

EU Qualified Certificate profile for Legal Person

Version History		
Date	Version	Changes
01/03/2017	1.0	
22/06/2018	1.1	Changes regarding key usage
26/07/2019	1.2	Add Certificate extensions regarding Non-QSCD, minor changes regarding PDS Location
01/03/2021	2.0	Following CPS changes

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 = ADACOM Qualified eSeals CA G1 O = ADACOM ADVANCED INTERNET APPLICATIONS S.A. 2.5.4.97 = VATEL-099554476 OU = ADACOM Qualified Trust Services C = GR
Subject DN	CN = Legal Person's name. O = Issuer organization name who made subscriber identification. 2.5.4.97 = Identification of the Subscriber organization different from the organization name OU = Issuer organization unit name (optional) C = 2 character ISO 3166 country code
Version	3
Serial Number	Unique serial number of the certificate
Key Size	2048 bits
Validity Start	First date of certificate validity
Validity End	Last date of certificate validity
Public Key Algorithm	Sha256withRSAEncryption

Certificate Extensions using Qualified Signature Creation Device

#	Critical	Standard Extension	Field	Value
1	NO	Authority Key Identifier	Key Identifier	59ed4c07593e9734df9159bfbe3ab9885f55ef8f
2	NO	Basic Constraint	End Entity	Yes
			Maximum Path Length	None
3	NO	Certificate Policies	Cert Policy ID	1.3.6.1.4.1.15976.1.1.0.2.0
			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	1.3.6.1.4.1.15976.1.1.2.3 (Local) / 1.3.6.1.4.1.15976.1.1.2.4 (Remote)
			Cert Policy ID	0.4.0.2042.1.2
			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/ADACOMSAQSealServices/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	0.4.0.1862.1.6.2
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	http://repo.adacom.com/certs/ca-qseal-g1.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
---	----	------------------------	----------------	---

Certificate Extensions using a non-Qualified Signature Creation Device

#	Critical	Standard Extension	Field	Value
1	NO	Authority Key Identifier	Key Identifier	59ed4c07593e9734df9159bfbe3ab9885f55ef8f
2	NO	Basic Constraint	End Entity	Yes
			Maximum Path Length	None
3	NO	Certificate Policies	Cert Policy ID	1.3.6.1.4.1.15976.1.1.0.2.0
			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	0.4.0.194112.1.1
4	NO	CRL Distribution Point	Distribution Point	Full Name
			Uniform Resource ID	http://crl.adacom.com/ADACOMSAQSealServices/LatestCRL.crl
5	NO	Key Usage	Digital Signature	Set
			Non-Repudiation	Set
6	NO	Qualified Certificate Statements	etsiQcsCompliance	0.4.0.1862.1.1
			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	0.4.0.1862.1.6.2			
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	http://repo.adacom.com/certs/ca-qseal-g1.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
---	----	------------------------	----------------	---