

ADACOM CA for EU Qualified e-Seals Certificate Profile

Version History		
Date	Version	Changes
01/03/2017	1.0	
19/09/2018	2.0	Minor changes regarding Certificate Extensions

This document describes minimal profile requirements for the Issuing CA of EU Qualified Certificates for electronic seals, in accordance with the X.509 version 3, the IETF RFC 5280 and clause 6.6 of ETSI EN 319 411-1.

Base Certificate

Field	Value
Issuer DN	C = US O = Symantec Corporation OU = Symantec Trust Network CN = Symantec Class 2 Public Primary Certification Authority – G6
Subject 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
Version	3
Serial number	0a 80 bc 74 9f 3f c8 f6 c5 0b de 23 1a f7 01 a6
Key Size	4096
Validity Start	02-03-2017
Validity End	02-03-2025
Public Key Algorithm	Sha256withRSAEncryption

Certificate Extensions

#	Critical	Standard Extension	Field	Value
1	NO	Authority Key Identifier	Key Identifier	87 8c 20 95 c8 98 4a d1 d6 80 06 4a 90 34 44 df 1c 4d bf b0
2	YES	Basic Constraint	CA	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
			Cert Policy ID	0.4.0.194112.1.3
			Cert Policy ID	0.4.0.2042.1.2
4	NO	CRL Distribution Point	Distribution Point	Full Name
			Uniform Resource ID	http://s.symcb.com/pca2-g6.crl
5	YES	Key Usage	keyCertSign	Set
			cRLSign	Set
			Off-line CRL Signing	Set
6	NO	Subject Alternative Name	Directory Name	CN = C1C2-4096-2
7	NO	Enhanced Key Usage	Client Authentication	1.3.6.1.5.5.7.3.2
			Secure Email	1.3.6.1.5.5.7.3.4
8	NO	Authority Information Access	Access Method	1.3.6.1.5.5.7.48.2
			Access Location	https://pki.adacom.com/repository/en/certs/production/files/pca-2-g6-en.crt
9	NO	Subject Key Identifier	Key Identifier	6e 33 ff cc d5 90 8e 5b be 5c cb 23 d0 cf 21 3c 51 e6 b7 20