

CMLA Service Provider Agreement

Date: 2009-12-18
Version: 1.4-20091218

CMLA Founders - Contact Information
admin@cm-la.com

**CMLA
Service Provider Agreement**

This CMLA Service Provider Agreement (“Agreement”) is effective as of the date of the last signature below (the “Effective Date”), by and between Content Management License Administrator, LLC. (“CMLA”), a Delaware limited liability company, the Founders, designating CMLA, as an attorney in fact, and the “Service Provider” named below (as used herein Service Provider includes its Participating Affiliates, if applicable):

Name of Service Provider

Description of Service Provider’s Business

Name of Main Contact Person

Main Contact person’s
phone no.

address,

fax no.,

email address

Location of Service Provider’s principal offices

State or Country of Incorporation

Year of Incorporation

RECITALS

WHEREAS, a group of companies identified below as the Founders desire to promote the use and interoperability of OMA DRM Specification 2.0 implementations;

WHEREAS, the Founders have therefore developed the CMLA Technical Specification (as defined below) for use with implementations of the OMA DRM Specification 2.0 (and its approved successors), together with a public key infrastructure, key generation, management and licensing/compliance framework for the purpose of furthering these goals and protecting certain digital content from unauthorized interception, transmission and copying, and the CMLA has developed or obtained the CMLA IP (as defined below) for the purpose of better protecting its interests in connection with the CMLA Technical Specification;

WHEREAS, the Founders have licensed certain rights pertaining to the CMLA Technical Specification to CMLA and authorized CMLA to further license those certain rights in the CMLA Technical Specification and administer such licenses and whereas the Founders and CMLA hereby license certain necessary patent claims, if any, directly to Service Provider and its Participating Affiliates, (as defined below), through this Agreement;

WHEREAS, the parties have agreed to comply with all obligations set out herein;

NOW THEREFORE, in consideration of the foregoing promises and the covenants and agreements set forth herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. DEFINITIONS

- 1.1 “Affiliate” means with respect to any person or entity, any other person or entity directly or indirectly controlling or controlled by or under direct or indirect common control with such person or entity. “Control” as used in this definition means the possession of beneficial ownership of more than fifty percent (50%) of the stock or other similar interest entitled to vote for election of the Board of Directors or similar managing authority.
- 1.2 “Authorized Reseller” means an entity that has executed a CMLA Authorized Reseller Agreement with CMLA.
- 1.3 “Authorized Reseller Agreement” means the CMLA Authorized Reseller Agreement in the form set forth in the sample agreement on the CMLA website between CMLA and Authorized Reseller.
- 1.4 “Certificate Revocation List” means a data object providing revocation status information for Device Certificates or Rights Issuer Certificates issued by CMLA.
- 1.5 “Client Adopter” means any entity and its Participating Affiliates, (including a Founder), that has executed an Client Adopter Agreement with CMLA provided that Client Adopter or its Affiliates that wish to participate as Content Participants or CMLA Service Providers may only do so pursuant to either Content Participant Agreement or a Service Provider Agreement.
- 1.6 “Client Adopter Agreement” or “CMLA Client Adopter Agreement” means any CMLA Technology License Agreement entered into by CMLA, Founders and a Client Adopter for the implementation of CMLA Technical Specification in a Participating Product Implementation, Licensed Product and/or Licensed Component for the protection of Digital Content in the form available on the CMLA website, and any other CMLA Technology License Agreement that includes licensing and covenant provisions which are not materially different than those embodied in the sample agreements available on the CMLA website.
- 1.7 “Client Adopter Transport Keys” has the same meaning as set forth in the CMLA Technical Specification.
- 1.8 “CMLA Client Adopter” means a Client Adopter or Fellow Client Adopter.
- 1.9 “CMLA Device Key Material” means Device Certificate and Device Private Key.
- 1.10 “CMLA IP” means the proprietary technology owned and licensed by CMLA pursuant to a CMLA Technology License Agreement, and as described with specificity in the CMLA Technical Specification.
- 1.11 “CMLA Service Provider” means the Service Provider and/or any Fellow Service Provider.

- 1.12 “CMLA Technical Specification” means the specification available under a CMLA Technology License Agreement from CMLA entitled CMLA Technical Specification, and updates if any approved during the term of this Agreement.
- 1.13 “CMLA Technology Licensee” means a party to which the CMLA Technical Specification is licensed pursuant to a CMLA Technology License Agreement.
- 1.14 “CMLA Technology License Agreement” means any of: a Service Provider Agreement with/without Developer Addendum, Content Participant Agreement, Client Adopter Agreement with/without Developer Addendum and a CMLA Authorized Reseller Agreement and associated Compliance and Robustness Rules and other exhibits thereto.
- 1.15 “Compliance Rules” means the technical requirements set out in Exhibit A hereto, which are applicable to a Participating Rights Issuer Implementation and a Licensed Service.
- 1.16 “Compliant” means, as applicable,(i) for a Client Adopter, that which (a) implements the mandatory portions of the CMLA Technical Specification, (b) complies with the Compliance Rules set forth in Exhibit A to the Client Adopter Agreement; and, (c) complies with the Robustness Rules set forth in Exhibit B to the Client Adopter Agreement; (ii) for a Service Provider, which (a) implements the mandatory portions of the CMLA Technical Specification; (b) complies with the Compliance Rules set forth in Exhibit A to the Service Provider Agreement; and, (c) complies with the Robustness Rules, set forth in Exhibit B, to the Service Provider Agreement.
- 1.17 “Confidential Information” means any and all information relating to the CMLA Technical Specification or CMLA’s or any Founder’s business practices relating to the CMLA Technical Specification, (a) which is made available to Service Provider directly by CMLA or its designees or representatives, Founders or by any CMLA Service Provider, Content Participant or Client Adopter prior hereto or during the term of this Agreement, including, without limitation, specifications, software, hardware, firmware, documentation, designs, flow charts, technical data, outlines, blueprints, notes, drawings, prototypes, templates, systems, manuals, know-how, processes and methods of operation, trade secrets, business plans, strategies, concepts, research, data bases, client or customer lists, financial data, other data or information that relates to CMLA’s or a Founder’s past, present or future research, development or business activities, and any other sensitive material belonging to CMLA or any Founder, and/or (b) which is marked “confidential” when disclosed in written form or indicated as “confidential” when disclosed orally, and confirmed in writing within thirty (30) days to be confidential.
- 1.18 “Content Participant” means an entity and its Affiliates that has executed a Content Participant Agreement with CMLA.
- 1.19 “Content Participant Agreement” means a Content Participant Agreement entered into by CMLA, Founders and a provider of Digital Content on substantially the terms set out in the sample agreements on the CMLA website.
- 1.20 “Contributor” means an entity that has executed a Founding Member Contribution Agreement or Contribution Agreement with CMLA.

- 1.21 “Developer Addendum” means a development addendum to the Client Adopter Agreement and/or Service Provider Agreement entered into by CMLA, Founders and a CMLA Technology Licensee
- 1.22 “Development Keys” means the key pairs and certificates issued from the Development System. These key pairs and certificates provided to a CMLA Technology Licensee are not interoperable with production PKI and the use is limited to development and testing of Licensed Service and License Service Elements only.
- 1.23 “Development System” means the development version of the public key infrastructure (“PKI”) as defined and instantiated by CMLA.
- 1.24 “Device Certificate” means a digitally signed certificate issued by CMLA which includes the Device public key that corresponds to a Device Private Key, as specified in the OMA DRM Specifications.
- 1.25 “Device Private Key” means a cryptographic value used by a Licensed Product or Licensed Component for decryption and signing operations, as specified by the OMA DRM Specifications.
- 1.26 “Digital Content” means materials commercially distributed in digital form including, but not limited to, games, software offerings, sound recordings or audiovisual works, which may only be reproduced, distributed, transmitted or performed with the authorization of the Content Participant or other entity or individual owning or having the right to license the rights therein.
- 1.27 “Eligible Content Participant” means a Content Participant that: (1) either (i) caused or permitted actual distribution or transmission of a minimum of five million United States Dollars of its Digital Content via Participating Product Implementation(s) or Participating Rights Issuer Implementation(s) in the preceding calendar year or (ii) caused or permitted actual distribution or transmission of its Digital Content via Participating Product Implementation(s) or Participating Rights Issuer Implementation(s) via at least fifteen (15) wireless carriers and in at least fifteen (15) countries in the preceding calendar year; and (2) is not in breach of any material term or condition of its Content Participant Agreement, which breach has not been cured, or is not capable of cure, within thirty (30) days of Content Participant’s receipt of notice thereof by CMLA.
- 1.28 “Fellow Service Provider” means any entity (other than the Service Provider) that has executed a Service Provider Agreement.
- 1.29 “Founder(s)” means Intel Corporation, a Delaware company, whose principal offices are at 2200 Mission College Blvd., Santa Clara, CA 95052, Panasonic Corporation a Japanese corporation having its principal place of business at 1006 Kadoma, Kadoma, Osaka 571-8501 Japan, Nokia Corporation, a Finnish company, whose principal offices are at Keilalahdentie 4, FIN-02150 Espoo, Finland and Samsung Electronics Co., Ltd., a Korean corporation having its principal place of business at 416 Maetan-3 Dong, Yeongtong-Gu, Suwon-City, Kyungki-Do, Korea.
- 1.30 “Highly Confidential Information” means information that is marked “Highly Confidential Information” when disclosed, pursuant to the Change Control provisions in Section 3 herein.
- 1.31 “Licensed Component” means those portions of a component, such as an integrated circuit, circuit board, or software module that (i) are manufactured and distributed under a CMLA

Technology License Agreement, (ii) are designed solely to be assembled into a Licensed Product and which is assembled into a Licensed Product, and (iii) embody a portion of the CMLA Technical Specification, but which by itself may not be Compliant.

- 1.32 “Licensed Product” means those portions of a device or hardware or software product manufactured or distributed under license from CMLA that implement the mandatory portions of the CMLA Technical Specification and that are designed solely to be integrated into a Participating Product Implementation and which are integrated into a Participating Product Implementation.
- 1.33 “Licensed Service” means those portions of a service performed and distributed under license from CMLA that implement the mandatory portions of the CMLA Technical Specification and that are designed solely to be integrated into a Participating Rights Issuer Implementation and which are integrated into a Participating Rights Issuer Implementation.
- 1.34 “Licensed Service Element” means those portions of a component such as a software module, that are (i) manufactured, and distributed under a CMLA Technology License Agreement (ii) are designed solely to be integrated and which is integrated into a Licensed Service, and (iii) embody a portion of the CMLA Technical Specification, but which by itself may not be Compliant.
- 1.35 “Necessary Claims” means those claims of patents or patent applications, under which, CMLA, any Founder or any CMLA Technology Licensee, or an Affiliate owns, controls or otherwise has the right, at any time during the term of this Agreement, to grant licenses within the bounds of the scope of use set forth in Section 2.2 of this Agreement that are necessarily infringed by those portions of Licensed Products, Licensed Components, Licensed Service or Licensed Service Element which implement the mandatory portions of CMLA Technical Specification. Notwithstanding anything else in this Agreement, "Necessary Claims" shall not include (1) any claims relating to aspects of any technology, codec, standard or product not disclosed with particularity in the CMLA Technical Specification even though such technology, codec, standard or product may be mentioned in the CMLA Technical Specification or required by the Compliance or Robustness Rules; (2) claims relating to implementation of the OMA DRM Specification, version 1.0, 2.0 and subsequent versions, if any, (even though such OMA DRM Specifications, version 1.0, 2.0 and subsequent versions, if any, may be mentioned or required by the CMLA Technical Specification), (3) claims relating to a standard or standards developed, administered, or offered, by an industry group consisting of two or more legal entities or promulgated by official standardization agencies or bodies; (4) other copy protection, compression, encoding or decoding ability or tamper resistance technology (even though such technology, standard or product may otherwise be mentioned or required by the CMLA Technical Specification); (5) claims which could be practiced in an implementation of a Licensed Product, Licensed Component, Licensed Service or Licensed Service Element in compliance with the CMLA Technical Specification where an alternative implementation exists that would not infringe such claim(s) (even if in the same patent as Necessary Claims); (6) claims that read solely on any implementations of any portion of the CMLA Technical Specification that are not within the bounds of the scope of use set forth in Section 2.2 or the equivalent section of the relevant CMLA Technology License Agreement(s); (7) claims related to data embedding, content formats and content downloading and delivery (other than as described with particularity in the CMLA Technical Specification); (8) claims which, if licensed, would require a payment of royalties or other consideration by the licensor to unaffiliated third parties; (9) claims relating to watermarking or waterscrambling technology, semiconductor and semiconductor manufacturing technology, compiler technology, programming languages and object-oriented

- technology, operating system, middleware and database technology, networking, intranet, extranet, Internet technology, telecommunications network technology (for example any technology relating to equipment, handsets, signal transmission) access control system technology, card access management technology, electronic payment technology, conditional access for television technology, television e-commerce access technology, broadcast stream access technology; (10) claims related to key management technology for use in encryption or signature applications, encryption technology or electronic signature technology, except as may be necessary or required for the use, development, manufacturing, implementation, sale (offer for sale), license and distribution of CMLA keys, self-generated CMLA keys, any aspect of CMLA technology, including, but not limited to key management software for use in encryption or signature applications licensed to CMLA by third parties, the CMLA Technical Specification, Licensed Products, Licensed Services, Licensed Components or Licensed Service Elements; or (11) claims related to applications, application programming interfaces and user interfaces, including the technology used to generate, display or interact with a use.
- 1.36 “OMA DRM Specification(s)” means Open Mobile Alliance DRM Specifications V2.0, DRM Architecture V2.0, OMA DRM Requirements V2.0, DRM Content Format V2.0, and/or OMA Rights Expression Language V2.0, each as amended from time to time, and all follow on versions of the same as approved by OMA, excluding the backward compatibility functions required by OMA DRM Specification V2.0 and defined in the OMA DRM version 1.0 specification.
- 1.37 “OCSP Responder” has the same meaning as set forth in the CMLA Technical Specification.
- 1.38 “Participating Affiliate” means an Affiliate of Service Provider, for which Service Provider agrees to assume obligations contained in the Agreement, which is identified by Service Provider; and which wishes to exercise the rights granted pursuant to the Section 2. Participating Affiliates shall be identified by Service Provider in the form attached hereto as Exhibit D.
- 1.39 “Participating Product Implementation” means those portions of a product that implement the OMA DRM Specifications, are Compliant and incorporate a Licensed Product.
- 1.40 “Participating Rights Issuer Implementation” means those portions of a Rights Issuer facility that implement the OMA DRM Specifications, are Compliant and incorporate a Licensed Service from which a Service Provider and/or its Participating Affiliates generate and distribute Rights Objects and/or DCF (DRM content format) in response to ROAP.
- 1.41 “Party” or “Parties” means the party or parties to this Agreement.
- 1.42 “Rights Issuer” has the same meaning as defined in the OMA DRM Specifications.
- 1.43 “Rights Issuer Certificate” is a digital certificate issued by CMLA for a public key corresponding to a Rights Issuer Private Key, as specified in the OMA DRM Specifications.
- 1.44 “Rights Issuer Private Key” is a cryptographic value used by the Rights Issuer to create digital signatures, as defined by the technical specifications contained in the OMA DRM Specifications.
- 1.45 “Rights Object” has the same meaning as defined in the OMA DRM Specifications.

- 1.46 “ROAP” means the rights object acquisition protocol as defined in the OMA DRM Specifications.
- 1.47 “Robustness Rules” means the requirements set out in Exhibit B hereto.
- 1.48 “Service Provider Agreement” means (i) this Agreement, and/or (ii) each other agreement in substantially the form in all material respects of this Agreement (including the Exhibits hereto), as executed by the CMLA, the Founders and any Fellow Service Provider.
- 1.49 “Third Party Beneficiary” means (in relation to the rights granted under this Agreement) any Eligible Content Participant.
- 1.50 “Threat” as used in the Robustness Rules attached hereto as Exhibit B, means an expression of the potential to exploit vulnerability. Estimation of the force of a threat depends upon the resources required to enact the threat together with the ability required to perpetrate the exploit.
- 1.51 “Third Party Beneficiary Claim” means a claim brought by an Eligible Content Participant as a Third Party Beneficiary as set forth in Section 8.5 through Section 8.9, hereto.

2. LICENSES GRANTED

2.1

- (a) Necessary Claims Patent License. Upon execution of this Agreement and in accordance with all of the terms and conditions of this Agreement including, but not limited to, payment of all fees required hereunder, but excluding any minor and/or remedied breaches, and subject to the scope of use limitations set forth in Section 2.2, Section 2.3, Section 2.4, and the reciprocal non-assert set forth in Section 2.5, each Founder (or its Affiliate which has the right to sublicense the Necessary Claims) grants to Service Provider and its Participating Affiliates, if applicable, and Service Provider and its Participating Affiliates, if applicable, accepts from each Founder (or its Affiliate) (in accordance with the terms and provisions of Section 6) a nonexclusive, nontransferable, nonsublicensable, revocable (only in the circumstances as set out in this Agreement), worldwide license under the Necessary Claims of such Founders (or their Affiliates) to use the CMLA Technical Specification and sample code included in the CMLA Technical Specification, if any, to use, make and have made (under contract with Service Provider or its Participating Affiliate and pursuant to Service Provider or its Participating Affiliate’s or subcontractor’s thereof, design for the sole account of Service Provider or its Participating Affiliate) a Participating Rights Issuer Implementation(s), and to use, make, and have made, market, sell, offer for sale, and import Licensed Service and Licensed Service Elements. However, such Licensed Services or Licensed Service Elements shall only be sold or transferred to Fellow Service Providers (and their Participating Affiliates, if applicable) for incorporation into a Participating Rights Issuer Implementation or to a CMLA Technology Licensee pursuant to a Developer Addendum solely for development in accordance with the Developer Addendum and this Agreement and/or to an Authorized Reseller pursuant to a CMLA Authorized Reseller Agreement solely for the resale and/or redistribution in accordance with the CMLA Authorized Reseller Agreement. Notwithstanding the foregoing, Licensed Services (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation) or Licensed Service Elements (or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service) consisting of

software object code may be furnished by Service Provider or its Participating Affiliates, if applicable, to persons other than Fellow Service Provider or Authorized Resellers if (i) the Licensed Service (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation) or Licensed Service Element (or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service) object code is encrypted using a commercially reasonable strength of encryption and the keys necessary to decrypt and use such object code are made available by the Service Provider and its Participating Affiliates, if applicable only to Fellow Service Providers (and their Participating Affiliates, if applicable) or Authorized Resellers; (ii) the Licensed Service or Licensed Service Element object code does not contain any Rights Issuer Private Keys; or if (iii) the CMLA Technical Specification implementation(s) in the Licensed Service or Licensed Service Elements are only activated when the Licensed Service or Licensed Service Elements are incorporated in a Participating Rights Issuer Implementation or Licensed Service, respectively.

