A Simple Mobile DRM solution

Xiaoyong Su, Chi-Cheng Chu, B. S. Prabhu and Rajit Gadh
Wireless Internet for the Mobile Enterprise Consortium (WINMEC) [http://winmec.ucla.edu/]
420 Westwood Plaza, University of California, Los Angeles, CA 90095

A general DRM solution includes: 1. Secure Content Creator Application (Content Encryption), 2. License Generator application (License Management), 3. Secure Content Playback Application (Client Application). There are two types of content delivery methods, one is combined delivery, and the other one is separated delivery. All the DRM solutions support one of two or both. Usually, because of the various content types and services, DRM solution is customized. There is no one-fit-all solution without any modification. We have to use available software development kits to create DRM solution to satisfy specific DRM business operation.

1. DRM Development Kits:

1.1 OMA DRM

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. OMA DRM has been deployed for some time already [1].

OMA DRM include following functionality [1]:
- Forward Lock. It prevents peer-to-peer distribution of low-value content and prevents contents from leaving device
- Combined Delivery. It adds rights definition. It not only prevents peer-to-peer distribution, but also controls the content usage. In this method, the DRM message contains two objects: the contents and a right object, which defines permissions and constraints for the use of content.
- Separate Delivery. It provides content encryption and supports super distribution. It is developed to protect higher value content and allows the device to forward the content but not the usage rights.

OMA provide a standard and framework of DRM. The latest version is DRM version 2.0. Same vendors have announced servers, mobile devices and software products supporting the open OMA DRM version 1.0 Enabler Release. The members who have OMA compliant DRM solution include Nokia, Ericsson, Beep Science, NDS, End2EndMobile, DMDSecure, CoreMedia, RSA Security, etc. Each members has it’s own development kits for DRM.

Advantages: Industry Standards for DRM, Supported by most vendor.
Disadvantages: each vendor has it’s own solution (SDK).
1.2 Microsoft DRM

Microsoft is a biggest competitor of OMA DRM standards. They developed their own DRM technology -- Microsoft Windows Media Rights Manager (Media DRM 9 Series, includes both server and client software SDK) [2].


![Windows Media Rights Manager Flow](image)

**Server side**: Windows Media Encoder 9 Series encoder (Content Encryption), Windows Media Rights Manager 9 (License Management).

**Client side**: Windows Media Player SDK (content playback)

**Client Hardware**: All devices that support Microsoft Media Player 9 (such as Pocket PC 2003, Smartphone 2003, etc).

**Disadvantages**: Only support windows media format.

**Advantages**: Rapid development, familiar and friendly UI.

1.3 RealNetworks DRM

RealNertwork’s DRM is based on Helix DRM (includes Helix Client Platform support, Helix universal server plug in, Helix format support) [4]

**Features**: It is a comprehensive and flexible platform for the secure media content delivery of standards-based as well as leading Internet formats, including RealAudio, RealVideo, MP3, MPEG-4, AAC, H.263 and AMR. Helix DRM makes it possible to deliver these formats not only to PCs but also to a wide array of non-PC devices, including mobile devices and home appliances.
Figure 2 Helix DRM work Mechanism [4]

**Server side:** Helix DRM Packager (Content encryption), Helix License Server (License Management)

**Client side:** Helix DRM Client (Content Playback Application)

**Client Hardware:** Helix DRM DNA Client Supported Device (Couldn’t find what exactly are, I guess something like PC, Pocket PC, mobile phone which support this client).

**Advantages:** Support most media format.

**Disadvantages:** Compete with Microsoft

### 1.4 LockStream DRM


**Features:** Support all data formats, Supports any file format, License Authority linking, Flexible implementation.

**Server Side:** Secure Package Creator (content encryption), License Generator Module (License Management).

**Client Side:** Secure Package Reader Module. (Content Playback Application)

**Client Hardware:** OMAP based mobile devices.

**Advantages:** Support most media format, Mainly optimized for mobile communication device.

**Disadvantages:** Mainly optimized for mobile communication device based on OMAP platform.

### 2. Implementations

There are many implementations in the industry. Here I just list three of them.
3 Simple DRM Solutions

Because there is no “one size fits all” DRM solution, we have to create our own DRM solution based these available DRM SDKs when we consider building a DRM system. Figure 3 shows a general DRM solution physic framework. Based on this framework. We describe two implementations respectively based on Microsoft Windows Media Right Manager 9 and OMA compliant DRM DMDMobile.

