

EU Qualified Certificate profile for Legal Person

Version History		
Date	Version	Changes
28-06-18	1.0	
01-03-2019	1.1	"Secure Email" field addition in #8

EU Qualified Certificates to legal persons is compiled in accordance with the X.509 version 3, IETF RFC 5280 [1] and ETSI EN 319 412-3.

Base Certificate

Field	Value
Issuer 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
Subject DN	CN = <i>Legal Person's name.</i> O = <i>Issuer organization name who made subscriber identification.</i> 2.5.4.97 = <i>Identification of the Subscriber organization different from the organization name</i> OU = <i>Issuer organization unit name (optional)</i> C = <i>2 character ISO 3166 country code</i>
Version	3
Serial Number	<i>Unique serial number of the certificate</i>
Key Size	2048 bits
Validity Start	<i>First date of certificate validity</i>
Validity End	<i>Last date of certificate validity</i>
Public Key Algorithm	Sha256withRSAEncryption

Certificate Extensions

#	Critical	Standard Extension	Field	Value
1	NO	Authority Key Identifier	Key Identifier	87 ed 3d c6 38 1f 8f d5 c7 49 58 96 f9 89 59 1a d0 3f 87 6a
2	NO	Basic Constraint	End Entity	Yes
			Maximum Path Length	None
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 ID	0.4.0.194112.1.3
4	NO	CRL Distribution Point	Distribution Point	Full Name
			Uniform Resource ID	http://pki.jcc.com.cy/crl/JCCPAYMENTSYSTEMSLTDLPforeSeals/LatestCRL.crl
5	NO	Key Usage	Digital Signature	Set
			Non-Repudiation	Set
6	NO	Qualified Certificate Statements	etsiQcsCompliance	0.4.0.1862.1.1
			etsiQcsQcSSCD	0.4.0.1862.1.4
			etsiQcPDS	0.4.0.1862.1.5
			PDS Location	https://pki.jcc.com.cy/repository/PDS/
			etsiQcType	0.4.0.1862.1.6
			etsiQcTypeEsign	0.4.0.1862.1.6.2
7	NO	Authority Information Access	Access Method	1.3.6.1.5.5.7.48.1
			Access Location	http://ocsp.jcc.com.cy
			Access Method	1.3.6.1.5.5.7.48.2
			Access Location	https://pki.jcc.com.cy/repository/certs/production/ca-eseal.crt
8	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
9	NO	Subject Key Identifier	Key Identifier	SHA-1 hash of the public key used to sign the certificate