

UPRAVA ZA INDIREKTNO OPOREZIVANJE
Bana Lazarevića bb, Banja Luka

UNO PROFILI POTVRDA

Verzija 1.0

UNO PROFILI POTVRDA

1. POPIS TIPOVA POTVRDA I NJIHOVIH PODRUČJA PRIMJENE	4
1.1. POPIS TIPOVA POTVRDA KOJE IZDAJE UINO ROOT CA	4
1.2. POPIS TIPOVA POTVRDA KOJI IZDAJE UINO ISSUING CA1	4
1.2. POPIS TIPOVA POTVRDA KOJI IZDAJE UINO ISSUING CA1	5
1.3. POPIS TIPOVA POTVRDA KOJE IZDAJE UINO ISSUING CA2	5
2. PROFILI POTVRDA	6
2.1. UNO KORIJENSKA POTVRDA - UINO ROOT CA	6
2.2. UNO POTVRDA PRVOG IZDAVAČKOG CA TIJELA - UINO ISSUING CA1	7
2.3. UNO POTVRDA DRUGOG IZDAVAČKOG CA TIJELA - UINO ISSUING CA2	8
2.4. UNO POTVRDA ZA POTPIS ODGOVORA OCSP SERVISA ZA UINO ROOT CA	9
2.5. UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS ZA FIZIČKE OSOBE (QCP-n-qscd)	10
2.6. UNO NEKVALIFICIRANA POTVRDA ZA AUTENTIKOVANJE FIZIČKIH OSOBA (NCP+)	11
2.7. UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS I AUTENTIKACIJU ZA FIZIČKE OSOBE (NCP+)	12
2.8. UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKO POTPISIVANJE I AUTENTIKACIJU U OBLIKU DATOTEKE PKCS#12 ZA FIZIČKE OSOBE (NCP)	13
2.9. UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS ZA FIZIČKE OSOBE POVEZANE SA PRAVNIM OSOBAMA (QSP-n-qscd)	14
2.10. UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS ZA STRANCE POVEZANE SA PRAVNIM OSOBAMA (QSP-n-qscd)	15
2.11. UNO NEKVALIFICIRANA POTVRDA ZA AUTENTIKOVANJE FIZIČKIH OSOBA POVEZANIH SA PRAVNIM OSOBAMA (NCP+)	16
2.12. UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS I AUTENTIKACIJU ZA FIZIČKE OSOBE POVEZANE SA PRAVNIM OSOBAMA (NCP+)	17
2.13. UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKO POTPISIVANJE I AUTENTIKACIJU U OBLIKU DATOTEKE PKCS#12 FORMATA ZA FIZIČKE OSOBE POVEZANE SA PRAVNIM OSOBAMA (NCP)	18
2.14. UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI PEČAT (QCP-l-qscd)	19
2.15. UNO POTVRDA ZA AUTENTIKACIJU MREŽNIH STRANICA (SSL) ZA PRAVNE OSOBE	20
2.16. UNO APLIKACIJSKA POTVRDA ZA ELEKTRONIČKO POTPISIVANJE ZA PRAVNE OSOBE (NCP)	21
2.17. UNO POTVRDA ZA KVALIFICIRANI ELEKTRONIČKI VREMENSKI ŽIG	22
2.18. UNO POTVRDA ZA POTPIS ODGOVORA OCSP SERVISA ZA UINO ISSUING CA1	23
2.19. UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS ZA ZAPOSLENE (QSP-n-qscd)	24
2.20. UNO NEKVALIFICIRANA POTVRDA ZA AUTENTIKACIJU ZA ZAPOSLENE (NCP+)	25
2.21. UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS I AUTENTIKACIJU ZA ZAPOSLENE (NCP+)	26
2.22. UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS I DOMENSKU AUTENTIKACIJU ZA ZAPOSLENE (NCP+)	27
2.23. UNO POTVRDA ZA ELEKTRONIČKO POTPISIVANJE I AUTENTIKACIJU U	