- (b) CMLA IP Licenses. Upon execution of this Agreement and in accordance with the terms and conditions of this Agreement including, but not limited to, payment of all fees required hereunder, but excluding any minor and/or remedied breaches, and subject to the scope of use limitations set forth in Section 2.2, 2.3, and 2.4 and the reciprocal non-assert in Section 2.5, CMLA grants to Service Provider, and its Participating Affiliates, if applicable, and Service Provider and its Participating Affiliates, if applicable, accepts from CMLA (in accordance with the terms and provisions of Section 6 a nonexclusive, nontransferable, nonsublicensable, revocable (only in the circumstance as set out in this Agreement), worldwide license under CMLA, LLC's patents or patent applications to use the CMLA Technical Specification and sample code included in the CMLA Technical Specification, if any, to use, make and have made (under contract with Service Provider or its Participating Affiliates and pursuant to Service Provider's, or its Participating Affiliate's or a subcontractor's thereof, design for the sole account of Service Provider or its Participating Affiliate) Participating Rights Issuer Implementation(s), and to use, make and have made, market, sell, offer for sale and import Licensed Services and Licensed Service Elements. However, such Licensed Service or Licensed Service Elements shall only be sold or transferred to (x) Fellow Service Providers or their Participating Affiliate for incorporation into a Participating Rights Issuer Implementation or (y) to a CMLA Technology Licensee who has signed a Developer Addendum pursuant to the terms of the Developer Addendum solely for development in accordance with the Developer Addendum and this Agreement and/or (z) to Authorized Resellers solely for resale and/or redistribution in accordance with the CMLA Authorized Reseller Agreement and this Agreement. Notwithstanding the foregoing, Licensed Services or Licensed Service Elements consisting of software object code may be furnished by Service Provider to persons other than Fellow Service Providers or Authorized Resellers if (i) the Licensed Service (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation) or Licensed Service Element (or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service) object code is encrypted using a commercially reasonable strength of encryption and the keys necessary to decrypt and use such object code are made available by the Service Provider and its Participating Affiliates, if applicable only to Fellow Service Providers (and their Participating Affiliates, if applicable) and Authorized Resellers; (ii) the Licensed Service (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation) or Licensed Service Element (or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service) object code does not contain any Rights Issuer Private Keys; or if

- (ii) the CMLA Technical Specification implementation(s) in those Licensed Service or Licensed Service Elements are only activated when those Licensed Service or Licensed Service Elements are incorporated in a Participating Rights Issuer Implementation.
- (c) Copyright License. Upon execution of this Agreement and subject to Service Provider and its Participating Affiliates, if applicable, compliance with all of the terms and conditions of this Agreement including, but not limited to, payment of all fees required hereunder, but excluding any minor and/or remedied breaches, and subject to the limitations set forth in Section 2.2, Section 2.3, and Section 2.4, and the reciprocal non-assert in Section 2.5, CMLA grants to Service Provider and its Participating Affiliates, if applicable, and Service Provider and its Participating Affiliates, if applicable accepts, a nonexclusive, nontransferable, nonsublicensable, revocable (only in the circumstances set out in this Agreement), worldwide license under those copyrights embodied in the CMLA Technical Specification and sample code included in the CMLA Technical Specification made available to Service Provider during the course of performance of this Agreement to reproduce and distribute internally the CMLA Technical Specification to design and develop Participating Rights Issuer Implementation(s), Licensed Service or Licensed Service Element and to distribute sample code in object code form, as part of a Licensed Service or Licensed Service Element. Service Provider or its Participating Affiliate, if applicable, may provide a subcontractor with the CMLA Technical Specification and sample code under terms of a separate agreement, setting forth the terms of this Section 2.1(c) as it applies to subcontractors, confidentiality obligations, if applicable, and other terms relating to subcontractor use, such as but not limited to, Section 2.4, for the subcontractor's design or development of Licensed Service (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation) or Licensed Service Elements (or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service) solely for the account of the Service Provider or its Participating Affiliates. In the event the Service Provider subcontractor receives Highly Confidential Information or Rights Issuer Private Keys such receipt shall be pursuant to Section 5.
- (d) Trade Secret License. Upon execution of this Agreement and subject to Service Provider and its Participating Affiliate's, if applicable, compliance with all of the terms and conditions of this Agreement including, but not limited to, payment of all fees required hereunder, but excluding any minor and/or remedied breaches, and subject to the scope of use limitations set forth in Section 2.2, Section 2.3, Section 2.4, and the reciprocal non-assert in Section 2.5, CMLA grants to Service Provider and its Participating Affiliate and Service Provider and its Participating Affiliates accepts, a nonexclusive, nontransferable, nonsublicensable, revocable (only in the circumstances set out in this Agreement), worldwide license under those trade secrets, Confidential Information and Highly Confidential Information embodied in the CMLA Technical Specification and Rights Issuer Private Keys and disclosed to Service Provider or its Participating Affiliates during the course of performance of this Agreement to be used in accordance with Sections 5.2 and 5.3 to use, develop and design Participating Rights Issuer Implementation(s), Licensed Service or Licensed Service Elements.
- (e) Development System License. In order to facilitate the research, development, evaluation or testing efforts of CMLA Technology Licensees, CMLA may provide to Service Provider and Participating Affiliates, if applicable, and their subcontractors for the sole account of Service Provider and Participating Affiliates, upon request and subject to the payment of applicable fees, and upon execution of this Agreement, and subject to the limitations set forth in Section 2.2, Section 2.3 and Section 2.4, and Section 2.5, a license to the Development

System and Development Keys for research, development, evaluation or testing use only. Neither the Development System or Development Keys shall be used in commercial production or services in any manner whatsoever. In order to facilitate the research and development efforts of CMLA Technology

- (f) The licenses granted in this Section 2.1, shall not extend to Service Provider or its Participating Affiliates if Service Provider or its Affiliates or Participating Affiliates are in violation of Section 2.5, and the assertion concerned is not withdrawn pursuant to Section 6.2.2.

2.2 Scope of Use. The copyright and trade secret licenses under Section 2.1 (c) and (d) extend only to the use of CMLA Technical Specification to implement in a Licensed Service or Licensed Service Element to protect Digital Content. The patent licenses in Section 2.1(a) and 2.1(b) are applicable solely to those portions of Licensed Services and/or Licensed Service Elements that are necessary to implement those mandatory requirements that are disclosed with particularity in the CMLA Technical Specification. The patent licenses granted under Section 2.1 (a) and 2.1 (b) extend only to Licensed Services or Licensed Service Elements within the scope and license grant set forth in those Sections, that are sold or transferred to a Fellow Service Provider or its Participating Affiliates, if applicable, or Authorized Reseller for incorporation into a Participating Rights Issuer Implementation and are in fact incorporated into a Participating Rights Issuer Implementation. The copyright, trade secret, and patent licenses granted in Section 2.1(a), (b), (c) and (d) also extend to the activities that are permitted under Section 4 of the Developer Addendum without regard to whether Service Provider has signed such Developer Addendum.

2.3 Notwithstanding anything else in this Agreement, patents, patent applications, copyrights and trade secrets which subsist in anything that is excluded from the definition of Necessary Claims or in other rights not expressly granted herein are not licensed pursuant to the licenses granted under Section 2.1 or under the Development Addendum.

2.4 Proper Use. Neither Service Provider nor its Affiliates or its Participating Affiliates, if applicable, shall use Highly Confidential Information, Rights Issuer Private Key, or the CMLA Technical Specification provided under this Agreement, nor produce or sell services, devices, software, or portions thereof under color of this Agreement, where such services, software or portions thereof are designed to circumvent the requirements or effectiveness of the CMLA Technical Specification, Rights Issuer Private Key, CMLA Device Key Material or Participating Rights Issuer Implementation, Participating Product Implementation, Licensed Services, Licensed Service Elements, Licensed Products or Licensed Components.

2.5 Reciprocal Non Assertion Covenant.

- (a) Service Provider, to the extent Service Provider has not provided a direct license in its role as Founder (whether such license has been granted directly or through its Affiliate that has a right to sublicense), on behalf of itself and its Affiliates, promises not to assert or maintain against Fellow Service Providers, Client Adopters, Content Participants and Affiliates thereof or any vendor, distributor, purchaser, customer or other person in the chain of distribution (for those parties) of Licensed Service, Licensed Service Element, Licensed Products or Licensed Components, and Service Provider and its Participating Affiliates accepts Fellow Service Providers', Client Adopters,' Content Participants' and their Affiliates' promise in their respective CMLA Technology License Agreements not to assert or maintain against it or them any claim of infringement under Service Provider's, Fellow Service Providers', Client Adopters', Content Participants' (and their respective Affiliates') Necessary Claims or their

trade secrets or copyrights in the CMLA Technical Specification, arising in connection with any such Party's or Parties' use, evaluation, testing, development, design, having designed, having developed, making or having made for the sole account of Fellow Service Provider, Client Adopter, Content Participant or any Participating Affiliate thereof any reproduction, distribution, display, performance, marketing, sale, offer for sale, and import or other transfer of Licensed Services, Licensed Service Elements, Licensed Products and Licensed Components.

(b) Service Provider on behalf of itself and its Affiliates promises not to assert or maintain against Founders or CMLA and Affiliates thereof any claim of infringement under Service Provider's or its Affiliates' patents, patent applications, trade secrets or copyrights necessary or required for, and solely to the extent that Founders or CMLA and Affiliates thereof use the same for, the administration and operation of CMLA for the purposes of the CMLA Technical Specification, including but not limited to, the operation of a key generation facility and the provision/sale of keys, certificates, the OCSP Responder, and any other services necessary for the operation of the key generation facility, administration of the CMLA License Agreements and the distribution and licensing of the CMLA Technical Specification or drafts thereof.

(c) Provided that (1) each such promise (as referred to in (a) above) only applies to those portions of such Licensed Service, Licensed Service Element, Licensed Products or Licensed Components which are required for compliance with the CMLA Technical Specification and which cannot be implemented without infringing (but for this covenant) the Necessary Claims and/or the trade secrets or copyrights in the CMLA Technical Specification, and further provided that (2) the benefit of such promise does not extend to any person or entity which is asserting its Necessary Claims, trade secrets or copyrights against the promissory, Founders, CMLA, Service Provider, Fellow Service Provider, Client Adopter, Content Participant or any Affiliates thereof where the promissory is not in breach of its obligations with respect to the reciprocal non assertion under its CMLA Technology License Agreement.

This Section 2.5 applies whether another entity has become a Fellow Service Provider, Client Adopter or Content Participant (or an Affiliate of any of the foregoing) before or after Service Provider signs this Agreement. For purposes of this Section 2.5, Necessary Claims shall include only those Necessary Claims that relate to the versions of the CMLA Technical Specification adopted and in effect in accordance with Section 3 of this Agreement during the term of this Agreement.

(d) Notwithstanding the foregoing in this Section 2.5(a) patents, patent applications, copyrights and trade secrets which subsist in anything that is excluded from the definition of Necessary Claims are not covered by the promise not-to-assert under Section 2.5(a).

2.6 CMLA Order Process: Service Provider and its Participating Affiliates agree to follow the CMLA authentication and order procedures using the CMLA order form(s). In the event Service Provider fails to follow such procedures, CMLA is under no obligation to perform Rights Issuer certification.

2.7 Warranties.

(a) CMLA represents and warrants, as of the Effective Date, its agent (Corporate Trust Center, 1209 Orange Street, Wilmington, DE 19801, attention CMLA, LLC), has not received written

notice of any claim, threatened or pending, from any third party, that the CMLA IP infringes any third party's intellectual property rights.

- (b) CMLA represents and warrants that it has full right, power and authority to enter into and perform this Agreement and that it has received a license from the Founders and Contributors authorizing CMLA to grant the copyright and trade secret licenses to Service Provider and its Participating Affiliates, if applicable, set forth herein and that such license from Founders and Contributors shall remain in effect during the term of this Agreement.
- (c) CMLA represents and warrants that it shall be bound by reasonable confidentiality obligations protecting sensitive information contained in (i) reports submitted further to Section 4.2 of this Agreement pursuant to CMLA approved order forms, and (ii) Rights Issuer Certificate orders or reports, submitted on CMLA approved order form, limited to the identity of the CMLA Technology Licensee placing the order, the number of certificates ordered or generated and certification requests; and, CMLA further represents and warrants that it will not provide Founders with order or fee related information except in its aggregate form.
- (d) In the event that CMLA receives written notice that CMLA IP technology allegedly infringes third party patents, CMLA will evaluate the claim and will consider commercially reasonable alternatives such as, but not limited to: (1) obtain a license from such third party to grant sublicenses for the benefits of all CMLA Technology Licensees, the cost of which shall be borne by all CMLA Technology Licensees; (2) modify, if possible, the CMLA Technical Specification, pursuant to Section 3, below; or (3) develop a work around for the CMLA IP technology. If no commercially reasonable alternative exists, CMLA has the right to terminate this Agreement pursuant to Section 6 below. CMLA agrees to provide prompt written notice to CMLA Technology Licensees in the event an infringement law suit is filed against CMLA related to CMLA IP. Service Provider agrees to provide prompt written notice to CMLA in the event an infringement law suit is filed against Service Provider or its Participating Affiliates related to CMLA IP.
- (e) Service Provider represents and warrants that it shall provide CMLA with prior written notice of its intent to add a Participating Affiliate. Such notification shall be in the form attached hereto as Exhibit D.
- (f) Service Provider represents and warrants that it has the full right and power to enter into and perform this Agreement according to the terms contained therein and that the person signing this Agreement is empowered to act on behalf of and to legally bind this Service Provider.
- (g) Affiliates. Service Provider represents and warrants that it has or will have the authority to bind its Affiliates to the terms of the non-assert in Section 2.5.
- (h) Founders represent and warrant that they have or will have the authority, either on their own behalf or that of their Affiliates, to grant the licenses contained in Section 2.1 of this Agreement.

3. ADDITIONAL RIGHTS GRANTED TO SERVICE PROVIDER.

- 3.1 Service Provider User Group. Service Provider shall have the right at all times during the term of this Agreement to participate in a user group consisting solely of CMLA Service Providers who choose to become members of such group (the "Service Provider User Group"). Service Provider shall notify CMLA in writing whether or not Service Provider will be a member of the Service Provider User Group. Service Provider may, by written notice to CMLA, change its status as a member or non-member of the Service Provider User Group which change in status shall be immediate. The members of the Service Provider User Group shall be entitled to establish the internal rules governing the operation of the Service Provider User Group. Upon request of the Founders or the Service Provider User Group, CMLA will use good faith efforts to undertake to have the Founders meet with, and take into account the views expressed by the Service Provider User Group with respect to (a) the Compliance Rules and Robustness Rules as of the Effective Date and any future technical or other amendments thereto, and (b) such other matters relating to CMLA Technical Specification as the members of the Service Provider User Group may agree to discuss, provided however, that the Service Provider User Group will not address issues related to the OMA DRM Specification that are not specifically related to the CMLA Technical Specification.
- 3.2 CMLA Advisory Board In maximum, three (3) selected representatives of the Content Participants, one of which will be a motion picture studio and one of which will be a music label, three (3) selected representatives of the Client Adopters (none of which may be a Founder), and three (3) elected representatives of the CMLA Service Providers, respectively selected by each user group, shall be appointed by CMLA to serve on the CMLA Advisory Board ("CAB") together with the Founders. The CAB shall consist of at most thirteen (13) members in total. For clarification, no participating entity (including signatory and all Affiliates) may participate on CAB in more than one category. The CAB will be managed by such thirteen members and such management shall include, but not be limited to, compliance with the procedures in Exhibit H. The CAB shall have meetings at least once per quarter, or at such times as the CAB may otherwise agree. Unless otherwise expressly stated in this Agreement, no decision of the CAB shall be valid unless taken by a Qualified Majority. In this Agreement, a "Qualified Majority" of the CAB means, in respect of any decision, that such decision has been approved, in writing, by (i) at least one (1) Client Adopter, one (1) Service Provider and one (1) Content Participant and, (ii) at least two-thirds of the voting members of the CAB. Founders shall not be entitled to vote in CAB decisions. Unless otherwise expressly stated in this Agreement, no decision of the CAB shall be valid unless taken by Qualified Majority. Every CMLA Technology Licensee shall be entitled to receive reasonable advance notice of meetings of CAB, shall be entitled to attend meetings of the CAB, and shall be afforded reasonable opportunity to have its views heard at meetings of the CAB.
- 3.3 The CAB shall use Exhibit E to submit CAB Change Requests to CMLA. CMLA shall consider such requests in good faith.
- 3.4 Changes. The CMLA Technical Specification, the Compliance Rules and the Robustness Rules may only be amended in accordance with this Section 3.
- 3.5 Changes Consequent on Changes to OMA DRM Specifications. Within thirty (30) days of the release of any new or amended OMA DRM Specifications (including the release of a new version, release or significant change request to an existing OMA DRM Specification) (each, a "New OMA DRM Specification"), the CAB shall evaluate the changes (if any) required to update the CMLA Technical Specification, or any Compliance Rules or Robustness Rules, subject to

Section 3.10 or 3.11, below to take account of such New OMA DRM Specification. The CAB will decide whether to recommend the foregoing be updated, by a Qualified Majority. In connection with such updates:

- (i) after consulting with other members of the CAB, each member and attendee of the CAB shall be entitled to request changes to the Compliance Rules or Robustness Rules (but not the OMA DRM Specification) or CMLA Technical Specification for the sole purpose of updating them to enable implementation of (or otherwise take account of) the New OMA DRM Specification; and
- (ii) the CAB will work to define such updates and to address issues of backward compatibility

3.6 Changes to Improve Commercial Viability and Integrity, Security, Performance or to Fix Bugs, or Correct Errors or Omissions. The following provisions of this Section 3.6 shall apply for the sole purpose of proposing changes or updates to the CMLA Technical Specification and/or Compliance Rules or Robustness Rules, subject to Section 3.10 or 3.11 below to improve commercial viability, integrity, security, performance or to correct bugs, errors or omissions.

If a Content Participant, Client Adopter, Service Provider or any member or members of the CAB proposes a change to the CMLA Technical Specification, Compliance Rules or Robustness Rules, CAB will assess whether the proposed change is an “Improving Change”, namely a change which, in the reasonably opinion of a Qualified Majority of the CAB would be likely to clarify and/or improve the commercial viability and integrity, security or performance of the CMLA Technical Specification, Compliance Rules or Robustness Rules or fix bugs or correct error/omissions. If the proposed change is not an Improving Change, the CAB shall promptly inform the entity that made the proposal of that fact, and CMLA shall then be under no further obligation with respect to the proposal. If the proposed change is an Improving Change, the CAB shall promptly submit a change request to CMLA and the procedure in Sections 3.13 and 3.14 will apply.

3.7 Timing of Compliance with Changes to Compliance Rules, Robustness Rules and the CMLA Technical Specifications. Service Provider shall be required to comply with all applicable amendments to the Compliance Rules, Robustness Rules or to the CMLA Technical Specification that do not require material modifications to the implementation or design of a Participating Rights Issuer Implementation, Licensed Service or Licensed Service Element within six (6) months after the effective date of the amendment or such longer period specified by CMLA. When proposing a change or amendment the CAB will also provide input or a recommendation related to timescales for complying with such proposed change or amendment. Service Provider shall be required to comply with all other applicable amendments to the Compliance Rules, Robustness Rules or to the CMLA Technical Specification within eighteen (18) months after the effective date of the amendment or such longer period specified by CMLA.

3.8 Additions and other Changes to Table X2 and Y2 of the Compliance Rules. CMLA will accept additions and other changes to Table X2 and Y2 of the Compliance Rules; provided that (1) the addition of new proprietary technology (and its associated mappings) will be accepted only from the technology supplier or with the consent of the technology supplier, (2) changes to an existing proprietary technology (and its associated mapping) will be accepted only from the technology supplier or with the consent of the technology supplier; and (3) the addition of other entries (e.g., non-proprietary technologies, quality parameters for CD burning, etc.) will be accepted from any proponent. Each such addition or changes will be designated as a new entry in Table X2 or Table Y2 and will be effected by CMLA when CMLA receives payment of an Administration Fee.

