Content Management License Administrator

CMLA: Frequently Asked Questions

1. What is the nature and purpose of CMLA? What is a trust model?
2. How does one participate in CMLA? Can I use CMLA to participate in new ecosystems such as UltraViolet™?
3. Who benefits from CMLA? What is the role of Founders?
4. What are the governance and operational principles of CMLA? Is there a level playing field for all parties relying on the CMLA trust model?
5. What is the scope of CMLA technical specification as distinct from the OMA DRM specifications? How is intellectual property handled?
6. How does CMLA affect interoperability?

Answers

1. What is the nature and purpose of CMLA? What is a trust model?

   The Content Management Licensing Administrator ("CMLA") is a Limited Liability Corporation ("LLC") created by four companies, Intel, Nokia, Panasonic and Samsung, to implement a "trust model" for the Open Mobile Alliance ("OMA") Digital Rights Management ("DRM") technical specification Version 2.0 standard and subsequent versions. The CMLA trust model defines a compliant implementation of this specification for use with a wide variety of digital client devices and applications (e.g. Smartphones, Tablets, CE Devices, Laptops, PCs and other digital clients and media distribution services. CMLA is not a standards body itself but enables the media ecosystem of the OMA standards body. The vision of CMLA is to enable a wide and trusted distribution of premium content to the large digital ecosystem. To accomplish this CMLA has these primary objectives:

   - Provide a justified confidence by participants in CMLA licensed devices, applications and services as being securely implemented, i.e. meeting CMLA Compliance and Robustness Rules.
   - Enablement of DRM content interoperability via utilization of the building blocks for interoperability provided by OMA DRM v2 and the consistent application of robustness and compliance between CMLA compliant products.
   - Enablement of an efficient and cost-effective trust model, including key and certificate generation and distribution system with CMLA required Compliance and Robustness Rules available to any manufacturer, software developer and service provider willing to join by agreement the CMLA.
   - Enablement of an effective method for the protection of the integrity of the CMLA system through practical and legal remedies, including certificate revocation, injunctive relief and financial sanctions.
   - Enablement of an efficient delivery of the trust function by use of continuous improvement methods to progressively reduce and minimize the cost of this function to implementers of the system.
   - Advance CMLA into future digital ecosystems by mapping/adapting the technical and business capabilities of CMLA and OMA DRM to these new ecosystems, i.e. support provided for Mobile Broadcast and the UltraViolet™ service from the Digital Entertainment Content Ecosystem LLC (DECE).

CMLA provides the following operational functions:

- A system of agreements setting out the rights, remedies and liabilities (including certain limitations of liability) of all participants wishing to utilize the CMLA trust model for the OMA DRM v2 specification
- Service Provider or Client Adopter (device manufacturer) robustness rules, setting forth requirements on the security of the services offered and device clients manufactured and application clients developed by CMLA licensees.
- Service Provider and Client Adopter compliance rules within which CMLA enabled clients and services must operate, in order to enable the intended content consumption within the user rights as authorized in each content Rights Object.
- A key generation, provisioning and certification system used by the Client Adopters and Service Providers.
- A root "certificate authority" serving as the trust anchor, which vouches for the authenticity of both client certificates and service provider certificates associated with the encryption keys used by CMLA Client Adopters and CMLA Service Providers.

For a detailed review of the CMLA trust model and its elements it is necessary to analyze the CMLA license agreements and CMLA Technical Specification, as well as the OMA DRM v2 specification.

2. How does one participate in CMLA? Can I use CMLA to participate in new ecosystems such and UltraViolet™?

   A company becomes a licensee of the CMLA system when they enter into one of the three participation agreements: Client Adopter Agreement, Service Provider Agreement or Content Participant Agreement. By signing these agreements a company joins the CMLA ecosystem and receives the rights and obligations associated with it.

   Similarly, a company wishing to join the UltraViolet™ ecosystem can simultaneously join both CMLA and UltraViolet™ by signing the chosen CMLA role agreement (and its UltraViolet™ Addendum) and its associated UltraViolet™ role agreement. CMLA is fully deployment approved in the UltraViolet™ ecosystem.

   Similarly, a company wishing to join the Mobile Broadcast ecosystem can join both CMLA and the Mobile Broadcast system by signing the CMLA role agreement and it's Mobile Broadcast Addendum.

3. Who benefits from CMLA? What is the role of Founders?

   In the broadest sense, all participants in the digital ecosystem can benefit as CMLA makes operational a standards-based DRM system targeted to enable trusted distribution of premium media. Consumers gain expanded digital media experiences. Other beneficiaries include:

   - Content Owners/Providers – CMLA provides a trusted environment to distribute premium content to consumers in digital form with its inherent added value proposition.
   - Client Adopters and Service Providers – CMLA provides the market with clear guidelines for robust and compliant DRM implementations making their DRM-enabled product development cycles faster and easier. CMLA opens up added market potential for their devices and services from enhanced consumer usability around premium content.
   - CMLA Founders have provided the financial resources necessary to form the LLC, start

up the operations and provide ongoing support and maintenance of the LLC. The Founders, in their capacity as members, govern the CMLA operational entity and processes described in the agreements. Founders have the ultimate authority regarding decisions of the CMLA, subject to the processes and requirements of the CMLA agreements. Founders must each also become a CMLA licensee and accept exactly the same obligations as any other participant, in order to provide CMLA compliant products (devices or applications) or services.