3.1 Microsoft DRM SDK based solution (Test Bed) [8]

Figure 4 shows a simple solution based on Microsoft DRM SDK. In this solution, first, Original content must be encoded into windows media format (.wma, .asf, .wmv). However, if the original contents are windows media format, this step can be ignored. Usually, content owner need to convert other content format (.rm, .mov, .mpeg, .avi, etc) to windows media format. The converting can be done either by using 3rd part software directly or using media 9 series encoder APIs.
Before distributed to end user, the digital content (windows media format) will be encrypted by using Windows Media Right Manager 9 (Packaging). In this solution, key ID or license acquisition URL will be packed into the encrypted media content. Content publishing can be fulfilled by window media show service (NetShow) or Windows Web Service (IIS, .Net). End user can browse the content and choose download or streaming. When he/she wants to watch or listen the content, he/she has to get the license key from license server to playback the encrypted. The key is related to client device and a trust must be established between client and the content. This solution is for Microsoft windows based device such as PC, Pocket PC, Media Center and Smart Phone etc. The limitation on this solution is that Microsoft DRM only support Windows Media format. The SDK is available on their website. You can sign up and get a copy. So the cost for this solution is just hardware cost and necessary programming.

Table 1 shows the function/service and used DRM technologies in this test bed.
Table 2 shows the requirements for establishing the test bed.

<table>
<thead>
<tr>
<th>Roles</th>
<th>Implemented Functions</th>
<th>Hardware Requirement</th>
<th>Software Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Server</td>
<td>Encrypt content, Publish content</td>
<td>P4 based desktop is good enough (P4 1.6G, 40GB HD, 512M RAM)</td>
<td>Windows 200x Operating System, IIS6.0, Microsoft .Net Framework 1.1, Microsoft Media 9 Series SDK, Microsoft NetShow Stream server, Microsoft Media Right Manager 9</td>
</tr>
<tr>
<td>License Server</td>
<td>Manager License</td>
<td>Same as content server</td>
<td>Windows 200x Operating System, Microsoft .Net Framework 1.1, Microsoft Media Right Manager 9</td>
</tr>
<tr>
<td>Client</td>
<td>Playback</td>
<td>Media 9 compliant device Pocket PC 2003, Smart Phone, Media Center</td>
<td>None</td>
</tr>
</tbody>
</table>
There are various implementations of OMA DRM standards. Some of them are based on 3rd part encryption production and some of them use their own encryption product. Since all the OMA based solutions are follow the same standards. The implementation methods are almost same. The only difference is the development tools and platform supporting. Here we pick DMDSecure’s products to build a test bed.

DMDSecure provides four products that support DRM: DMDFusion, DMDLicenser, DMDPackager, and DMDMobile. DMDMobile DRM enable the entire digital right processes: content encryption and delivery, license generation and management, client request license. Since DMDMobile doesn’t provide content delivery function, we use Microsoft Media service and web service to publish and deliver contents. In this solution, key ID or license acquisition URL will be packed into the encrypted media content. The work scenario is same as the solution based on Microsoft DRM Solution. End user can browse the content and choose download or streaming. When he/she wants to watch or listen the content, he/she has to get the license key from license server to playback the encrypted. The key is related to client device and a trust must be established between client and the content. This solution is mainly for cell phones such as Smartphone, Symbian, and other phones with multimedia capability. The contents can be various, from picture, image to video, audio clips.

The cost for implement this solution is the cost of the SDK and hardware plus necessary programming.

Figure 5 shows the solution based on DMDMobile DRM.

Table 2 shows the functions/services used DRM in this test bed

<table>
<thead>
<tr>
<th>Function/Service</th>
<th>Users</th>
<th>Actions</th>
<th>DMDMobile DRM</th>
</tr>
</thead>
</table>

Figure 5 solution based on DMDMobile DRM (Modified from DMDMobile DRM Flow) [10]
Table 2 shows the requirements for establishing the test bed

<table>
<thead>
<tr>
<th>Roles</th>
<th>Implemented Functions</th>
<th>Hardware Requirement</th>
<th>Software Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Server</td>
<td>Encrypt content, Publish content</td>
<td>P4 based desktop is good enough (P4 1.6G, 40GB HD, 512M RAM)</td>
<td>Windows 200x Operating System, IIS6.0, Microsoft .Net Framework 1.1, DMDMobile Protection Component, Microsoft NetShow Stream server</td>
</tr>
<tr>
<td>License Server</td>
<td>Manager License</td>
<td>Same as content server</td>
<td>Windows 200x Operating System, Microsoft .Net Framework 1.1, DMDMobile License Component</td>
</tr>
<tr>
<td>Client</td>
<td>Playback</td>
<td>OMA DRM 1.0 Compliant device such as Pocket PC, Smart Phone, Symbian, etc.</td>
<td>Applications (Player) that are OMA DRM1.0 compliant.</td>
</tr>
</tbody>
</table>

Reference:


