

CMLA Overview and Answers

1. What is the nature and purpose of CMLA?

The Content Management Licensing Administrator (“CMLA”) is an LLC created by four companies, Intel, Nokia, MEI/Panasonic and Samsung, to implement a “trust model” for the Open Mobile Alliance (“OMA”) Digital Rights Management (“DRM”) technical specification version 2.0 standard. 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. cell phones, PDAs and PCs). CMLA does not replace or modify the specification, nor is it a prerequisite or requirement of the OMA DRM 2.0 specification. Other trust models may be created in addition to CMLA.

The overall objective of CMLA is to enable a wide and trusted distribution of premium content to the large digital ecosystem. To accomplish this overall objective CMLA has these additional goals:

- A justified confidence by participants in CMLA licensed devices, applications and services as being well 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 v2.0 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.

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 2.0 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.
 - The licensing of a CMLA Technical Specification for the implementation of CMLA licensed clients and services.

- 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 2.0 specification. This document is only a brief introduction.

2. Is CMLA a standards body?

CMLA is not a standards body. CMLA is a limited liability corporation formed by the Founders referenced in (1) above to provide a trust model for the OMA DRM V2.0 enabler release with its specific functions being those also referenced in (1) above. CMLA however, encourages CMLA licensee participation in OMA activities and the CMLA advisory board (CAB). Details of CAB mechanisms are set out in the CMLA license agreements.

3. What is a trust model?

We use the term ‘trust model’ to refer to the full processes and implementation necessary to complete a system in order to provide the level of confidence to all participants with assets at risk to place their trust in using the system to transact business with their assets. With CMLA the implementation described in (1) above provides the added elements in addition to the OMA DRM 2.0 specification to provide the trust necessary for content participants to risk their media assets for distribution within the CMLA ecosystem and for service providers and client adopters to make service and product line investments to enable the CMLA ecosystem.

4. Who will ultimately benefit from the CMLA operation?

In the broadest sense all participants in the digital ecosystem can benefit as CMLA makes operational the first standards-based DRM system targeted to enable trusted distribution of premium media. This will bring to consumers the realization of digital system benefits for premium media. Other beneficiaries will be:

- Content Owners/Providers – CMLA will provide a trusted environment to distribute their content to consumers in digital form with its inherent added value proposition.
- Client Adopters and Service Providers – CMLA will provide them with a market environment with clear guidelines for robust and compliant DRM implementations making their DRM-enabled product development cycles faster and easier. CMLA will also open up added market potential for their devices and services from enhanced consumer usability around premium content.
- End Users – Consumers will benefit from the expected availability of exciting premium content and introduction of novel usage models, which CMLA is aiming to enable by its trusted DRM environment. CMLA has been formed to realize the consumer’s long awaited desire to have access to their preferred content (such as music, video clips and games) in devices that have been designed to meet their user expectations.

5. How does one participate in CMLA?

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. In signing one of these agreements the party is accepting the CMLA trust model and agreeing to be bound by the rights and obligations associated with it.

6. Are there other participation categories? What is the role of Founders? What is the role of Founding Contributors?

CMLA is organized as a legal entity – it is registered as CMLA, LLC in the State of Delaware, USA – with four founding “members”, the founders of CMLA. CMLA is not currently contemplating any additions to its founding members. Membership in the LLC entity is not required for participation as a CMLA licensee.

CMLA Founder Role: Intel, Nokia, Panasonic (Matsushita Electric Industrial Co.) and Samsung have provided the financial contributions and resources necessary to form the LLC and start up the operations of CMLA. The Founders, in their capacity as members, govern the CMLA operational entity and processes described in this document. Founders have the ultimate authority regarding decisions of the CMLA, subject to the processes and requirements of the CMLA agreements.

Founders have permanent representation in CMLA change management and decision making processes but Founders do not have double representation (i.e. they cannot both act as CMLA advisory board (“CAB”) representatives on behalf of Client Adopters or Service Providers and participate in the CMLA advisory board as Founder).

The four 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.

CMLA Founding Contributor Role: Founders extended an invitation to OMA members as representatives of the three key industry segments most relevant to CMLA to join in the CMLA development process as Founding Contributors. Thirteen companies joined the Founders in this process. The industry segments represented were service providers, manufacturers and content providers. During the development phase Founding Contributors made valuable contributions in refining the CMLA trust model. They also made very significant contributions in drafting the license agreements and technical documentation required by the CMLA ecosystem. For development efficiency reasons, it was not possible to open the process to all interested parties. These Founding Contributors have played an important role in the generation and development of the CMLA trust model, however, this Founding Contributor role is completed with the public availability of the CMLA documentation for adoption.

The Founding Contributors 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..