OBLIKU DATOTEKE PKCS #12 FORMATA (NCP)	28
2.24. UNO POTVRDA ZA AUTENTIKACIJU MREŽNIH STRANICA (SSL)	29
2.25. UNO KERBEROS POTVRDA ZA DOMEN KONTROLER (DOMEN KONTROLER KDC)	30
2.26. UNO APLIKATIVNA POTVRDA ZA AUTENTIKACIJU U OBLIKU DATOTEKE PKCS #12 FORMATA (NCP)	31
2.27. UNO POTVRDA ZA VREMENSKI ŽIG.....	32
2.28. UNO POTVRDA ZA POTPIS ODGOVORA OCSP SERVISA ZA UINO ISSUING CA2	33
2.29. UNO POTVRDA ZA POTPISIVANJE KODA (NCP+)	34

1. POPIS TIPOVA POTVRDA I NJIHOVIH PODRUČJA PRIMJENE

1.1. POPIS TIPOVA POTVRDA KOJE IZDAJE UINO ROOT CA	
NAZIV GRUPE	NAZIV TIPIA POTVRDA
UINO ROOT CA POTVRDA	POTVRDA UNO KORIJENSKOG CA TIJELA
UINO ISSUING CA1 POTVRDA	POTVRDA PRVOG UNO IZDAVAČKOG CA TIJELA
UINO ISSUING CA2 POTVRDA	POTVRDA DRUGOG UNO IZDAVAČKOG CA TIJELA
UNO POTVRDA ZA OCSP SERVIS	POTVRDA ZA POTPIS ODGOVORA OCSP SERVISA ZA UINO ROOT CA

1.2. POPIS TIPOVA POTVRDA KOJI IZDAJE UINO ISSUING CA1		
NAZIV GRUPE	NAZIV TIPIA POTVRDE	PODRUČJE PRIMJENE POTVRDE
POTVRDA ZA FIZIČKE OSOBE	UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS ZA FIZIČKE OSOBE (QCP-n-qscd)	IZDAJE SE FIZIČKIM OSOBAMA ZA IZRADU KVALIFICIRANOG ELEKTRONIČKOG POTPISA.
	UNO NEKVALIFICIRANA POTVRDA ZA AUTENTIKACIJU ZA FIZIČKE OSOBE (NCP+)	IZDAJE SE FIZIČKIM OSOBAMA I KORISTI ZA JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS I AUTENTIKACIJU ZA FIZIČKE OSOBE (NCP+)	IZDAJE SE FIZIČKIM OSOBAMA I KORISTI ZA IZRADU ELEKTRONIČKOG POTPISA, JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKO POTPISIVANJE I AUTENTIKACIJU U OBLIKU DATOTEKE PKCS#12 FORMATA (NCP)	IZDAJE SE FIZIČKIM OSOBAMA ZA IZRADU ELEKTRONIČKOG POTPISA, JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
POTVRDA ZA PRAVNE OSOBE	UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS ZA FIZIČKE OSOBE POVEZANE SA PRAVNIM OSOBAMA (QCP-n-qscd)	IZDAJE SE FIZIČKIM OSOBAMA POVEZANIM S POSLOVNIM SUBJEKTOM ZA IZRADU KVALIFICIRANOG ELEKTRONIČKOG POTPISA U POSLOVNE SVRHE.
	UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS ZA STRANCE POVEZANE SA PRAVNIM OSOBAMA (QCP-n-qscd)	IZDAJE SE STRANCIMA POVEZANIM S POSLOVNIM SUBJEKTOM ZA IZRADU KVALIFICIRANOG ELEKTRONIČKOG POTPISA U POSLOVNE SVRHE.
	UNO NEKVALIFICIRANA POTVRDA ZA AUTENTIKACIJU FIZIČKIH OSOBA POVEZANIH SA PRAVNIM OSOBAMA (NCP+)	IZDAJE SE FIZIČKIM OSOBAMA POVEZANIM S POSLOVNIM SUBJEKTOM ZA JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA U POSLOVNE SVRHE.
	UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS I AUTENTIKACIJU ZA FIZIČKE OSOBE POVEZANE SA PRAVNIM OSOBAMA (NCP+)	IZDAJE SE FIZIČKIM OSOBAMA POVEZANIM SA POSLOVNIM SUBJEKTOM ZA IZRADU ELEKTRONIČKOG POTPISA, JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA U POSLOVNE SVRHE.
	UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKO POTPISIVANJE I AUTENTIKACIJU U OBLIKU DATOTEKE PKCS#12 FORMATA ZA FIZIČKE OSOBE POVEZANE SA PRAVNIM OSOBAMA (NCP)	IZDAJE SE FIZIČKIM OSOBAMA POVEZANIM S POSLOVNIM SUBJEKTOM. KORISTI SE ZA POTREBE ELEKTRONIČKOG POTPISIVANJA, JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	UNO APLIKATIVNA POTVRDA ZA ELEKTRONIČKO POTPISIVANJE ZA PRAVNE OSOBE (NCP)	IZDAJE SE APLIKACIJAMA I INFORMACIJSKIM SUSTAVIMA PRAVNIH OSOBA ZA IZRADU ELEKTRONIČKOG POTPISA.
POTVRDA ZA ELEKTRONIČKI PEČAT	UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI PEČAT (QCP-l-qscd)	IZDAJE SE PRAVNIM OSOBAMA ZA IZRADU KVALIFICIRANOG ELEKTRONIČKOG PEČATA.

