



Cloakware DRM Solutions

OMA DRM 2.0 cross-platform client architecture



Cloakware OMA DRM 2.0 Client is an optimized cross-platform implementation of the Open Mobile Alliance™ (OMA) DRM 2.0 standard. In addition to enhancing security, the OMA DRM 2.0 specification envisions a more sophisticated and complex range of business models for secure media delivery.

The future of mobile content security. Today.

Leveraging extensive experience based on five years of proprietary and OMA DRM 1.0 Client deployments, Cloakware's team of DRM experts has produced a full implementation of the OMA DRM 2.0 specification in a high-performance, low-footprint package.

In partnership with leading mobile operating system and microprocessor providers, Cloakware has designed the OMA DRM 2.0 Client for ease of integration, cross-platform portability, and security. With an API that is consistent across all hardware platforms and operating systems, device manufacturers can now confidently rely upon a single OMA DRM solution for their entire product portfolio.

Fully backward compatible with OMA DRM 1.0 content, the OMA DRM 2.0 Client allows mobile users to experience more robust functionality while affording content owners the high level of protection they demand for premium content.

Progressive Architecture

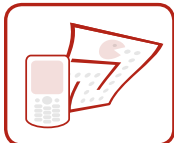
The OMA DRM 2.0 Client has been built on a progressive cross-platform client architecture. It is designed to meet a range of device requirements, from less robust feature phones to the highest performance smartphones, and support whatever security levels are needed.

The client architecture organizes core components into platform-specific and platform-neutral tiers. By compartmentalizing components in this manner, the OMA DRM 2.0 Client promotes easy portability across hardware and software platforms.

For security, the architecture is designed across “trusted” and “untrusted” layers. Communication with the client is restricted to the untrusted layer, while communication with the trusted layer is tightly controlled. As a result, a OMA DRM 2.0 Client solution can incorporate any level or type of security.



RINGTONES



GAMES

**MUSIC
DOWNLOAD**



**VIDEO
DOWNLOAD**

Other upgrades to the client architecture enhance the portability and performance of the solution. Instead of relying on proprietary utilities, the client can rely on components common to most platforms to maintain a small footprint and take advantage of platform component efficiency. This flexibility enables device manufacturers to incorporate advanced features, such as leveraging cryptographic cores available in certain processors, implementing CM-LA robustness and compliance rules.

Client Tiers

The architecture of the OMA DRM 2.0 Client consists of three main tiers:

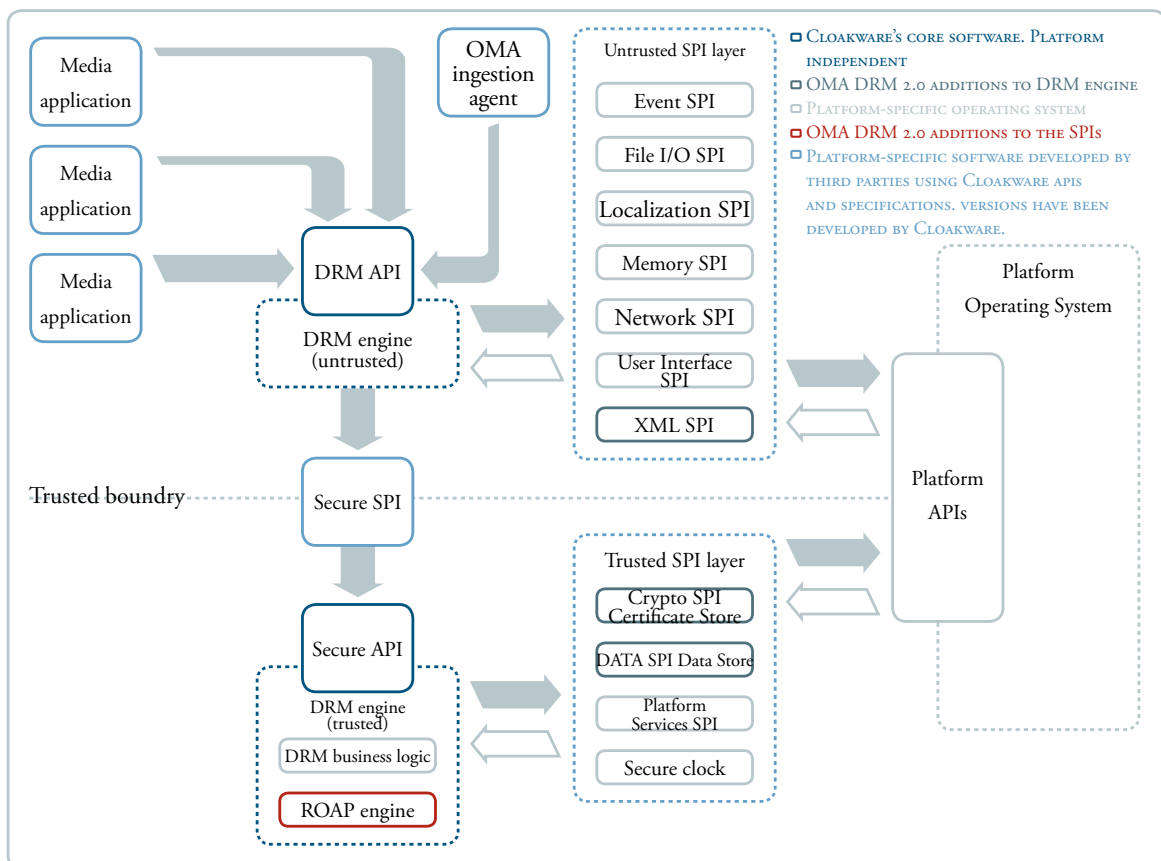
- > **DRM Engine:** Contains core DRM logic for managing OMA-protected media content.
- > **SPI Layer:** Abstracts platform-specific components used by the DRM Engine.
- > **Application Interface:** Exposes DRM Engine functionality for OMA content ingestion and content rendering.

