

Certificate Profile
ZIPPER Timestamping CA

Affiliate Name: ZIPPER SERVICES SRL

Affiliate Address: Romania, Cluj-Napoca, str. Fabricii nr. 93-103, CP 400632, jud. Cluj

Base Certificate

Field	Value		
Issuer DN	CN = ZIPPER Root CA G1 O = ZIPPER SERVICES SRL C = RO		
Subject DN	CN = ZIPPER TSA G1 O = ZIPPER SERVICES SRL 2.5.4.97 = VATRO-16723187 OU = ZIPPER Time Stamping Services C = RO		
Field	Value	Field	Value
Validity Start	Key Ceremony Date	Version	2*
Validity End	Key Ceremony Date + 10 years	Serial number	Supplied during key ceremony
Public Key Algorithm	sha256withRSAEncryption (1.2.840.113549.1.1.11)	Key Size	4096 bit**
		Parameters	NULL

* The value 2 denotes a version 3 X.509 certificate. For the applicable certificate extensions and signature lines please see page 2 of this naming application.

Certificate Extensions

#	Critical	Standard Extension	Field	Value
1	NO	Authority Key Identifier	Key Identifier	Calculated per Method 1
			Authority Cert Issuer	n/a
			Cert Serial Number	n/a
2	NO	Authority Information Access	Access Method	1.3.6.1.5.5.7.48.2
			Access Location	http://pki.ca.ezipper.ro/repository/ZIPPER-ROOT.crt
3	YES	Basic Constraint	CA	Yes
			Maximum Path Length	0
4	NO	Certificate Policies	Cert Policy ID	1.3.6.1.4.1.57570.1.1
			Cert Policy Qualifier ID	1.3.6.1.4.1.57570.1.1.1 (CPS Pointer)
			Cert Qualifier	https://pki.ca.ezipper.ro/repository
			Cert Policy ID	0.4.0.2042.1.2
			Cert Policy ID	0.4.0.2023.1.1
5	NO	CRL Distribution Point	Distribution Point	Full Name

			Uniform Resource ID	http://crl.ca.ezipper.ro/tsa/root.crl
6	YES	Key Usage	keyCertSign	Set
			cRLSign	Set
			Off-line CRL Signing	Set
7	NO	Extended Key Usage	Time Stamping	1.3.6.1.5.5.7.3.8
8	NO	Subject Key Identifier	Method 1	Yes
			Method 2	n/a