1.2. POPIS TIPOVA POTVRDA KOJI IZDAJE UINO ISSUING CA1

NAZIV GRUPE	NAZIV TIPA POTVRDE	PODRUČJE PRIMJENE POTVRDE
POTVRDA ZA AUTENTIKACIJU MREŽNIH STRANICA ZA PRAVNE OSOBE	UNO NEKVALIFICIRANA POTVRDA ZA AUTENTIKACIJU MREŽNIH STRANICA (SSL) ZA PRAVNE OSOBE	IZDAJE SE PRAVNIM OSOBAMA ZA AUTENTIKACIJU MREŽNIH STRANICA.
POTVRDA ZA OCSP SERVIS	UNO POTVRDA ZA OCSP SERVIS UINO ISSUING CA1	IZDAJE SE OCSP SERVISU ZA POTPIS OCSP ODGOVORA CA TIJELA UINO ISSUING CA1.
KVALIFICIRANA POTVRDA ZA VREMENSKI ŽIG	UNO KVALIFICIRANA POTVRDA ZA VREMENSKI ŽIG	IZDAJE SE SERVISU ZA IZDAVANJE KVALIFICIRANIH VREMENSKIH ŽIGOVA I KORISTI ZA POTPISIVANJE KVALIFICIRANIH VREMENSKIH ŽIGOVA.

1.3. POPIS TIPOVA POTVRDA KOJE IZDAJE UINO ISSUING CA2

NAZIV GRUPE	NAZIV TIPA POTVRDE	PODRUČJE PRIMJENE POTVRDE
POTVRDA ZA ZAPOSLENE	UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS ZA ZAPOSLENE (QCP-n-qscd)	IZDAJE SE ZAPOSLENIMA ZA IZRADU KVALIFICIRANOG ELEKTRONIČKOG POTPISA.
	UNO NEKVALIFICIRANA POTVRDA ZA AUTENTIKACIJU ZA ZAPOSLENE (NCP+)	IZDAJE SE ZAPOSLENIMA ZA JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS I AUTENTIKACIJU ZA ZAPOSLENE (NCP+)	IZDAJE SE ZAPOSLENIMA ZA IZRADU ELEKTRONIČKOG POTPISA, JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS I DOMENSKU AUTENTIKACIJU ZA ZAPOSLENE (NCP+)	IZDAJE SE ZAPOSLENIMA ZA IZRADU ELEKTRONIČKOG POTPISA I DOMENSKU AUTENTIKACIJU.
	UNO POTVRDA ZA ELEKTRONIČKO POTPISIVANJE I AUTENTIKACIJU U OBLIKU DATOTEKE PKSC#12 FORMATA ZA ZAPOSLENE (NCP)	IZDAJE SE ZAPOSLENIMA, A KORISTI SE ZA POTREBE ELEKTRONIČKOG POTPISIVANJA, JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	UNO APLIKACIJSKA POTVRDA ZA AUTENTIKACIJU U OBLIKU DATOTEKE PKCS #12 FORMATA (NCP)	IZDAJE SE SOFTVERSKIM MODULIMA INFORMACIJSKOG SUSTAVA UNO I KORISTI ZA NJIHOVO AUTENTIKACIJU DRUGIM MODULIMA I INFORMACIJSKIM SUSTAVIMA UNO I ENKRIPCIJU KLJUČA.
	UNO POTVRDA ZA AUTENTIKACIJU MREŽNIH STRANICA (SSL)	IZDAJE SE ZAPOSLENIMA-ADMINISTRATORIMA POSLUŽITELJA ZA AUTENTIKACIJU MREŽNIH STRANICA.
	UNO KERBEROS POTVRDA ZA DOMEN KONTROLER (DOMEN KONTROLER KDC)	IZDAJE SE ZAPOSLENIMA-ADMINISTRATORIMA ACTIVE DIRECTORY DOMENA ZA AUTENTIKOVANJE DOMEN KONTROLERA.
	UNO POTVRDA ZA VREMENSKI ŽIG	IZDAJE SE INTERNOM SERVISU ZA IZDAVANJE VREMENSKIH ŽIGOVA I KORISTI ZA POTPISIVANJE VREMENSKIH ŽIGOVA.
	UNO POTVRDA ZA POTPISIVANJE KODA (NCP+)	IZDAJE SE ZAPOSLENIMA ZA POTPISIVANJE FAJLOVA INFORMACIJSKOG SUSTAVA UNO.
	UNO POTVRDA ZA OCSP SERVIS UINO ISSUING CA2	IZDAJE SE OCSP SERVISU ZA POTPIS OCSP ODGOVORA CA TIJELA UINO ISSUING CA2.