CMLA Participant Role: CMLA participants fall into three major categories, with a particular standard agreement governing the rights and obligations of any participant in their respective category. These categories are

- Content Participant
- Service Provider
- Client Adopter

Additional categories is are 1) Authorized Resellers who are entities enabled to receive Licensed Products, Licensed Components, Licensed Services and/or Licensed Elements from CMLA Client Adopters and/or CMLA Service Providers and to distribute the same to other CMLA Client Adopters and/or CMLA Service Providers, and 2) Developers (either for Client Adopters or Service Providers) who by signing Developer Addendums to either the Client Adopter Agreement or the Service Provider Agreement are able to develop Licensed Products, Licensed Components, Licensed Services or Licensed Elements for CMLA Client Adopters or CMLA Service Providers respectively.. The issues dealt with in the three category related standard agreements are briefly described in section 7 below.

7. 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. This section of this document describes how CMLA plans to approach core questions that are of interest to stakeholders.

The founders realize trust is not something one can achieve on the basis of a document or a declaration and that CMLA needs to earn the trust of all stakeholders in its operations, particularly in its neutrality and non-discriminatory manner of applying its decisions. This requirement to build trust must be balanced with the requirements to run CMLA operations efficiently as well as the need to be able to make decisions when needed. CMLA must be able to adjust the operational and administrative plans of CMLA and to make business decisions related to CMLA success factors – e.g. those affecting the acceptance and trust of CMLA by the relevant stakeholders. CMLA must also be able to make decisions in light of operational experience and feedback and requirements from all key constituencies - often requiring a choice to be made while maintaining a balance between conflicting priorities.

The Founders' response to the trust and impartiality needs of the CMLA ecosystem participants is to provide important participation to stakeholder groups in CMLA change management through the CMLA user groups and CMLA Advisory Board and to provide information that enables the stakeholders to verify the way the CMLA is run and the direction it is taking. Furthermore, 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.

The main vehicle for participation in the CMLA change management is the CMLA Advisory Board ("CAB"), consisting of three representatives from each of the Service Providers, Client Adopters and Content Participants, plus the four

Founders. There thus are a total of thirteen members in the CAB. While the decisions of CMLA on issues referred to the CAB are finally taken by the CMLA, the CAB procedures set forth in the agreements contain very tight guidelines ensuring a transparent process, a very substantial review and contribution by the CAB and, in certain circumstances, an arbitration process for challenging changes. Taken together, the measures adopted provide a level of comfort to the main stakeholder groups about the evenhanded governance of CMLA.

Have all Founding Contributors concerns been satisfied during the development process? CMLA has attempted to consider all industry segment viewpoints in the development of CMLA. On certain issues, however, there have been divergent opinions on what would be best for the long-term design of CMLA. The CMLA Founders have seriously considered all viewpoints and then made decisions it determined were best for the long-term ability of CMLA to meet its objective of enabling wide and trusted distribution of premium content to the large digital ecosystem. The change process outlined above will continue to be a forum for deliberation on issues that may be of continuing concern to participants.

8. 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 2.0 Specification. CMLA compliance is premised upon conformance with the OMA DRM 2.0 specification. The technology necessary to implement to the OMA DRM 2.0 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 however have technology it licenses to implement the CMLA trust model. CMLA has developed a 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 will generate and distribute 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.

In the event that the OMA DRM 2.0 specification changes over time, the updates will be reviewed by the CAB 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 will not change or alter the OMA DRM 2.0 specification in any way.

In one material aspect the CMLA Technical Specification introduces additional functionality not shared by other (non-CMLA) OMA DRM 2.0 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 patent applications have been filed ("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 should help 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.

9. Why wasn't CMLA developed and launched within OMA? What is CMLA relationship with OMA?

OMA is chartered to develop technical specifications that enable interoperable services and applications. CMLA was formed to address the issues beyond OMA scope such as compliance and robustness requirements in devices, applications and services implementing OMA DRM 2.0 specifications.

The development of CMLA was spurred by the observation of the founder companies of the need to establish a trust model in support of the OMA DRM 2.0 specification. It was deemed important to have this trust model available to implementers of the OMA DRM 2.0 specification shortly after the specification was formally ratified by OMA.

CMLA supports OMA DRM 2.0 and has adhered to the OMA specification. Founders have active participation in the development of the OMA DRM 2.0 specification.

10. How does CMLA affect interoperability?

OMA DRM 2.0 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 2.0 compliant and therefore can be used in a non-CMLA environment.

11. What are the main provisions of the participant agreements?

There is no substitute for close reading and legal analysis of the agreements issued by CMLA. Each party must take an informed decision on whether the agreements and the commercial solutions reflected in them are appropriate for that party. The following list is a high-level overview of matters addressed in the agreements. There is much in common

between the three principle agreement types, and it is important to understand the totality of how the agreements work together.

