|  |
| --- |
|  |

|  |  |
| --- | --- |
| Input Contribution | |
| Meeting ID\* | SDS#49 |
| Title:\* | DRM existing standards |
| Source:\* | JaeSeung Song, KETI, jssong@sejong.ac.kr  Minbyeong Lee, Hyundai Motors, [minbyeong.lee@hyundai.com](mailto:minbyeong.lee@hyundai.com) |
| Date:\* | 2021-01-19 |
| Input related to\* | TR-0066 V 0.1.0 |
| Intended purpose of  document:\* | Decision  Discussion  Information  Other <specify> |
| Impacted other TS/TR(s) |  |
| Decision requested or recommendation:\* | Agree for inclusion in TR-0066 |
| Template Version: January 2017 (Do not modify) | |

**oneM2M Notice**

The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in Annex 1 of the Partnership Agreement.

# Introduction

This contribution introduces DRM as an existing standards related to data license.

### -----------------------Start of change 2-------------------------------------------

## 6.2 Related Solutions and Standards

*Editor’s Note: The section introduces related solutions managing data license and standards such as DRM.*

## 6.2.1 Related Solutions

## 6.2.2 Related Standards

In this section, existing standards that contain data license management are introduced.

Open Mobile Alliance Date License Managemennt (OMA).

OMA DRM is a digital rights management (DRM) system invented by the Open Mobile Alliance, whose members represent mobile phone manufacturers, mobile system manufacturers, mobile phone network operators, and information technology companies. OMA DRM provides a way for content creators to set enforced limits on the use and duplication of their content by customers. A system that uses OMA DRM is implemented on many recent phones.

The OMA DRM group standardized two versions of OMA DRM specifications, i.e., DRM 1.0 and DRM 2.0.

OMA DRM 1.0 was first drafted in November 2002, and approved in June 2004. It provides basic Digital Rights Management, without strong protection. The standard specifies three main methods: Forward Lock, Combined Delivery (combined rights object / media object), and Separate Delivery (separated rights object and encrypted media object).

OMA DRM 2.0 was drafted in July 2004 and approved in March 2006. The new feature of DRM 2.0 is the extension of DRM 1.0's Separate Delivery mechanism. Each participating device in OMA DRM 2.0 has an individual DRM Public key infrastructure (PKI) certificate, with a public key and the corresponding private key. Each Rights Object (RO) is individually protected for one receiving device by encrypting it with the device public key. The RO in turn contains the key that is used to decrypt the media object. Delivery of Rights Objects requires a registration with the Rights Issuer (the entity distributing Rights Objects). During this registration, the device certificate is usually validated against a device blacklist by means of an Online Certificate Status Protocol (OCSP) verification.

OMA's DLDRM (Download and DRM) Working Group has carried out the follow-up work of DRM 2.0 in three directions. First, DRM extension support for mobile streaming services, which are emerging as mobile TV, and second, Secure Content Exchange (SCE), which enables non-OMA DRM content to be used as OMA DRM or exchange of various and secure contents. And third, it is intended to provide convenient content use using Secure Removable Media (SRM) such as smart card, SD, and UFD that are gradually being installed in mobile phones.

Figure 6.2.2-1 shows the functional architecture of DRM. Before content is delivered to a consumer, a content owner sends the encrypted content and the key to a content provider and a right issuer. The content is encrypted with the security key to protect it from unauthorized access (e.g., play a music). A content issuer delivers DRM Content, and a rights issuer generates a Rights Object. When the consumer is interested in the content, an encrypted content is delivered to the consumer. The content can be accessed by the consumer only after the license of the content is purchased by the consumer. The license contains the secret key to decript the encrypted content. The license can also includes the access rights of the content.



Figure 6.2.2-1 A conceptual DRM architecture

As described above, the DRM system delivers encrypted contents to Consumer to protect it from unauthorized access. The system allows end devices (e.g., smart phone) to decide access rights and control policy based on purchased license.

Issues of using DRM for open data license are as follows:

* Introduces encryption cost for contents with open license
* Increases the cost of IoT applications to manage secret key and decryption process
* Needs a mechanism to accredit the use of open data

Although data is parts of contents managed in a mobile phone, the main functions of OMA DRM is to develop a system that can interwork with the network system to issue licenses and provide contents to clients if a proper license is purchased for the use of target contents. It specifies some functions about the expiration date of the contents, buying rights objects for another user and using contents on multiple devices. However, details terms and conditions for the use of data are not specified.

### -----------------------End of change 2-------------------------------------------