

CMLA Technical Specification Change History

The following is a list of all the relevant changes that have occurred to versions subsequent to version 1.00 of the CMLA Technical Specification.

From version 1.00-051221 to version 1.1-20090123

Chapter	Changes
Cover Page	- Draft changed to Approved
Page 2 Notice	- Deleted "Draft" references - Deleted Confidential Version of the Technical Specification requiring NDA.
Chapter 2 References	-Deleted "Note for Contributors"
Chapter 6: Certificates Section 6.1 CMLA Root CA Certificates	- Validity – "CMLA will decide during 2010 the key lengths and certificate validity periods that will be used after 2011." - SubjectPublicKeyInfo -- "During 2004-2011: carries a 2048 bit RSA public key identified with the pkcs-1 algorithm identifier as defined in Error! Reference source not found. CMLA will decide during 2010 the key lengths and certificate validity periods that will be used after 2011."
Chapter 6: Certificates Section 6.2 Device CA Certificates	- Validity – "During 2004-2011: expires 30 years from the issuance date but not later than the certificate of the corresponding CMLA Root CA Certificate. CMLA will decide during 2010 the key lengths and certificate validity periods that will be used after 2011." - SubjectPublicKeyInfo -- "During 2004-2011: carries a 2048 bit RSA public key identified with the pkcs-1 algorithm identifier as defined in Error! Reference source not found. CMLA will decide during 2010 the key lengths and certificate validity periods that will be used after 2011."

<p>Chapter 6: Certificates Section 6.3 Rights Issuer CA Certificate</p>	<p>- Validity – “During 2004-2011: expires 30 years from the issuance date but not later than the certificate of the corresponding CMLA Root CA Certificate. CMLA will decide during 2010 the key lengths and certificate validity periods that will be used after 2011.”</p> <p>- SubjectPublicKeyInfo -- “During 2004-2011: carries a 2048 bit RSA public key identified with the pkcs-1 algorithm identifier as defined in Error! Reference source not found.</p> <p>CMLA will decide during 2010 the key lengths and certificate validity periods that will be used after 2011.”</p>
<p>Chapter 6: Certificates Section 6.4 OCSP Responder Certificate</p>	<p>- Validity – “During 2004-2011: expires 30 years from the issuance date but not later than the certificate of the corresponding CMLA Root CA Certificate. CMLA will decide during 2010 the key lengths and certificate validity periods that will be used after 2011.”</p> <p>- SubjectPublicKeyInfo -- “During 2004-2011: carries a 2048 bit RSA public key identified with the pkcs-1 algorithm identifier as defined in Error! Reference source not found.</p> <p>CMLA will decide during 2010 the key lengths and certificate validity periods that will be used after 2011.”</p>
<p>Chapter 6: Certificates Section 6.5 Device Certificate</p>	<p>- Validity – “During 2004-2011: expires 30 years from the issuance date but not later than the certificate of the corresponding CMLA Root CA Certificate. CMLA will decide during 2010 the key lengths and certificate validity periods that will be used after 2011.”</p> <p>- SubjectPublicKeyInfo -- “During 2004-2011: carries a 2048 bit RSA public key identified with the pkcs-1 algorithm identifier as defined in Error! Reference source not found.</p> <p>CMLA will decide during 2010 the key lengths and certificate validity periods that will be used after 2011.”</p>

<p>Chapter 6: Certificates Section 6.6 Rights Issuer Certificate</p>	<p>- Validity – “During 2004-2011: expires 30 years from the issuance date but not later than the certificate of the corresponding CMLA Root CA Certificate. CMLA will decide during 2010 the key lengths and certificate validity periods that will be used after 2011.”</p> <p>- SubjectPublicKeyInfo -- “During 2004-2011: carries a 2048 bit RSA public key identified with the pkcs-1 algorithm identifier as defined in Error! Reference source not found.</p> <p>CMLA will decide during 2010 the key lengths and certificate validity periods that will be used after 2011.”</p>
<p>Appendix A. CMLA IP Source Code A1, A2 and A3</p>	<p>-Deleted following sentence in each of A1, A2 and A3, “This material also contains confidential information which may not be disclosed to others without the prior written consent of CMLA LLC.</p>

From version 1.1-20090123 to version 1.2-20090511

Chapter	Changes
Page 2 Notice	<p>- Deleted “And Confidential” -Changed “MEI/Panasonic” to “ Panasonic”</p>
Chapter 2 References	<p>-Added following references: 18Crypt 18Crypt Profile specified in ETSI TS 102474 V1.1.1: Digital Video Broadcasting (DVB): IP Datacast over DVB-H: Service Purchase and Protection or most recent version. IEC62455 IEC 62455 First Edition 2007-06: Internet protocol (IP) and transport stream (TS) based service access or most recent version. OMABCAST-SCPv1 DRM Profile specified in OMA</p>

	<p>BCAST specification OMA-TS-BCAST_SvcCntProtection-V1_0: Service and Content Protection for Mobile Broadcast Services.</p> <p>OMADRM-XBS OMA-TS-DRM_XBS-V1_0: OMA DRM V2.0 Extensions for Broadcast Support.</p>
Chapter 3: Definitions	- Added Definition: Tag Length Format A syntax defined in the references [18Crypt], [IEC62455], and [OMABCAST-SCPv1] used to hold keyset blocks.
Chapter 4: Abbreviations	- Added Abbreviations: BCRO Broadcast Rights Object DP Device Public Key ROT Root Of Trust SK Session Key TAA Trust Authority Algorithm TLF Tag Length Format
Chapter 15 CMLA Mobile Broadcast	- Chapter is added in its entirety.

From version 1.2-20090511 to version 1.3-20091103

Chapter	Changes
All pages Footnote Notice	- Added © CMLA, LLC. US Patent Nos. 7,564,970 and 7577250; US and foreign patents pending
Chapter 16	- Chapter is added in its entirety