CMLA Technical Specification Change History

From Version 1.42-20120817 to 1.43-20131218

Reference section 2	Update DECE specifications references and add a XML signature reference
Add to section 17.4	DSP access to domain key was changed and use of the new DomainInformationRequest() was add to end of section

From Version 1.41-20120320 to Version 1.42-20120817

Def:CMLA-DSP	Replace cmla-kp-dece-dm with cmla-kp-dece-dsp
Add to end of 1st paragraph 10.1	Both development and production keying material is sent to adopter on 4 DVDs: Production CMLA Root CA Certificate, Production Transport Keys, Development CMLA Root CA Certificate, and Development CMLA Transports Keys.
Add 10.1 1 paragraph 2	public key part of the 2048 bit RSA key pair of the CMLA Transport key as a
Add colon to end of 10.1 paragraph 3 of number 3	
Add to paragraph below figure 2 in 10.4	(refer to section 4.1.2.7 of [RFC3280])
Correction in 17.5.1	Replace cmla-kp-dece-dsp with cmla-kp-dece-dm

From Version 1.40-20111104 to Version 1.41-20120320

Correct reference 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 17.4.1, 17.5,	Changed to Appendix E
Remove all reference to key length change from specification as that should be handled in separate notice to adopters and via the CAB process	Delete “CMLA will decide during 2011 the key lengths and certificate validity periods that will be used after 2012”
	Delete “During 2004-2012 carries” and replace with “Is”
	CMLA will decide during 2011 the key lengths and certificate validity periods that will be used after 2012. Current expectation is that 2048 bit Device keys will be used after 2012.

From Version 1.32-20110610 to Version 1.40-20111104

Add new Chapter 17	Add support for CMLA DECE implementation as associated reference changes due to C17.

From Version V1.31-20101209 to Version 1.32-20110610

Change bit length value	Replace all “1536” with “2048”

From Version 1.3-20091103 to Version V1.31-20101209

Global date change associated with key lengths in Certificates section	Replace 2010 with 2011 Replace 2011 with 2012

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 Primary change was to add SRM support	- Chapter is added in its entirety

From Version 1.1-20090123 to Version 1.2-20090511

Primary change was to add support for Mobile Broadcast

Chapter	Changes
Page 2 Notice	- Deleted "And Confidential" -Changed "MEI/Panasonic" to " Panasonic"
Chapter 2 References	-Added following references: 18Crypt18Crypt 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 BCAST specification OMA-TS-BCAST_SvcCntProtection-V1_0: Service and Content Protection for Mobile Broadcast Services. OMADRM-XBS OMA-TS-DRM_XBS-V1_0: OMA DRM V2.0 Extensions for Broadcast Support.
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 1.00-041221 to Version 1.1-20090123

Primary change readjust dates with respect to key lengths

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.”
Chapter 6: Certificates Section 6.3 Rights Issuer CA Certificate	- 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.”
Chapter 6: Certificates Section 6.4 OCSP Responder Certificate	- 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.”
Chapter 6: Certificates Section 6.5 Device Certificate	- 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."
Chapter 6: Certificates Section 6.6 Rights Issuer Certificate	- 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."
Appendix A. CMLA IP Source Code A1, A2 and A3	-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.