CMLA will include for reference, a comment field and a contact field for each technology on Table X2 and Y2. Once accepted, the comment field and the contact field are the only fields that can be appended. For clarification, additions and changes pursuant to this Section 3.8 are not subject to the change management provisions of this Section or Section 3.19 of the Content Participant Agreement. For avoidance of doubt, changes to Table X1 and Y1 are subject to the change management provisions of this Section 3 or Section 3.19 of the Content Participant Agreement.

- 3.9 Changes to the Annual Administration Fees and Usage Fees. Changes to the Annual Administration Fees and Usage Fees shall be permitted only as set out in Sections 4.1 and 4.2. All other modifications to Section 4 and the Fee Schedule attached as Exhibit C, (including, without limitation the inclusion of new categories of Usage Fee and any completely new category of fees in addition to the Annual Administration Fees and Usage Fees) shall be subject to Section 10.2.
- 3.10 Changes to the CMLA Technical Specification. CMLA may make such changes to the CMLA Technical Specification as it deems necessary or appropriate until version 1.0 of the given CMLA Technical Specification is released. Version 1.0 of the CMLA Technical Specification will be released no later than June 30, 2005. After version 1.0 of the CMLA Technical Specification has been released, CMLA shall make no material changes to the CMLA Technical Specification (including any changes that would expand the CMLA Technical Specification to require the inclusion of new technical features not included in version 1.0 of the CMLA Technical Specification or make Licensed Service or Licensed Products designed or manufactured prior to such changes incompatible with the new version of the CMLA Technical Specification) except pursuant to a proposal or request made as envisaged by Sections 3.5 and 3.6. Without limiting the foregoing, the following changes shall not be considered “material” for the purpose of this Section 3.10: (i) mapping or porting the CMLA Technical Specification to different technologies as set forth in Section 3.8, (ii) correction of any errors or omissions in the CMLA Technical Specification, and (iii) making changes that would clarify, but not materially amend, alter or expand the CMLA Technical Specification. Founders or CMLA shall not make any revisions to the Compliance Rules or Robustness Rules that would materially increase the cost or complexity of implementations of Licensed Products or Licensed Service unless such change may be required by a new OMA DRM Specification. Such changes are subject to Section 3.12 and 3.13.
- 3.11 Changes to the Compliance Rules or Robustness Rules. Except as CMLA can, by the preponderance of evidence, demonstrate is necessary to provide for protection of Content Participants’ Digital Content, CMLA shall not (i) make any revisions to the Service Provider Compliance Rules or Robustness Rules that would materially increase the cost or complexity of Participating Rights Issuer Implementations or (ii) amend the Client Adopter Compliance Rules or Content Participant Agreement to require Content Providers or Service Providers to include mandatory “move” or “copy” permissions in a Rights Object with respect to Digital Content; (iii) otherwise amend the Compliance Rules to permit Participating Product Implementation to “move” or “copy” Digital Content other than as set forth in the Rights Object; (iv) amend Sections 1.2.1, 1.2.2 and 1.2.3 of the Service Provider Compliance Rules; (v) with respect to the Service Provider Compliance Rules, amend the consumer notification requirement set forth in Section 1.5 or the timing synchronization requirements set forth in Section 1.7, or amend or add other similar provisions relating to Service Provider business operations, unless such change(s) may be required by a new OMA DRM Specification. Except where specifically not required, CMLA agrees to apply the procedures set forth in Section 3.14 of the Content Participant Agreement when considering any change to the Compliance or Robustness Rules.

3.12 Notice of Changes to Compliance Rules, Robustness Rules and CMLA Technical Specification. Without limiting the foregoing, CMLA shall provide Service Provider with at least thirty (30) days' notice of any changes to the Compliance Rules, Robustness Rules or to the CMLA Technical Specification. The effective date of such changes shall be specified in the notices provided to Service Provider and such effective date shall not be earlier than thirty (30) days after issuance of the notice.

3.13 Review of Proposed Changes – Procedure. Upon receipt of a change request pursuant to this Section 3 or upon a change to be initiated by CMLA pursuant to this Section 3, CMLA will post details of the same to a CMLA Technology Licensee website for CMLA Technology Licensee review. All comments made by Service Provider or any other CMLA Technology Licensee in respect of any such change request will be considered promptly and in good faith by CAB. The CAB shall post its recommendation and reason for recommendation to the CMLA Technology Licensee website within sixty (60) days of posting the change request to the website. CMLA will post to CMLA Technology Licensee website notice of a change to be made to the Compliance or Robustness Rules or the CMLA Technical Specification, whether made pursuant to a CAB recommendation or otherwise.

3.13.1 CMLA shall consider in good faith implementing each Improving Change unless (in the reasonable opinion of the CMLA, such change would:

- (1) materially amend, alter or expand the CMLA Technical Specification after it has been released in version 1.0; or
- (2) impose additional substantial obligations on Founders, CMLA or CMLA Service Providers or on the operation of a Participating Rights Issuer Implementation; or
- (3) necessarily result in a patent right (which was not a “Necessary Claim” before such change) becoming a Necessary Claim by such change; or
- (4) amend or augment the OMA DRM Specifications in a manner not specifically related to the CMLA Technical Specification; or

If an Improving Change or any CAB recommendation would do any of the things listed in (1) to (4) of Section 3.13.1, CMLA will cooperate with the entity proposing the change to seek alternatives to the proposed change, but shall have the right ultimately to reject any and all such proposed changes in its good faith judgment.

3.14

- (a) For the term of this Agreement, as long as Service Provider is not in breach of any material terms of this Agreement, Service Provider shall have the right to file a written objection to any CMLA change pursuant to this Section 3 (whether the change is based on a CAB recommendation or CMLA change) which would have an alleged material and adverse effect on the integrity, security or the costs or complexity, of the implementation of the CMLA Technical Specification, the commercial viability of the CMLA Technical Specification, or the rights of Service Provider with respect to the CMLA Technical Specification (“CMLA Proposed Adverse Action”). Any such objection shall set forth with specificity the alleged material and adverse effects on the integrity or security or the costs or complexity of the implementation of the CMLA Technical Specification or the rights of Service Provider with respect to CMLA Technical Specification, and shall be delivered to CMLA no later than

thirty (30) days after the CMLA change is posted. CMLA agrees to consider any such objection in good faith. If CMLA rejects such objection, it shall provide prompt written notice thereof to Service Provider that filed a written objection explaining the reasons for such rejection, including the benefits that would be afforded by the CMLA Proposed Adverse Action. Absent receipt by CMLA of a written objection from one or more CMLA Service Provider pursuant to this Section 3.14, CMLA may take the action described in the change notice delivered pursuant to Section 3.12.

- (b) If Service Provider and a sufficient number of Fellow Service Providers (including Service Provider) object to a CMLA Proposed Adverse Action pursuant to Section 3.14(a), then CMLA Service Providers that filed objections (the “Arbitrating CMLA Service Providers”) shall have the right within thirty (30) days from service of CMLA’s rejection of such objection pursuant to Section 3.14(a), to initiate an arbitration in accordance with the provisions of this Section 3.14(b), provided that such arbitration shall be initiated only if there is a sufficient number of Fellow Service Providers joining in the initiation action. For purposes of this Section 3.14, a “sufficient number of CMLA Service Providers” shall be at least two-thirds of the total number of entities that are CMLA Service Providers as at date CMLA change was posted. Any such arbitration shall proceed according to the following:
- (i) In such arbitration, the Arbitrating CMLA Service Providers shall have the burden of demonstrating, based on the preponderance of evidence, that the CMLA Proposed Adverse Action shall have the alleged material and adverse effect. Changes which only insignificantly diminish the integrity or security of the CMLA Technical Specification, or the rights of CMLA Service Providers with respect to CMLA Technical Specification shall not be deemed to have a material and adverse effect. Notwithstanding the above, the arbitrator may, in his or her discretion take into consideration the cumulative effect of multiple related changes that are both “insignificant” and “adverse” when considered in isolation, provided that in any such consideration the arbitrator shall (1) afford countervailing weight to any changes, whether related or not, that have had or are intended to have beneficial effect on the integrity or security of the CMLA Technical Specification, or the rights of Service Provider with respect to the CMLA Technical Specification (“Beneficial Changes”); and (2) consider only the cumulative effect of changes, whether (x) related “insignificant” and “adverse” changes, or (y) Beneficial Changes, made by CMLA and/or Founders over the preceding two year period.
- (ii) If the Arbitrating CMLA Service Providers have carried the burden set forth in Section 3.14(b)(i), then CMLA may not take the CMLA Proposed Adverse Action unless CMLA demonstrates, based on clear and convincing evidence, that the CMLA Proposed Adverse Action provides a material legal benefit in the form of avoidance of a reasonably perceived significant potential legal liability to CMLA, Founders, Service Providers or Client Adopters which cannot practicably be achieved except by taking the CMLA Proposed Adverse Action.
- (iii) The Arbitrating CMLA Service Providers, on the one hand, and CMLA, on the other shall share equally the costs of arbitration set forth in Section 3.14(b)(iv)(g). The arbitrator shall award the prevailing party or parties all of its or their costs and expenses, other than attorneys’ fees and expenses. In addition, if the arbitrator finds that either CMLA or the Arbitrating CMLA Service Providers has or have advanced its or their position in bad faith or frivolously, it shall order such party or parties to reimburse the other party or parties for its or their reasonable attorneys’ fees and expenses.

- (iv) The arbitration specified in this Section 3.14(b) shall be conducted in accordance with the following provisions:
- (a) There shall be a sole arbitrator who shall be selected by the American Arbitration Association from its National Panel of Commercial Arbitrators. The arbitrator shall have a minimum of fifteen (15) years knowledge or experience in the telecommunications, computer or software industries.
 - (b) The arbitration shall be conducted in New York, New York, in accordance with the International Arbitration Rules of the American Arbitration Association. The arbitration shall be conducted in English.
 - (c) The arbitrator shall be directed to complete the arbitration within sixty (60) days but may otherwise conduct the arbitration in such manner as it shall deem appropriate, including the imposition of time limits that it considers reasonable for each phase of the proceeding, but with due regard for the need to act, and make a final determination, in an expeditious manner.
 - (d) The arbitrator shall permit and facilitate such limited discovery as he or she shall determine is reasonably necessary, taking into account the needs of the parties and the desirability of making discovery as expeditious and cost-effective as possible.
 - (e) The parties and the arbitrator shall treat the arbitration proceedings, any related discovery, documents and other evidence submitted to, and the decision of, the arbitrator as Confidential Information. In addition, and as necessary, the arbitrator may issue orders to protect the confidentiality of proprietary information, trade secrets and other sensitive information disclosed in discovery or otherwise during the arbitration.
 - (f) The arbitrator is empowered solely to determine whether the parties have carried their respective burdens, as provided in Section 3.14(b)(i). Any such determination by the arbitrator shall be final and binding on the parties, except that whether the arbitrator exceeded his or her authority in determining the remedy (including exceeding his or her authority as to any award of costs under Section 3.14(b)(iii)), or otherwise, as specifically described in this Section 3.13, shall be fully reviewable by a court of competent jurisdiction. The Arbitrator shall be obliged to reduce the decision to writing and provide reasons supporting the decision. Judgment upon any award shall be entered in a court of competent jurisdiction.
 - (g) The arbitrator shall be compensated at his or her hourly rate, determined at the time of appointment, for all time spent in connection with the arbitration, and shall be reimbursed for reasonable travel and other expenses. The arbitrator shall determine all costs of the arbitration, including his or her fees and expenses, the costs of expert advice and other assistance engaged by the arbitrator, the cost of a transcript and the costs of meeting and hearing facilities.
- (v) If (i) no arbitration has been initiated with respect to the CMLA Proposed Adverse Action pursuant to Section 3.14(b); (ii) the arbitrator determines that the Arbitrating CMLA Service Providers have not carried the burden set forth in Section 3.14(b)(i); or (iii) notwithstanding the arbitrator's determination that the Arbitrating CMLA Service Providers have carried such burden, set forth in Section 3.14(b)(i), or (iv) if the arbitrator further determines that CMLA has carried its burden set forth in Section 3.14(b)(ii), then CMLA may take the CMLA Proposed Adverse Action, and such action may be effective, according to its terms, thirty (30) days after service of CMLA's rejection pursuant to Section 3.14(a) or such final determination of the arbitrator, whichever is later. If the

arbitrator determines (x) that the Arbitrating CMLA Service Providers have carried the burden set forth in Section 3.14(b)(i) and (y) that the CMLA has not carried its burden set forth in 3.14(b)(ii), then the CMLA Proposed Adverse Action shall not be taken, provided that in the event that the inability to take the CMLA Proposed Adverse Action exposes CMLA or Founders to significant potential legal liabilities such as in the form of claims (including direct, contributory, and/or inducement) of infringement of intellectual property, or inducement of infringement of intellectual property, which cannot practicably be avoided except by taking the CMLA Proposed Adverse Action, CMLA may elect to terminate this Agreement and any CMLA Technology License Agreements and the Founders may elect to terminate all licenses to Necessary Claims. In the event that the inability to take the CMLA Proposed Adverse Action exposes one or more, but not all of the Founders to potential legal liabilities which cannot practicably be avoided except by taking the CMLA Proposed Adverse Action, such Founder(s) may, elect to convert any licenses to Necessary Claims to a reciprocal covenant not to assert Necessary Claims, provided that the Arbitrating CMLA Service Provider(s) indemnify such Founder(s) against any claims, actions, liabilities, losses or damages, including reasonable attorneys fees, for inducement to infringe a third party's intellectual property rights arising from the inability to take the CMLA Proposed Adverse Action.

4 FEES.

- 4.1 Annual Administration Fees. Within thirty (30) days of the Effective Date, Service Provider licensed under Section 2.1 shall pay CMLA the Annual Administration Fees as set forth in the Fee Schedule attached as Exhibit C. Service Provider shall not be entitled to any refund thereof for any reason. Upon each anniversary of the Effective Date (the "Annual Payment Date"), Service Provider shall pay CMLA the Annual Administration Fee for the following year which fee shall be used to offset the costs associated with the CMLA's administration of the CMLA Technical Specification and CMLA Technology License Agreements. CMLA may, upon at least thirty (30) days notice to Service Provider, modify or change the Annual Administration Fee payable for the period beginning on the next Annual Payment Date, provided that any increase or change in such fees shall not exceed an amount commensurate with CMLA's costs. Such costs shall be reviewed and increased based upon the principles more fully set forth in the CMLA Q & A document posted on the CMLA website. Without limiting the foregoing, where costs per CMLA Service Provider decrease, CMLA shall use commercially reasonable efforts to reduce the Annual Administration Fee.
- 4.2 Usage Fees. Service Provider licensed under Section 2.1 shall pay fees as set forth in the Fee Schedule attached as Exhibit C. Payment for all Usage Fees are due within thirty (30) days of receipt of invoice except Processing Fees and Development System Fees which are payable in advance. CMLA will supply Service Provider written invoice for Usage/Processing Fees upon receiving Service Provider's or its Participating Affiliate's order. Service Provider shall report to CMLA on a quarterly basis the number of Active Subscribers being served in that quarter. CMLA shall prepare an invoice based on the Service Provider quarterly report and submit to Service Provider for payment. Service Provider shall not be entitled to any refund thereof except as provided herein. In the event CMLA fails to deliver the order or orders of necessary Rights Issuer Certificates, where such order or orders are complete (contain all the necessary information and Service Provider or its Participating Affiliate has fulfilled all requirements for order processing) and CMLA is unable to cure through delivery of the ordered Rights Issuer Certificates within thirty (30) days, Service Provider's sole remedy will be a refund of Usage Fees paid for the Rights Issuer Certificates not delivered. CMLA may, upon at least thirty (30) days notice to Service Provider, modify, add (subject to Section 3.9) or change any Usage Fee, provided that any increase in such fees shall not exceed an amount commensurate with CMLA's

costs. For the avoidance of doubt, creation of new categories of Usage Fees pursuant to Section 3.9 may not lead to an increase in Usage Fees that exceeds the above mentioned criteria.

4.1.1 A completed Exhibit C-1 is required for Service Provider and each Participating Affiliate submitting orders. Service Provider shall submit a completed Exhibit C-1, with the Service Provider Agreement. Additional Participating Affiliates may be added by submitting a new Exhibit C-1. Each Exhibit C-1 will form part of this Agreement. Failure to provide Exhibit C-1, as required, will result in a delay of an order.

4.3 Gross Payments. Any fees paid by Service Provider hereunder will be paid without deduction or withholding for or on account of any present or future tax, assessment, or governmental charge imposed or levied, unless in each case the withholding or deduction of such tax, assessment or governmental charge is required by law. In the event such withholding or deduction is so required, Service Provider shall include with its payment written notification of such withholding and shall forward to CMLA in a timely manner evidence of such withholding adequate to permit CMLA and/or the Founders to claim relevant tax credits under applicable treaties. Service Provider assumes full responsibility for remitting such withholding to the proper authority.

4.4 Audit. CMLA shall have the right to appoint an independent third party auditor selected by CMLA, whose identity has been approved by the Service Provider (such approval not unreasonably to be withheld) to audit Service Provider's records, no more than annually, unless an underpayment of greater than five (5%) percent is discovered. In the event of an underpayment, CMLA shall have the right to re-audit one time for each audit identifying an underpayment. Each audit shall be conducted during Service Provider's normal business hours, for the sole purpose of determining the sufficiency of the Usage Fee payments made by Service Provider hereunder. The CMLA shall ensure that, in respect of each such audit:

4.4.1 no such audit is carried out unless the auditor is bound by a nondisclosure agreement which is at least as protective, of the information obtained as a result of the audit, as the applicable terms of Section 5 of this Agreement are with respect to Confidential Information;

4.4.2 the only information disclosed by the auditor to any person (including the Founders or CMLA) as a result of the audit is a certificate specifying whether the Service Provider has paid the correct Usage Fees pursuant to this Agreement and, if not, the discrepancy between (a) actual payments made and (b) the payments which ought to have been made;

4.4.3 the audit shall be conducted with commercially reasonable (and, in any event, not less than thirty (30) days') notice and using commercially reasonable means designed to minimize the disruption to Service Provider's business; and

4.4.4 the Service Provider has the right to accompany the auditor throughout the audit and to provide written objections to the auditor's findings in the event the Service Provider does not agree with them.

In the event an underpayment of greater than five (5%) percent is found, Service Provider shall be responsible for payment of auditor fees in addition to any payment due to CMLA.

