

**УПРАВА ЗА ИНДИРЕКТНО ОПОРЕЗИВАЊЕ**  
**Бана Лазаревића бб, Бања Лука**

**УИО ПРОФИЛИ ПОТВРДА**

Верзија 1.0

## УИО ПРОФИЛИ ПОТВРДА

1. ПОПИС ТИПОВА ПОТВРДА И ЊИХОВИХ ПОДРУЧЈА ПРИМЈЕНЕ.....	4
1.1. ПОПИС ТИПОВА ПОТВРДА КОЈЕ ИЗДАЈЕ <i>UINO ROOT CA</i> .....	4
1.2. ПОПИС ТИПОВА ПОТВРДА КОЈИ ИЗДАЈЕ <i>UINO ISSUING CA1</i> .....	4
1.2. ПОПИС ТИПОВА ПОТВРДА КОЈИ ИЗДАЈЕ <i>UINO ISSUING CA1</i> .....	5
1.3. ПОПИС ТИПОВА ПОТВРДА КОЈЕ ИЗДАЈЕ <i>UINO ISSUING CA2</i> .....	5
2. ПРОФИЛИ ПОТВРДА.....	6
2.1. УИО КОРИЈЕНСКА ПОТВРДА - <i>UINO ROOT CA</i> .....	6
2.2. УИО ПОТВРДА ПРВОГ ИЗДАВАЧКОГ СА ТИЈЕЛА - <i>UINO ISSUING CA1</i> .....	7
2.3. УИО ПОТВРДА ДРУГОГ ИЗДАВАЧКОГ СА ТИЈЕЛА - <i>UINO ISSUING CA2</i> .....	8
2.4. УИО ПОТВРДА ЗА ПОТПИС ОДГОВОРА <i>OCSP</i> СЕРВИСА ЗА <i>UINO ROOT CA</i> .....	9
2.5. УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ФИЗИЧКА ЛИЦА ( <i>QCP-n-qscd</i> ).....	10
2.6. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ ФИЗИЧКИХ ЛИЦА ( <i>NCP+</i> ).....	11
2.7. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И АУТЕНТИФИКАЦИЈУ ЗА ФИЗИЧКА ЛИЦА ( <i>NCP+</i> ) .....	12
2.8. УИО ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ И АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ <i>PKCS#12</i> ЗА ФИЗИЧКА ЛИЦА ( <i>NCP</i> ) .....	13
2.9. УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА ( <i>QSP-n-qscd</i> ).....	14
2.10. УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА СТРАНЦЕ ПОВЕЗАНЕ СА ПРАВНИМ ЛИЦИМА ( <i>QSP-n-qscd</i> ).....	15
2.11. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ ФИЗИЧКИХ ЛИЦА ПОВЕЗАНИХ СА ПРАВНИМ ЛИЦИМА ( <i>NCP+</i> ) .....	16
2.12. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И АУТЕНТИФИКАЦИЈУ ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА ( <i>NCP+</i> ).....	17
2.13. УИО ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ И АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ <i>PKCS#12</i> ФОРМАТА ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА ( <i>NCP</i> ) .....	18
2.14. УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПЕЧАТ ( <i>QCP-l-qscd</i> )....	19
2.15. УИО ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ МРЕЖНИХ СТРАНИЦА ( <i>SSL</i> ) ЗА ПРАВНА ЛИЦА .....	20
2.16. УИО АПЛИКАТИВНА ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ ЗА ПРАВНА ЛИЦА ( <i>NCP</i> ).....	21
2.17. УИО ПОТВРДА ЗА КВАЛИФИКОВАНИ ЕЛЕКТРОНСКИ ВРЕМЕНСКИ ЖИГ ....	22
2.18. УИО ПОТВРДА ЗА ПОТПИС ОДГОВОРА <i>OCSP</i> СЕРВИСА ЗА <i>UINO ISSUING CA1</i> .....	23
2.19. УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ЗАПОСЛЕНЕ ( <i>QSP-n-qscd</i> ).....	24
2.20. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ ЗА ЗАПОСЛЕНЕ ( <i>NCP+</i> ) .....	25
2.21. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И АУТЕНТИФИКАЦИЈУ ЗА ЗАПОСЛЕНЕ ( <i>NCP+</i> ).....	26
2.22. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И ДОМЕНСКУ АУТЕНТИФИКАЦИЈУ ЗА ЗАПОСЛЕНЕ ( <i>NCP+</i> ) .....	27

