ADACOM OCSP Responder for EU Qualified e-Signatures Certificate Profile

Version History		
Date	**Version**	**Changes**
01/03/2017	1.0	

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	C = **EL** O = **ADACOM S.A.** OU = **Symantec Trust Network** OU **= Class 2 Managed PKI Individual Subscriber CA** OU = **Adacom Trust Services** 2.5.4.97 = **VATEL-099554476** CN = **ADACOM CA for EU Qualified e-Signatures**
Subject DN	C = **EL** O = **ADACOM S.A.** OU = **Symantec Trust Network** OU = **Adacom Trust Services** CN = **ADACOM OCSP Responder for EU Qualified e-Signatures**
Version	**3**
Serial number	**51 35 3e b4 c7 af 72 b3 23 4e b1 48 09 d1 ff b7**
Key Size	**2048**
Validity Start	**01-03-2017**
Validity End	**27-02-2025**
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	**YES**	**Basic Constraint**	End Entity	**Yes**
			Maximum Path Length	**0**
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 Qualifier ID	**1.3.6.1.5.5.7.2.2** (User Notice)
			Cert Qualifier	**https://pki.adacom.com/rpa**
4	NO	**Key Usage**	Digital Signature	**Set**
5	NO	**Enchanced Key Usage**	OCSP Signing	**Set**
6	NO	**OCSP No Revocation Checking**	ocsp-nocheck	**Set**
7	NO	**Subject Alternative Name**	Directory Name	**CN = OCSP2048-1-16**
8	NO	**Subject Key Identifier**	Key Identifier	**c9 b7 e7 1f 3f a3 63 51 9f f3 a8 a7 fb c6 83 9d 61 f3 9e c2**