Fina Demo subordinirani CA certifikat

Polje	Atribut	Vrijednost
Osnovna polja		
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	16 ili 17 okteta, 32 do 34 HEX znamenki, 64 bita entropija
signatureAlgorithm	AlgorithmIdentifier	sha256WithRSAEncryption
signatureValue		Potpis izdavatelja certifikata
Issuer	commonName	Fina Demo Root CA
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + 10 godina.
Subject	commonName	Fina Demo CA 2020
	organizationName	Financijska agencija
	countryName	HR
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ CA: 4096 bit

Polje	Kritično	Vrijednost	
Ekstenzije			
KeyUsage	DA	KeyCertSign, cRLSign	
BasicConstraints	DA	cA=true pathLen=0	
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))	
SubjectKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))	
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: http://demo-pki.fina.hr/cps/cpdemoroot1-0.pdf cPSuri: http://demo-pki.fina.hr/cps/cpdemoroot1-0-en.pdf
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo2014-ocsp.fina.hr
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/demo2014_root_ca.cer
CRLDistributionPoints	NE	DistributionPoint	[1]URI: : http://demo-pki.fina.hr/crl/DemoRoot2014.crl

Osnovna polja i ekstenzije profila Fina Demo subordiniranog CA certifikata