ADACOM Qualified eSignatures CA G1 Certificate Profile

Version History		
Date	**Version**	**Changes**
01/03/2017	1.0	
19/09/2018	2.0	Minor changes regarding Certificate Extensions
01/03/2021	3.0	Following CPS updates

This document describes minimal profile requirements for the Issuing CA of EU Qualified Certificates for electronic signatures, 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 = ADACOM Global Qualified CA** **O = ADACOM S.A.** **2.5.4.97 = VATEL-099554476** **OU = ADACOM Trust Services** **C = GR**
Subject 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**
Version	**3**
Serial number	**6eabd7c45f83e09486d070e86ee73381**
Key Size	**4096**
Validity Start	**10-08-2020**
Validity End	**10-08-2030**
Public Key Algorithm	**Sha256withRSAEncryption**

Certificate Extensions

#	*Critical*	*Standard Extension*	*Field*	*Value*
1	NO	**Authority Key Identifier**	Key Identifier	**edb3b8c9a2b25e52aa44fcd1ad068efee98037f5**
2	**YES**	**Basic Constraint**	CA	**Yes**
			Maximum Path Length	**0**
3	NO	**Certificate Policies**	**Cert Policy ID**	**1.3.6.1.4.1.15976.1.1.1**
			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	**0.4.0.194112.1.0**
			Cert Policy ID	**0.4.0.194112.1.2**
			Cert Policy ID	**0.4.0.2042.1.1**
			Cert Policy ID	**0.4.0.2042.1.2**
4	NO	**CRL Distribution Point**	Distribution Point	**Full Name**
			Uniform Resource ID	**http://crl.adacom.com/ca/qroot.crl**
5	**YES**	**Key Usage**	keyCertSign	**Set**
			cRLSign	**Set**
			Off-line CRL Signing	**Set**
6	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**
7	NO	**Subject Alternative Name**	Directory Name	**CN=PRIVATE-4096-5**
8	NO	**Authority Information Access**	Access Method	**1.3.6.1.5.5.7.48.2**
			Access Location	**http://repo.adacom.com/certs/root-qglobal.crt**
9	NO	**Subject Key Identifier**	Key Identifier	**3e5fd1baf98336a3a0a55fe4abdb07abcfabc3d1**