- Definitions: There are many carefully defined terms used in the agreements
- Licenses: An important license aspect relates to the “Necessary Claims” patent licenses granted by the Founders and the CMLA to each party who becomes a licensee. This license relates only to the CMLA Technical Specification and is subject to certain important limitations. As an example the license does not cover any licenses required to implement the OMA DRM specifications. There additionally are copyright and trade secret licenses. Parallel reciprocal non-assertion covenants from licensees are also included in the agreement.
- The CMLA Advisory Board: The purpose, role, processes – including arbitration - and each member category’s representation at the CAB is set forth in the agreements. Importantly, the agreements set forth requirements on CMLA to publish pending proposals and the changes made by CMLA.
- Fees: Each participant actively taking part in the CMLA ecosystem will be required to pay fees linked to 1) annual administrative fees, 2) unit fees related to keys and certificates, and 3) OCSF responder (Service Providers only) activity.
- Audit provisions are included for verification of certain information reported by CMLA participants and for product or service compliance.
- Confidentiality: The CMLA agreements involve special obligations relating to “Highly Confidential Information”, primarily the Client Adopter and Service Provider keys, to prevent their unauthorized dissemination or other misuse.
- Term: The initial term is 10-years and is renewable and terminable as set forth in the agreements.
- Limitations of liability: Besides exclusions of certain kinds of liability, there are important provisions setting certain predetermined fixed financial damages and/or maximums (caps) for certain kinds of liabilities that can arise under the agreements. These limits have been developed to provide both a meaningful remedy to encourage parties to comply with the contractual obligations and to manage the level of liability exposure that otherwise might at least in theory be unlimited or disproportionate.
- Injunctive relief: Content Participants have been provided a set of rights, subject to important limitations and safeguards, to obtain injunctive relief (under provisions called “Third Party Beneficiary Rights”), in certain limited circumstances as more fully set forth in the agreements. Content Participants retain their statutory and other judicial remedies in certain circumstances.
- Revocation of certificates: If either the Client Adopter and/or Service Provider keys have been compromised, the respective client certificates and/or Service Provider certificates can be revoked. This revocation possibility also is subject to important limitations and safeguards set forth in the agreements, including arbitration.
- Robustness rules: Service Providers (as rights issuers) and Client Adopters (as device manufacturers or application developers) must agree to implement a technical environment where keys and certificates (and CMLA / OMA DRM protected content) are stored and handled in ways that reduce the risk of compromising either the keys/certificates or the content.
- Compliance rules: Service Providers and Client Adopters must further agree to implement the technical environments of service infrastructure and devices in a manner designed by CMLA for the purpose that the business rules imposed by CMLA Rights Issuers achieve the intended result in actual use and consumption situations. Of particular importance in the Compliance Rules are the tables X1/X2 and Y1/Y2 which describe what kinds of outputs and interoperability with other protection systems are supported by CMLA devices either by default (X1, Y1) or through Rights Issuer express authorization (X2, Y2)

12. What is the CMLA development and availability schedule?

The CMLA Founders group was officially formed in January, 2004 and CMLA was formally announced publicly on February 4, 2004. In late February the Founding Contributors group was first formed to start the collaboration phase and included a public commenting period in Q4, 2004 in order to receive comments from the full community of interested parties. CMLA is now making the licensing agreements available for adoption by interested entities.

CMLA also developed the license administration and key generation infrastructure in parallel with the licensing agreements development and is now taking and delivering development key and certificate orders and production key and certificate orders from licensees.

13. Where is CMLA based?

The management of CMLA's operations is outsourced to a professional management company that has special expertise in this area. This company is License Management International, LLC (LMI) . LMI can be contacted at (408) 776-2014. CMLA is an LLC (Limited Liability Company) organization; it has no employees or physical location of its own.

14. What will be the CMLA cost allocation and revenue principles – is it a “nonprofit” entity or will it generate a return on investment to the Founders?

The CMLA is not a nonprofit organization. CMLA fee structure is based on a cost recovery model. CMLA needs to recover its operational costs and it must recover the initial investment that the founders have advanced to create the CMLA and to get it up and running. Any material investment that the CMLA may need to expend in the future must also be recovered. CMLA currently plans to recover investments during periods of up to five years. Also, CMLA may need to reserve some funds for contingencies but its essential nature will be to set its fees so that they, over time, recover costs, investments and contingencies but do not generate a sustained surplus.

The CMLA will operate a fee model that includes administrative charges, key generation/distribution charges, and OCSP responder charges. These fees, over time, enable the CMLA to recoup its investments and costs. The CMLA fee model will necessarily be based on multiple assumptions so that, as the CMLA cost and revenue development unfolds, those assumptions will have to be adjusted and the fee structures with it. The cost recovery principles are however designed so that they should remain in place for the long term.

The CMLA plans to make available, from time to time, information it considers appropriate to provide comfort to CMLA licensees regarding how its financial operations reflect the foregoing principles.