4. What are the governance and operational principles of CMLA? Is there a level playing field for all parties relying on the CMLA trust model?

   The CMLA operating principles have been developed with the intention of maximizing the trust of all participants in the value chain and providing as fair and neutral an operation as can be done within the objectives of CMLA. Both providers and consumers of content must have confidence in the CMLA trust model. Founders realize that trust is not achieved on the basis of a document or a declaration but earned but with collaboration, neutrality and non-discriminatory manner of making and applying its decisions. This must be balanced with the requirements to run CMLA operations efficiently and effectively over a long period of time. CMLA must also make decisions coming from the operational experience and feedback and requirements from all key constituencies maintaining a balance between the needs and priorities of adopters. Founders therefore have provided important participation to stakeholder groups in CMLA change management through the CMLA Advisory Board. Founders are bound by the same agreements as all other Service Providers, Client Adopters or Content Participants (as applicable) when they use the CMLA ecosystem for their products and services.

5. What is the scope of CMLA Technical Specification as distinct from the OMA DRM specifications and how is intellectual property handled?

   The technical foundation of the CMLA environment adheres to OMA DRM v2 specification. CMLA compliance is premised upon conformance with the OMA DRM v2 specification. The technology necessary to implement to the OMA DRM v2 specification is licensed by the relevant IPR owners and is not licensed by CMLA. For information about OMA IPR guidelines, interested parties must contact the OMA.

   CMLA does have technology it licenses to implement the CMLA trust model. CMLA has developed the CMLA Technical Specification that sets forth the technical requirements that must be met by CMLA licensees in order to provide device and application clients or services that are CMLA compliant. This specification generally deals with issues related to distribution and management of keys and certificates issued by the CMLA. Key generation and provisioning must comply with the CMLA-specified security requirements and involves a compliant central facility for the root Certificate Authority and technical and administrative arrangements for the generation and distribution of keys and certificates for use by the service providers and client manufacturers. CMLA generates and distributes millions of keys and certificates. CMLA also maintains a revocation mechanism which makes it possible to prevent further consumption of new content by devices whose keys have become compromised. As the OMA DRM v2 specification changes over time, the updates are reviewed for viability, security, backwards compatibility and other factors at an appropriate time following the change. CMLA may minimally interpret OMA DRM specifications for the purpose of correction of errors and omissions in the CMLA Technical Specification without incorporating additional functionality. Modifications of the CMLA Technical Specification including for error correction will balance multiple factors, including backwards compatibility and user convenience. The CMLA Technical Specification does not change or alter the

underlying OMA DRM specification in any way. CMLA does however advance as the OMA DRM specification advances. CMLA does support the OMA DRM specification version 2.1 for example.

In one material aspect the CMLA Technical Specification introduces additional functionality not shared by other (non-CMLA) OMA DRM v2 devices. This is a CMLA Trust Module adding an additional layer of trust in that devices that are able to respond to authentication challenges unique to CMLA will be recognized as coming from sources that have accepted the CMLA requirements regarding robustness and compliance. The Trust Module incorporates technology specially developed by CMLA to provide this necessary functionality for which patents exist ("CMLA IP"). An added benefit from including the Trust Module will be, subject to successful patent prosecution, the ability of CMLA to carry out legal IPR enforcement actions against parties using CMLA IP without signing license agreements. Such actions could be employed to stop such parties from making and selling circumvention devices. The ability to pursue such claims helps protect and enhance the success of the CMLA environment. The CMLA fee schedule does not include a royalty specific to the Trust Module. A license for the Trust Module is included in each of the Client Adopter, Service Provider, Content Participant, and Reseller license agreements. The cost for developing the Trust Module, including the patenting of IP, are reflected in the startup costs of the CMLA and will be recovered through the overall fee structure.

CMLA was developed to provide the business/legal and authentication system whereby trusted implementation in support of the OMA DRM v2 specification could be brought to market with confidence and new extensions could be enabled into new markets over time.

CMLA supports OMA DRM v2 specification but also extends its reach into new markets as opportunities arise. Founders also had active participation in the development of the OMA DRM 2.0 specification as did myriad other companies in the mobile digital ecosystem.

6. How does CMLA affect interoperability?

OMA DRM v2 provides the building blocks for interoperability through well-defined protocols and behaviors. However, DRM interoperability also contains an element of security measures. By introducing a common trust framework, CMLA seeks to improve DRM interoperability by introducing a system where devices from multiple vendors are expected to have equal access to DRM protected content because all CMLA devices conform to an agreed level of robustness and compliance. CMLA compliant devices and applications are also OMA DRM v2 compliant and therefore can be used in a non-CMLA environment.