

Content Management License Administrator

A Compliance & Licensing Entity for
Open Mobile Alliance (OMA)
Digital Rights Management (DRM)
Release 2.0

admin@cm-la.com

CMLA Overview
November 2004

What is CMLA?

CMLA provides a 'trust model'
for OMA DRM Release 2.0

completing the content protection ecosystem

Content Protection Ecosystem

Content Providers

- **Will not release digital content without adequate protection and secure devices and applications**
- Seek to maximize content availability (need for interoperable solutions)
- Rely on legal means to protect against bad implementations

Service Providers

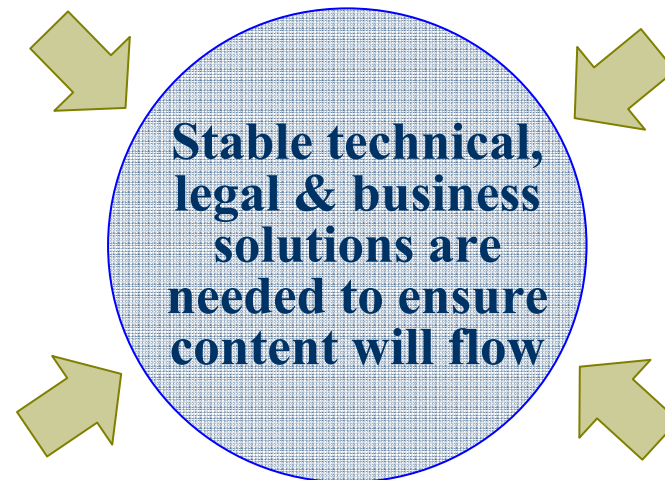
- **Will use content to maximize profits and retain subscribers**
- Ensure content released only to compliant devices or applications
- Do not want liability for faulty implementations

Device/Application Vendors

- **Will weigh cost and liability of DRM implementation** (materials, engineering, complexity, etc...)
- Availability of compelling content increases the market for media capable devices and applications.
- Rogue or negligent products put DRM system at risk (detrimental to trust)

Government

- **Will establish regulation if market forces fail to protect content without governmental mandate**



OMA DRM Release 2.0

- ◆ OMA has finalized release 2.0 of the only **Open-Standard DRM**
- ◆ Release 2.0's specification addresses the **Converged Media Space**
 - music, video, etc...
 - playback in multiple devices or applications
 - applicable across various device categories

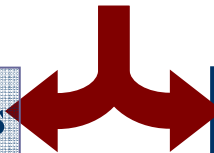
BUT

How do we complete the ecosystem so that content owners will release their content?

→ By establishing appropriate *trust mechanisms* AND ensuring implementations comply with an overall *trust model*

OMA Specifies the Trust Mechanisms

CMLA Provides the Trust Model



What is in a Trust Model?

OMA specifications enable

- ◆ Interoperability of Clients, Rights Issuers and Certificate Authorities
- ◆ Uniform processing of Rights Objects

CMLA's Trust Model provides

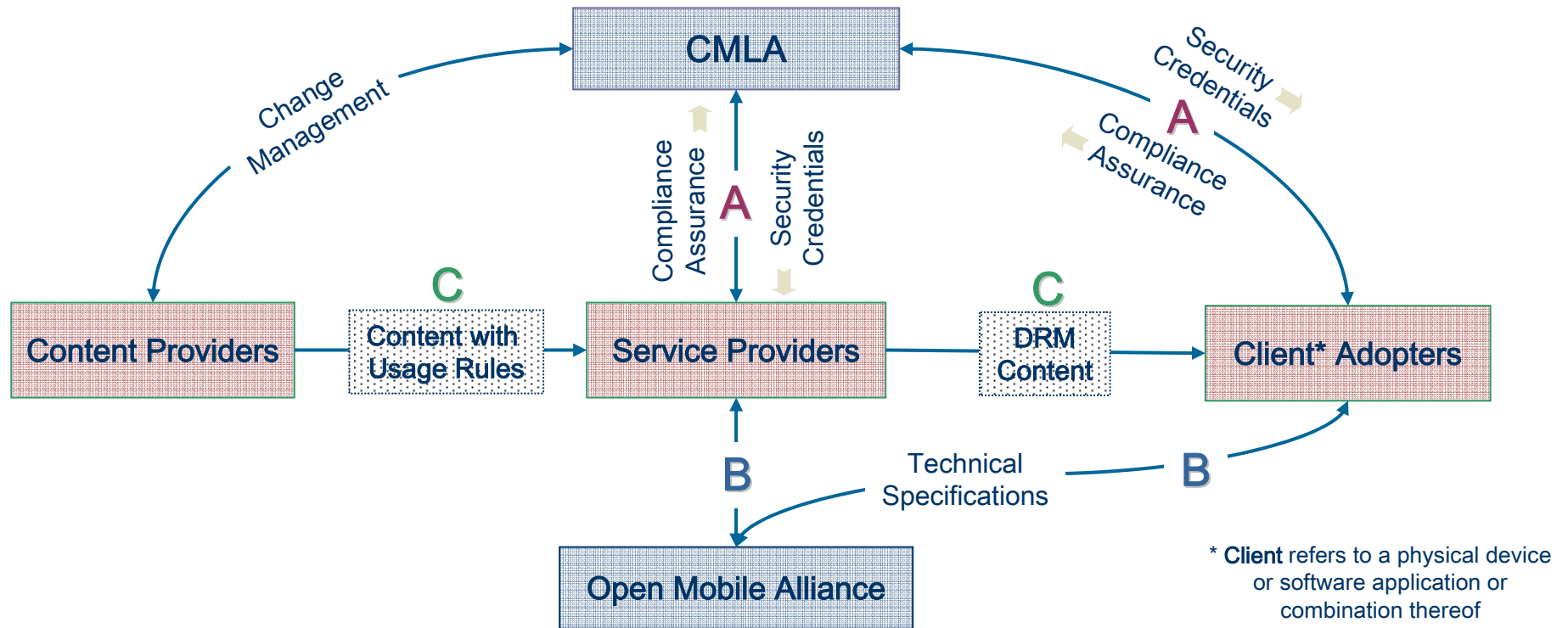
- ◆ Compliance and Robustness Rules
 - Establishing an implementation standard for devices, applications and services
- ◆ Understood and enforceable legal liabilities and obligations
 - for Client Adopters, Service Providers and Content/Rights Holders
- ◆ Keys and certificates provisioning
 - secure and renewable system for Client Implementations and Services Providers