DRM engine components, and the SPIs that support them, are deployed on both sides of the trusted boundary. The robustness of this boundary depends on the design of the marshalling layer, which manages all interaction across the boundary. For example, the Windows CE version developed by Cloakware deploys the trusted layer as a device driver. This architecture also supports hardware-based security solutions. Other scenarios include integrating the trusted layer onto a chip or a device SIM card.

DRM ENGINE

The DRM engine contains the core logic for managing OMA-protected content received on a client device. The DRM engine is platform-neutral, relying on communication with the SPI layer for platform-specific operations. DRM engine components include:

- > **DRM Business Logic:** Evaluates license constraints and controls how OMA content is consumed. For content with valid licensing, this component enables access to content files.
- > **Content Ingestion:** Handles OMA messages received on the device, including encrypting and storing content files, and storing licenses, encryption keys, and security certificates.
- > **Roap Engine:** Manages device registration, license acquisition, and domain membership processes based on OMA DRM 2.0 Rights Object Acquisition Protocol (ROAP) for security.



ABOUT CLOAKWARE

Cloakware, an Irdeto company and part of the Naspers group, provides innovative, secure, proven software technology solutions that enable customers to protect business and digital assets in enterprise, consumer and government markets. Cloakware's two main product lines include: Cloakware Datacenter Solutions help organizations meet governance, risk management and compliance (GRC) objectives for privileged password management while ensuring business continuity and the security of mission-critical data and IT infrastructure. Cloakware Consumer Product Solutions protect software and content on PCs, set-top boxes, mobile phones and media players. Protecting over more than billion deployed applications today, Cloakware is the security cornerstone of many of the world's largest, most recognizable and technologically advanced companies. Headquartered in Vienna, VA and Ottawa, Canada, Cloakware has regional sales offices worldwide.

CONTACT INFORMATION

Corporate Headquarters

Cloakware Inc.
8219 Leesburg Pike, Suite 350
Vienna, VA, USA 22182
Tel. +1.703.752.4830

Canada

Cloakware Corporation
84 Hines Road, Suite 300
Ottawa, ON, Canada
K2K 3G3
Tel. +1.613.271.9446

www.cloakware.com

SPI LAYER

The service provider interfaces (SPIs) abstract platform-specific operations required by the platform-neutral DRM engine. SPIs ported to a platform must conform to the SPI specifications.

SPI components include:

- > **Application SPI:** Operations for retrieving application-related information.
- > **Crypto SPI:** Encryption/decryption operations and Certificate Store access.
- > **Data SPI:** Data store access operations.
- > **File I/O SPI:** System-level file data operations.
- > **Localization SPI:** Application data localization.
- > **Memory SPI:** Memory-related operations.
- > **Network SPI:** Network access operations.
- > **Platform Services SPI:** Operations for retrieving platform-related information.
- > **User Interface SPI:** UI display operations for a consistent UI experience across platforms.
- > **XML SPI:** XML parser operations.

Platform-specific components required by the DRM engine include:

- > **Secure Clock:** Tracks changes in the device clock to protect timed licenses.
- > **Data Store:** Manages OMA-related data, including licenses, rights issuers, and content.
- > **Certificate Store:** Manages certificate verification data provided by rights issuers.

APPLICATION INTERFACE

The OMA DRM 2.0 Client solution provides a robust API that enables device applications to access DRM engine functionality.

- > **Content Ingestion:** Function set for ingesting OMA-protected content and licenses received on a device. Version 2.0 has been streamlined for efficiency and expanded to support streamed content and non-OMA content.
- > **Content Rendering:** Function set enabling media applications to render OMA content according to licensing guidelines, access content and license data, renew licenses, and tent and license data, renew licenses, and share content.

Client Integration

Cloakware has ported the OMA DRM 2.0 Client to several mobile platforms. Solution integration includes installation and configuration of Client software and development media applications with OMA content rendering functionality.

Cloakware provides integration guides and an application development guide. For organizations requiring a customized solution, Cloakware provides a comprehensive software development kit (SDK), including SPI specifications, development guides, sample code, and test utilities.

*Cloakware is a subsidiary of Irdeto which is a Member of the Open Mobile Alliance

© Cloakware Inc., 2009. All rights reserved.

This document is provided "as is" with no warranties, expressed or implied, including but not limited to any implied warranty of merchantability, fitness for a particular purpose, or freedom from infringement. Cloakware Corporation and/or Cloakware Inc. may have patents or pending patent applications, or other intellectual property rights that relate to the described subject matter. 'Cloakware' and its logo are registered trademarks of Cloakware Corporation, a subsidiary of Cloakware Inc. and are used under license. All other names herein are the trademarks or registered trademarks of their respective holders. The furnishing of this document does not provide any license, expressed or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights. Cloakware Inc. assumes no responsibility for error or omissions in this document; nor does Cloakware Inc. make any commitment to update the information contained herein. This document is subject to change without notice.

CW-CDS-DS-USE-200901