

EU Qualified Certificate profile for Natural Person associated with Legal Person

Version History		
Date	Version	Changes
01/03/2017	1.0	
26/07/2019	1.1	Changes regarding PDS Location

EU Qualified Certificates to natural persons associated with legal persons is compiled in accordance with the X.509 version 3, IETF RFC 5280 [1] and ETSI EN 319 412-2.

Base Certificate

Field	Value
Issuer DN	CN = ADACOM CA for EU Qualified e-Signatures 2.5.4.97 = VATEL-099554476 OU = Adacom Trust Services OU = Class 2 Managed PKI Individual Subscriber CA OU = Symantec Trust Network O = ADACOM S.A. C = EL
Subject DN	CN = <i>Space separated Person Given name and Surname.</i> G = <i>Person given names in UTF8 format according to RFC5280</i> SN = <i>Person surnames in UTF8 format according to RFC5280</i> SERIALNUMBER = <i>Random code as specified in clause 5.1.3 of ETSI EN 319 412-1</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	8d 9f 06 f4 ba a8 cb 96 19 46 f9 af ad 14 be 53 50 c5 02 88
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.adacom.com/cps
			Cert Policy ID	0.4.0.194112.1.2
4	NO	CRL Distribution Point	Distribution Point	Full Name
			Uniform Resource ID	http://crl.adacom.com/ADACOMSALegalPersoneSignature/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.adacom.com/repository/PKIPDS-EN.pdf
				https://pki.adacom.com/repository/PKIPDS-EL.pdf
			etsiQcType	0.4.0.1862.1.6
etsiQcTypeEsign	0.4.0.1862.1.6.1			
7	NO	Authority Information Access	Access Method	1.3.6.1.5.5.7.48.1
			Access Location	http://ocsp.adacom.com
			Access Method	1.3.6.1.5.5.7.48.2
			Access Location	https://pki.adacom.com/repository/en/certs/production/files/ca-esignature.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
10	NO	Subject Alternative Name	RFC822 Name	E-mail address of Subject