2. PROFILI POTVRDA

2.1. UNO KORIJENSKA POTVRDA - UINO ROOT CA

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	00 a1 4b 09 ce 74 e2 56 36 00 00 00 00 5e 62 20 c2 64 bita entropije, 16 ili 17 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
Signature hash algorithm		Sha512
Issuer	commonName (CN)	UINO Root CA
	OrganizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 20 godina.
Subject	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	Javni ključ CA: 4096 Bits

EKSTENZIJE

POLJE	KRITIČNO	VRIJEDNOST
KeyUsage	DA	Certificate Signing – potpisivanje potvrde Off-line CRL Signing – potpisivanje van mreže CRL Signing (06) - CRL potpisivanje
BasicConstraints	DA	Subject Type=CA Path Length Constraint=None
AuthorityKeyIdentifier	NE	a4 7b dc d4 04 c0 1d 87 b2 85 df 05 13 c7 e9 e8 bc cc c5 d7 The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits) prema RFC 5280, točka 4.2.1.2 metoda (1)
SubjectKeyIdentifier	NE	a4 7b dc d4 04 c0 1d 87 b2 85 df 05 13 c7 e9 e8 bc cc c5 d7 The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits) prema RFC 5280, točka 4.2.1.2 metoda (1)

2.2. UNO POTVRDA PRVOG IZDAVAČKOG CA TIJELA - UINO ISSUING CA1

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	11 0a fc c0 4c 5d 59 67 00 00 00 00 5e 62 20 fb 64 bita entropije, 16 ili 17 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 20 godina.
Subject	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	Javni ključ CA: 4096 bit

EKSTENZIJE

POLJE	KRITIČNO	VRIJEDNOST	
KeyUsage	DA	Certificate Signing - potpisivanje potvrde Off-line CRL Signing - potpisivanje van mreže CRL Signing (06) - CRL potpisivanje	
BasicConstraints	DA	Subject Type=CA Path Length Constraint=0	
AuthorityKeyIdentifier	NE	a4 7b dc d4 04 c0 1d 87 b2 85 df 05 13 c7 e9 e8 bc cc c5 d7 The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits) prema RFC 5280, točka 4.2.1.2 metoda (1))	
SubjectKeyIdentifier	NE	c9 88 2c 2c 92 f1 f3 fc ff ea f5 9b 63 bc 81 12 42 b8 01 4a The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits) prema RFC 5280, točka 4.2.1.2 metoda (1))	
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.1.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/CPS/UINO-CPS1-0-bs.pdf CPS uri: http://ca.uino.gov.ba/CPS/UINO-CPS1-0-sr.pdf CPS uri: http://ca.uino.gov.ba/CPS/UINO-CPS1-0-hr.pdf CPS uri: http://ca.uino.gov.ba/CPS/UINO-CPS1-0-en.pdf
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINORootCA.cer
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINORootCA.crl [2] URI: http://cdp.uinoca.ba/CRL/UINORootCA.crl

2.3. UNO POTVRDA DRUGOG IZDAVAČKOG CA TIJELA - UINO ISSUING CA2

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	00 f6 0d 3e 65 bd 52 2a 8e 00 00 00 00 5e 62 20 fc 64 bita entropije, 16 ili 17 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme potvrde + 20 godina.
Subject	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	Javni ključ CA: 4096 bit