2.23. УИО ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ И АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ <i>PKCS #12</i> ФОРМАТА ( <i>NCP</i> ).....	28
2.24. УИО ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ МРЕЖНИХ СТРАНИЦА ( <i>SSL</i> ).....	29
2.25. УИО КЕРБЕРОС ПОТВРДА ЗА ДОМЕН КОНТРОЛЕР (ДОМЕН КОНТРОЛЕР <i>KDC</i> ) .....	30
2.26. УИО АПЛИКАТИВНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ <i>PKCS #12</i> ФОРМАТА ( <i>NCP</i> ).....	31
2.27. УИО ПОТВРДА ЗА ВРЕМЕНСКИ ЖИГ .....	32
2.28. УИО ПОТВРДА ЗА ПОТПИС ОДГОВОРА <i>OCSP</i> СЕРВИСА ЗА <i>UINO ISSUING CA2</i> .....	33
2.29. УИО ПОТВРДА ЗА ПОТПИСИВАЊЕ КОДА ( <i>NCP+</i> ).....	34

# 1. ПОПИС ТИПОВА ПОТВРДА И ЊИХОВИХ ПОДРУЧЈА ПРИМЈЕНЕ

## 1.1. ПОПИС ТИПОВА ПОТВРДА КОЈЕ ИЗДАЈЕ *UINO ROOT CA*

НАЗИВ ГРУПЕ	НАЗИВ ТИПА ПОТВРДА
<i>UINO ROOT CA</i> ПОТВРДА	ПОТВРДА УИО КОРИЈЕНСКОГ СА ТИЈЕЛА
<i>UINO ISSUING CA1</i> ПОТВРДА	ПОТВРДА ПРВОГ УИО ИЗДАВАЧКОГ СА ТИЈЕЛА
<i>UINO ISSUING CA2</i> ПОТВРДА	ПОТВРДА ДРУГОГ УИО ИЗДАВАЧКОГ СА ТИЈЕЛА
УИО ПОТВРДА ЗА <i>OCSP</i> СЕРВИС	ПОТВРДА ЗА ПОТПИС ОДГОВОРА <i>OCSP</i> СЕРВИСА ЗА <i>UINO ROOT CA</i>

## 1.2. ПОПИС ТИПОВА ПОТВРДА КОЈИ ИЗДАЈЕ *UINO ISSUING CA1*

НАЗИВ ГРУПЕ	НАЗИВ ТИПА ПОТВРДЕ	ПОДРУЧЈЕ ПРИМЈЕНЕ ПОТВРДЕ
<b>ПОТВРДА ЗА ФИЗИЧКА ЛИЦА</b>	УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ФИЗИЧКА ЛИЦА ( <i>QCP-n-qscd</i> )	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА ЗА ИЗРАДУ КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПОТПИСА.
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ ФИЗИЧКИХ ЛИЦА ( <i>NCP+</i> )	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА И КОРИСТИ ЗА ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И АУТЕНТИФИКАЦИЈУ ЗА ФИЗИЧКА ЛИЦА ( <i>NCP+</i> )	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА И КОРИСТИ ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА, ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ И АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ <i>PKCS#12</i> ФОРМАТА ЗА ФИЗИЧКА ЛИЦА ( <i>NCP</i> )	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА, ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
<b>ПОТВРДА ЗА ПРАВНА ЛИЦА</b>	УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА ( <i>QCP-n-qscd</i> )	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА ПОВЕЗАНИМ С ПОСЛОВНИМ СУБЈЕКТОМ ЗА ИЗРАДУ КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПОТПИСА У ПОСЛОВНЕ СВРХЕ.
	УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА СТРАНЦЕ ПОВЕЗАНЕ СА ПРАВНИМ ЛИЦИМА ( <i>QCP-n-qscd</i> )	ИЗДАЈЕ СЕ СТРАНЦИМА ПОВЕЗАНИМ С ПОСЛОВНИМ СУБЈЕКТОМ ЗА ИЗРАДУ КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПОТПИСА У ПОСЛОВНЕ СВРХЕ.
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ ФИЗИЧКИХ ЛИЦА ПОВЕЗАНИХ СА ПРАВНИМ ЛИЦИМА ( <i>NCP+</i> )	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА ПОВЕЗАНИМ С ПОСЛОВНИМ СУБЈЕКТОМ ЗА ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА У ПОСЛОВНЕ СВРХЕ.
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И АУТЕНТИФИКАЦИЈУ ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА ( <i>NCP+</i> )	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА ПОВЕЗАНИМ СА ПОСЛОВНИМ СУБЈЕКТОМ ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА, ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА У ПОСЛОВНЕ СВРХЕ.
	УИО ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ И АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ <i>PKCS#12</i> ФОРМАТА ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА ( <i>NCP</i> )	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА ПОВЕЗАНИМ С ПОСЛОВНИМ СУБЈЕКТОМ. КОРИСТИ СЕ ЗА ПОТРЕБЕ ЕЛЕКТРОНСКОГ ПОТПИСИВАЊА, ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	УИО АПЛИКАТИВНА ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ ЗА ПРАВНА ЛИЦА ( <i>NCP</i> )	ИЗДАЈЕ СЕ АПЛИКАЦИЈАМА И ИНФОРМАЦИОНИМ СИСТЕМИМА ПРАВНИХ ЛИЦА ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА.

