EU Qualified Certificate profile for Natural Person

Version History		
Date	**Version**	**Changes**
01/03/2017	1.0	
26/07/2019	1.1	Changes regarding PDS location
01/03/2021	2.0	Following CPS updates

EU Qualified Certificates to natural 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 Qualified eSignatures 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 = Space separated Person Given name and Surname.** **G = Person given names in UTF8 format according to RFC5280** **SN = Person surnames in UTF8 format according to RFC5280** **SERIALNUMBER = Random code as specified in clause 5.1.3 of ETSI EN 319 412-1 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 Algorith	**Sha256withRSAEncryption**

Certificate Extensions

#	*Critical*	*Standard Extension*	*Field*	*Value*
1	NO	Authority Key Identifier	Key Identifier	**3e5fd1baf98336a3a0a55fe4abdb07abcfabc3d1**
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**
				1.3.6.1.4.1.15976.1.1.1.3 (Local) / 1.3.6.1.4.1.15976.1.1.1.4 (Remote)
				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/ADACOMSAQSignServices/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	**http://repo.adacom.com/certs/ca-qsign-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**
10	NO	Subject Alternative Name	RFC822 Name	**E-mail address of Subject**