EKSTENZIJE

POLJE	KRITIČNO	VRIJEDNOST	
KeyUsage	DA	Certificate Signing - potpisivanje potvrde Off-line CRL Signing - potpisivanje van mreže CRL Signing (06) - CRL potpisivanje	
BasicConstraints	DA	Subject Type=CA Path Length Constraint=None	
AuthorityKeyIdentifier	NE	a4 7b dc d4 04 c0 1d 87 b2 85 df 05 13 c7 e9 e8 bc cc c5 d7 The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits) prema RFC 5280, točka 4.2.1.2 metoda (1))	
SubjectKeyIdentifier	NE	b5 36 a9 12 b0 e0 75 77 d4 80 b0 a2 29 c9 55 c6 a4 81 e2 c0 The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits) prema RFC 5280, točka 4.2.1.2 metoda (1))	
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.1.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/CPS/UINO-CPS1-0-bs.pdf CPS uri: http://ca.uino.gov.ba/CPS/UINO-CPS1-0-sr.pdf CPS uri: http://ca.uino.gov.ba/CPS/UINO-CPS1-0-hr.pdf CPS uri: http://ca.uino.gov.ba/CPS/UINO-CPS1-0-en.pdf
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINORootCA.cer
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINORootCA.crl [2] URI: http://cdp.uinoca.ba/CRL/UINORootCA.crl

2.4. UNO POTVRDA ZA POTPIS ODGOVORA OCSP SERVISA ZA UINO ROOT CA

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 12 mjeseci
Subject	commonName (CN)	UINO Root OCSP
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Banja Luka
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
extKeyUsage	NE	ocspSigning	OID: 1.3.6.1.5.5.7.3.9
id-pkix-ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.0.16.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINORootCA.crl [2] URI: http://cdp.uinoca.ba/CRL/UINORootCA.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINORootCA.cer