5 CONFIDENTIALITY/EXPORT

- 5.1 Permitted Use. Service Provider and its Participating Affiliates shall not disclose Confidential Information to any third party except as specifically authorized under this Agreement and shall use Confidential Information (and tangible embodiments of any of the foregoing) only in accordance with the terms of this Agreement, and shall not use such information to circumvent the methods disclosed in Confidential Information nor any obligations under this Agreement. Service Provider and its Participating Affiliates, if applicable, shall use Highly Confidential Information and Rights Issuer Private Keys (and tangible embodiments of any of the foregoing) only in accordance with the terms of this Agreement and shall not use such information or any mentally retained recollection thereof to circumvent or copy the methods disclosed in Highly Confidential Information or Rights Issuer Private Keys or to circumvent any obligation under this Agreement.
- 5.2 Confidential Information. Service Provider may disclose Confidential Information to its Participating Affiliates. Service Provider and its Participating Affiliates shall maintain the confidentiality of Confidential Information in the following manner:
- 5.2.1 Service Provider and its Participating Affiliates shall employ procedures for safeguarding Confidential Information at least as rigorous as Service Provider and its Participating Affiliates would employ for its or their own Confidential Information, but no less than a reasonable degree of care.
- 5.2.2 Service Provider and its Participating Affiliates may disclose Confidential Information to (1) its employees; (2) its attorneys, auditors or other professional advisers and agents who have a reasonable need to know the Confidential Information and who owe Service Provider or its Participating Affiliates a duty of confidentiality at least as protective of such Confidential Information as the applicable terms of this Section 5; (3) its third party service suppliers and to third parties who develop or make, for the sole account of the Service Provider (and/or its Participating Affiliates), Licensed Services or Licensed Service Element and to individuals retained as independent contractors, provided that the Service Provider (and/or its Participating Affiliates) shall remain responsible for the maintenance of the confidentiality of the Confidential Information provided to such third parties and shall execute a nondisclosure agreement with such third parties at least as protective of the Confidential Information as the applicable terms of this Section 5 of this Agreement; and, (4) to other CMLA Technology Licensees.
- 5.3 Highly Confidential Information & Rights Issuer Private Keys. Service Provider and its Participating Affiliates shall maintain the confidentiality of Highly Confidential Information and Rights Issuer Private Keys in the following manner:
- 5.3.1 (a) Service Provider may disclose Highly Confidential Information or provide Rights Issuer Private Keys to its Participating Affiliates. Service Provider and its Participating Affiliates shall employ procedures for safeguarding Highly Confidential Information and Rights Issuer Private Keys at least as rigorous as the Service Provider or its Participating Affiliates would employ for their own most highly confidential information, such procedures to include, at a minimum: (1) maintaining on the Service Provider's or Participating Affiliates' premises a secure location(s) in which any and all Highly Confidential Information and Rights Issuer Private Keys shall be stored, where such a location(s) may include electronic storage that is at least as secure with respect to the Highly Confidential Information as the security standards set forth in the Robustness

Rules, with respect to the protection of Rights Issuer Private Keys; (2) that any Highly Confidential Information or Rights Issuer Private Keys stored in such a location(s) shall be accessible only by Authorized Employees (as defined below); and (3) when Highly Confidential Information or Rights Issuer Private Keys are not in use, such information shall be stored in a locked safe at such secure location or shall be stored electronically in a form that is at least as secure as the security standards set forth in the Robustness Rules with respect to the protection of Rights Issuer Private Keys.

(b) To the extent that Service Provider has incorporated Highly Confidential Information into a Licensed Service Element (or what or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service) or Licensed Service (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation), the provisions of this section shall be deemed to be met if such Licensed Service Element (or what or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service) or Licensed Service (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation) meets the security standard set forth in the Service Provider Robustness Rules.

5.3.2 Service Provider and its Participating Affiliates may disseminate Highly Confidential Information and Rights Issuer Private Keys only to a reasonable number of its and their employees and its and their respective suppliers and subcontractors: (1) who have a need to know or use such Highly Confidential Information or Rights Issuer Private Keys in order to enable Service Provider or any of its Participating Affiliates, if applicable, to exercise its (or their) rights and perform its (or their) obligations under this Agreement; and (2) who are bound in writing by obligations of confidentiality at least as protective of the Highly Confidential Information of Rights Issuer Private Keys as to the applicable terms of this Agreement, which obligations shall survive the termination of employment; (“Authorized Employee”). Service Provider shall cause (or, as appropriate shall require the relevant Participating Affiliates causes) Authorized Employees to abide by their obligations hereunder and shall use (or, as appropriate shall require the relevant Participating Affiliate to use) the same efforts to enforce the confidentiality obligations of each Authorized Employee during and after the termination of his/her employment as Service Provider (or each of its Participating Affiliates) uses to enforce with respect to Service Provider’s (or Participating Affiliates’) own similarly confidential information, provided that not less than reasonable efforts shall be used in such enforcement and provided that Service Provider (or its Participating Affiliates) shall maintain a list of all Authorized Employees (such list to include both current Authorized Employees and all individuals, whether or not still employed by Service Provider and/or its Participating Affiliates, who were Authorized Employees at any time). Upon CMLA’s request, Service Provider and/or its Participating Affiliate shall provide CMLA with the list of Authorized Employees described in the preceding sentence. Service Provider shall make reasonable efforts to assist CMLA in relation to any claim, action, suit, proceeding, or litigation with respect to the access of Service Provider’s (or Participating Affiliates) former employee to Highly Confidential Information or Rights Issuer Private Keys provided under this Section 5.3.2. For the avoidance of doubt, subcontractors of Service Provider and its Participating Affiliates receiving Rights Issuer Private Keys or Highly Confidential Information and Service Provider shall sign a Highly Confidential Information Non-Disclosure Agreement with CMLA the form of which is attached hereto as Exhibit F.

Notwithstanding any contrary provision, neither Service Provider nor any Participating Affiliate shall disseminate any Highly Confidential Information or Rights Issuer Private Keys to more than a reasonable number of Authorized Employees per Licensed Service. Service Provider and Participating Affiliates may add Authorized Employees without limit, but in doing so shall abide by the terms of Section 5.

Service Provider and Participating Affiliates may disclose Highly Confidential Information or Right Issuer Private Keys to third parties with whom Service Provider (and/or any such Participating Affiliate) has contracted to provide Licensed Service and Licensed Service Elements, for the sole account of the Service Provider (and/or any such Participating Affiliates), provided that the Service Provider shall remain responsible for maintaining the confidentiality of the Highly Confidential Information and Rights Issuer Private Keys provided to such third parties and provided that such third parties have executed a the Highly Confidential Non Disclosure Agreement set forth hereto as Exhibit F. To the extent that Service Provider has incorporated Highly Confidential Information or Rights Issuer Private Keys into a Licensed Service Element (or what or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service) or Licensed Service (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation) in a manner that fulfills the terms of Section 5.3.1 and 5.3.2, may transfer such Licensed Service Element (or what or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service) or Licensed Service (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation) to third parties with whom Service Provider has contracted to make a Participating Rights Issuer Implementation, Licensed Service (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation) or Licensed Service Element (or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service), for the sole account of the Service Provider without need for such third party to enter the Highly Confidential Non Disclosure Agreement set forth as Exhibit F, provided that Service Provider and such third party have a written agreement that prohibits the third party from reverse engineering the Licensed Service Element (or what or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service) or Licensed Service (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation).

5.3.3 Prior to the receipt of Highly Confidential Information, Service Provider and Participating Affiliate may refuse to accept Highly Confidential Information by providing written notice to CMLA. Such refusal does not relieve Service Provider or any Participating Affiliates' of its or their obligations under this Agreement for its or their Participating Rights Issuer Implementation, Licensed Service or License Service Element. In the event such Highly Confidential Information is required by the Compliance and Robustness Rules, any such refusal by Service Provider shall be considered notice of termination pursuant to Section 6.2.1.

5.4 Rights Issuer Private Keys. In the case of conflict of any of the provisions contained in this Section 5, and the Rights Issuer Robustness Rules relating to the use of Rights Issuer Private Keys, the terms of this Section 5 shall prevail.

5.5 Copies of Highly Confidential Information or Rights Issuer Private Keys. Except as set forth in the Rights Issuer Robustness Rules, Service Provider shall not (and shall ensure that those of its

- Participating Affiliates in possession of Highly Confidential Information or Rights Issuer Private Keys pursuant to Section 5.3.2 shall not) make any copies of any document containing Highly Confidential Information or Rights Issuer Private Keys, except when required for use by different business units designated to operate Licensed Service but located in different premises. Service Provider or its Participating Affiliate shall notify CMLA in the event such copies are made. Service Provider or its Participating Affiliates may request that CMLA provide Service Provider or its Participating Affiliate with additional copies of Highly Confidential documents for a fee as more fully set forth in the fee schedule. For copies of Highly Confidential Information such fee to be submitted to CMLA with each request. CMLA may, in its sole discretion, fulfill any such request provided that CMLA shall not unreasonably refuse to provide requested additional copies.
- 5.6 Service Provider/Participating Affiliates Contact Person. Service Provider shall have the right to designate on behalf of itself and/or its Participating Affiliates eight (8) employees who shall have the right to request and receive, and/or authorize a request for, a Rights Issuer Certificate (the “Service Provider Contact or Participating Affiliate Contact”) pursuant to Exhibit G which must be completed. The designation of additional Service Provider Contacts or Participating Affiliate Contacts or changes thereto, shall be subject to an additional fee as set forth in Exhibit C.
- 5.7 Notification of Unauthorized Use or Disclosure. Service Provider or its Participating Affiliates shall notify CMLA in writing promptly upon discovery of any unauthorized use or disclosure of a Rights Issuer Certificate, Rights Issuer Certificate request, Rights Issuer Private Keys, Confidential Information and/or Highly Confidential Information, and will cooperate with CMLA and the Founders in every reasonable way to regain possession of such information and to prevent its further unauthorized use or disclosure.. The procedures contained in Section 9 (Revocation of Rights Issuer Certificates) of this Agreement shall also apply.
- 5.8 Notification of Alleged Unauthorized Use by Others. Service Provider or Client Adopter may, in its sole discretion, provide CMLA with information regarding the alleged unauthorized use or misuse of Participating Product Implementations or Participating Rights Issuer Implementations, Licensed Products, Licensed Service or Digital Content by end users, Client Adopters or Fellow Service Providers. CMLA shall provide Content Participants with the information, in confidence, within a reasonable period of time. Service Provider understands and acknowledges that CMLA may receive such information regarding Service Provider and/or its Participating Affiliates and agrees that CMLA shall have no liability whatsoever in regards to the transmission of such information to Content Participants, save for its obligation to disclose it to Content Participants in confidence.
- 5.9 Disclosure of Service Provider Status. CMLA and Service Provider shall have the right to disclose to third parties the fact that Service Provider has obtained a license to implement the CMLA Technical Specification and CMLA intends to publish a list of CMLA Service Providers and other CMLA Technology Licensees at least once per quarter. Upon Service Provider’s written request to CMLA, CMLA shall maintain the fact that Service Provider has obtained a license to implement the CMLA Technical Specification confidential (and shall accordingly not include Service Provider on the list referred to in the previous sentence) until such time that Service Provider has publicly announced that it or any of its Participating Affiliates intends to offer a Participating Rights Issuer Implementation or Licensed Service or has begun marketing such a Licensed Service, whichever is earliest. In the event that Service Provider exercises this option, such Service Provider shall promptly notify CMLA when it has publicly announced its product plans or begins marketing a Licensed Service or Licensed Service Element.

- 5.10 Disclosure Required By Law. In the event Service Provider or any of its Participating Affiliates is required by law, regulation or order of a court or other authority of competent jurisdiction to disclose Confidential Information and/or Highly Confidential Information, (1) Service Provider shall take reasonable steps to notify CMLA prior to disclosure or (2) where notice to CMLA prior to disclosure is not reasonably possible, Service Provider shall take reasonable steps to challenge or restrict the scope of such required disclosure and notify CMLA as soon as possible thereafter. In either case, and at CMLA's cost, Service Provider shall take reasonable steps to seek to maintain the confidentiality of the information required to be disclosed and to cooperate with CMLA in any effort undertaken by CMLA to challenge the scope of such required disclosure. Notwithstanding anything herein to the contrary, any Party (and any employee, representative, or other agent of any Party) may disclose the U.S. federal tax treatment and tax structure (and all materials related to the tax treatment and tax structure) of the transactions contemplated by this Agreement, in the manner and to the extent contemplated by U.S. Treasury Regulations § 1.6011-4(b)(3)(iii).
- 5.11 Confidentiality Exceptions. The following information shall not be considered "Highly Confidential Information" and/or "Confidential Information" for the purpose of this Agreement: information which Service Provider can demonstrate (1) is or has been developed by Service Provider (or any of its Participating Affiliates') employees without reliance on or use of, such Highly Confidential Information and/or Confidential Information (including translations, derivations or abstractions of such Highly Confidential Information and/or Confidential Information) and without breach of this Agreement; or (2) is or has been disclosed to Service Provider (or its Participating Affiliates), without obligation of confidentiality, by a third party who has developed such information without reliance on or use of such Highly Confidential Information and/or Confidential Information and without any breach of such third party's obligations to CMLA, Founders, or Content Participants, Client Adopters or a Fellow Service Provider, or (3) at the time of its disclosure by CMLA to Service Provider or its Participating Affiliates, was already in its possession without obligation of confidence; or (4) is or has been disclosed by CMLA to another person without obligation of confidentiality; or (5) is in the public domain, other than as a result of breach of any obligation of confidentiality.
- 5.12 Confidentiality Period. The confidentiality obligations, related to Confidential Information, set forth in Section 5.2 shall be in effect during the term of this Agreement and shall continue thereafter until three (3) years after termination of this Agreement. The confidentiality obligations, related to Highly Confidential Information and Rights Issuer Private Keys, set forth in Section 5.3 shall be in effect during the term of this Agreement and shall continue thereafter until the later of (1) three (3) years after the last commercial use of the CMLA Technical Specification by CMLA or any Service Provider or Participating Affiliates, or (2) the expiration of the last copyright related to any CMLA Technical Specification encrypted/scrambled Digital Content which then exists in any country adhering to the Agreement on Trade Related Aspects of Intellectual Property Rights of the World Trade Organization dated April 15, 1994. Confidentiality obligations shall not apply to Rights Issuer Private Keys for which Rights Issuer Certificates have been revoked and destroyed in accordance with the revocation and destruction procedures contained in this Agreement.
- 5.13 Export. Service Provider shall comply with all applicable laws and regulations of the United States, European Union, Japan, Korea and other countries and jurisdictions relating to the export or re-export of commodities, software, and technical data insofar as they relate to activities under this Agreement, and shall obtain any approval required under such laws and regulations whenever it is necessary for such export or re-export. Service Provider agrees and understands that commodities, software and technical data provided under this Agreement may be subject to

restrictions under the export control laws of the United States, European Union, Japan, Korea and other countries and jurisdictions, as applicable, including but not limited to the US Export Administration Act, the US Export Administration Regulations, Council Regulation (EC) No. 1334/2000, the Japanese Foreign Exchange and Foreign Trade Law, and the Korean Foreign Trade Act, and shall obtain any approval required under such laws and regulations whenever it is necessary for such export or re-export. CMLA will, upon request, provide the Service Provider with the Export Control Classification Numbers for use in other jurisdictions.

5.14 Publicity. Except as set forth Section 5.9, CMLA shall obtain approval from Service Provider before issuing any press release(s) related to Service Provider (or any of its Participating Affiliates) use of the CMLA Technical Specification that identifies Service Provider (or any such Participating Affiliate), provided that such approval shall not be unreasonably withheld.

5.15 CMLA will use reasonable and robust procedures and methods in its key generation facility.

6. TERM/TERMINATION

6.1 Term. In general and subject to the termination provisions in Section 6.2, below, this Agreement shall have an initial term of ten (10) years from the Effective Date and may be renewed by mutual consent of parties. In the event CMLA continues to offer licenses to CMLA Technical Specification upon the expiration of this Agreement, CMLA will do so under fair, reasonable and non-discriminatory terms.

6.2 Termination. This Agreement shall commence upon the Effective Date and shall continue until terminated in accordance with any of the following events:

6.2.1 Termination by Service Provider. Service Provider shall have the right to terminate this Agreement at any time upon ninety (90) days prior written notice to CMLA and Founders.

6.2.2 Necessary Claim. CMLA may terminate this Agreement by written notice to Service Provider if Service Provider or any of its Affiliates asserts, against any CMLA Technology Licensee, a Necessary Claim in breach of Section 2.5, and such assertion is not withdrawn with thirty (30) days of the Service Provider receiving notice of the fact of the assertion from the CMLA (such notice to (i) provide sufficient information about the assertion that the Service Provider is able to identify the assertion and parties involved, and (ii) contain a warning that failure to withdraw the assertion may lead to termination of this Agreement). The termination shall become effective at the end of the above thirty (30) day period if the Service Provider or its Affiliates has not withdrawn the assertion.

6.2.3 Breach. CMLA may terminate this Agreement for any material breach by Service Provider or its Participating Affiliates, and Service Provider may terminate this Agreement for any material breach by CMLA or Founders, by providing prior written notice, specifying the material breach, to the breaching parties on becoming aware of the material breach and affording the breaching parties an opportunity to cure the breach. If the breach is not fully cured within thirty (30) days of receiving such notice the Agreement may be terminated. At the end of the thirty (30) day period, the party alleging breach will notify the other party as to whether or not it considers that the breach has been cured and/or the Agreement is terminated. The non-breaching party may set the effective termination date not more than sixty (60) days from date of receipt of notice of termination.

For the avoidance of doubt, termination of this Agreement on the grounds of breach by a Participating Affiliate(s) may be applied solely in relation to the Participating Affiliate that is in breach rather than affect this Agreement or the licenses granted to Service Provider or any other Participating Affiliate that is not in breach.

6.2.4 Dispute Resolution. In the event of a dispute between the CMLA and Service Provider regarding an alleged breach of this Agreement (except for the material breach of obligations regarding Highly Confidential Information or Rights Issuer Private Keys), the Parties agree to attempt to resolve such dispute by having senior management for each party, including a Founders' representative, discuss the issues within thirty (30) days of written notice specifying the issues to be resolved. The Parties agree to provide comments on a resolution proposal without undue delay.

6.2.5 Avoidance of Legal Liability.

- (i) CMLA may terminate this Agreement; or
- (ii) CMLA may terminate the license to CMLA IP, after reviewing alternatives set forth in Section 2.7, in the event CMLA provides a license to an alternative technology; or
- (iii) a Founder or its Affiliate may terminate any licenses granted hereunder to Necessary Claims (and if it does so, that Founder or its Affiliate shall automatically be subject to a reciprocal covenant not to assert such Necessary Claims, as more fully set forth in Section 2.5).

In the event CMLA (acting reasonably) determines it is necessary to do so to avoid potential legal liability for CMLA, Founders, or substantially all of the CMLA Technology Licensees, by providing thirty (30) days written notice to Service Provider.

6.3 Effect of Termination. On the effective date of termination or expiration of this Agreement, Service Provider and its Participating Affiliates shall promptly cease all activities under licenses granted under Section 2, including but not limited to ceasing the use of any and all Rights Issuer Private Keys and Rights Issuer Certificates which will be revoked by CMLA. Licenses to Necessary Claims from the Founders shall terminate upon the effective date of termination or expiration of this Agreement and for cases set forth in Section 6.2.5, above, Founders shall automatically be subject to the reciprocal covenants not to assert as set forth in Section 2.5. Within thirty (30) days after the effective date of termination or expiration of this Agreement, Service Provider and/or its Participating Affiliate(s) shall return all Confidential Information and Highly Confidential Information to CMLA or, at CMLA's option, destroy all such information in its possession, retaining no copies thereof, and provide to CMLA a written certification of such destruction signed by a senior official or officer of the Service Provider. Service Provider and its Participating Affiliates, if applicable, shall immediately cease use of Rights Issuer Private Key and no longer offer, provide or distribute a Participating Rights Issuer Implementation, Licensed Service or Licensed Service Elements upon termination or expiration of this Agreement. Service Provider and its Participating Affiliates, if applicable, shall within five (5) days from termination or expiration of this Agreement destroy all copies of Rights Issuer Private Keys, from wherever located, within and provide CMLA, within an additional fifteen (15) days, with written certification of such destruction signed by a senior official or officer of the Service Provider and its Participating Affiliates, if applicable.

6.4 Survival. The Reciprocal Non-Assertion Covenant (Section 2.5) and such other sections of this Agreement that, by their own terms survive termination or expiration of this Agreement, shall continue in full force after termination or expiration of this Agreement until by their terms they are fulfilled. For purposes of clarity, Section 2.5 shall survive for the CMLA Technical Specification adopted and effective during the term of the Agreement with Service Provider and not to new versions of the CMLA Technical Specification adopted after termination of the Service Provider Agreement.