<b>ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПЕЧАТ</b>	УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПЕЧАТ ( <i>QCP-l-qscd</i> )	ИЗДАЈЕ СЕ ПРАВНИМ ЛИЦИМА ЗА ИЗРАДУ КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПЕЧАТА.
-------------------------------------	--	--

### 1.2. ПОПИС ТИПОВА ПОТВРДА КОЈИ ИЗДАЈЕ *UINO ISSUING CA1*

НАЗИВ ГРУПЕ	НАЗИВ ТИПА ПОТВРДЕ	ПОДРУЧЈЕ ПРИМЈЕНЕ ПОТВРДЕ
<b>ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ МРЕЖНИХ СТРАНИЦА ЗА ПРАВНА ЛИЦА</b>	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ МРЕЖНИХ СТРАНИЦА ( <i>SSL</i> ) ЗА ПРАВНА ЛИЦА	ИЗДАЈЕ СЕ ПРАВНИМ ЛИЦИМА ЗА АУТЕНТИФИКАЦИЈУ МРЕЖНИХ СТРАНИЦА.
<b>ПОТВРДА ЗА <i>OCSP</i> СЕРВИС</b>	УИО ПОТВРДА ЗА <i>OCSP</i> СЕРВИС <i>UINO ISSUING CA1</i>	ИЗДАЈЕ СЕ <i>OCSP</i> СЕРВИСУ ЗА ПОТПИС <i>OCSP</i> ОДГОВОРА <i>CA</i> ТИЈЕЛА <i>UINO ISSUING CA1</i> .
<b>КВАЛИФИКОВАНА ПОТВРДА ЗА ВРЕМЕНСКИ ЖИГ</b>	УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ВРЕМЕНСКИ ЖИГ	ИЗДАЈЕ СЕ СЕРВИСУ ЗА ИЗДАВАЊЕ КВАЛИФИКОВАНИХ ВРЕМЕНСКИХ ЖИГОВА И КОРИСТИ ЗА ПОТПИСИВАЊЕ КВАЛИФИКОВАНИХ ВРЕМЕНСКИХ ЖИГОВА.