2.5. UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS ZA FIZIČKE OSOBE (QCP-n-qscd)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signaturehashAlgorithm		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP , gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	localityName (L)	Mjesto prebivališta potpisnika
	countryName (C)	Država potpisnika
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.10.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	qcp-natural-qscd (2), OID: 0.4.0.194112.1.2
qcStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-4	OID: 0.4.0.1862.1.4
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 http://ca.uino.gov.ba/bs/dokumenti/pds-bs.pdf , bs http://ca.uino.gov.ba/sr/dokumenti/pds-sr.pdf , sr http://ca.uino.gov.ba/hr/dokumenti/pds-hr.pdf , hr http://ca.uino.gov.ba/en/dokumenti/pds-en.pdf , en
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.6. UNO NEKVALIFICIRANA POTVRDA ZA AUTENTIKOVANJE FIZIČKIH OSOBA (NCP+)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signaturehashAlgorithm		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP , gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	localityName (L)	Mjesto prebivališta potpisnika
	countryName (C)	Država potpisnika
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.10.2.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	ncplusplus (2), OID: 0.4.0.2042.1.2
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.7. UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS I AUTENTIKACIJU ZA FIZIČKE OSOBE (NCP+)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signaturehashAlgorithm		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP , gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	localityName (L)	Mjesto prebivališta potpisnika
	countryName (C)	Država potpisnika
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.10.3.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	ncplusplus (2), OID: 0.4.0.2042.1.2
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.8. UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKO POTPISIVANJE I AUTENTIKACIJU U OBLIKU DATOTEKE PKCS#12 ZA FIZIČKE OSOBE (NCP)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP , gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	localityName (L)	Mjesto prebivališta potpisnika
	countryName (C)	Država potpisnika
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
Key Usage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.10.4.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	nep (1), OID: 0.4.0.2042.1.1
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.9. UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS ZA FIZIČKE OSOBE POVEZANE SA PRAVNIM OSOBAMA (QSP-n-qscd)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP, gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Poreski identifikacijski broj (PIB) pravne osobe).
	organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.
	localityName (L)	Mjesto sjedišta poslovnog subjekta
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.11.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	qcp-natural-qscd (2), OID: 0.4.0.194112.1.2
qcStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-4	OID: 0.4.0.1862.1.4
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 http://ca.uino.gov.ba/bs/dokumenti/pds-bs.pdf, bs http://ca.uino.gov.ba/sr/dokumenti/pds-sr.pdf, sr http://ca.uino.gov.ba/hr/dokumenti/pds-hr.pdf, hr http://ca.uino.gov.ba/en/dokumenti/pds-en.pdf, en
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.10. UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS ZA STRANCE POVEZANE SA PRAVNIM OSOBAMA (QSP-n-qscd)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP, gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Poreski identifikacioni broj (PIB) pravne osobe).
	organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.
	localityName (L)	Mjesto sjedišta poslovnog subjekta
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.11.2.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	qcp-natural-qscd (2), OID: 0.4.0.194112.1.2
qCStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-4	OID: 0.4.0.1862.1.4
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 http://ca.uino.gov.ba/bs/dokumenti/pds-bs.pdf , bs http://ca.uino.gov.ba/sr/dokumenti/pds-sr.pdf , sr http://ca.uino.gov.ba/hr/dokumenti/pds-hr.pdf , hr http://ca.uino.gov.ba/en/dokumenti/pds-en.pdf , en
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.11. UNO NEKVALIFICIRANA POTVRDA ZA AUTENTIKOVANJE FIZIČKIH OSOBA POVEZANIH SA PRAVNIM OSOBAMA (NCP+)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP , gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Poreski identifikacioni broj PIB pravne osobe).
	organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.
	localityName (L)	Mjesto sjedišta poslovnog subjekta
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	Digital Signature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.11.3.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	ncplusplus (2), OID: 0.4.0.2042.1.2
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.12. UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS I AUTENTIKACIJU ZA FIZIČKE OSOBE POVEZANE SA PRAVNIM OSOBAMA (NCP+)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP , gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Poreski identifikacijski broj PIB pravne osobe)
	organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.
	localityName (L)	Mjesto sjedišta poslovnog subjekta
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	Digital Signature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.11.4.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	ncplusplus (2), OID: 0.4.0.2042.1.2
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.13. UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKO POTPISIVANJE I AUTENTIKACIJU U OBLIKU DATOTEKE PKSC#12 FORMATA ZA FIZIČKE OSOBE POVEZANE SA PRAVNIM OSOBAMA (NCP)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP , gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Poreski identifikacijski broj PIB pravne osobe).
	organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran
	localityName (L)	Mjesto sjedišta poslovnog subjekta
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	Digital Signature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.11.5.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	ncp (1), OID: 0.4.0.2042.1.1
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.14. UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI PEČAT (QCP-I-qscd)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Potpis izdavaoca potvrde
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Naziv koji subjekat koristi za svoje predstavljanje
	serialNumber	CA:BA-JIP, gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Poreski identifikacijski broj PIB pravne osobe).
	organizationName (O)	Puni registrirani skraćeni naziv pravne osobe ili naziv pravne osobe ako skraćeni naziv nije registriran
	localityName (L)	Mjesto sjedišta pravne osobe
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.12.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	qcp-legal-qscd (3), OID: 0.4.0.194112.1.3
qcStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-4	OID: 0.4.0.1862.1.4
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 http://ca.uino.gov.ba/bs/dokumenti/pds-bs.pdf, bs http://ca.uino.gov.ba/sr/dokumenti/pds-sr.pdf, sr http://ca.uino.gov.ba/hr/dokumenti/pds-hr.pdf, hr http://ca.uino.gov.ba/en/dokumenti/pds-en.pdf, en
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.2
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.15. UNO POTVRDA ZA AUTENTIKACIJU MREŽNIH STRANICA (SSL) ZA PRAVNE OSOBE

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 398 dana
Subject	commonName (CN)	Samo jedan puni kvalificirani naziv poslužitelja (FQDN)
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Poreski identifikacijski broj - PIB pravne osobe).
	organizationName (O)	Puni registrirani skraćeni naziv pravne osobe ili naziv pravne osobe ako skraćeni naziv nije registriran
	localityName (L)	Mjesto sjedišta pravne osobe
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	ServerAuth	1.3.6.1.5.5.7.3.1
		clientAuth	1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.13.1.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	ovcp (7), OID: 0.4.0.2042.1.7
		policyIdentifier	organization-validated (2), OID: 2.23.140.1.2.2
subjectAltName	NE	dnsName	Puni kvalificirani naziv poslužitelja (FQDN)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.16. UNO APLIKACIJSKA POTVRDA ZA ELEKTRONIČKO POTPISIVANJE ZA PRAVNE OSOBE (NCP)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Naziv aplikacije ili informacijskog sustava
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Poreski identifikacijski broj - PIB pravne osobe).
	organizationName (O)	Puni registrirani skraćeni naziv pravne osobe ili naziv pravne osobe ako skraćeni naziv nije registriran
	localityName (L)	Mjesto sjedišta pravne osobe
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.14.1.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	nep (1), OID: 0.4.0.2042.1.1
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.17. UNO POTVRDA ZA KVALIFICIRANI ELEKTRONIČKI VREMENSKI ŽIG

