



Open Mobile Alliance Digital Rights Management

Short Paper



OMA – specifying mobile service enablers

OMA is designed to be a center for mobile service enabler specification work, stimulating and contributing to the creation of interoperable services. OMA's organizational goals include: Deliver quality, open technical specifications based upon market requirements that drive modularity, extensibility, and consistency. In addition, OMA service enabler specifications provide interoperability across different devices, geographies, service providers, operators, and networks, and facilitate interoperability of the resulting product implementations.

Market need for Digital Rights Management

Downloading content to a mobile phone, or receiving content by messaging services, has become one of the most popular mobile data services. The typical content consumed by a mobile device today includes limited value content types such as ringtones, screensavers and background images. As new smartphones and other smart devices penetrate the market, and mobile network capacities increase, a demand for new, higher value content types emerge.

OMA began working on mobile Digital Rights Management (DRM) specification in 2001 in response to clear market demand. Content and service providers saw mobile phones as a lucrative channel to distribute their copyright protected content, thus a content copyright protection system was needed to protect their investment.

OMA identified the market need for various levels of protection that is needed commensurate with the value of the content being protected. Service providers and mobile vendors wanted a solution that was timely and inexpensive to deploy, which can be implemented in mass market mobile devices, and should not require costly infrastructure to be rolled out.

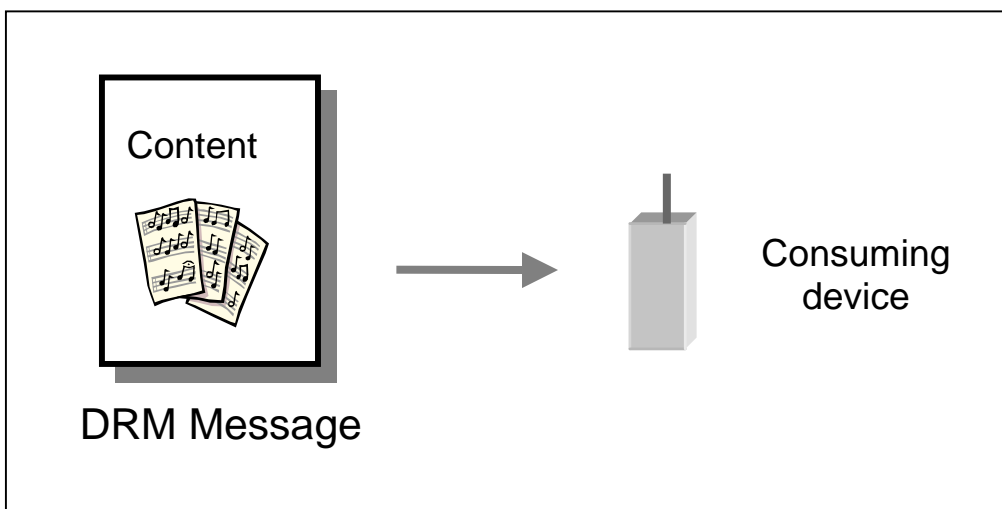
OMA Digital Rights Management 1.0 Enabler Release

The OMA DRM 1.0 Enabler Release was developed rapidly in order to reduce time to market. The Enabler Release was published in November 2002 and was immediately available for companies to implement in their mobile products.

OMA DRM version 1.0 Enabler Release was created to meet the above listed content and service provider, and vendor requirements. OMA DRM 1.0 includes three levels of functionality:

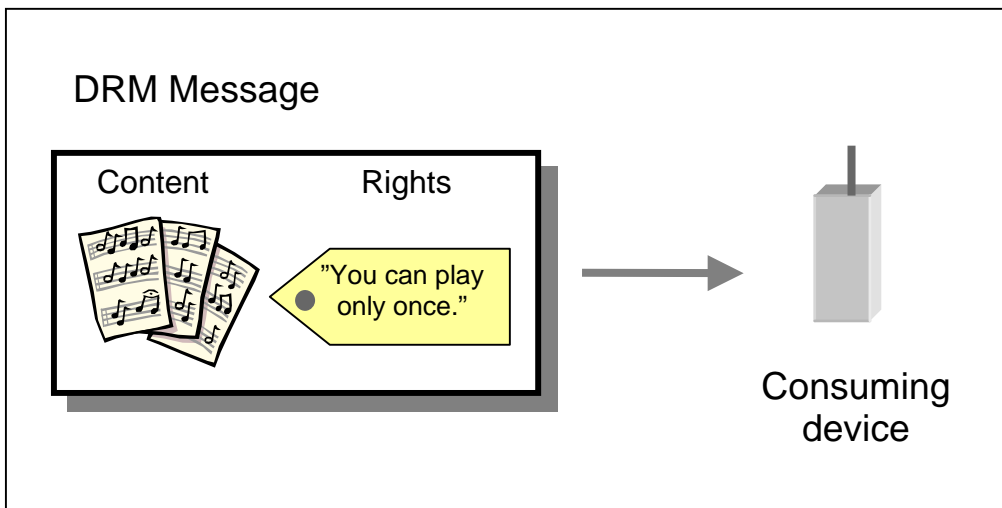
- ✓ Forward Lock; prevents content from leaving device
- ✓ Combined Delivery; adds rights definition
- ✓ Separate Delivery; provides content encryption and supports superdistribution