7 **DISCLAIMER & LIMITATION ON LIABILITY**

7.1 Generally. The following terms, inter alia, limit the ability of the Service Provider to recover any damages from CMLA or the Founders in excess of fees actually paid to the CMLA by Service Provider. These provisions are an essential part of the bargain, without which CMLA would not be willing to enter into this Agreement, and the Founders would not be willing to license their Necessary Claims.

7.2 Disclaimer. ALL INFORMATION, INCLUDING CMLA TECHNICAL SPECIFICATION IS PROVIDED “AS IS.” EXCEPT FOR THE WARRANTY SET FORTH IN SECTION 2.7(a), CMLA, FOUNDERS AND THEIR AFFILIATES MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EXPRESSLY DISCLAIM IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION THAT MIGHT ARISE FROM ANY ACTIVITIES OR INFORMATION DISCLOSURES RELATING TO THIS AGREEMENT. CMLA, FOUNDERS, AND AFFILIATES FURTHER DISCLAIM ANY WARRANTY THAT ANY IMPLEMENTATION OF THE CMLA TECHNICAL SPECIFICATION, IN WHOLE OR IN PART, WILL BE FREE FROM INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY OR PROPRIETARY RIGHTS.

7.3 Limitation of Liability.

7.3.1 TO THE MAXIMUM EXTENT PERMITTED BY LAW, NEITHER CMLA NOR FOUNDERS OR THEIR AFFILIATES, NOR ANY OF THEIR DIRECTORS, OFFICERS, AGENTS, MEMBERS, REPRESENTATIVES, EQUIVALENT CORPORATE OFFICIALS, OR EMPLOYEES ACTING IN THEIR CAPACITIES AS SUCH (COLLECTIVELY THE “AFFECTED PARTIES”) SHALL BE LIABLE TO SERVICE PROVIDER OR ITS AFFILIATES, IF APPLICABLE, FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES ARISING OUT OF ANY CAUSE OF ACTION RELATING TO THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, REVOCATION OF RIGHTS ISSUER CERTIFICATES, OR BASED ON ANY PERSON’S USE OF OR MAKING, USING, SELLING OR IMPORTING ANY SERVICES OF SERVICE PROVIDER THAT IMPLEMENT CONFIDENTIAL OR HIGHLY CONFIDENTIAL INFORMATION OR RIGHTS ISSUER PRIVATE KEYS OR THE CMLA TECHNICAL SPECIFICATION, WHETHER UNDER THEORY OF CONTRACT, TORT, INDEMNITY, INTELLECTUAL PROPERTY INFRINGEMENT (DIRECT, CONTRIBUTORY OR OTHERWISE) PRODUCT LIABILITY OR OTHERWISE.

7.3.2 TO THE EXTENT THAT ANY COURT OF COMPETENT JURISDICTION RENDERS JUDGMENT AGAINST ANY OF THE AFFECTED PARTIES, NOTWITHSTANDING THE LIMITATION IN SECTION 7.3.1, ABOVE, OR WITH

RESPECT TO DIRECT DAMAGES, THE AFFECTED PARTIES' AGGREGATE LIABILITY TO SERVICE PROVIDER OR ITS AFFILIATES IN CONNECTION WITH THIS AGREEMENT SHALL IN NO EVENT EXCEED THE FEES PAID BY SERVICE PROVIDER AND ITS PARTICIPATING AFFILIATES, IF APPLICABLE, TO CMLA HEREUNDER.

7.3.3 TO THE MAXIMUM EXTENT PERMITTED BY LAW, NEITHER SERVICE PROVIDER NOR ITS PARTICIPATING AFFILIATES, NOR ANY OF THEIR DIRECTORS, OFFICERS, AGENTS, MEMBERS, REPRESENTATIVES, EQUIVALENT CORPORATE OFFICIALS, OR EMPLOYEES ACTING IN THEIR CAPACITIES AS SUCH (COLLECTIVELY THE "SERVICE PROVIDER AFFECTED PARTIES") SHALL BE LIABLE TO CMLA, FOUNDERS, OR THEIR AFFILIATES OR TO ANY OTHER SERVICE PROVIDER, CLIENT ADOPTER OR CONTENT PARTICIPANT FOR INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES ARISING OUT OF ANY CAUSE OF ACTION RELATING TO THIS AGREEMENT, WHETHER UNDER THEORY OF CONTRACT, TORT, INDEMNITY, INTELLECTUAL PROPERTY INFRINGEMENT (DIRECT, CONTRIBUTORY OR OTHERWISE) PRODUCT LIABILITY OR OTHERWISE. NOTWITHSTANDING SUCH LIMIT, SERVICE PROVIDER OR ITS PARTICIPATING AFFILIATES, IF APPLICABLE, MAY BE LIABLE FOR DAMAGES OR OTHER RELIEF IN THE CIRCUMSTANCES EXPRESSLY SET FORTH AND/OR REFERENCED IN SECTION 8 AND/OR ACKNOWLEDGED IN SECTION 8.9.

8. REMEDIES

8.1 Indemnification for Wrongful Acts. Service Provider and its Participating Affiliates, if applicable, shall indemnify and hold CMLA, Founders and their respective officers, members, representatives, agents, directors, equivalent corporate officials, and employees (each, an "Indemnified Person"), harmless from and against any and all defense costs and expenses, including without limitation, reasonable attorney's fees and all related costs and expenses, to be paid in connection with the defense of any suit at law or litigation against such Indemnified Person, which result from any breach of any covenant, agreement, representation or warranty herein or negligent acts committed by the Service Provider, its Participating Affiliates and its or their employees (whilst acting in their capacity as such) and agents (whilst acting in their capacity as such). Where any or all damages, defense costs and/or expenses are awarded or otherwise finally obtained by an Indemnified Person in any such suit at law or litigation, such damages, costs and expenses shall first be applied to offset any and all costs and expenses paid by the Service Provider in respect thereof pursuant to this Section 8.1.

8.2 Inspection/Audit If requested, Service Provider and/or its Participating Affiliates shall provide reasonable cooperation in affording an independent third party auditor (the "Auditor") access to, during normal business hours, relevant Service Provider facilities, for the sole purpose of auditing any Participating Rights Issuer Implementation, Licensed Service or Licensed Service Element performed or used hereunder and shall provide to the auditor, under the terms of the Non-Disclosure Agreement referred to below, the service manual for any such Participating Service Implementation, Licensed Service or Licensed Service Element and any further details available to the Service Provider or its Participating Affiliate which are necessary to determine whether Service Provider or its Participating Affiliates' Participating Rights Issuer Implementation, Licensed Service or Licensed Service Element is Compliant. Service Provider may, at its option,

provide information relevant to determine the Compliance of a Participating Rights Issuer Implementation, Licensed Service or Licensed Service Element. CMLA shall provide a list of three independent auditors approved by CMLA from which the Service Provider the may choose within thirty (30) days from date of notice of audit. The cost of the Auditor will be at CMLA's expense. CMLA shall ensure that, in respect of each such audit:

- 8.2.1 no such audit is carried out unless the Auditor is bound by a Non-Disclosure Agreement which is at least as protective, of the information obtained as a result of the audit, as the applicable terms of Section 5 of this Agreement are with respect to Confidential Information;
- 8.2.2 the only information disclosed by the Auditor to any person (including the Founders or CMLA) as a result of the audit is a certificate specifying whether the Participating Rights Issuer Implementation, Licensed Service or Licensed Service Element performed hereunder to determine whether they are Compliant;
- 8.2.3 the audit shall be conducted with commercially reasonable (and, in any event, not less than thirty (30) days') notice using commercially reasonable means and in such a way as to reasonable means to minimize any disruption caused to Service Provider or its Participating Affiliates business; and
- 8.2.4 the Service Provider or the relevant Participating Affiliate has the right to accompany the Auditor throughout the audit and to provide written objections to CMLA regarding the Auditor's findings in the event the Service Provider or the relevant Participating Affiliate does not agree with them.

Nothing in this Section 8.2 shall grant a license or permission for CMLA or any Auditor to decompile or disassemble Service Provider's software object code. Nothing in this Section 8.2 shall grant a license or permission for CMLA, Founder or any auditor to take any actions or make use of information resulting from such examination or evaluation for any purpose other than for verifying whether Service Provider's or its relevant Participating Affiliates' Participating Rights Issuer Implementation, License Service or Licensed Service Element is Compliant. Such audit shall occur no more frequently than annually per type or model of Participating Service Implementation, Licensed Service or Licensed Service Element.

- 8.3 Equitable Relief. Service Provider agrees that if it or its Participating Affiliate(s) materially breaches its or their obligations under Section 5 (Confidentiality), the Compliance Rules or the Robustness Rules, and such breach is not cured after notice thereof, in accordance with Section 6.2.3, money damages are inadequate to compensate an injured party due to the unique nature of certain provisions of this Agreement and the lasting effect and harm from any breach of such provisions, including making available the means for and/or providing an incentive for widespread circumvention of the CMLA Technical Specification and unauthorized copying of Digital Content intended to be protected using the CMLA Technical Specification. Service Provider further agrees that, as provided by law, injunctive relief may be an appropriate remedy to prevent or limit the adverse consequences of actual or threatened material breaches of this Agreement. CMLA agrees that failures of CMLA Technical Specification, or any aspect of CMLA Technical Specification, that are not caused by material breaches by Service Provider or its Participating Affiliates shall not trigger application of the provisions of this Section 8.3 or Section 8.4 to Service Provider or Participating Affiliates and/or its or their Participating Rights Issuer Implementation, Licensed Service or License Service Element.

8.4 Damages Measures and Limitation. The parties agree that it may be impossible to estimate the amount of damages in the event of certain breaches. Service Provider agrees that in the event of those material breaches by Service Provider or its Participating Affiliates described below in Sections 8.4.1-8.4.3, CMLA, in addition to any other remedies in equity, but in lieu of any and all other claims for monetary damages, may recover liquidated damages for each material breach in the amount set forth below, such amounts to be the exclusive monetary remedies available for any and all such breaches under this Agreement by Service Provider. For purposes of this Section 8.4, any series of substantially related events arising from the same event; or series of connected events, shall constitute a single material breach. For the avoidance of doubt, in the event that Service Provider or its Participating Affiliates pays the amount designated in this Section 8.4 in connection with a material breach by Service Provider or its Participating Affiliates of this Agreement, Service Provider or its Participating Affiliates shall have no liability (whether to CMLA, Founders or any other CMLA Technology Licensee, except as set forth in Section 8.9, below) for additional monetary damages (regardless of the legal theory, including negligence, contract, tort, indemnity, intellectual property infringement (direct, contributory or otherwise) product liability or otherwise) based in whole or in part on the act(s) or omission(s) of the Service Provider or any of its Participating Affiliates that gave rise to such material breach.

8.4.1 Material Breach of Confidentiality Provisions.

- (i) In the event of a material breach by the Service Provider or its Participating Affiliate of the Confidentiality provisions set forth in Section 5.3 and 5.4. of this Agreement, and such breach is not cured in accordance with Section 6.2.3, Service Provider shall be liable for **one million U.S. dollars (US\$1,000,000)**.
- (ii) Notwithstanding the foregoing, Service Provider shall be liable for **one hundred thousands U.S. dollars (US\$100,000)** in the event of material breach of the Confidentiality Provisions by itself or its Participating Affiliate set forth in Section 5.2 of this Agreement which breach is not cured in accordance with Section 6.2.3.
- (iii) In addition to the provisions of Section 8.4.4, there is no material breach of the applicable provisions (as referred to in Section 8.4.1 (i) and 8.4.1 (ii)) if no Confidential Information and/or Highly Confidential Information was released to a third party not permitted hereunder to have such information or could not reasonably have been expected to have been released to such third party as a result of the breach. For the avoidance of doubt, if such material breach of Sections 5.3, 5.4 or 5.5 consists of a material breach of the Compliance or Robustness Rules only, the provisions of Section 8.4.2 only and not of this Section 8.4.1 shall apply to such material breach.

8.4.2 Breach of Compliance or Robustness Rules. In the event of a material breach of the Compliance Rules or Robustness Rules that results in a Participating Rights Issuer Implementation, Licensed Service or Licensed Service Element being used, manufactured, distributed or performed that fails to comply with the requirements of the Compliance Rules and Robustness Rules and such breach is not cured in accordance with Section 6.2.3, Service Provider or its Participating Affiliates shall be liable in an amount equal to its profits on such Participating Rights Issuer Implementation, Licensed Service or Licensed Service Element and in no event less than **one million U.S. dollars (US\$1,000,000)** nor more than **eight million U.S. dollars (US\$8,000,000)**. Systemic failures of CMLA Technical Specification that are not caused by material breaches of this Agreement by Service Provider or its Participating Affiliate shall not trigger application

of the provisions of this Section 8.4.2 to Service Provider, its Participating Affiliate and/or its or their products or services.

8.4.3 Other Material Breaches. In the event of a material breach by Service Provider or its Participating Affiliates of any other provision of this Agreement, and such breach is not cured in accordance with Section 6.2.3, Service Provider or its Participating Affiliate, shall be liable in an amount equal to its profits on the affected Participating Rights Issuer Implementation, Licensed Service and/or Licensed Service Element, and in no event more than *eight million U.S. dollars (US\$8,000,000)*.

8.4.4 For purposes of Section 8.3 and this Section 8.4, a breach shall be “material” only if the claiming party, by the preponderance of evidence, demonstrates that it has resulted in commercially significant harm to other CMLA Technology Licensees or a significant threat to the integrity or security of the CMLA Technical Specification. In addition, the following is a non-exclusive list of circumstances in which there is no material breach of the applicable provisions:

- (1) if Service Provider or its relevant Participating Affiliate maintains a documented internal program to assure compliance with its relevant obligations under this Agreement (including, in respect of Section 8.4.1, a program to assure the secure storage of Rights Issuer Private Keys and maintenance of Licensed Service (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation), Licensed Service Elements, other inventory, samples, and confidentiality of information for purposes in addition to compliance with this Agreement); or
- (2) the material breach was inadvertent or otherwise unintentional, and the breach did not have a material adverse effect on the integrity or security of the CMLA Technical Specification; or
- (3) if Service Provider brought the breach to CMLA’s attention in a timely manner as required by this Agreement and such breach did not have a material adverse effect on the integrity or security of the CMLA Technical Specification.

8.5 Eligible Content Participant Third Party Beneficiary Rights.

8.5.1 The parties agree that Service Provider and its applicable Participating Affiliate’s compliance with the terms and conditions of this Agreement is essential to maintain the value and integrity of the CMLA Technical Specification. As part of the consideration granted herein, a Service Provider agrees that each Eligible Content Participant shall be a Third Party Beneficiary of this Agreement and shall be entitled to bring a Third Party Beneficiary Claim to enforce certain rights against Service Provider or its Participating Affiliates in accordance with the procedures set out in Sections 8.3 and 8.5, and subject to the provisions of Section 10.6, 10.7 and 10.8, with respect to Service Provider or its Participating Affiliates’ use and implementation of the CMLA Technical Specification, so long as Content Participant is an Eligible Content Participant with respect to such Participating Rights Issuer Implementation, Licensed Service or Licensed Service Element that receives, transmits or plays data in a format protected by CMLA Technical Specification in Participating Rights Issuer Implementations, Licensed Service or Licensed Service Elements. For an Eligible Content Participant fulfilling the above criteria, Third Party Claims will be limited to seeking injunctive relief against:

- (i) the performance, commercial use and sale of Service Provider's or its Participating Affiliates' Participating Rights Issuer Implementation, Licensed Service or Licensed Service Element that are in material breach of the Compliance Rules or Robustness Rules; and
- (ii) against disclosure of Highly Confidential Information or Rights Issuer Private Keys, in breach of this Agreement, where such breach materially and adversely affects the integrity of the CMLA Technical Specification or the security of Digital Content owned or controlled by Content Participant.

The prevailing party in any action brought under Sections 8.5 or 8.6 of this Agreement shall additionally be entitled to an award of its reasonable attorneys fees incurred in relation to the Third Party Beneficiary Claim in an amount to be fixed either pursuant to stipulation by the parties to a given case or the court provided that (a) the prevailing party if it is an Eligible Content Participant, establishes by clear and convincing evidence that the Service Provider or its Participating Affiliates has materially breached or engaged in a pattern or practice of breaching the Compliance Rules or Robustness Rules or disclosing Highly Confidential Information or Rights Issuer Private Keys; (b) the court in its discretion may elect to make no award of attorneys fees in any given case, and in any event, shall be limited to an award of no more than US\$1,000,000 (one million U.S. dollars); and (c) no award of attorneys fees shall be available against any Founder, unless such Founder is in a role of a CMLA Technology Licensee.

8.5.2 Service Provider acknowledges and agrees that an Eligible Content Participant may seek, and a court may, in its discretion, grant the following additional remedies in relation to any Participating Product Implementation subject to an injunction issued pursuant to 8.5.1 (i), in the Client Adopter Agreement:

- (a) The court may authorize Service Providers and/or Participating Affiliates to refuse service to Client Adopter product or class of product using DeviceDetails by requiring the Service Provider and/or its Participating Affiliates to deny service to a Participating Product Implementation that is subject to an already-issued injunction under section 8.5.1(i), pursuant to the Client Adopter Agreement, based on a determination that the DeviceDetails identify the particular Participating Product Implementation as one subject to the injunction. For purposes of this Section 8.5.2. (Service Provider waives any objections it might otherwise have to any such joinder.) "DeviceDetails" means an extension defined in the OMA DRM Specifications for the ROAP protocol. DeviceDetails extension, when used, requires the software or device to respond to the Rights Issuer with the appropriate information (manufacturer, model, & version number) during the Rights Object Acquisition Protocol (ROAP) (as defined in the OMA DRM 2.0 Specification).
- (b) For the avoidance of doubt, the remedies authorized pursuant to third party beneficiary rights as described in sections (a) above is intended to be, and should be, whenever feasible, strictly limited to the specific Participating Product Implementation subject to the injunction issued pursuant to 8.5.1(i) of the Client Adopter Agreement and may be extended to a class of products or the entirety of Device Certificates of a Client Adopter only when such far-reaching relief is determined by the court to be both necessary and justified, after having considered all

relevant interests and circumstances and consequences of the actions requested from the court.

Nothing in Section 8.5.2 of the Client Adopter or Service Provider Agreement limits a Content Participant's ability to contract directly with Client Adopter or Service Provider to develop and implement denial of service and customer filtering regimes not covered by this Agreement.

