Content Management License Administrator

Licensing: Frequently Asked Questions

Answers

1. 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. The following is a high-level overview of matters addressed in the agreements. There is significant commonality between the three agreement types; it is important to understand 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 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.
   - Changes: Procedures are provided for making amendments to the CMLA Technical Specification, Compliance Rules, or Robustness Rules. The agreements also set forth requirements on CMLA to publish pending proposals and any 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) OCSP 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)

2. What are compliance and robustness rules?

   Service Providers (as rights issuers) and Client Adopters (as device manufacturers or application developers) must agree to implement a robust technical environment where CMLA protected content and associated security elements are stored and handled in ways that reduce the risk of compromising such data.

   Service Providers and Client Adopters must further agree to implement the technical environments of a service infrastructure and devices (or applications) 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 the outputs and interoperability with other protection systems that can supported by CMLA devices either by default (X1, Y1) or through rights issuer express authorization (X2, Y2).

3. How is robustness achieved in the system?

   Service Providers and Client Adopters are obligated by the CMLA License agreement to develop services and/or products that conform to the CMLA Robustness and Compliance rules set forth in the respective CMLA License agreements. The CMLA Compliance/ Robustness rules are based on compliance and robustness rules used by hundreds of licensees in other content protection initiatives of a similar nature, such as compliance/ robustness requirements for CPRM/CPPM, HDCP, DTCP and others.

   These rules were developed also with the help of a group of Founding Contributors that included implementers, service providers, broadcasters and content providers. The CMLA License agreements have provisions for remedies to address breaches of compliance/

robustness which include revocation of keys or certificates.

4. Where are CMLA implementations verified and certified?

   CMLA licensees are responsible for ensuring their implementations meet CMLA compliance and robustness rules. CMLA licensees create a check list to verify the process used to meet CMLA compliance and robustness requirements. CMLA licensees may use the CMLA development system to verify their implementations.

5. How are the different levels of compromise severity handled?

   The steps of correction and enforcement are described here.

   Correction: When CMLA receives a complaint regarding a CMLA licensee’s product or service it promptly takes the following steps: (i) notifies licensee of problem and provides all information received by CMLA and sets expectation of continued dialogue until complaint resolved; (ii) reviews CMLA licensee corrective action plan; (iii) provides oversight until correction action plan completed. It is anticipated that a CMLA licensee corrective action plan may include updates (software or otherwise) or other remedial solutions; If the complaint identifies a specific device private key or rights issuer private key, CMLA may encourage the licensee to agree to revoke the certificate corresponding to the identified key. CMLA license agreements also contain a dispute resolution process.

   Enforcement: CMLA license agreements provide for different types of enforcement, in the event a complaint is not resolved. In the event, CMLA and/or its Eligible Content Participants determine enforcement is required, CMLA may initiate the process to enforce the CMLA license agreements. Enforcement includes both revocation and injunctive relief, in addition to other contractual remedies. In addition, CMLA license agreements give Content Participants third party beneficiary rights providing Content Participants with the ability to seek injunctive relief in certain circumstances. The CMLA licenses provides for substantial liquidated damages for certain material breaches of the CMLA license agreements. Finally, CMLA content owners may have additional (extra or outside the CMLA license) remedies available to it (e.g., for copyright infringement caused by the defective products or services).

6. What is the role of CMLA in the case of leaking device implementations?

   CMLA is very focused on maintenance of the integrity of its trust model and therefore may take the following actions to address leaking implementations, as needed:

   1. CMLA has the ability to change the CMLA Technical Specifications and compliance and robustness rules under certain circumstances, including changes to meet new threats. CMLA licensees are required to comply with such changes within specific time periods.
   2. In instances where device or service implementations have not met the CMLA specification or compliance/robustness requirements, and the CMLA licensees have not corrected their problems, within the cure period, if applicable, CMLA may exercise its contractual rights to enforce the CMLA license agreements and Eligible Content Participants may exercise their third party beneficiary rights in certain circumstances. Examples of remedies include injunctive relief (from further manufacture), revocation of device/rights issuer certificates, liquidated damages and/or termination of the CMLA agreement.
   3. CMLA may enforce its intellectual property rights in the event of non-licensed products/services or circumvention devices.

7. Who is responsible to fix leaking device implementations?

   Each CMLA licensee has the ability to respond to allegations of non-compliant implementations which they have brought to market. CMLA's role in this correction process is to help expedite these corrections or to take other remedial action as permitted under the CMLA License Agreements.

8. Explain the CMLA device revocation procedure.

   The CMLA revocation process is defined in the Agreements (Section 9). The revocation process is initiated when/if the revocation criteria have been met and CMLA is made aware of the problem. At a high level, the revocation criteria require that a private key (device or rights issuer) has been disclosed in a manner not permitted under the CMLA License Agreement. A licensee is notified that one or more of its CMLA implementations has been compromised such that a private key has been disclosed and either (i) the licensee agrees to revoke the private key; or (ii) the licensee can dispute the allegations in which case the matter is referred to expedited arbitration.

9. Can CMLA devices receive software updates rather than revocation?

   CMLA licensees may use a software update to correct a breach of the compliance/robustness rules in products already deployed. Such an update must be done according to the CMLA license agreements. CMLA would anticipate a licensee would use whatever best methods it can to expeditiously remedy a breach of the requirements of the CMLA technical specification, license agreements, including compliance and robustness rules. This being said, there still could be instances where revocation of keys/certificates is required.