### 1.3. ПОПИС ТИПОВА ПОТВРДА КОЈЕ ИЗДАЈЕ *UINO ISSUING CA2*

НАЗИВ ГРУПЕ	НАЗИВ ТИПА ПОТВРДЕ	ПОДРУЧЈЕ ПРИМЈЕНЕ ПОТВРДЕ
<b>ПОТВРДА ЗА ЗАПОСЛЕНЕ</b>	УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ЗАПОСЛЕНЕ ( <i>QCP-n-qscd</i> )	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА ЗА ИЗРАДУ КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПОТПИСА.
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ ЗА ЗАПОСЛЕНЕ ( <i>NCP+</i> )	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА ЗА ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И АУТЕНТИФИКАЦИЈУ ЗА ЗАПОСЛЕНЕ ( <i>NCP+</i> )	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА, ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И ДОМЕНСКУ АУТЕНТИФИКАЦИЈУ ЗА ЗАПОСЛЕНЕ ( <i>NCP+</i> )	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА И ДОМЕНСКУ АУТЕНТИФИКАЦИЈУ.
	УИО ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ И АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ <i>PKCS#12</i> ФОРМАТА ЗА ЗАПОСЛЕНЕ ( <i>NCP</i> )	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА, А КОРИСТИ СЕ ЗА ПОТРЕБЕ ЕЛЕКТРОНСКОГ ПОТПИСИВАЊА, ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	УИО АПЛИКАТИВНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ <i>PKCS #12</i> ФОРМАТА ( <i>NCP</i> )	ИЗДАЈЕ СЕ СОФТВЕРСКИМ МОДУЛИМА ИНФОРМАЦИОНОГ СИСТЕМА УИО И КОРИСТИ ЗА ЊИХОВУ АУТЕНТИФИКАЦИЈУ ДРУГИМ МОДУЛИМА И ИНФОРМАЦИОНИМ СИСТЕМАМА УИО И ЕНКРИПЦИЈУ КЉУЧА.
	УИО ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ МРЕЖНИХ СТРАНИСА ( <i>SSL</i> )	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА- АДМИНИСТРАТОРИМА СЕРВЕРА ЗА АУТЕНТИФИКАЦИЈУ МРЕЖНИХ СТРАНИЦА.
	УИО КЕРБЕРОС ПОТВРДА ЗА ДОМЕН КОНТРОЛЕР (ДОМЕН КОНТРОЛЕР <i>KDC</i> )	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА- АДМИНИСТРАТОРИМА <i>ACTIVE DIRECTORY</i> ДОМЕНА ЗА АУТЕНТИФИКАЦИЈУ ДОМЕН КОНТРОЛЕРА.
	УИО ПОТВРДА ЗА ВРЕМЕНСКИ ЖИГ	ИЗДАЈЕ СЕ ИНТЕРНОМ СЕРВИСУ ЗА ИЗДАВАЊЕ ВРЕМЕНСКИХ ЖИГОВА И КОРИСТИ ЗА ПОТПИСИВАЊЕ ВРЕМЕНСКИХ ЖИГОВА.
	УИО ПОТВРДА ЗА ПОТПИСИВАЊЕ КОДА ( <i>NCP+</i> )	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА ЗА ПОТПИСИВАЊЕ ФАЈЛОВА ИНФОРМАЦИОНИХ СИСТЕМА УИО.
	УИО ПОТВРДА ЗА <i>OCSP</i> СЕРВИС <i>UINO ISSUING CA2</i>	ИЗДАЈЕ СЕ <i>OCSP</i> СЕРВИСУ ЗА ПОТПИС <i>OCSP</i> ОДГОВОРА <i>CA</i> ТИЈЕЛА <i>UINO ISSUING CA2</i> .

## 2. ПРОФИЛИ ПОТВРДА

### 2.1. УИО КОРИЈЕНСКА ПОТВРДА - *UINO ROOT CA*

#### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	<i>X.509 V3</i>
serialNumber	CertificateSerialNumber	00 a1 4b 09 ce 74 e2 56 36 00 00 00 00 5e 62 20 c2 64 бита ентропије, што је 16 или 17 октета серијског броја, (32-34 hex бројева)
signatureAlgorithm	AlgorithmIdentifier	<i>Sha512RSA</i>
Signature hash algorithm		<i>Sha512</i>
Issuer	commonName (CN)	<i>UINO Root CA</i>
	OrganizationName (O)	<i>Uprava za indirektno-neizravno oporezivanje</i>
	countryName (C)	<i>BA</i>
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 20 година.
Subject	commonName (CN)	<i>UINO Root CA</i>
	organizationName (O)	<i>Uprava za indirektno-neizravno oporezivanje</i>
	countryName (C)	<i>BA</i>
subjectPublic KeyInfo	AlgorithmIdentifier	<i>RSA</i>
	subjectPublicKey	Јавни кључ <i>CA: 4096 Bits</i>

#### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	ВРИЈЕДНОСТ
KeyUsage	ДА	<i>Certificate Signing</i> – потписивање потврде <i>Off-line CRL Signing</i> – потписивање ван мреже <i>CRL Signing (06)</i> - <i>CRL</i> потписивање
BasicConstraints	ДА	<i>Subject Type=CA</i> <i>Path Length Constraint=None</i>
AuthorityKeyIdentifier	НЕ	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-бит SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused бита) према RFC 5280, тачка 4.2.1.2 метода (1)
SubjectKeyIdentifier	НЕ	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-бит SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused бита) према RFC 5280, тачка 4.2.1.2 метода (1)

## 2.2. УИО ПОТВРДА ПРВОГ ИЗДАВАЧКОГ СА ТИЈЕЛА - UINO ISSUING CA1

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	X.509 V3
serialNumber	CertificateSerialNumber	11 0a fc c0 4c 5d 59 67 00 00 00 00 5e 62 20 fb 64 бита ентропије, што је 16 или 17 октета серијског броја, (32-34 хех бројева)
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 20 година
Subject	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	Јавни кључ СА: 4096 бит