- 8.6 Procedures for Third Party Beneficiary Claims. Prior to initiating any Third Party Beneficiary Claim, the Eligible Content Participant seeking to institute such a claim must, as a condition to its right to assert such a claim hereunder, provide CMLA written notice of its intent to pursue such a claim. Such Eligible Content Participant shall likewise provide CMLA notice of the actual filing of any Third Party Beneficiary Claims, and shall at CMLA's request provide copies of material documents to be filed in such Third Party Beneficiaries initiation, institution or pursuit of such Third Party Beneficiary Claim. CMLA shall offer reasonable cooperation to such Third Party Beneficiary in providing appropriate and necessary information in connection with the Third Party Beneficiary Claim to the extent that such cooperation is consistent with protecting the integrity and security of the CMLA Technical Specification and does not otherwise interfere with CMLA's obligations to other CMLA Technology Licensees. Third Party Beneficiaries shall not be obligated to provide copies of documents filed (or to be filed) under seal. CMLA shall have the option of requiring that any information or documents provided by CMLA, Founders, Client Adopters, CMLA Service Providers to Third Party Beneficiary be filed under seal. Documents provided to CMLA under the procedures set out herein shall not include any documents filed or to be filed under seal in connection with such Third Party Beneficiary Claim.
- 8.7 Joining Third Party Beneficiary Claims. CMLA shall provide timely notice to all Content Participants, CMLA Service Providers and Client Adopters of receipt of any notice of a Third-Party Beneficiary Claim against a defendant ("Defendant"). Within 30 days of the date of mailing of such notice, each Eligible Content Participant, shall elect whether to join the Third Party Beneficiary Claim and provide notice of intent to join such Third Party Beneficiary Claim to CMLA. The failure by a particular Content Participant, to provide notice to CMLA and to move to join such Third Party Beneficiary Claim within the allotted thirty (30) day period shall be deemed a waiver of such Content Participant's right to be a Third Party Beneficiary under its Content Participant Agreement, with respect to all claims it may have against Defendant arising out of the alleged breach asserted pursuant to the notified Third Party Beneficiary Claim. The Third Party Beneficiary instituting or initiating a Third Party Beneficiary Claim shall support, and Defendant shall not object to, any motion by another Eligible Content Participant to so join provided it is instituted within the thirty (30) day period following mailing of notice by CMLA of a Third Party Beneficiary Claim. Judgment entered upon such Third Party Beneficiary Claims shall be binding on all Content Participants, who received notice from CMLA as if they had joined such Third Party Beneficiary Claim. Neither a Content Participant, CMLA Service Provider and/or Client Adopter's failure to notify and consult with CMLA, nor CMLA's failure to give notice to any Content Participant, CMLA Service Provider or Client Adopter in accordance with these Third Party Beneficiary Claim procedures shall be a defense to any Third Party Beneficiary Claim or grounds for a request to delay the granting of preliminary relief requested.
- 8.8 Settlement of Third Party Beneficiary Claims. Third Party Beneficiaries shall have no right to, and Service Provider and its Participating Affiliates agrees that it shall not, enter into any settlement of any Third Party Beneficiary Claim that: (1) amends any material term of any CMLA Technology License Agreement; or (2) has an adverse effect on the integrity and/or security of the CMLA Technical Specification; or (3) adversely affects or lowers the value of any

of CMLA's or the Founder's rights in and to the CMLA Technical Specification or any intellectual property right related to it (embodied therein) unless CMLA and the Founders shall have provided prior written consent thereto.

- 8.9 No Limitations of Remedies. Service Provider acknowledges that Content Participant's exercise of its right to be a Third Party Beneficiary under this Section 8 shall not constitute an election against any statutory or other non-contractual remedy against a Service Provider which may be available to Eligible Content Participant for the same act that gave rise to the Third Party Beneficiary Claim.

9. REVOCATION OF RIGHTS ISSUER CERTIFICATES

- 9.1 Generally. The OMA DRM Specifications include the means by which Rights Issuer Certificate status can be communicated to Participating Product Implementations or Licensed Products during the Rights Object Acquisition Protocol (ROAP). The OMA DRM Specifications also require the software or devices to check the revocation status of the Rights Issuer prior to accepting any Rights Objects from that Rights Issuer. Once a Rights Issuer Certificate is revoked, the revocation status will be indicated in the OCSP responses provided by the OCSP Responders run by CMLA. The Rights Issuer, during the course of ROAP transactions, will convey this OCSP Response to the Participating Product Implementation or Licensed Product. The effect of revocation is that ROAP transactions with devices will fail and hence disable the Rights Issuer from issuing any new Rights Objects. Service Provider understands and agrees that if CMLA determines that circumstances warranting revocation of a Rights Issuer Certificate exist, all Rights Issuer services incorporating the corresponding Rights Issuer Private Key shall be affected.

- 9.2 Circumstances Warranting Rights Issuer Certificate Revocation. CMLA may revoke a Rights Issuer Certificate, pursuant to the procedures in Sections 9.3 to 9.5, either at its own initiative, or that of any Client Adopter, Eligible Content Participant, (so long as the Content Participant is an Eligible Content Participant with respect to any Participating Rights Issuer Implementation, Licensed Service or Licensed Service Element offered by Service Provider and/or its Participating Affiliates) or CMLA Service Provider (other than the "Affected Service Provider", being the Service Provider to which the Rights Issuer Certificate in question relates), when CMLA determines, based on the facts presented to it, that one of the following criteria (the "Revocation Criteria") are met:

- (1) a Rights Issuer Private Key corresponding to that Rights Issuer Certificate has been cloned such that the same Rights Issuer Private Key is found in a Participating Rights Issue Implementation or Licensed Service offered by more than one entity (the Service Provider and each of its Participating Affiliates each being considered a separate "entity" for these purposes) (except that this Section 9.2(1) shall not apply in respect of any cloning which is expressly permitted by any relevant CMLA Technology License Agreement);
- (2) a Rights Issuer Private Key corresponding to that Rights Issuer Certificate has been made public, lost, stolen, intercepted or otherwise misdirected or disclosed.

In addition, CMLA may revoke a Rights Issuer Certificate when directed to do so by law, court order or by a competent governmental security agency or other competent government authority having the power to require revocation of a Rights Issuer Certificate or pursuant to the arbitration procedures set forth in Section 9.5(d) and (e). CMLA shall not revoke a Rights Issuer Certificate except as expressly stated in this Section 9.2.

- 9.3 Consultation with Affected Service Provider. In the event CMLA receives a request to revoke a Rights Issuer Certificate based on a sworn affidavit from an Eligible Content Participant, CMLA Service Provider (not being the Affected Service Provider) or Client Adopter, as set out in Section 9.5(a), CMLA shall promptly provide the Affected Service Provider with a copy of such affidavit and request its consent to revoke the applicable Rights Issuer Certificate. (As used in this Agreement “sworn affidavit” shall mean, in the case of countries where a sworn affidavit is unknown or unacknowledged, the official comparable legal document of such country, in which at least the identity of the person giving the statement is confirmed and verified by local officials). The Affected Service Provider shall respond to CMLA’s request within fifteen (15) days of the receipt of notice in accordance with the notice procedures of this Agreement, indicating whether or not it consents to the proposed revocation, and shall not unreasonably withhold such consent. In the event the Affected Service Provider provides notice that it does not consent to revocation, it shall provide reasons why the affidavit did not provide facts that would satisfy the Revocation Criteria and it shall supply any additional facts in its own sworn affidavit, within an additional fifteen (15) days, that establish why the Revocation Criteria have not been met, and shall thereafter promptly submit to arbitration, upon obtaining an assurance (including as to the payment of the costs of the arbitration) from the party seeking the revocation, in accordance with the procedures set forth in Section 9.5(d)
- 9.4 Service Provider Request for Rights Issuer and Device Certificate Revocation. Service Provider may seek Rights Issuer and Device Certificate revocation by providing CMLA with an affidavit as set out in Section 9.5(a).
- 9.5 Procedures for Revocation.
- (a) The entity (which may include CMLA) initiating a proposal for revocation of a Rights Issuer Certificate or Device Certificate may only do so by providing proof in a sworn affidavit of facts indicating that a particular Rights Issuer Certificate or Device Certificate should be revoked because the Revocation Criteria or equivalent under the Client Adopter Agreement (together the “Applicable Revocation Criteria”) has been met. Each such affidavit shall be sufficiently detailed such that it is possible to determine, solely on the basis of such affidavit, whether the facts averred are sufficient to satisfy the Applicable Revocation Criteria.
- (b) Upon receipt of a sworn affidavit from a Fellow CMLA Service Provider, Client Adopter or Eligible Content Participant, as provided above, CMLA shall review it in light of the Applicable Revocation Criteria and, in accordance with CMLA’s procedures, promptly determine whether Rights Issuer Certificate or Device Certificate Revocation is warranted.
- (c) If (either at its own initiation or following receipt of an affidavit from a CMLA Service Provider, Client Adopter or Eligible Content Participant) CMLA determines that either or both of the Applicable Revocation Criteria are met, CMLA shall promptly provide the Affected Service Provider or Client Adopter (Affected Party) with a copy of the affidavit and request the Affected Party’s consent to revoke the applicable Rights Issuer Certificates or Device Certificate. If the Affected Party consents, CMLA shall take steps to revoke the applicable Rights Issuer Certificate or Device Certificate by updating the OCSP Responder so it reflects the correct status.
- (d) If (A) CMLA determines that neither of the Applicable Revocation Criteria are met; or (B) the Affected Party objects to CMLA’s request to revoke the Rights Issuer Certificates or Device Certificate within fifteen (15) days of receipt of the affidavit supplied under Section 9.5(c) or does not respond to CMLA’s request to revoke the Rights Issuer Certificate or

Device Certificate within fifteen (15) days, the matter shall be submitted to arbitration by CMLA upon obtaining an assurance (including as to the payment of the costs of the arbitration) from the party seeking the revocation and unless the entity that initiated a proposal for revocation withdraws such request for revocation. At such arbitration the party or parties seeking revocation shall bear the burden of proof to demonstrate by a preponderance of the evidence that the applicable Revocation Criteria have been met. Any CMLA Technology Licensee that can demonstrate to CMLA by a preponderance of the evidence that it may (or any of its Affiliates may) be adversely affected by a proposed revocation may participate in such arbitration and provide evidence and information as an interested party either in support of the Affected Party or in support of another CMLA Technology Licensee.

- (e) Any arbitration pursuant to this section 9.5 shall be conducted in accordance with the following procedures:
- (i) There shall be a sole arbitrator who shall be selected by the American Arbitration Association from its National Panel of Commercial Arbitrators. The arbitrator shall have a minimum of fifteen (15) years knowledge or experience in the telecommunications, computer or software industries.
 - (ii) The arbitration shall be conducted in New York, N.Y. in accordance with the International Arbitration Rules of the American Arbitration Association. The arbitration shall be conducted in English.
 - (iii) The arbitrator shall be directed to complete the arbitration within sixty (60) days but may otherwise conduct the arbitration in such manner as it shall deem appropriate, including the imposition of time limits that it considers reasonable for each phase of the proceeding, but with due regard for the need to act, and make a final determination, in an expeditious manner.
 - (iv) The arbitrator shall permit and facilitate such limited discovery as he or she shall determine is reasonably necessary, taking into account the needs of the parties and the desirability of making discovery as expeditious and cost-effective as possible.
 - (v) The parties and the arbitrator shall treat the arbitration proceedings, any related discovery, documents and other evidence submitted to, and the decision of, the arbitrator as confidential information and shall not disclose it to any third parties nor use such confidential information for any purpose other than the arbitration proceedings, provided that CMLA may disclose the fact of a revocation of a Rights Issuer Certificate or Device Certificate. In addition, and as necessary, the arbitrator may issue orders to protect the confidentiality of proprietary information, trade secrets and other sensitive information disclosed in discovery or otherwise during the arbitration.
 - (vi) The arbitrator is empowered solely to determine whether either of the Revocation Criteria have been met. The arbitrator shall be obliged to reduce the decision to writing and provide reasons supporting the decision. Any such determination shall be final and binding on the parties, except that whether the arbitrator exceeded his or her authority in determining the remedy, or otherwise, shall be fully reviewable by a court of competent jurisdiction. Judgment upon any award shall be entered in a court of competent jurisdiction.

(vii) The arbitrator shall be compensated at his or her hourly rate, determined at the time of appointment, for all time spent in connection with the arbitration, and shall be reimbursed for reasonable travel and other expenses. The arbitrator shall determine all costs of the arbitration, including his or her fees and expenses, the costs of expert advice and other assistance engaged by the arbitrator, the cost of a transcript and the costs of meeting and hearing facilities. The arbitrator shall assess the losing party or parties for the costs of the arbitration set forth in this subsection (vii) provided that “party or parties” for purposes of this sentence shall not include CMLA, unless CMLA sought the revocation on its own initiative, and shall include the CMLA Technology Licensee(s) seeking the revocation and the Service Provider or Client Adopter whose certificate is the subject of the revocation request.

10. MISCELLANEOUS

- 10.1 Ownership. All Confidential and/or Highly Confidential Information, copyrighted or patented information, and media containing any of the above as provided by CMLA to Service Provider or its Participating Affiliate shall remain the property of CMLA, the Founders, or their suppliers. Except as expressly provided herein, this Agreement does not give Service Provider any license or other rights to any information provided under this Agreement.
- 10.2 Entire Agreement. This Agreement, provisions of other CMLA Technology License Agreements specifically referenced herein, the Exhibits hereto and the CMLA Technical Specification constitute the entire agreement between the parties with respect to the subject matter involved and supersede all prior or contemporaneous oral or written agreements. This Agreement shall not be modified except by written agreement dated subsequent to the date of this Agreement and signed by all parties. Any changes to the CMLA Technology License Agreements shall be notified by CMLA to each current CMLA Technology Licensee. For purposes of this Section 10.2, notice shall be deemed delivered by means of a message on the CMLA website for all CMLA Technology Licensees.
- 10.3 Currency. All fees shall be paid to CMLA or to its order in United States dollars by wire transfer or such other means as CMLA may reasonably specify.
- 10.4 Assignment. The rights and licenses granted to Service Provider (and to Service Provider’s Participating Affiliates) by this Agreement are personal to Service Provider (and to such Participating Affiliates) and shall not be assigned or otherwise transferred except: (1) to any party with the written approval of CMLA and with respect to Necessary Claims, written approval of the Founders, which approval shall not be unreasonably withheld or delayed; (2) to a corporation controlling, controlled by or under common control with Service Provider (and for these purposes, “control” has the meaning given in the definition of “Affiliate” in Section 1, and “controlling” and “controlled” shall be construed accordingly); or (3) to the purchaser of all or substantially all of the outstanding capital stock or assets and obligations of Service Provider or of all or substantially all of the outstanding capital stock or assets and obligations of the business unit of Service Provider that is making use of the Confidential and/or Highly Confidential Information and/or Rights Issuer Private Keys in its business activities or the surviving entity in a merger, reorganization, or other business combination; provided written notice of such assignment has been provided in advance to CMLA and the surviving or acquiring company has agreed in writing to be bound by the terms of this Agreement. Subject to the limitations set forth in this Agreement, this Agreement shall inure to the benefit of and be binding upon the parties, their successors and permitted assigns. CMLA or Founders may assign or transfer this

Agreement to a party that agrees to assume the transferors obligations hereunder, and will provide Service Provider with written notice of such assignment or transfer.

10.5 Presumptions. In construing the terms of this Agreement, no presumption shall operate in any party's favor as a result of its counsel's role in drafting the terms or provisions hereof.

10.6 Governing Law. THIS AGREEMENT, AND ALL THIRD PARTY BENEFICIARY CLAIMS BROUGHT PURSUANT TO IT, SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW YORK APPLICABLE TO AGREEMENTS MADE AND TO BE PERFORMED ENTIRELY IN SUCH STATE, WITHOUT REGARD TO THAT STATE'S CONFLICT OF LAWS PRINCIPLES. IN ANY DISPUTE ACTION OR CLAIM ARISING OUT OF OR IN RELATION TO THIS AGREEMENT, THE PARTY ASSERTING A DISPUTE, ACTION OR CLAIM MAY AT ITS OPTION ARBITRATE SUCH DISPUTE, ACTION OR CLAIM. THE RULES GOVERNING ARBITRATION SHALL BE THE ARBITRATION RULES SET FORTH IN SECTION 9.5(e), ABOVE.

The rights and obligations of the Parties shall not be governed by the provisions of the U.N. Convention on Contracts for the International Sale of Goods, 1980; rather, the Parties' rights and obligations shall be governed by the domestic law of the state of New York, U.S.A., including without limitation its version of the Uniform Commercial Code.

10.7 Consent to Jurisdiction. SUBJECT TO SECTION 3.14 AND 9.5, IN CONNECTION WITH ANY LITIGATION ARISING OUT OF OR IN RELATION TO THIS AGREEMENT BETWEEN THE PARTIES HERETO OR IN CONNECTION WITH ANY THIRD PARTY BENEFICIARY CLAIM MUST BE BROUGHT EXCLUSIVELY IN THE FEDERAL OR STATE COURTS LOCATED IN THE COUNTY OF NEW YORK, STATE OF NEW YORK, TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN CONNECTION WITH SUCH LITIGATION OR CLAIM, EACH PARTY (1) IRREVOCABLY SUBMITS AND CONSENTS TO THE EXCLUSIVE JURISDICTION OF AND VENUE IN THE FEDERAL OR STATE COURTS LOCATED IN THE STATE OF NEW YORK AND SAID COURTS AND EACH PARTY IRREVOCABLY WAIVES ANY CLAIMS THAT SUCH LITIGATION BROUGHT IN SAID COURTS HAS BEEN BROUGHT IN AN INCONVENIENT FORUM; AND (2) IRREVOCABLY CONSENTS TO THE SERVICE OF PROCESS OF SAID COURTS BY ANY METHOD AS PROVIDED BY NEW YORK LAW AND IN ADDITION BY PERSONAL DELIVERY BY OVERNIGHT MAIL OR INTERNATIONAL COURIER, WHICH REQUIRES SIGNING ON RECEIPT, POSTAGE PREPAID, TO SUCH PARTIES AT THE ADDRESS SPECIFIED IN THIS AGREEMENT, OR TO THE AGENT TO BE APPOINTED BY IT PURSUANT TO SECTION 10.9 BELOW.

10.8 Waiver of Jury Trial. TO THE MAXIMUM EXTENT PERMITTED BY LAW, EACH PARTY HERETO HEREBY, KNOWINGLY, VOLUNTARILY, AND INTENTIONALLY WAIVES ANY RIGHTS IT MAY HAVE TO A TRIAL BY JURY IN ANY LITIGATION OF ANY CLAIM WHICH IS BASED HEREON, OR ARISES OUT OF, UNDER , OR IN CONNECTION WITH THIS AGREEMENT OR ANY TRANSACTIONS RELATING HERETO, WHETHER IN CONTRACT, IN TORT OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ANY THIRD PARTY BENEFICIARY CLAIM, EACH PARTY ACKNOWLEDGES THAT THE WAIVERS IN SECTION 10.7 AND IN THIS SECTION 10.8 ARE A MATERIAL INDUCEMENT FOR THE OTHER PARTIES TO ENTER INTO THIS AGREEMENT, THE WAIVERS IN SECTION 10.7 AND THIS SECTION 10.8 ARE IRREVOCABLE, MEANING THAT THEY MAY NOT BE MODIFIED EITHER ORALLY

OR IN WRITING, AND THESE WAIVERS SHALL APPLY TO ANY SUBSEQUENT AMENDMENTS, SUPPLEMENTS AND REPLACEMENTS TO OR OF THIS AGREEMENT. IN THE EVENT OF LITIGATION, THIS AGREEMENT MAY BE FILED AS A WRITTEN CONSENT TO WAIVER OF A JURY TRIAL AND TO TRIAL BY THE COURT.