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 4 godine
Subject	commonName (CN)	UINO QTSA 2020 <redni broj izdane potvrde>
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Banja Luka
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 3072 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
privateKeyUsage Period	NE	notBefore	Vrijeme izdavanja potvrde
		notAfter	Vrijeme izdavanja potvrde + 1 godina
extKeyUsage	DA	timeStamping	OID: 1.3.6.1.5.5.7.3.8
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.15.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
qcStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 http://ca.uino.gov.ba/bs/dokumenti/pds-bs.pdf, bs http://ca.uino.gov.ba/sr/dokumenti/pds-sr.pdf, sr http://ca.uino.gov.ba/hr/dokumenti/pds-hr.pdf, hr http://ca.uino.gov.ba/en/dokumenti/pds-en.pdf, en
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.2
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.18. UNO POTVRDA ZA POTPIS ODGOVORA OCSP SERVISA ZA UINO ISSUING CA1

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 12 mjeseci
Subject	commonName (CN)	UINO Issuing CA1 OCSP
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Banja Luka
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
extKeyUsage	NE	ocspSigning	OID: 1.3.6.1.5.5.7.3.9
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.1.16.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer

2.19. UNO KVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS ZA ZAPOSLENE (QSP-n-qscd)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP, gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Mjesto sjedišta UNO ili regionalnog centra.
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.2.11.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	qcp-natural-qscd (2), OID: 0.4.0.194112.1.2
qcStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-4	OID: 0.4.0.1862.1.4
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 http://ca.uino.gov.ba/bs/dokumenti/pds-bs.pdf , bs http://ca.uino.gov.ba/sr/dokumenti/pds-sr.pdf , sr http://ca.uino.gov.ba/hr/dokumenti/pds-hr.pdf , hr http://ca.uino.gov.ba/en/dokumenti/pds-en.pdf , en
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA2.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer

2.20. UNO NEKVALIFICIRANA POTVRDA ZA AUTENTIKACIJU ZA ZAPOSLENE (NCP+)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP, gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Mjesto sjedišta UNO ili regionalnog centra.
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	Digital Signature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.2.11.2.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	ncplusplus (2), OID: 0.4.0.2042.1.2
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA2.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer

2.21. UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS I AUTENTIKACIJU ZA ZAPOSLENE (NCP+)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP, gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Mjesto sjedišta UNO ili regionalnog centra.
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	Digital Signature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.2.11.3.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	nepplus (2), OID: 0.4.0.2042.1.2
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA2.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer

2.22. UNO NEKVALIFICIRANA POTVRDA ZA ELEKTRONIČKI POTPIS I DOMENSKU AUTENTIKACIJU ZA ZAPOSLENE (NCP+)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP, gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Mjesto sjedišta UNO ili regionalnog centra
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	Digital Signature	Uključen digitalSignature bit
		NonRepudiation	Uključen NonRepudiation bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		Smart Card Logon	OID: 1.3.6.1.4.1.311.20.2.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.2.11.4.1 policyQualifierId: id-qt-cps { id-qt 1 }
		policyQualifiers	CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	ncpplus (2), OID: 0.4.0.2042.1.2
subjectAltName	NE	rfc822Name	Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA2.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer

2.23. UNO POTVRDA ZA ELEKTRONIČKO POTPISIVANJE I AUTENTIKACIJU U OBLIKU DATOTEKE PKCS #12 FORMATA (NCP)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 60 mjeseci
Subject	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	serialNumber	CA:BA-JIP, gdje je JIP (Jedinstveni identifikator potvrde) pseudoslučajno generirani broj
	givenName	Ime potpisnika kako je navedeno u identifikacijskoj ispravi
	surname(SN)	Prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Mjesto sjedišta UNO ili regionalnog centra.
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	Digital Signature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.2.11.5.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	ncp (1), OID: 0.4.0.2042.1.1
subjectAltName	NE	rfc822Name	Opcionalno. Sadrži e-mail adresu potpisnika.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA2.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer