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	ВРИЈЕДНОСТ	
KeyUsage	ДА	<i>Certificate Signing</i> - потписивање потврде <i>Off-line CRL Signing</i> - потписивање ван мреже <i>CRL Signing (06)</i> - CRL потписивање	
BasicConstraints	ДА	<i>Subject Type=CA</i> <i>Path Length Constraint=0</i>	
AuthorityKeyIdentifier	НЕ	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-бит <i>SHA-1</i> hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits) према RFC 5280, тачка 4.2.1.2 метода (1))	
SubjectKeyIdentifier	НЕ	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-бит <i>SHA-1</i> hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits) према RFC 5280, тачка 4.2.1.2 метода (1))	
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.1.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: <a href="http://ca.uino.gov.ba/CPS/UINO-CPS1-0-bs.pdf">http://ca.uino.gov.ba/CPS/UINO-CPS1-0-bs.pdf</a> CPS uri: <a href="http://ca.uino.gov.ba/CPS/UINO-CPS1-0-sr.pdf">http://ca.uino.gov.ba/CPS/UINO-CPS1-0-sr.pdf</a> CPS uri: <a href="http://ca.uino.gov.ba/CPS/UINO-CPS1-0-hr.pdf">http://ca.uino.gov.ba/CPS/UINO-CPS1-0-hr.pdf</a> CPS uri: <a href="http://ca.uino.gov.ba/CPS/UINO-CPS1-0-en.pdf">http://ca.uino.gov.ba/CPS/UINO-CPS1-0-en.pdf</a>
Authority Information Access	НЕ	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: <a href="http://ocsp.uino.gov.ba">http://ocsp.uino.gov.ba</a>
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: <a href="http://cdp.uino.gov.ba/AIA/UINORootCA.cer">http://cdp.uino.gov.ba/AIA/UINORootCA.cer</a>
CRLDistributionPoints	НЕ	DistributionPoint [1] URI: <a href="http://cdp.uino.gov.ba/CRL/UINORootCA.crl">http://cdp.uino.gov.ba/CRL/UINORootCA.crl</a> [2] URI: <a href="http://cdp.uinoca.ba/CRL/UINORootCA.crl">http://cdp.uinoca.ba/CRL/UINORootCA.crl</a>	

### 2.3. УИО ПОТВРДА ДРУГОГ ИЗДАВАЧКОГ СА ТИЈЕЛА - *UINO ISSUING CA2*

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
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 бита ентропије, што је 16 или 17 октета серијског броја, (32-34 хех бројева)
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме потврде + 20 година
Subject	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	Јавни кључ СА: 4096 бит

#### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	ВРИЈЕДНОСТ	
KeyUsage	ДА	<i>Certificate Signing</i> - потписивање потврде <i>Off-line CRL Signing</i> - потписивање ван мреже <i>CRL Signing (06)</i> - CRL потписивање	
BasicConstraints	ДА	Subject Type=CA Path Length Constraint=None	
AuthorityKeyIdentifier	НЕ	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-бит <i>SHA-1</i> hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused бита) према RFC 5280, тачка 4.2.1.2 метода (1))	
SubjectKeyIdentifier	НЕ	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-бит <i>SHA-1</i> hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused бита) према RFC 5280, тачка 4.2.1.2 метода (1))	
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.1.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: <a href="http://ca.uino.gov.ba/CPS/UINO-CPS1-0-bs.pdf">http://ca.uino.gov.ba/CPS/UINO-CPS1-0-bs.pdf</a> CPS uri: <a href="http://ca.uino.gov.ba/CPS/UINO-CPS1-0-sr.pdf">http://ca.uino.gov.ba/CPS/UINO-CPS1-0-sr.pdf</a> CPS uri: <a href="http://ca.uino.gov.ba/CPS/UINO-CPS1-0-hr.pdf">http://ca.uino.gov.ba/CPS/UINO-CPS1-0-hr.pdf</a> CPS uri: <a href="http://ca.uino.gov.ba/CPS/UINO-CPS1-0-en.pdf">http://ca.uino.gov.ba/CPS/UINO-CPS1-0-en.pdf</a>
Authority Information Access	НЕ	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: <a href="http://ocsp.uino.gov.ba">http://ocsp.uino.gov.ba</a>
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: <a href="http://cdp.uino.gov.ba/AIA/UINORootCA.cer">http://cdp.uino.gov.ba/AIA/UINORootCA.cer</a>
CRLDistributionPoints	НЕ	DistributionPoint [1] URI: <a href="http://cdp.uino.gov.ba/CRL/UINORootCA.crl">http://cdp.uino.gov.ba/CRL/UINORootCA.crl</a> [2] URI: <a href="http://cdp.uinoca.ba/CRL/UINORootCA.crl">http://cdp.uinoca.ba/CRL/UINORootCA.crl</a>	



