

OCF 2.0 – Digital Signature Bit – Security WG CR 2611

Legal Disclaimer

THIS IS A DRAFT SPECIFICATION DOCUMENT ONLY AND HAS NOT BEEN ADOPTED BY THE OPEN CONNECTIVITY FOUNDATION. THIS DRAFT DOCUMENT MAY NOT BE RELIED UPON FOR ANY PURPOSE OTHER THAN REVIEW OF THE CURRENT STATE OF THE DEVELOPMENT OF THIS DRAFT DOCUMENT. THE OPEN CONNECTIVITY FOUNDATION AND ITS MEMBERS RESERVE THE RIGHT WITHOUT NOTICE TO YOU TO CHANGE ANY OR ALL PORTIONS HEREOF, DELETE PORTIONS HEREOF, MAKE ADDITIONS HERETO, DISCARD THIS DRAFT DOCUMENT IN ITS ENTIRETY OR OTHERWISE MODIFY THIS DRAFT DOCUMENT AT ANY TIME. YOU SHOULD NOT AND MAY NOT RELY UPON THIS DRAFT DOCUMENT IN ANY WAY, INCLUDING BUT NOT LIMITED TO THE DEVELOPMENT OF ANY PRODUCTS OR SERVICES. IMPLEMENTATION OF THIS DRAFT DOCUMENT IS DONE AT YOUR OWN RISK AMEND AND IT IS NOT SUBJECT TO ANY LICENSING GRANTS OR COMMITMENTS UNDER THE OPEN CONNECTIVITY FOUNDATION INTELLECTUAL PROPERTY RIGHTS POLICY OR OTHERWISE. IN CONSIDERATION OF THE OPEN CONNECTIVITY FOUNDATION GRANTING YOU ACCESS TO THIS DRAFT DOCUMENT, YOU DO HEREBY WAIVE ANY AND ALL CLAIMS ASSOCIATED HERewith INCLUDING BUT NOT LIMITED TO THOSE CLAIMS DISCUSSED BELOW, AS WELL AS CLAIMS OF DETRIMENTAL RELIANCE.

The OCF logo is a trademark of Open Connectivity Foundation, Inc. in the United States or other countries. *Other names and brands may be claimed as the property of others.

Copyright © 2018 Open Connectivity Foundation, Inc. All rights reserved.

Copying or other form of reproduction and/or distribution of these works are strictly prohibited.

***** **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** *****

DRAFT