ADACOM Qualified eSignatures CA G1 Certificate Profile

Version History		
Date	**Version**	**Changes**
01/03/2017	1.0	
01/03/2021	2.0	Following CPS updates

This document describes minimal profile requirements for the OCSP Responder Certificate of EU Qualified Certificates for electronic signatures, in accordance with the X.509 version 3, the IETF RFC 6960 and clause 6.6 of ETSI EN 319 411-1.

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 = ADACOM Qualified eSignatures OCSP G1-1** **O = ADACOM ADVANCED INTERNET APPLICATIONS S.A.** **OU = ADACOM Revocation Status Services** **C = GR**
Version	**3**
Serial number	**1cb02b02f2661ed706aa713f1016ee89**
Key Size	**2048**
Validity Start	**10-08-2020**
Validity End	**10-08-2025**
Public Key Algorithm	**Sha256withRSAEncryption**

Certificate Extensions

#	*Critical*	*Standard Extension*	*Field*	*Value*
1	NO	**Authority Key Identifier**	Key Identifier	**3e5fd1baf98336a3a0a55fe4abdb07abcfabc3d1**
2	**YES**	**Basic Constraint**	End Entity	**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**
4	**YES**	**Key Usage**	Digital Signature	**Set**
			Non-Repudation	**Set**
5	NO	**Enhanced Key Usage**	OCSP Signing	**Set**
6	NO	**OCSP No Revocation Checking**	ocsp-nocheck	**Set**
7	NO	**Subject Alternative Name**	Directory Name	**CN=OCSP2048-1-25**
8	NO	**Subject Key Identifier**	Key Identifier	**caae5a79dd1c6a73224743ef16db464c2669c751**