- 10.9 Agent. SERVICE PROVIDER SHALL APPOINT AN AGENT WITHIN THE UNITED STATES, WITHIN 90 DAYS AFTER THE EFFECTIVE DATE, FOR ACCEPTANCE OF SERVICE OF PROCESS PROVIDED FOR UNDER THIS AGREEMENT AND SHALL NOTIFY CMLA OF THE IDENTITY AND ADDRESS OF SUCH AGENT.
- 10.10 Notice. Any notice required to be given under this Agreement shall be in writing (which, for these purposes includes facsimile but excludes email) and shall be by overnight mail or international courier, which requires signing on receipt, postage prepaid (or, for notices given by facsimile, shall only be considered given if the sender has received a successful fax transmission report recording the correct number of pages), to the parties at the address or facsimile number specified in this Agreement. Such notices shall be deemed served when received by addressee or, if delivery is not accomplished by reason of some fault of the addressee, when tendered for delivery. Any Party shall give written notice of a change of address or facsimile number and, after notice of such change has been received, any notice or request shall thereafter be given to such party at such changed address or facsimile number.
- 10.11 Severability; Waiver. Should any part of this Agreement judicially be declared to be invalid, unenforceable, or void, the Parties agree that the part or parts of this Agreement so held to be invalid, unenforceable, or void shall be reformed by the entity having jurisdiction thereover without further action by the Parties hereto and only to the extent necessary to make such part or parts valid and enforceable. A waiver by any of the Parties hereto of any of the covenants or promises to be performed by the other Parties or any breach thereof shall not be effective unless made in writing and signed by the waiving Party and shall not be construed to be a waiver of any succeeding breach thereof or of any covenant herein contained.
- 10.12 Language. The Parties agree and acknowledge that the official language of CMLA is English and all business transactions shall be conducted in English. The parties further agree and acknowledge that this English language version of the Agreement is the only valid version of the Agreement.

SO AGREED AS OF THE DATE FIRST ABOVE WRITTEN.

This Agreement may be executed in multiple counterparts.

CMLA:	Service Provider:
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

The Founders sign below for purpose of agreeing to all Sections of this Agreement except for Sections 3.1, 8.2, 8.3, 8.5, 8.6, 8.7, 8.8, 8.9 and 9.

By: _____
CMLA, LLC as attorney-in-fact for Founders;
LMI, LLC, as attorney-in-fact for CMLA, LLC

Name: _____

Title: _____

CMLA, LLC as attorney-in-fact for Founders:

By: _____

Name: _____

Title: _____

Addresses and facsimile for notices

CMLA LLC:
c/o LMI, LLC
225 B Cochrane Circle
Morgan Hill, CA 95037

Service Provider:

Intel Corporation:
Office of General Counsel
2200 Mission College Blvd
Santa Clara, CA USA 95052
Facsimile: 01-408-765-1859
Copy to Jeffrey Lawrence,
Director of Content Policy,
facsimile number 01-503-264-9564

Panasonic Corporation:
General Manager
Corporate Legal Affairs Division
Panasonic Corporation
1006 Kaoma, Osaka 571-8501 JAPAN
(tel) +81-6-6908-5836
(fax) +81-6-6906-3760

Nokia Corporation:
Technology Platforms Legal Department
Attn. Vice President, Legal
P.O.Box 100, FI-00045 NOKIA GROUP
Keilalahdentie 4, 02150 Espoo, Finland
tel. +358-7180 08000
fax. +358-7180 38677

Samsung Electronics Co., Ltd:
EUISUK CHUNG (Vice President)
Samsung Electronics IT Center 24th floor
Maetan 3 Dong Youngtong-Gu
Suwon Kyounggi Korea (ROK)
Telephone : 82-31-279-6400
Fax : 82-31-279-6501

Exhibit A

RIGHTS ISSUER COMPLIANCE RULES

PART 1: GENERAL AND DEFINITIONS

Applicability and general requirements

- 1.1 Where a capitalized term is used, but not otherwise defined in this Exhibit A, the meaning ascribed thereto elsewhere in the Agreement or CMLA Technical Specification or OMA DRM Specifications shall apply.

PART 2: COMPLIANCE RULES FOR RIGHTS ISSUERS

1. Applicability and general requirements

- 1.1 This Exhibit A is applicable to all Participating Rights Issuer Implementations and Licensed Services.
- 1.2 Content: Rights Issuers shall issue Rights Objects only for Digital Content as authorized by the content's owner. Subject to the foregoing:
 - 1.2.1 Up until the end of December 2009, for any Digital Content constituting an audiovisual work in Substantially Equivalent Distribution, with Computer Monitor outputs enabled other than as a selectable output, Rights Issuers shall issue Rights Objects for such Digital Content with explicit authorization for Computer Monitor outputs when distributing such Digital Content from a Participating Rights Issuer Implementation and/or Licensed Service to a Participating Product Implementation.
 - 1.2.2 Up until the end of August 2012, for any Digital Content constituting an audiovisual work in Substantially Equivalent Distribution with Standard Definition Analog outputs enabled other than as a selectable output, Rights Issuers shall issue Rights Objects for such Digital Content with explicit authorization for Standard Definition Analog outputs when distributing such Digital Content from a Participating Rights Issuer Implementation and/or Licensed Service to a Participating Product Implementation.
 - 1.2.3 For purposes of the preceding, any "Digital Content constituting an audiovisual work" shall include Digital Content that is substantially equivalent to such Digital Content constituting an audiovisual work. For purposes of clarity, mere distribution to a distribution platform and/or content protection system that permits protected digital outputs that subsequently may result in content being available over Computer Monitor or Standard Definition Analog outputs (such as DTCP or CPRM) shall not constitute distribution with such outputs enabled. A "Substantially Equivalent Distribution" of Digital Content shall mean that the same Digital Content constituting an audiovisual work has been actively distributed within the preceding twenty-four (24) months or is being distributed in the same territory, with rights holder permission, in any other distribution system, except any distribution of Digital Content constituting an audiovisual work in respect of which one or more of the following factors would be expected to provide a material positive differentiation in the perception of the consumer (from the other distribution of Digital Content constituting an audiovisual work): (i) earlier release/distribution window; (ii) better price or less sponsorship or advertising to consumer; (iii) more flexible use model; or (iv) substantially and qualitatively different viewing experience based on concrete, objective

differentiation factors (e.g., three dimensional or multiple viewing angles, higher resolution or higher quality codec.)

- 1.3 Use of Rights Issuer Keys: The Rights Issuer generated Rights Issuer Private Key and the CMLA issued Rights Issuer Certificate shall only be used for the specific purpose of protecting and issuing content by and through a Licensed Service to Licensed Products.
- 1.4 Licensed Services shall conduct Rights Object Acquisition Protocol defined in OMA DRM Specifications using the Rights Issuer generated Rights Issuer Private Key and CMLA issued Rights Issuer Certificate in addition to other requirements for Compliance.
- 1.5 Clear labeling: Rights Issuer shall ensure that consumers are affirmatively informed of the rights and terms under which said rights are acquired prior to consumer commitment to the transaction (and especially that any limitations are subject to clear information) except when the transaction is part of a subscription distribution (where prior user consent has been obtained at the time such subscription is purchased by the user).
- 1.6 Accurate Time: Rights Issuers shall synchronize their Participating Rights Issuer Implementation time to CMLA OCSP Responder time references at regular intervals to ensure the use of accurate time in Rights Object Acquisition Protocol transactions.
- 1.7 Time Synchronization: Rights Issuers shall not¹, to the extent commercially reasonable, require the Device to synchronize its DRM Time unless the Device DRM Time is off by 60 minutes or more in comparison to the reference time maintained within the Participating Rights Issuer Implementation.
- 1.8 Ability to ‘move’ content to other DRM systems: CMLA recommends that if a Rights Issuer detects that a Device requesting Rights Objects supports Export “Move” of OMA DRM Version 2 Protected Content and Rights into one or more of the DRM or copy protection technologies listed in Table Y1, the Rights Issuer should include the Export “Move” Permission for the supported technologies in Rights Objects for that Device. For the avoidance of doubt, this recommendation (a) is not a requirement, and (b) does not by implication grant a copyright license to the Rights Issuer with respect to any Digital Content.

¹ Rights Issuers should carefully consider this issue in order to minimize the load on the CMLA OCSP Responders and adversely affecting the CMLA infrastructure, and the potential inconvenience caused to consumers if time synchronization is forced frequently. Please refer to the Agreement for additional information on fees associated with the CMLA OCSP Responder usage.

Exhibit B

RIGHTS ISSUER ROBUSTNESS RULES

1. DESIGN AND OPERATION

- 1.1 **Generally.** Rights Issuer facilities shall be designed and operated in a manner clearly designed to effectively frustrate attempts to compromise the confidentiality or integrity requirements while not compromising the availability by denying access to legitimate parties.
- 1.2 **Maintain Confidentiality and Integrity.** Rights Issuer facilities shall be designed and operated in a manner that is clearly designed to effectively frustrate attempts by unauthorized parties to (a) discover or reveal Rights Issuer Private Keys and other confidential values as described in the Confidentiality and Integrity Table in Appendix X or (b) modify values identified as requiring integrity in the Confidentiality and Integrity Table in Appendix X.
- 1.3 **Copying of Rights Issuer Private Keys.** Rights Issuer is permitted to generate copies of Rights Issuer Private Keys within a particular physical device or server, for performance reasons, and is permitted to create a backup copy of Rights Issuer Private Keys for secure offline storage. These copies of Rights Issuer Private Keys shall be subject to the requirements of this Exhibit C, which shall apply in full to such copies in the same manner as they would to the original Rights Issuer Private Key as securely generated within the Rights Issuer facilities. Rights Issuer shall promptly and securely destroy copies of Rights Issuer Private Keys when they are no longer required.
- 1.4 **Accountability.** Right Issuer facilities shall be maintained so that all access to the system on which the private key resides, and in particular, all access to the Rights Issuer Private Key itself, shall be logged. Further, all copying and destruction of Rights Issuer Private Keys as permitted under Section 1.3 above shall be logged, and in such a way that examination of the log files shall permit the Rights Issuer or any other examiner of the log files to know how many copies of Rights Issuer Private Keys were in existence in what location at any previous moment in time. Audit tools shall be available for forensic examination of the log files. Sufficient measures shall be implemented to ensure the integrity of the log files.
- 1.5 **Controls.** Rights Issuers shall implement controls to reduce risk to an level that will result in the Rights Issuer facilities having the level of protection described in Section 3 or better. Rights Issuers shall define system components in terms of their security function and shall control their access to and by other components accordingly.
- 1.6 **Policy.** Rights Issuers shall create, implement and maintain a policy detailing the security objectives and methods that will be put in place in order to reduce risks to a level that will result in the Rights Issuer facilities having the level of protection described in Section 3 or better. This policy shall be consistent with the guidelines in [ISO 17799] and any updated version of it. (As used herein ISO 17799 refers to: ISO/IEC 17799:2000, Information technology -- Code of practice for information security management)

- 1.7 **Standards and Procedures.** Rights Issuers shall create, implement and maintain security standards and procedures detailing how the policy will be implemented. These standards and procedures shall be consistent with the guidelines in [ISO 17799] and any updated version of it.
- 1.8 **Risk Register.** Rights Issuer shall maintain a Risk Register listing the risks that are not met by the controls (as described in section 1.4) implemented by the Rights Issuer. Rights Issuer shall ensure the Risk Register is kept up to date.

2. **METHODS OF PRESERVING CONFIDENTIALITY AND INTEGRITY.**

Rights Issuer facilities shall be designed and operated using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to compromise the confidentiality or integrity of Rights Issuer Private Keys, as set forth below in Sections 2.1, 2.2, 2.3 and Section 2.4.

2.1 **Software.** Any portion of the Rights Issuer facilities capable of accessing Rights Issuer Private Keys in usable form by Software shall include all of the characteristics set forth in Sections 1.1 and 1.2 of this Exhibit B. For the purposes of these Rights Issuer facilities Robustness Rules, "Software" shall mean the implementation of the content protection requirements which this Agreement requires Rights Issuer facilities to be compliant through any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware. Such implementations shall:

2.1.1 Comply with Sections 1.1 and 1.2 of this Exhibit B by a reasonable method including but not limited to: encryption, execution of a portion of the implementation in privileged or supervisor mode, execution on a hardened operation system, and/or embodiment in a secure physical implementation.

2.1.2 Be designed so that checking of the integrity of the component parts occurs such that modifications must be recorded and processes will promptly assess whether these modifications were authorized or unauthorized. For the purpose of this provision, a "modification" includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to Sections 1.1 and 1.2 of this Exhibit B. The Rights Issuer shall describe in the security policy, standards and procedures (as described in sections 1.5 and 1.6) how this provision is satisfied.

2.2 **Hardware.** Any portion of the Rights Issuer facilities capable of accessing Rights Issuer Private Keys in usable form in Hardware shall include all of the characteristics set forth in Sections 1.1 and 1.2 of this Exhibit C. For the purposes of these Robustness Rules, "Hardware" shall mean a physical device, including a component, that implements any of the content protection requirements as to which this Agreement requires that Rights Issuer facilities be compliant and that (i) does not include instructions or data other than such instructions or data that are permanently embedded in such device or component; or (ii) includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such Rights Issuer facilities and/or can only be accessed under the control of the Rights Issuer by authorized parties. Such implementation shall:

- 2.2.1 Comply with Sections 1.1 and 1.2 of this Exhibit B by any reasonable method including but not limited to embedding Rights Issuer Private Keys in a Hardware Security Module (HSM) that provides the level of protection described in section 3. Rights Issuers that wish to employ an HSM should use an HSM that meets FIPS 140-2 Level 3 or higher, or an equivalent level of protection as defined in an alternative internationally accepted standard.
- 2.2.2 Be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would compromise the content protection requirements of the CMLA would pose a serious risk of rendering the Rights Issuer facilities unable to issue Rights Objects and would be promptly detected as described in section 2.1.2.
- 2.3 **Hybrid.** The interfaces between Hardware and Software portions of Rights Issuer facilities shall be designed so that the Hardware portions comply with the level of protection that would be provided by a pure Hardware implementation, and the Software portions comply with the level of protection, which would be provided by a pure Software implementation.
- 2.4 **Operation.** Rights Issuer facilities shall be operated in a manner that implements all of the characteristics set forth in Section 1.1 and 1.2 of this Exhibit C. The Rights Issuer facilities shall be implemented in a manner as to be able to generate regular audit reports to assess compliance to these robustness rules as stated in Section 1.3. The physical security and operation policies, standards and procedures of the Rights Issuer facilities shall be taken into account when determining whether or not Rights Issuer facilities meet this requirement, when these documents are made available for inspection as required by section 4.1.

3. LEVEL OF PROTECTION

The confidentiality and integrity of Rights Issuer Private Keys shall be preserved for the purposes of Section 2 by a reasonable method such that, in the event of unauthorized access to the systems on which the Rights Issue Private Keys reside, the entity obtaining the unauthorized access:

- 3.1 Cannot compromise the confidentiality or integrity of Rights Issuer Private Keys merely by obtaining unauthorized access (either physical or logical) to the Rights Issuer facilities or merely by using general-purpose tools or equipment that are widely available (including being available on the Internet) at a reasonable price such as screwdrivers, jumpers, clips, soldering irons, packet sniffers, port scanners, vulnerability scanners, exploit scripts, software capable exploiting replay attacks, dictionary attacks and information gathered using search engines ("Widely Available Tools"), or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or decompilers ("Specialized Tools"), other than devices or technologies whether Hardware or Software that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies required by CMLA DRM ("Circumvention Devices").

- 3.2 Can only with difficulty compromise the confidentiality or integrity of Rights Issuer Private Keys using professional tools or equipment, such as logic analyzers, chip disassembly systems, or in-circuit emulators or any other tools, equipment, methods, or techniques not described in Section 2.6.1 of this Exhibit B, such as would be used primarily by persons of professional skill and training, but not including professional tools or equipment that are made available only on the basis of a non-disclosure agreement or Circumvention Devices.
- 3.3 **Threats that must be met.** The Rights Issuer shall implement a security policy, standards and procedures, as specified in sections 1.5 and 1.6 that meet, as a minimum, the threats listed below or reduce the risk caused by the these threats to an acceptable level. The list of threats below is not an exhaustive list and Rights Issuers should consider additional threats that might apply in their context.

3.3.1 Physical Threats

- Unauthorized physical access to any system components
- Destruction of any or all system component(s) by accident or design
- Availability compromised by physical disconnection or other physical intervention
- Modification or interruption of power supplies and network connections
- Eavesdropping on local networks, for example using a protocol analyzer (hybrid threat)

3.3.2 Logical (Platform and Network)

- Unauthorized access via a console or a network terminal.
- Man in the middle attacks.
- Destruction of key material.
- Installation of eavesdropping facilities on system components.
- Improper or unauthorized creation, modification or deletion of user accounts.
- Improper or unauthorized creation, modification or deletion of database contents.
- Improper or unauthorized creation, modification or deletion of database access controls.
- Faults in vendor's software operating systems or applications
- Misconfiguration of vendor's software

3.3.3 Operational

- Exploitation of input control (buffer overflows) to undermine availability and escalate privilege.
- Unauthorised acquisition of cipher and/or plaintext.
- Unauthorised modification of operational log files
- Obtaining unauthorised access by misrepresentation ("social engineering")

3 ADVANCE OF TECHNOLOGY

Although an implementation of a Rights Issuer facilities when designed and first shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design of a particular Rights Issuer facilities, would have caused such products to fail to comply with these

Robustness Rules (“New Circumstances”). If a Rights Issuer has (a) actual notice of New Circumstances, or (b) actual knowledge of New Circumstances (the occurrence of (a) or (b) hereinafter referred to as “Notice”), then within eighteen (18) months after Notice such Rights Issuer shall cease operation of Rights Issuer facilities that are not compliant with the Rights Issuer Robustness Rules in view of the then-current circumstances and shall only operate Rights Issuer facilities that are compliant with the Rights Issuer Robustness Rules in view of the then-current circumstances, whether these be new or upgraded Rights Issuer facilities.

4. EXAMINATION

- 4.1 **Inspection of Security Policy, Standards, Procedures and Risk Register.** Rights Issuer shall make their security policy, standards, procedures and risk register available for inspection by an independent third party auditor appointed by the CMLA, according to the requirement in section 8.2 of the Service Provider Agreement.

Appendix X – Confidentiality & Integrity Tables

The tables in this appendix enumerate the cryptographic and other values that must be provided with specific protections (confidentiality and/or integrity) within CMLA Rights Issuer implementations. If a value is inherently confidentiality/integrity protected (such as certificates), then there would be no additional confidentiality/integrity protection to be provided by implementations. For all other values, the implementations must provide the type of protection as listed in these tables.

Value	Confidentiality Required [†] ?	Integrity Required [†] ?	Consideration (Informative)
<i>RI Private Key</i>	Yes	Yes	
<i>RI Certificate (Chain)</i>	No	Yes	
<i>Trusted Device Authorities Certificate</i>	No	Yes	
<i>Domain Context</i>	-	-	
<i>Domain ID</i>	No	Yes	
<i>Domain Key</i>	Yes	Yes	
<i>Expiry Time</i>	No	Yes	
<i>Device Context</i>	-	-	
<i>agreed protocol parameters</i>	No	Yes	
<i>protocol version</i>	No	Yes	
<i>Trusted RI Authorities</i>	No	Yes	
<i>Device ID</i>	No	Yes	
<i>Information whether a Device has stored RI Certificate</i>	No	Yes	
<i>Expiry Time</i>	No	Yes	
<i>Device Certificate</i>	No	Yes	
<i>Device Details</i>	No	Yes	
<i>Device RO / Domain RO</i>	-	-	
<i>Permission/Constraint</i>	No	Yes	
<i>Content Encryption Key</i>	Yes	Yes	
<i>Z</i>	Yes	Yes	
<i>Key Encryption Key</i>	Yes	Yes	
<i>Rights Encryption Key</i>	Yes	Yes	
<i>MAC Key</i>	Yes	Yes	
<i>GroupKey</i>	Yes	Yes	The GroupKey is included in the extended headers of a DCF within an OMADRMGroupID box.

