

CA for EU Qualified e-Seals Certificate Profile

Version History		
Date	Version	Changes
28-06-18	1.0	

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	CN = Symantec Class 2 Public Primary Certification Authority - G6 OU = Symantec Trust Network O = Symantec Corporation C = US
Subject DN	CN = JCC CA for EU Qualified e-Seals 2.5.4.97 = VATCY-10029914L OU = JCC PAYMENT SYSTEMS Trust Services OU = Class 2 Managed PKI Individual Subscriber CA OU = Symantec Trust Network O = JCC PAYMENT SYSTEMS LTD C = CY
Version	3
Serial Number	17 a0 cb a3 17 88 2e a3 f7 25 0f bf 04 9b fe 0a
Key Size	4096 bits
Validity Start	14-Jun-2018
Validity End	14-Jun-2026
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.jcc.com.cy/cps
			Cert Policy Qualifier ID	1.3.6.1.5.5.7.2.2 (User Notice)
			Cert Qualifier	https://pki.jcc.com.cy/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 Address	CN=C1C2-4096-4
7	NO	Authority Information Access	Access Method	1.3.6.1.5.5.7.48.2
			Access Location	https://pki.jcc.com.cy/repository/certs/production/pca-2-g6-en.crt
8	NO	Subject Key Identifier	Key Identifier	87 ed 3d c6 38 1f 8f d5 c7 49 58 96 f9 89 59 1a d0 3f 87 6a
9	YES	Enhanced Key Usage	Client Authentication	1.3.6.1.5.5.7.3.2