OCF 2.0 – Digital Signature Bit – Security WG CR 2611

Legal Disclaimer

****** Section 9.3.2.1 Certificate Profile and Fields ******

The following X.509 v3 extensions are required for Root CA Certificates:

Extension	Required/ Optional	Criticality	Value / Notes
authorityKeyIdentifier	OPTIONAL	Non-critical	
subjectKeyIdentifier	OPTIONAL	Non-critical	
keyUsage	REQUIRED	Critical	keyCertSign (5) & cRLSign (6) bits SHALL be enabled digitalSignature(0) bit MAY be enabled All other bits SHALL NOT be enabled
basicConstraints	REQUIRED	Critical	cA = TRUE pathLenConstraint = not present (unlimited)

Table 1 - X.509 v3 extensions for Root CA Certificates

...

The following X.509 v3 extensions are required for Intermediate CA Certificates:

Extension	Required /Optional	Criticality	Value / Notes
authorityKeyIdentifier	OPTIONAL	Non-critical	
subjectKeyIdentifier	OPTIONAL	Non-critical	
keyUsage	REQUIRED	Critical	keyCertSign (5) & cRLSign (6) bits SHALL be enabled digitalSignature (0) bit MAY be enabled All other bits SHALL NOT be enabled
basicConstraints	REQUIRED	Critical	cA = TRUE pathLenConstraint = 0 (can only sign end-entity certs)
certificatePolicies	OPTIONAL	Non-critical	(no stipulation)
cRLDistributionPoints	OPTIONAL	Non-critical	1 or more URIs where the Certificate Revocation List (CRL) from the Root can be obtained.
authorityInformationAccess	OPTIONAL	Non-critical	OCSP URI – the URI of the Root CA's OCSP Responder

Table 2 - X.509 v3 extensions for Intermediate CA Certificates

****** End of Change ******