CMLA Trust Model in the Content Ecosystem

A In return for compliance assurance CMLA provisions keying material

- to Client Adopters with which to manufacture devices or applications
- and service providers with which to provision rights

B DRM Release 2.0 technology specifications come from OMA



C OMA DRM protected content/rights are served to compliant devices

Compliance & Robustness Rules

◆ Compliance Rules

- Augment the OMA specifications by defining device, application and service implementations
- Govern the functionality of licensed products and services

◆ Robustness Rules

- Setting standards for how licensed products and services must be designed to make reverse engineering or other modification difficult
- Ensuring the
 - Confidentiality of client keys and integrity of certificates
 - Integrity of the elements of the specification and compliance rules
 - Prevention of unauthorized access to content

A NECESSARY ELEMENT OF ALL PROTECTION STANDARDS

A Tool-Box for Enforcement

◆ Revocation Enforcement

- Rules governing due process whereby devices, applications or services identified as having their keys compromised are revoked

◆ Contractual Remedies

- 3rd party beneficiary claims for cases of inadequate implementation

◆ Patent Infringement Claims

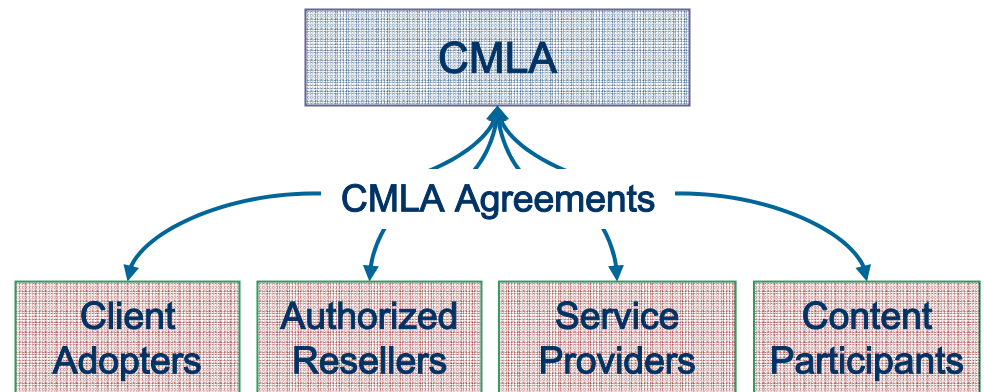
- Can be exercised against those who would create circumvention devices outside of the CMLA licensing framework

CMLA Issues Keys and Certificates

- ◆ CMLA
 - provides the necessary keys & certificates to Client Adopters
 - certifies/signs Service Provider's Public Keys
- ◆ In return, Client Adopters and Service Providers agree to implement per CMLA's Compliance & Robustness rules
- ◆ Adopter Agreements also cross-reference one another describing each party's mutual rights & commitments
 - 3rd party beneficiary rights
 - Revocation enforcement

CMLA License Agreements

- ◆ CMLA has created legal agreements that establish the Trust Model for OMA DRM Release 2
 - Content Participants
 - Client Adopter
 - Authorized Resellers
 - Service Providers



CMLA Agreement Provisions

Agreement Provisions	Content Participant	Service Provider	Client Adopter	CMLA Reseller
Keys, certificate and technology* licensing		✓	✓	
Continual evaluation and migration to newer versions of the OMA specifications	✓	✓	✓	✓
Key revocation procedures	✓	✓	✓	
Compliance and robustness obligations		✓	✓	✓
Adoption of material specifications	✓			
Third party enforcement (injunctive relief)	✓	✓	✓	

* **Technology = CMLA IP**

Going Forward

- ◆ Public Comment Period
 - CMLA is making the CMLA license agreements available for public comment beginning 1 November 2004 and ending 30 November 2004
 - To view and comment on these agreements please visit www.cm-la.com
- ◆ Licensing
 - CMLA intends to begin licensing soon thereafter, enabling the timely introduction of OMA DRM 2.0 & CMLA capable products and services.

CMLA Summary

- ◆ Creates global pool of trust for digital media devices and services
 - All products having “CMLA” DRM key can be trusted
 - CMLA defines & administers revocation policies and procedures
- ◆ Provides common compliance and robustness rules for implementations of an open DRM standard
 - Compliance and Robustness rules define the security level of implementations
 - Complements technical interoperability provided by OMA DRM 2.0
- ◆ Facilitates agreements between device/applications vendors, network operators, service providers, IT companies, and content providers
 - Reduces the complexity of bilateral licensing deals with content owners
- ◆ Encourages content providers to make their content available
 - Assures content providers that devices, applications and services provide a high barrier to unauthorized distribution as they all must implement compliance and robustness rules