2.24. UNO POTVRDA ZA AUTENTIKACIJU MREŽNIH STRANICA (SSL)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 2 godine
Subject	commonName (CN)	Samo jedan puni kvalificirani naziv poslužitelja (FQDN)
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Mjesto sjedišta UNO ili regionalnog centra.
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	serverAuth	1.3.6.1.5.5.7.3.1
		clientAuth	1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.2.13.1.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
subjectAltName	NE	dnsName	Puni kvalificirani naziv poslužitelja (FQDN)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA2.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer

2.25. UNO KERBEROS POTVRDA ZA DOMEN KONTROLER (DOMEN KONTROLER KDC)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 2 godine
Subject	commonName (CN)	Samo jedan puni kvalificirani naziv poslužitelja (FQDN)
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Puni registrirani skraćeni naziv pravne osobe ili naziv pravne osobe ako skraćeni naziv nije registriran (UNO)
	localityName (L)	Mjesto sjedišta UNO ili regionalnog centra.
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
	NE	serverAuth	1.3.6.1.5.5.7.3.1
		clientAuth	1.3.6.1.5.5.7.3.2
extKeyUsage	NE	Smart card logon	1.3.6.1.4.1.311.20.2.2
		keyPurposeKdc	1.3.6.1.5.2.3.5
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.2.13.10.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
subjectAltName	NE	dnsName	Puni kvalificirani naziv poslužitelja (FQDN)
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA2.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer

2.26. UNO APLIKATIVNA POTVRDA ZA AUTENTIKACIJU U OBLIKU DATOTEKE PKCS #12 FORMATA (NCP)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 24 mjeseca
Subject	commonName (CN)	Naziv aplikacije, softverskog modula ili informacijskog sustava
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Mjesto sjedišta UNO ili regionalnog centra
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	Digital Signature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.2.14.1.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	ncp (1), OID: 0.4.0.2042.1.1
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA2.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer

2.27. UNO POTVRDA ZA VREMENSKI ŽIG

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 4 godine
Subject	commonName (CN)	UINO TSA 2020 <redni broj izdane potvrde >
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Banja Luka
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 3072 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
privateKeyUsage Period	NE	notBefore	Vrijeme izdavanja potvrde
		notAfter	Vrijeme izdavanja potvrde + 1 godina
extKeyUsage	DA	timeStamping	OID: 1.3.6.1.5.5.7.3.8
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.2.15.1.1 policyQualifierId: id-qt-cps { id-qt 1 }
		policyQualifiers	CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA2.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer

2.28. UNO POTVRDA ZA POTPIS ODGOVORA OCSP SERVIS ZA UINO ISSUING CA2

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 12 mjeseci
Subject	commonName (CN)	UINO Issuing CA2 OCSP
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Banja Luka
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 2048 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
extKeyUsage	NE	ocspSigning	OID: 1.3.6.1.5.5.7.3.9
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.2.16.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer

2.29. UNO POTVRDA ZA POTPISIVANJE KODA (NCP+)

OSNOVNA POLJA

POLJE	ATRIBUT	VRIJEDNOST
Version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	95 bita entropije, 20 bajtova
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 36 mjeseci
Subject	commonName (CN)	Uprava za indirektno-neizravno oporezivanje
	organizationIdentifier (2.5.4.97)	VATBA-PIB UNO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Banja Luka
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Javni ključ subjekta duljine 3072 bita

EKSTENZIJE

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
extKeyUsage	NE	codeSigning	OID: 1.3.6.1.5.5.7.3.3
certificatePolicies	NE	policyIdentifier	UNO OID: 1.3.6.1.4.1.46134.10.2.2.17.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: http://ca.uino.gov.ba/bs/dokumenti CPS uri: http://ca.uino.gov.ba/sr/dokumenti CPS uri: http://ca.uino.gov.ba/hr/dokumenti CPS uri: http://ca.uino.gov.ba/en/documents
		policyIdentifier	ncplusplus (2), OID: 0.4.0.2042.1.2
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA2.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		CA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.uino.gov.ba
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer