Chapter IV
Overview of OMA Digital Rights Management

Mercè Serra Joan
Fraunhofer Institute for Integrated Circuits IIS, Germany

Bert Greevenbosch
Fraunhofer Institute for Integrated Circuits IIS, Germany

Anja Becker
Fraunhofer Institute for Integrated Circuits IIS, Germany

Harald Fuchs
Fraunhofer Institute for Integrated Circuits IIS, Germany

Stefan Krägeloh
Fraunhofer Institute for Integrated Circuits IIS, Germany

ABSTRACT

This chapter gives an overview of the Open Mobile Alliance™ Digital Rights Management (OMA DRM) standard, which allows for the secure distribution and usage of protected digital content. Additionally, the DRM Profile of the OMA Mobile Broadcast Services standard, which is an extension of the OMA DRM standard to support mobile broadcast applications, is discussed. This chapter also introduces the associated OMA Secure Removable Media (OMA SRM) and OMA Secure Content Exchange (OMA SCE) standards, which increase the portability of DRM-protected content and offer a better user experience. The aim of this chapter is to give the reader insight in the above mentioned standards, their technical background, and possible usage scenarios.
INTRODUCTION

Digital Rights Management (DRM) is a technology that allows content and service providers to securely distribute digital content and to control its access and use.

The Open Mobile Alliance (OMA) Digital Rights Management standard (OMA DRM) offers protection and secure access control for digital content. The OMA Mobile Broadcast Services standard (BCAST) specifies the protected content delivery for mobile broadcast applications such as mobile TV. These two standards complement each other enabling further functionalities and use cases.

This chapter provides a technical overview of the OMA DRM standard including its latest developments. Further, the OMA BCAST standard is described, focusing on the DRM profile for service and content protection.

BASIC TERMS AND CONCEPTS OF DIGITAL RIGHTS MANAGEMENT

Digital Rights Management (DRM) comprises the complete process of managing and controlling the access and consumption of protected content.

In a DRM system, content is cryptographically protected and access to the content is governed through licenses issued by a license server. Licenses contain the keys to access the content and express usage rights and constraints for the content using a rights expression language (REL). Collectively, the modules that handle the license information are known as key management system (KMS).

Through the separation of protected content and controlling license, various business models are facilitated, such as superdistribution and subscription, while maintaining support for other established business models, such as pay-per-view or play-count/play-time variations. Since the protected content cannot be accessed without a license, it can be distributed without fear of misuse. Therefore content distribution is not limited to controlled networks.

The usage rules and rights are enforced at consumption time by a secure agent (secure player implementation). The agent is also responsible for secure storage of information that has to be kept secret or temper proof, like root certificates, private device keys and state information (e.g. play counts).

Cryptographically signed certificates are used to authenticate devices and to establish and verify trust between all involved parties. Trusted certification authorities that are part of a public key infrastructure (PKI) issue these certificates.

Licenses are bound to an anchor, e.g. a unique hardware property or user identification, to ensure control over the content. Providing a common anchor for a group of devices is known as domain concept. An example is the home domain, where a number of devices belonging to a single household share a common anchor allowing a single domain license to be used on any of the domain’s devices.

THE OPEN MOBILE ALLIANCE™ AND OMA DRM

The Open Mobile Alliance™ (OMA) is a consortium of major companies active in the area of mobile communications. At the time of writing, OMA has about 400 members worldwide, including mobile operators, device and network suppliers, information technology companies and content providers.

The OMA DRM standard is one of the first open, standardized DRM specifications. The first version – OMA DRM v1.0 – was released in 2004. This version focuses on basic functionality: although the content is encrypted and a rights expression language is specified, the protection of the content encryption key (CEK) remains unspecified, such that the security relies on the
Related Content

Correlation-Based Ranking for Large-Scale Video Concept Retrieval
Lin Lin and Mei-Ling Shyu (2012). Methods and Innovations for Multimedia Database Content Management (pp. 28-42).
www.igi-global.com/chapter/correlation-based-ranking-large-scale/66686?camid=4v1a

Synthetic Video Generation for Evaluation of Sprite Generation
Yi Chen and Ramazan S. Aygün (2010). International Journal of Multimedia Data Engineering and Management (pp. 34-61).
www.igi-global.com/article/synthetic-video-generation-evaluation-sprite/43747?camid=4v1a

Past-Blogging: Defining a Practice
www.igi-global.com/chapter/past-blogging/189466?camid=4v1a

Automatic Live Sport Video Streams Curation System from User Generated Media
Kazuki Fujisawa, Yuko Hirabe, Hirohiko Suwa, Yutaka Arakawa and Keiichi Yasumoto (2016). International Journal of Multimedia Data Engineering and Management (pp. 36-52).
www.igi-global.com/article/automatic-live-sport-video-streams-curation-system-from-user-generated-media/152867?camid=4v1a