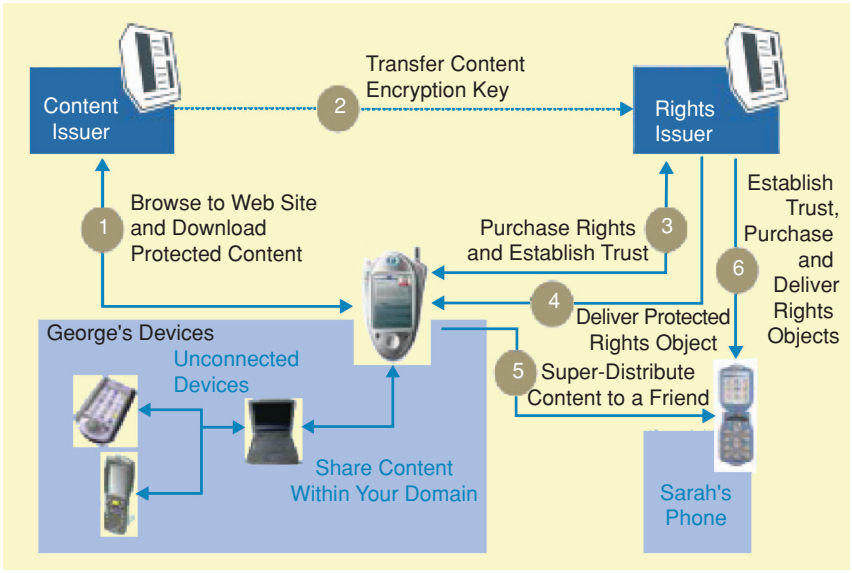


[FIG1] **Basic block diagram of an OMA DRM 2.0 system.**

ARCHITECTURE

The functional architecture of OMA DRM 2.0 is illustrated in Figure 2. Let us assume that a user is browsing the Web site of a content issuer; there he/she finds exciting content and decides to download it. By means of information contained within the downloaded data, the OMA DRM 2.0 agent connects to the RI to allow purchase of the rights to consume the content. After mutual authentication and trust verification between the RI and the device, the rights associated to the downloaded content are purchased, upon which the RI delivers the protected RO. In this example, the rights allow consumption on the devices within a specific domain.

If the user is enthusiastic about the purchased content, he/she may send the downloaded content (or its URL) to a friend with a promotional message. That friend can then purchase the content following the same procedure. This example shows the OMA DRM 1.0 concept of superdistribution, which is further developed in OMA DRM 2.0. Users are free to share protected content, and free previews may be available to enable users to sample content, but the rights to fully use the content must be purchased separately by each consumer.



[FIG2] **The OMA DRM 2.0 functional architecture.**

COMPARISON WITH OTHER STANDARDS

Several proprietary standards have entered the market, each controlled by a single company. In contrast to proprietary standards, OMA DRM is an open, global DRM standard with major market adoption on over 460 mobile phone models and server-side implementations on five continents. OMA DRM offers unique and compelling features and enables a competitive and innovative market with offerings from many different vendors. Further, OMA DRM offers implementers the ability to innovate and distinguish in the market by means of manufacturer-specific added value.

Other open DRM standards are evolving too, some of which provide a framework for DRM systems rather than a complete end-to-end solution, thereby offering choices on how to achieve interoperability across networks, devices, and geographies and putting interoperability at risk. While technology choices in other DRM systems may differ from those of OMA DRM, it should be noted that these choices do not have a strong impact on market adoption. Far more important are the provided security and user convenience features of the DRM system, which, in the case of OMA DRM, are born out of successful industry-wide cooperation within the OMA.

PERFORMANCE

Because interoperability is crucial in a standards-driven industry, the OMA organizes Test Fests to enable vendors to verify and test the interoperability of their product implementations. In May 2005, the interoperability of OMA DRM 2.0 implementations was tested for the first time at an OMA Test Fest. Five more Test Fests followed in subsequent