Exhibit C

CMLA Service Provider Fee Schedule

1. GENERAL

- All Fees are in US Dollars
- All Fees are non-refundable

2. ANNUAL ADMINISTRATIVE FEES

The following Administrative Fees are payable annually as set forth below and in advance. The full Fee is due upon execution of the required CMLA agreement(s). The annual Administrative Fee is due upon the anniversary of the execution date of the CMLA agreement(s). An invoice will be sent 90 days prior to the anniversary date.

- Service Provider Development Annual Administrative Fee **\$7,500**
 - Service Providers that want to develop CMLA services must execute both the Service Provider Adopter Agreement and Service Provider Adopter Development Addendum and pay only the Development Annual Administrative Fee of \$7,500.
 - Note, CMLA will reduce the amount of the Service Provider Adopter Annual Administration Fee by the amount of the Adopter Development Annual Administrative Fee if an adopter wants to become a Service Provider Adopter.
 - Service Provider Developers that want also to be a Client Adopter Developer must also execute the CMLA “Client Adopter agreement and Client Adopter Development Addendum. No additional Annual Fee is required.
- Service Provider Annual Administrative Fee **\$19,000**
 - Service Providers that want to also be a Client Adopter must execute the CMLA Client Adopter Agreement in addition to the CMLA Service Provider Agreement. No additional Annual Fee is required.

3. PROCESSING FEES

Processing Fees are per incident fees specific to activities performed by CMLA at the explicit request of CMLA Technology Licensees.

- Additional Service Provider Adopter Contact Fee **\$500 per Update**
 - This Fee is due upon the licensee’s request for additional Contacts beyond the number allowed in the License (refer to section 5.6 of the Service Provider Adopter Agreement) and will be prorated for the remainder of the year beginning and ending upon the anniversary of the execution date of the CMLA agreement, and shall later be included and due annually along with the Licensee’s Service Provider Adopter Annual Administrative Fee.
 - Note, this fee does not apply to Service Provider contacts relating to CMLA ON-Line System operation and support.

- Contact Addendum Update Fee **\$400 per Update**
 - This processing Fee shall be charged when the Service Provider Adopter Developer Addendum is NOT Executed at the same time as the CMLA Service Provider Adopter Agreement.
 - To be clear, this processing Fee is not applicable when a licensee executes both the CMLA Service Provider Adopter Agreement and Service Provider Adopter Development Addendum.
- Service Provider Certificate Signing Fee (Production) **\$ 1,500 per certificate**
- CMLA Approved Output Submission Fees
 - Tables X1 or Y1 **\$3,000**
 - Tables X2 or Y2 **\$1,000**
- Highly Confidential Information Copy Fee² **\$<to be determined>**

4. **SERVICE PROVIDER SUBSCRIBER FEES**

- Service Provider Subscriber Fees are tiered and based upon a Service Providers number of Active Subscribers
- An Active Subscriber is a single customer who has in a given quarter i) downloaded a CMLA rights object or CMLA domain key except through use of the CMLA Development System, or ii) has completed the 2-pass RO Request/Response protocol, 1-pass RO Response protocol, or the Join Domain protocol.
- Active Subscriber Fees are billed quarterly and in arrears, based upon the Service Providers self-reported Active Subscriber count.
- Quarterly Service Provider Subscriber Fees

1-5000 Active Subscribers	\$1500
5001-100,000 Active Subscribers	\$2500
100,001-250,000 Active Subscribers	\$4500
250,001-1/2 Million Active Subscribers	\$7,000
1/2-1 Million Active Subscribers	\$9,450
1-2 Million Active Subscribers	\$12,750
2-4 Million Active Subscribers	\$17,225
4-8 Million Active Subscribers	\$23,250
8-16 Million Active Subscribers	\$31,400
16-32 Million Active Subscribers	\$42,400
32 Million or more Active Subscribers	\$57,250
- Active Subscriber count is due 60 days after the close of the quarter, for the quarters ending 31 March, June 30, September 30 and Dec 31 respectively.

² The HCI copy fee is not currently applicable.

4.1 Service Provider OCSP Fee³

- The Service Provider OCSP fee is a per transaction fee based upon the number of OCSP responses requested by a specific Service Provider.
- The Service Provider OCSP fee is billed quarterly.

Service Provider OCSP Fee **0.0000 ¢ (Cents) per OCSP request**

5. DEVELOPMENT KEYING MATERIAL FEES

- | | |
|---|------------------------|
| <ul style="list-style-type: none"> ▪ Sample Development Keying Material Kit <ul style="list-style-type: none"> ○ Is Provided on CMLA Website and the following is a summarized list of content of the Sample Kit <ul style="list-style-type: none"> ▪ DEV_Device_CA.cer ▪ DEV certificates (50 unique hash_cert.der) ▪ DEV keys (50 unique hash_key.der) ▪ DEV_Rights_Issuer_CA_Certs.der ▪ DEV_Rights_Issuer_CMLA_TEST_0106_00.der ▪ DEV_RI_Private_Key_00.der ▪ DEV_RI_Private_Key_00.pem ▪ DEV_RI_Public_key_00.der ▪ DEV_Rights_Issuer_CMLA_TEST_0106_01.der ▪ DEV_RI_Private_Key_01.der ▪ DEV_RI_Private_Key_01.pem ▪ DEV_RI_Public_Key_01.der ▪ DEV_CMLA_Roo_CA_Certificate_00.der | <p>Free</p> |
| <ul style="list-style-type: none"> ▪ 2,000 Client Development Credentials <ul style="list-style-type: none"> ○ 1 batch of 1000 device development key pairs & certificates ○ 1 batch with 1000 revoked device development key pairs & certificates | <p>\$3,000</p> |
| <ul style="list-style-type: none"> ▪ 11,000 Client Development Credentials <ul style="list-style-type: none"> ○ 1 batch with 10000 device development key pairs & certificates ○ 1 batch with 1000 revoked device development key pairs & certificates | <p>\$10,000</p> |
| <ul style="list-style-type: none"> ▪ 51,000 Client Development Credentials <ul style="list-style-type: none"> ○ 1 batch with 50000 device development key pairs & certificates ○ 1 batch with 1000 revoked device development key pairs & certificates ○ 20 revoked certificates from another batch | <p>\$25,000</p> |
| <ul style="list-style-type: none"> ▪ Development System Rights Issuer Certificate Signing Fee <ul style="list-style-type: none"> ○ Per Certificate signing Fee | <p>\$1,500</p> |
| <ul style="list-style-type: none"> ▪ Development System Rights Issuer Certificate Signing Fee <ul style="list-style-type: none"> ○ Up to 5 certificates for 5 RI public keys ○ With the option of having up to 4 certificates to be revoked | <p>\$3,000</p> |
| <ul style="list-style-type: none"> ▪ Development System On-line Access Fee <ul style="list-style-type: none"> ○ Development OCSP Responder ○ Development CRL | <p>Free</p> |

³ The Service Provider OCSP Fee is intended to more fairly allocate costs across the Service Providers, should CMLA's OCSP response costs become i) a significant cost within the CMLA Key and Certificate Infrastructure and ii) should the OCSP requests from SP's turn out to be disproportional to their number of active subscribers.

6. LATE FEES

Delinquent fees shall be subject to a late fee of one and one-half percent (1.5%) per month of the delinquent fees.

EXHIBIT C-1

FOR SERVICE PROVIDER AGREEMENT

**PRE-POPULATED FIELDS OF THE SUBJECT NAME STRUCTURE OF THE RIGHTS
ISSUER CERTIFICATE REQUEST**

**THIS EXHIBIT MUST BE COMPLETED FOR SERVICE PROVIDER AND IT'S
PARTICIPATING AFFILIATE(S) AND SUBMITTED WITH SERVICE
PROVIDER AGREEMENT &
PRIOR TO PLACING AN ORDER
FAILURE TO DO SO WILL RESULT IN A DELAY OF THE ORDER**

The following are the values of the *SubjectName* attribute fields that the Service Provider will include in all of the Rights Issuer Certificate requests:

SubjectName attribute		
Field	Value (to be filled-in)	Description / Example
<i>organizationName</i>		The company legal name as it appears in the agreement. 64-character maximum
<i>commonName</i>		The company legal name (as for the <i>organizationName</i>) or a commonly well recognized name that uniquely identify the company 64-chatacters maximum
<i>countryName</i>		Country of operation, as defined by the 2-characters, in accordance with ISO 3166

Optional fields can be specified in the ordering form.

EXHIBIT D

To CMLA SERVICE PROVIDER AGREEMENT

DESIGNATION OF PARTICIPATING AFFILIATE(S) ACKNOWLEDGMENT AND AGREEMENT (duplicate as necessary)

_____ (Company Name), a _____

corporation having a principal place of business at _____

(Participating Affiliate as defined in the Agreement), hereby acknowledges and agrees that:

- (i) it is a Participating Affiliate of the Service Provider identified below, as defined in Section 1.37 of the Service Provider Agreement executed on _____ between CMLA and the Service Provider (the "Agreement");
- (ii) it has read and understood the Agreement and the Exhibits thereto and agrees to abide by all of the terms and conditions and the same obligations as the Service Provider, including without limitation, the covenant not to sue in Section 2.5 of the Agreement;
- (iii) in the event the Participating Affiliate fails to abide by the terms of the Agreement, CMLA and/or Eligible Content Participants (as Third Party Beneficiaries) shall, in their respective sole discretion, be entitled to exercise their third party beneficiary rights under this Agreement or, for CMLA bring an action at law or in equity against Participating Affiliate or Service Provider to enforce the terms of this Agreement.

Service Provider hereby acknowledges and agrees that:

- (i) Subject to the limitation of liability terms of the Agreement, Service Provider and Participating Affiliate are jointly and severally liable for claims at law or in equity against Participating Affiliate to enforce the terms of this Agreement.

IN WITNESS WHEREOF, Participating Affiliate and Service Provider have executed this Acknowledgment and Agreement as of the date written below:

Service Provider

Participating Affiliate

Signature _____

Signature _____

Print Name _____

Print Name _____

Title _____

Title _____

Date _____

Date _____

EXHIBIT E

CMLA Advisory Board Request for Amendment

The signatory/signatories below, each members of the CMLA Advisory Board, hereby request that the following amendment(s) be made to the

- Content Participant Agreement
- Client Adopter Agreement
- Service Provider Agreement
- CMLA Technical Specification
- Other (specify) _____:

Description of Action:

(List section(s) to be amended and provide text of amendments. Attach an explanation of the benefits)

The signatory/signatories certify that they have consulted with the members of the CMLA Client Adopter, Service Provider and Content Participant User Groups and have submitted the proposed amendment to CMLA pursuant to the process established by CMLA for notification of change requests in Section 3 of the CMLA Technology License Agreements and the change requested is approved by a “Qualified Majority” as required:

- Yes No. (if no please provide reason)

The following CMLA User groups oppose the change requested:

- Service Provider User Group
- Client Adopter User Group
- Content Participants User Group

(Please Specify reasons for opposition)

Below is a checklist to be used by CAB as a guide; not all of the boxes must necessarily be completed and additional considerations may be added.

- The change requested does not have a material adverse effect on content protection provided by the CMLA Technical Specification.
- The change requested does not impose additional substantial burdens on Client Adopters, Service

Provider or on the operation of licensed products as more fully set forth in Section 3.

- The change request is an Improving Change, as defined. Please specify reasons why change request is an Improving Change.
- Requests relating to OMA DRM Specification updates.
- Recommended timescales for compliance with proposed recommendation.

For CAB

By: _____
Name: _____
Title: _____
Date: _____

By: _____
Name: _____
Title: _____
Date: _____

Exhibit F

CMLA CONFIDENTIALITY AGREEMENT

& ACKNOWLEDGMENT BY SUPPLIERS AND SUBCONTRACTORS

_____ [name, address] (“Company”), a contractor of _____ (“the Licensee”), hereby agree to the following:

For the purposes of this document, “Highly Confidential Information” means (i) Rights Issuer Private Keys, (ii) CMLA Device Private Keys and CMLA Client Adopter Transport Keys regardless of whether or not they are marked “Highly Confidential,” and (iii) other information that is marked “Highly Confidential Information” when disclosed by the Licensee to Company.

Other capitalized terms are defined in the CMLA Service Provider Agreement and Client Adopter Agreement, as applicable, and such agreements are available on CMLA’s website at www.cm-la.com.

The Company is allowed to use the Highly Confidential Information for the sole purpose of performing its obligations under its contract with the Licensee. The Company may not take any copies of Highly Confidential Information. Company shall maintain the confidentiality of Highly Confidential Information in the following manner:

The Company shall employ procedures for safeguarding Highly Confidential Information at least as rigorous as the Company would employ for its own most highly confidential information, such procedures to include, at a minimum:

- (1) maintaining on the Company’s premises secure locations in which any and all Highly Confidential Information shall be stored, where such locations may include electronic storage that are at least as secure with respect to the Highly Confidential Information as the security standards set forth in the Compliance and Robustness Rules, with respect to the protection of Device Private Keys and Client Adopter Transport Keys;
- (2) that any Highly Confidential Information stored in such locations shall be accessible only by Authorized Employees (as defined below); and
- (3) when Highly Confidential Information is not in use, such information shall be stored in (i) a locked safe at such secure locations or (ii) shall be stored electronically in a form that is at least as secure as the security standards set forth in the Service Provider Robustness Rules with respect to the protection of Rights Issuer Private Keys.

To the extent that Company has incorporated Highly Confidential Information into a Licensed Service Element (or what or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service) or Licensed Service (or what would be a Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation), the above requirements shall be deemed to be met if such Licensed Service Element (or what or what would be a Licensed Service Element but for the fact that it is not yet incorporated into a Licensed Service) or Licensed Service (or what would be a

Licensed Service but for the fact that it is not yet incorporated into a Participating Rights Issuer Implementation) meets the security standard set forth in the Service Provider Robustness Rules.

The Company may disseminate Highly Confidential Information only to a reasonable number of its employees (1) who have a need to know or use such Highly Confidential Information in order to perform Company's obligations under the contract between Licensee and the Company; and (2) who are bound in writing by obligations of confidentiality at least as protective of the Highly Confidential Information as to the applicable terms of this Agreement, which obligations shall survive the termination of employment ("Authorized Employee"), provided that Company shall maintain a list of all Authorized Employees (such list to include both current Authorized Employees and all individuals, whether or not still employed by the Company, who were Authorized Employees at any time). Upon Licensee's request, the Company shall provide Licensee with the list of Authorized Employees described in the preceding sentence. The Company shall cause Authorized Employees to abide by their obligations hereunder.

Within thirty (30) days after the effective date of termination or expiration of the contract between Licensee and the Company, the Company shall return to Licensee all Highly Confidential Information, or, at Licensee's option, destroy all such information in its possession, retaining no copies thereof and upon request of Licensee, shall provide a written certification of such destruction signed by a senior official or officer of the Company.

The provisions of this Agreement in respect of Highly Confidential Information shall apply for a term of Contract between the Licensee and the Company and thereafter without limit in time.

Agreed on behalf of the COMPANY

Signed: _____

Name: _____

Date: _____

cc: CMLA, LLC.

EXHIBIT G
TO CMLA SERVICE PROVIDER AGREEMENT
Service Provider and/or its Participating Affiliates Contact

THIS DOCUMENT MUST BE SIGNED BY CORPORATE OFFICER(S) (OR EQUIVALENT) WITH AUTHORITY TO BIND SERVICE PROVIDER AND/OR PARTICIPATING AFFILIATE(S) AND WITH SUFFICIENT AUTHORITY TO NOMINATE SERVICE PROVIDER AND/OR PARTICIPATING AFFILIATE(S) CONTACTS.

	Service Provider Contact	Alternate Service Provider Contact
Company Name:		
Participating Affiliate (yes/no)		
Email:		
Name		
Initials:		
Fax number:		
Phone number:		
Mobile Phone number:		
Address Line1		
Address line 2		
Town/City		
Post Code:		
Country:		

Please list all the locations authorized by the above Service Provider Contact and Alternate Service Provider Contact persons:

List of Shipping Address:

Shipping Address 1:

Company Name:
 Participating Affiliate (yes/no):
 Address Line1 (Street address)

Address Line 2 (unit, building, floor)

Town / City:

County:

Post Code:

Country:

Phone number:

Site fax:

Time Zone:

Shipping Address 2:

.

.

.

The undersigned certifies and agrees that he/she has sufficient authority to designate the above-named Contact and Alternate Contact Persons to order and receive CMLA Highly Confidential Information and/or Rights Issuer Private Keys on behalf of Service Provider and/or its Participating Affiliate(s)

Signature:

Name:

Title:

Date:

EXHIBIT H

CMLA Advisory Board Recommended Procedures

1. Background

CMLA and the CMLA Technology Licensees may establish a CMLA Advisory Board (CAB) which consists of elected representatives of Content Participant, Service Provider and Client Adopter User Groups in addition to the Founders of CMLA

2. Proposed Principles for Building the CAB

CMLA and CMLA Technology Licensees wish to reduce or eliminate complex voting mechanisms and issues involving for majorities. For this reason the following recommended procedures are provided as one idea to avoid voting for nominating representatives, as long this is not requested by the companies CMLA Technology Licensees within in a User Group, and to include CMLA Technology Licenses, which join the CMLA ecosystem at a later point of time, as well. Especially with regard to an ongoing process of signing a Content Participant, Client Adopter or Service Provider Agreement, the CAB should be a workable council independently of how many companies are already entered the CMLA.

The proposed principles are:

- All CMLA Technology Licensees (except Authorized Resellers and those CMLA Technology Licensees electing only to exercise the Developer Addendum) are eligible to participate in a User Group and are entitled to act as representatives in the CAB.
- CMLA Technology Licensees (except Authorized Resellers and those CMLA Technology Licensees electing only to exercise the Developer Addendum) may participate in a User Group and represent that User Group on the CAB category according to their agreement. A CMLA Technology Licensee (except Authorized Resellers and those CMLA Technology Licensees electing only to exercise the Developer Addendum) having entered into one or more CMLA Technology License Agreements, must select/announce a CAB User Group category in which it would like to participate. In no event, may a CMLA Technology Licensee participate on the CAB as a representative in more than one User Group CAB category.
- Participation in only one User Group category, does not however, preclude a CMLA Technology Licensee from providing input to other User Groups and CAB participant representatives, as it deems appropriate.
- The CAB will make a reasonable effort to permit participation of all CMLA Technology Licensees and Founders at CAB meetings; including providing forty-five (45) days notice of meetings.

- The CAB representatives for each User Group may rotate and the CAB should decide on a reasonable rotation schedule.
- As long as no other mechanisms are agreed within each CAB category / the User Group, of each CAB category the representatives are determined according to the order in which each User Group participant became a CMLA Technology Licensee. The first two (2) CMLA Technology Licensees in each CAB User Group category will become the user group CAB representatives for that User Group by default.
- Absent the a User Group adopting an alternative procedure, each half year the CMLA Technology Licensees participating in each User Group will rotate to permit new CMLA Technology Licensees in each CAB User Group category to participate on the CAB. Such a process shall continue until all CMLA Technology Licensees in a User Group wishing to participate as representative will have an opportunity to do so, at which point the process will restart.
- Any CMLA Technology Licensee may decline to participate in as a CAB category as representative for its selected User Group.
- CMLA Technology Licensees, as representatives in each CAB User Group category, may change any of these procedures by a simple majority vote of all of the then current CMLA Technology Licensees in that User Group a particular category.
- CMLA will provide information to each new signatory about current CAB representatives for each User Group to enable the CMLA Technology Licensee to contact the representatives and to be included in work of the selected User Group.
- As long as no other mechanisms are decided in the User Groups the principle of a simple majority will be used to come to decisions on open issues. Based on these decisions the representatives will act in the CAB.