The purpose of *Forward Lock* is to prevent peer-to-peer distribution of low-value content. This applies often to subscription-based services, such as news, sports etc. The plaintext content is packaged inside a DRM message that is delivered to the terminal. The device is allowed to play, display or execute the content, but it cannot forward the object.



Forward Lock

Combined delivery equally prevents peer-to-peer distribution, but it also controls the content usage. In combined delivery method, the DRM message contains two objects, the content and a rights object. The rights object defines permissions and constraints for the use of content. These can be, for example a permission to play a tune only once, or using the content only for x number of days. Neither content nor the rights object can be forwarded from the target device.



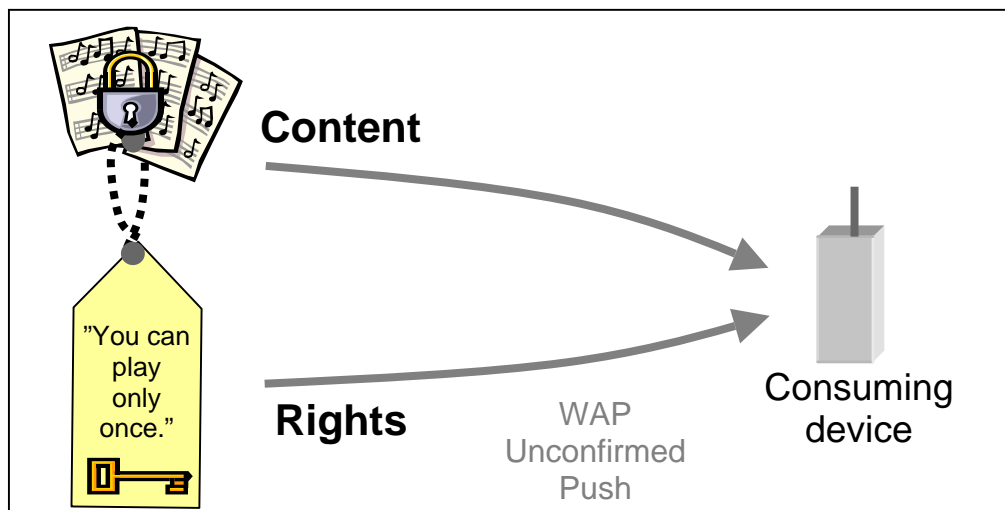
Combined Delivery

The purpose of *Separate Delivery* is to protect higher value content. It enables so called *superdistribution*, which allows the device to forward the content, but not the usage rights. This is achieved by delivering the media and usage rights via separate channels.

The content is encrypted into DRM Content Format (DCF) using symmetric encryption; the DCF provides plaintext headers describing content type, encryption algorithm, and other useful information.

Rights object holds the symmetric Content Encryption Key (CEK), which is used by the DRM User Agent in the device for decryption. The Rights Object is created by using OMA Rights Expression Language (REL). OMA Right Expression Language is a mobile profile of ODRL (Open Digital Rights Language) 1.1.

Superdistribution is an application of Separate Delivery that also requires a Rights Refresh mechanism that allows additional rights for the media. Recipients of superdistributed content must contact the content retailer to obtain rights to either preview or purchase the media. Thus, the separate delivery method enables viral distribution of media maximizing the number of potential customers while retaining control for the content provider through centralised rights acquisition.



Separate Delivery



Interoperability

Open Mobile Alliance facilitates Interoperability Test Fests as a service for OMA member companies to test their OMA implementations for interoperability against other vendors' OMA implementations. The first OMA Test Fest for OMA DRM Enabler Release was organized in November 2003. Other Interoperability Test Fest for OMA DRM implementations will follow regularly as the specification and the product implementations evolve.