## 2.4. УИО ПОТВРДА ЗА ПОТПИС ОДГОВОРА OCSP СЕРВИСА ЗА UINO ROOT CA

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 12 мјесеци
Subject	commonName (CN)	UINO Root OCSP
	organizationIdentifier (2.5.4.97)	VATBA-PIB UIO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Banja Luka
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	RSA
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
		nonRepudiation	Укључен <i>nonRepudiation</i> бит
extKeyUsage	НЕ	ocspSigning	OID: 1.3.6.1.5.5.7.3.9
id-pkix-ocsp-nocheck	НЕ		OID: 1.3.6.1.5.5.7.48.1.5
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.2.0.16.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: <a href="http://ca.uino.gov.ba/bs/dokumenti">http://ca.uino.gov.ba/bs/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/sr/dokumenti">http://ca.uino.gov.ba/sr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/hr/dokumenti">http://ca.uino.gov.ba/hr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/en/documents">http://ca.uino.gov.ba/en/documents</a>
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: <a href="http://cdp.uino.gov.ba/CRL/UINORootCA.crl">http://cdp.uino.gov.ba/CRL/UINORootCA.crl</a> [2] URI: <a href="http://cdp.uinoca.ba/CRL/UINORootCA.crl">http://cdp.uinoca.ba/CRL/UINORootCA.crl</a>
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: <a href="http://ocsp.uino.gov.ba">http://ocsp.uino.gov.ba</a>
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: <a href="http://cdp.uino.gov.ba/AIA/UINORootCA.cer">http://cdp.uino.gov.ba/AIA/UINORootCA.cer</a>

2.5. УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ФИЗИЧКА ЛИЦА (QCP-n-qscd)

ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signaturehashAlgorithm		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме како је наведено у идентификационој исправи
	serialNumber	CA:BA-JIP, гдје је JIP (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификационој исправи
	localityName (L)	Мјесто пребивалишта потписника
	countryName (C)	Држава потписника
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	nonRepudiation	Укључен nonRepudiation бит
certificatePolicies	НЕ	policyIdentifier	UIO 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	НЕ	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/pds/PDS-bs.pdf, bs http://ca.uino.gov.ba/pds/PDS-sr.pdf, sr http://ca.uino.gov.ba/pds/PDS-hr.pdf, hr http://ca.uino.gov.ba/pds/PDS-en.pdf, en
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	НЕ	rfc822Name	Опционално. Садржи е-mail адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ ФИЗИЧКИХ ЛИЦА (NCP+)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност =“2“
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signaturehashAlgorithm		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	CA:BA-JIP, гдје је JIP (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификацијској исправи
	localityName (L)	Мјесто пребивалишта потписника
	countryName (C)	Држава потписника
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
		keyEncipherment	Укључен <i>keyEncipherment</i> бит
extKeyUsage	НЕ	clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	НЕ	policyIdentifier	UIO 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	ncplus (2), OID: 0.4.0.2042.1.2
subjectAltName	НЕ	rfc822Name	Опционално. Садржи е-маил адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И АУТЕНТИФИКАЦИЈУ ЗА ФИЗИЧКА ЛИЦА (NCP+)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signaturehashAlgorithm		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	CA:BA-JIP, гдје је JIP (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификационој исправи
	localityName (L)	Мјесто пребивалишта потписника
	countryName (C)	Држава потписника
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
Key Usage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
		keyEncipherment	Укључен <i>keyEncipherment</i> бит
extKeyUsage	НЕ	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	НЕ	policyIdentifier	UIO 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	ncpplus (2), OID: 0.4.0.2042.1.2
subjectAltName	НЕ	rfc822Name	Опционално. Садржи е-mail адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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. УИО ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ И АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ  
PKCS#12 ЗА ФИЗИЧКА ЛИЦА (NCP)**

**ОСНОВНА ПОЉА**

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	CA:BA-JIP, гдје је JIP (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификационој исправи
	localityName (L)	Мјесто пребивалишта потписника
	countryName (C)	Држава потписника
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