OMA DRM PRODUCTS

- OMA DRM 1.0: It is used by many mobile operators in their services across the globe—mainly for ring tone distribution and full music track downloads—and accepted by all music labels today protecting revenues worth billions of U.S. dollars. It is currently supported on more than 550 handset models, with superdistribution supported on more than 280 handset models. An overview of OMA 1.0 handset models is available at http://www.coremedia.com/ en/88632/drm
- OMA DRM 2.0: First (pre-)commercial OMA DRM 2.0-based services for music delivery, mobile TV, and games services were introduced/announced by several mobile operators, such as Deutsche Telekom, Digita, Orange, SK Telecom, Vodafone, and others.
- The first handsets with OMA DRM 2.0 support are available on the market, with more being developed. An overview of OMA 2.0 handset models is available at http://www.coremedia.com/en/88632/drm
- OMA DRM 2.0 clients (for mobile phones, media players, and PCs) and servers available from various parties. An impression of involved companies can be retrieved from http://product.openmobilealliance.org/, which also includes lists of (publicly known) DRM 2.0 Test Fest participants.

months, with testing of 64 client and 28 server implementations over a period of six months. By the end of 2005, more than 10,000 interoperability tests were conducted successfully in over 200 intercompany product combinations. Based on the success of this extensive testing, OMA decided to approve OMA DRM 2.0 in March 2006.

The OMA DRM 2.0 Test Fests continue after the publication of the approved enabler for the sole purpose of testing product implementations, but only as long as sufficient vendors participate in such tests. To help new vendors in the OMA DRM 2.0 market, the OMA also decided to support the development of an official OMA DRM 2.0 client conformance test tool (CTT) provided by CoreMedia for conformance testing. The CCT provides a complete DRM environment for testing devices and enables companies to check their DRM agent implementation against the OMA DRM 2.0 client conformance tests. Participation in OMA DRM 2.0 Test Fests is open to OMA members, but devices are required to reach a sufficient level of maturity in conformance testing prior to Test Fest participation. Therefore, any vendor wishing to attend the Test Fest with an OMA DRM 2.0 client implementation is required to submit a client CTT report to gain entry.

FURTHER TECHNICAL DEVELOPMENTS

The OMA continues to work on extensions of OMA DRM 2.0, which will lead to separate enablers that will reference OMA DRM 2.0. Each of these extensions can be used alone and will have their own interoperability testing programs to allow progress from candidate to approved enabler. The extensions underway include a mechanism for detailed metering of content usage (to be specified in OMA DRM 2.1 and to be fully compatible with OMA DRM 2.0) as well as extensions in the following areas: 1) *broadcast* of OMA DRM protected content to enable secure content services across broadcast channels such as DVB-H, MBMS, BCMCS, DMB, and DAB. For this purpose, binary Ros are defined, as well as save permissions (for superdistribution of broadcast content), subscriber groups, key stream handling, token-based metering of content usage, etc.; 2) *secure removable media* to enable binding of protected content to secure removable media such as MultiMediaCard (MMC) or Secure Digital memory card (SD), so that the content can be consumed by an OMA DRM agent. In this context; it should be noted that OMA DRM 2.0 binds content rights to devices or domains and that this extension will specify the additional capability of binding content rights to secure removable media; and 3) *secure content exchange* to address the import of content protected by non-OMA systems and various domain enhancements. This extension specifies mechanisms for a trusted device within the home to "translate" imported content into OMA DRM protected content. A user can be subscribed to more than one service with involvement of multiple RIs, which easily leads to multiple domain definitions for the same user. To improve user convenience in such cases, the option to create a user-centric domain on top of one or more OMA DRM 2.0 domains is defined. Furthermore, the capability of sharing OMA DRM protected content with other users is extended.

RESOURCES

Relevant resources for the OMA DRM standards are listed in the "OMA DRM Resources." Test Fests are organized for testing purposes, and a test tool is available for device implementations.

PRODUCTS

OMA DRM 1.0 is very successful on the market, with an estimated market penetration of 97%. Following the announcement of the publication of OMA DRM 2.0 earlier in 2006, several mobile carriers announced OMA DRM 2.0-compliant content services. Typically, this reflects a natural migration path from OMA DRM 1.0 to OMA DRM 2.0. The first handsets with OMA DRM 2.0 support have already entered the market. A summary of relevant products is included in "OMA DRM Products".

AUTHORS

Willms Buhse (willms.buhse@coremedia.com) is head of products and marketing with CoreMedia, Hamburg, Germany, and is vice chair of the OMA working group that develops the OMA DRM System within the OMA.

Jan van der Meer (jan.vandermeer@philips.com) is senior standardization manager with Philips Electronics, Eindhoven, The Netherlands, and chairs the OMA working group that develops the OMA DRM system within the OMA. SP