

ADACOM OCSP Responder for EU Qualified e-Seals Certificate Profile

Version History		
Date	Version	Changes
01/03/2017	1.0	

This document describes minimal profile requirements for the OCSP Responder Certificate of EU Qualified Certificates for electronic seals, in accordance with the X.509 version 3, the IETF RFC 6960 and clause 6.6 of ETSI EN 319 411-1.

Base Certificate

Field	Value
Issuer DN	C = EL O = ADACOM S.A. OU = Symantec Trust Network OU = Class 2 Managed PKI Individual Subscriber CA OU = Adacom Trust Services 2.5.4.97 = VATEL-099554476 CN = ADACOM CA for EU Qualified e-Seals
Subject DN	C = EL O = ADACOM S.A. OU = Symantec Trust Network OU = Adacom Trust Services CN = ADACOM OCSP Responder for EU Qualified e-Seals
Version	3
Serial number	75 13 7f e5 b3 7c fa c6 0c 0c 50 d9 c3 26 cb 50
Key Size	2048
Validity Start	01-02-2017
Validity End	27-02-2025
Public Key Algorithm	Sha256withRSAEncryption

Certificate Extensions

#	Critical	Standard Extension	Field	Value
1	NO	Authority Key Identifier	Key Identifier	6e 33 ff cc d5 90 8e 5b be 5c cb 23 d0 cf 21 3c 51 e6 b7 20
2	YES	Basic Constraint	End Entity	Yes
			Maximum Path Length	0
3	NO	Certificate Policies	Cert Policy ID	2.16.840.1.113733.1.7.23.2
			Cert Policy Qualifier ID	1.3.6.1.5.5.7.2.1 (CPS Pointer)
			Cert Qualifier	https://pki.adacom.com/cps
			Cert Policy Qualifier ID	1.3.6.1.5.5.7.2.2 (User Notice)
			Cert Qualifier	https://pki.adacom.com/rpa
4	NO	Key Usage	Digital Signature	Set
5	NO	Enhanced Key Usage	OCSP Signing	Set
6	NO	OCSP No Revocation Checking	ocsp-nocheck	Set
7	NO	Subject Alternative Name	Directory Name	CN = OCSP2048-1-17
8	NO	Subject Key Identifier	Key Identifier	d7 05 10 25 aa 2f 53 7c a4 29 f3 10 81 91 80 39 7f 23 43 f5