**ЕКСТЕНЗИЈЕ**

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
Key Usage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
		keyEncipherment	Укључен <i>keyEncipherment</i> бит
extKeyUsage	НЕ	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.2.1.10.4.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: <a href="http://ca.uino.gov.ba/bs/dokumenti">http://ca.uino.gov.ba/bs/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/sr/dokumenti">http://ca.uino.gov.ba/sr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/hr/dokumenti">http://ca.uino.gov.ba/hr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/en/documents">http://ca.uino.gov.ba/en/documents</a>
		policyIdentifier	nep (1), OID: 0.4.0.2042.1.1
subjectAltName	НЕ	rfc822Name	Опционално. Садржи е-mail адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: <a href="http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl">http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl</a> [2] URI: <a href="http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl">http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl</a>
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: <a href="http://ocsp.uino.gov.ba">http://ocsp.uino.gov.ba</a>
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: <a href="http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer">http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer</a>

**2.9. УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА (QSP-n-qscd)**

**ОСНОВНА ПОЉА**

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност =“2“
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавање потврде
	notAfter	Вријеме издавање потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	CA:BA-JIP, гдје је JIP (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификационој исправи
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Порески идентификациони број (ПИБ) правног лица).
	organizationName (O)	Пуни регистровани скраћени назив пословног субјекта или назив пословног субјекта ако скраћени назив није регистрован.
	localityName (L)	Мјесто сједишта пословног субјекта
subjectPublic KeyInfo	countryName (C)	BA
	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

**ЕКСТЕНЗИЈЕ**

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	nonRepudiation	Укључен nonRepudiation бит
certificatePolicies	НЕ	policyIdentifier	UIO 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	НЕ	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/pds/PDS-bs.pdf, bs http://ca.uino.gov.ba/pds/PDS-sr.pdf, sr http://ca.uino.gov.ba/pds/PDS-hr.pdf, hr http://ca.uino.gov.ba/pds/PDS-en.pdf, en
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	НЕ	rfc822Name	Опционално. Садржи е-mail адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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. УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА СТРАНЦЕ ПОВЕЗАНЕ СА ПРАВНИМ ЛИЦИМА (QSP-n-qscd)**

**ОСНОВНА ПОЉА**

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	CA:BA-JIP, гдје је JIP (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификационој исправи
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Порески идентификациони број (ПИБ) правног лица).
	organizationName (O)	Пуни регистровани скраћени назив пословног субјекта или назив пословног субјекта ако скраћени назив није регистрован.
	localityName (L)	Мјесто сједишта пословног субјекта
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

**ЕКСТЕНЗИЈЕ**

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	nonRepudiation	Укључен nonRepudiation бит
certificatePolicies	НЕ	policyIdentifier	UIO 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	НЕ	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/pds/PDS-bs.pdf, bs http://ca.uino.gov.ba/pds/PDS-sr.pdf, sr http://ca.uino.gov.ba/pds/PDS-hr.pdf, hr http://ca.uino.gov.ba/pds/PDS-en.pdf, en
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	НЕ	rfc822Name	Опционално. Садржи е-mail адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ ФИЗИЧКИХ ЛИЦА ПОВЕЗАНИХ СА ПРАВНИМ ЛИЦИМА (NCP+)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	СА:ВА-ЈИР, гдје је ЈИР (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификационој исправи
	organizationIdentifier (2.5.4.97)	VATVA-PIB (Порески идентификациони број ПИБ правног лица).
	organizationName (O)	Пуни регистровани скраћени назив пословног субјекта или назив пословног субјекта ако скраћени назив није регистрован.
	localityName (L)	Мјесто сједишта пословног субјекта
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	Digital Signature	Укључен digitalSignature бит
		keyEncipherment	Укључен keyEncipherment бит
extKeyUsage	НЕ	clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	НЕ	policyIdentifier	UIO 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	ncpplus (2), OID: 0.4.0.2042.1.2
subjectAltName	НЕ	rfc822Name	Опционално. Садржи е-mail адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UIINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UIINOIssuingCA1.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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/UIINOIssuingCA1.cer



