

CLOAKWARE DRM SOLUTIONS

OMA DRM 2.0 CROSS-PLATFORM CLIENT ARCHITECTURE

INTRODUCTION

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

KEY FEATURES:

- Easy to use tools
- Control Flow Transformations
- Data Flow Transformations Key Hiding

KEY BENEFITS:

- Secures your software and IP in non trusted environments
- Reduces time to market for your application or device without compromising security

Supported Platforms:

- ANSI C and C++ for all major platforms
- Linux, Macintosh, Windows, Symbian
- Embedded devices



incorporate any level or type of security.

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:

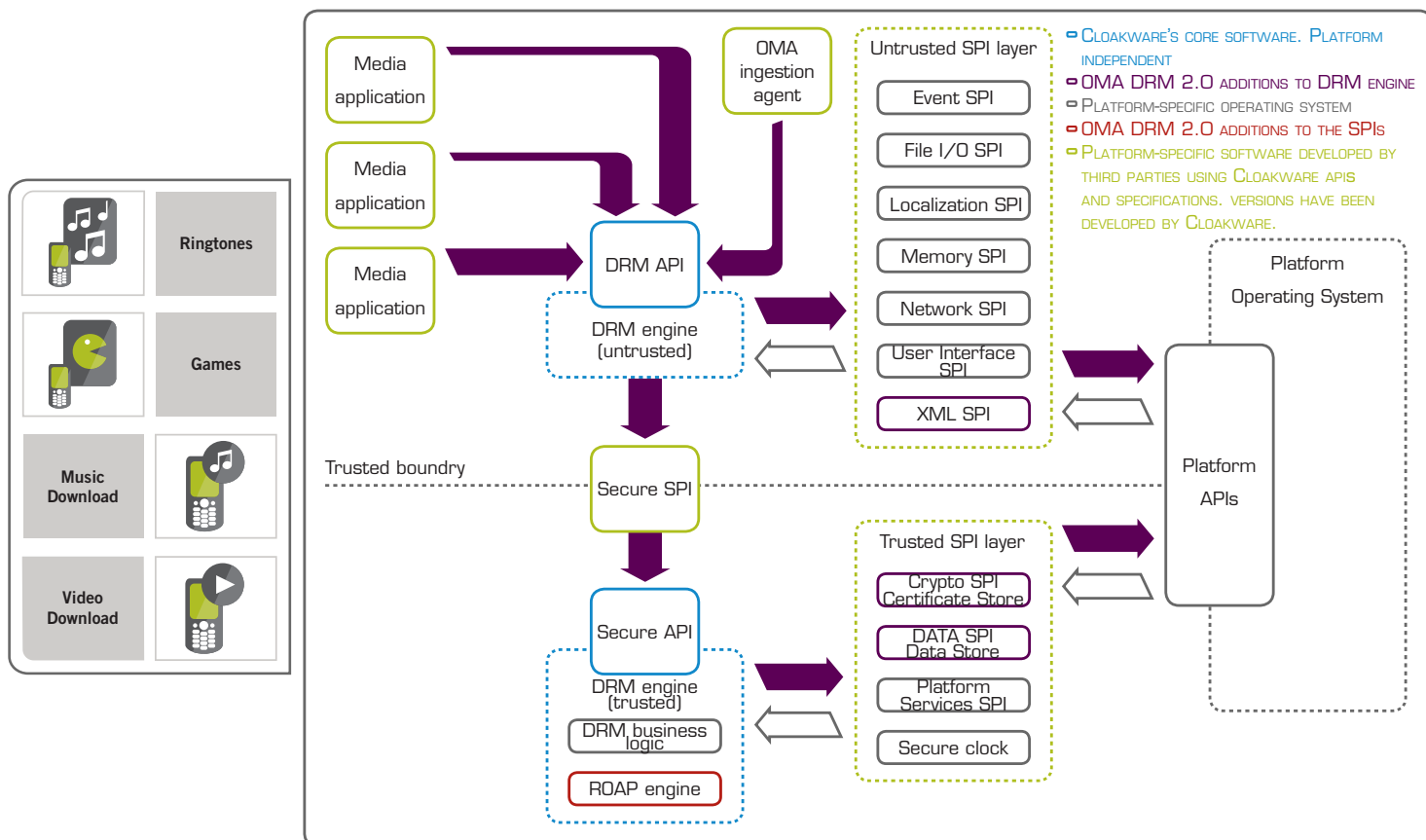
- **DRM Business Logic:** Evaluates license constraints and controls how OMA content is consumed. For content with valid licensing, this component enables access to content files.
- **Content Ingestion:** Handles OMA messages received on the device, including encrypting and storing content files, and 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.

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.