OMA evolving the DRM solution

DRM solution is evolving with the mobile industry. The higher bandwidth provided by 2,5G and 3G cellular networks allow larger content files to be transmitted over the air. Proliferation of wireless Internet "hotspots" makes Internet access easily available to consumers. Smart mobile devices with removable media and larger color screens support downloading and streaming rich media content. Content and service providers are eager to release rich audio/video content and applications into the mobile marketplace.

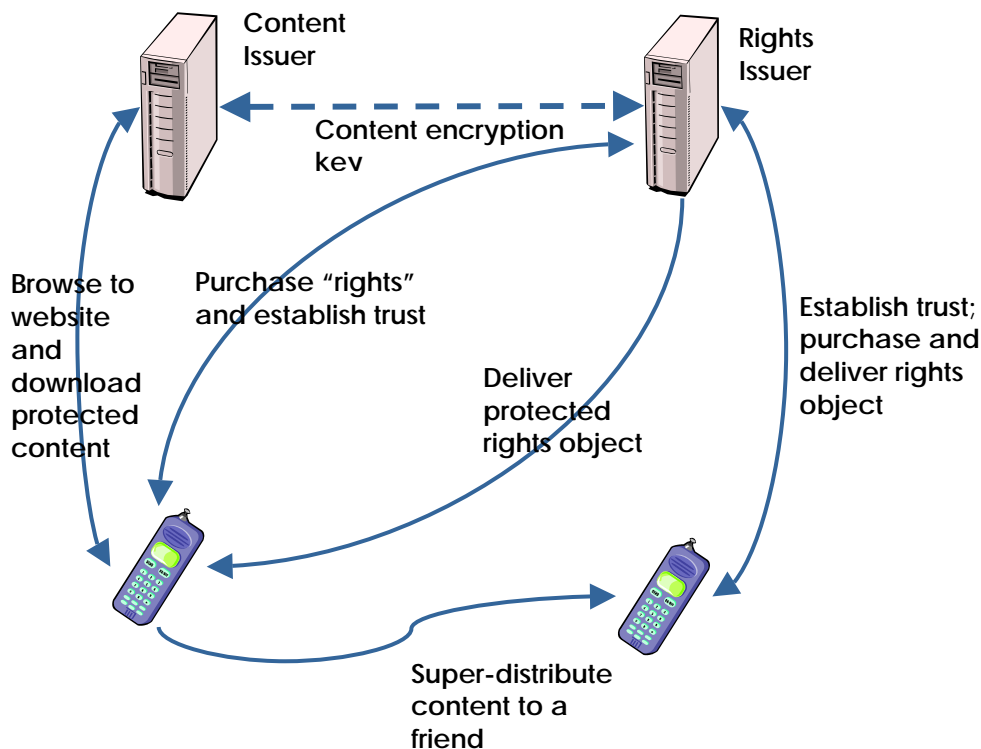
All these factors contribute to the requirements of continuously enhanced OMA DRM solution. Greater security and trust management is required to protect the high value content. There's a need to ensure that the target device can be trusted to keep the content and secrets safe. Greater security is also needed in order to prevent content from leaking out during the acts of downloading and other distribution.

The Open Mobile Alliance is meeting these market needs by upgrading the existing OMA DRM Enabler Release with enhanced features.

The next version of OMA DRM will add enhanced security by encrypting the rights object and the content encryption key by using the device's public key to bind them to the target device. Integrity protection for both content and the rights object will be added to reduce the risk of tampering.

In addition to these enhanced security features, additional trust elements will be introduced. Mutual authentication between the device and the rights issuer, i.e. the content retailer, will add trust to the downloading or messaging scenario. The rights issuer will be able to accurately identify the device in order to determine the revocation status of the transaction.

New version of OMA DRM will also support for a wide variety of distribution and payment use cases.



Example of DRM deployment

Open DRM specifications generate business growth

OMA is an open organization with representation from the whole mobile value chain, including mobile operators, content, service and applications providers, wireless vendors and IT companies. Any company can join OMA and participate in the technical specification work. Implementing the open specifications and interfaces in mobile products, however, is not tied to the membership. All OMA enabler releases can be downloaded from the OMA website and be used in product development by anyone.

OMA DRM has been deployed for some time already. Several vendors have announced servers, mobile devices and software products



supporting the open OMA DRM version 1.0 Enabler Release. Mobile network operators and other service providers are offering DRM-based services for their customers. These service models, together with offered content types, are being continually enhanced with the overall technical development in the mobile industry.

New ideas and experiences will drive OMA DRM in new directions. New use cases, technical requirements, and business models will influence the future direction of the OMA DRM specification.

For more information, please visit

www.openmobilealliance.org.