## 2.12. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И АУТЕНТИФИКАЦИЈУ ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА (NCP+)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	CA:BA-JIP, гдје је JIP (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификационој исправи
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Порески идентификациони број ПИБ правног лица).
	organizationName (O)	Пуни регистровани скраћени назив пословног субјекта или назив пословног субјекта ако скраћени назив није регистриран.
	localityName (L)	Мјесто сједишта пословног субјекта
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	Digital Signature	Укључен <i>digitalSignature</i> бит
		keyEncipherment	Укључен <i>keyEncipherment</i> бит
extKeyUsage	НЕ	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.2.1.11.4.1 policyQualifierId: id-qt-cps { id-qt 1 }
		policyQualifiers	CPS uri: <a href="http://ca.uino.gov.ba/bs/dokumenti">http://ca.uino.gov.ba/bs/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/sr/dokumenti">http://ca.uino.gov.ba/sr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/hr/dokumenti">http://ca.uino.gov.ba/hr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/en/documents">http://ca.uino.gov.ba/en/documents</a>
		policyIdentifier	ncpplus (2), OID: 0.4.0.2042.1.2
subjectAltName	НЕ	rfc822Name	Опционално. Садржи <i>e-mail</i> адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: <a href="http://cdp.uino.gov.ba/CRL/UIINOIssuingCA1.crl">http://cdp.uino.gov.ba/CRL/UIINOIssuingCA1.crl</a> [2] URI: <a href="http://cdp.uinoca.ba/CRL/UIINOIssuingCA1.crl">http://cdp.uinoca.ba/CRL/UIINOIssuingCA1.crl</a>
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: <a href="http://ocsp.uino.gov.ba">http://ocsp.uino.gov.ba</a>
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: <a href="http://cdp.uino.gov.ba/AIA/UIINOIssuingCA1.cer">http://cdp.uino.gov.ba/AIA/UIINOIssuingCA1.cer</a>

**2.13. УИО ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ И АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ  
PKCS#12 ФОРМАТА ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА (NCP)**

**ОСНОВНА ПОЉА**

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	CA:BA-JIP, гдје је JIP (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификационој исправи
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Порески идентификациони број ПИБ правног лица).
	organizationName (O)	Пуни регистровани скраћени назив пословног субјекта или назив пословног субјекта ако скраћени назив није регистрован
	localityName (L)	Мјесто сједишта пословног субјекта
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

**ЕКСТЕНЗИЈЕ**

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	Digital Signature	Укључен <i>digitalSignature</i> бит
		keyEncipherment	Укључен <i>keyEncipherment</i> бит
extKeyUsage	НЕ	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.2.1.11.5.0 policyQualifierId: id-qt-cps { id-qt 1 }
		policyQualifiers	CPS uri: <a href="http://ca.uino.gov.ba/bs/dokumenti">http://ca.uino.gov.ba/bs/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/sr/dokumenti">http://ca.uino.gov.ba/sr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/hr/dokumenti">http://ca.uino.gov.ba/hr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/en/documents">http://ca.uino.gov.ba/en/documents</a>
		policyIdentifier	nsp (1), OID: 0.4.0.2042.1.1
subjectAltName	НЕ	rfc822Name	Опционално. Садржи е-mail адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: <a href="http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl">http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl</a> [2] URI: <a href="http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl">http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl</a>
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: <a href="http://ocsp.uino.gov.ba">http://ocsp.uino.gov.ba</a>
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: <a href="http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer">http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer</a>

## 2.14. УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПЕЧАТ (*QCP-l-qscd*)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Потпис издаваоца потврде
Issuer	commonName (CN)	<i>UINO Issuing CA1</i>
	organizationName (O)	<i>Uprava za indirektno-neizravno oporezivanje</i>
	countryName (C)	<i>BA</i>
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Назив који субјекат користи за своје представљање
	serialNumber	<i>CA:BA-JIP</i> , гдје је <i>JIP</i> (Јединствени идентификатор потврде) псеудослучајно генерисан број
	organizationIdentifier (2.5.4.97)	<i>VATVA-PIB</i> (Порески идентификациони број ПИБ правног лица).
	organizationName (O)	Пуни регистровани скраћени назив правне особе или назив правне особе ако скраћени назив није регистрован
	localityName (L)	Мјесто сједишта правног лица
	countryName (C)	<i>BA</i>
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
certificatePolicies	НЕ	policyIdentifier	УИО <i>OID</i> : 1.3.6.1.4.1.46134.10.2.1.12.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: <a href="http://ca.uino.gov.ba/bs/dokumenti">http://ca.uino.gov.ba/bs/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/sr/dokumenti">http://ca.uino.gov.ba/sr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/hr/dokumenti">http://ca.uino.gov.ba/hr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/en/documents">http://ca.uino.gov.ba/en/documents</a>
		policyIdentifier	qcp-legal-qscd (3), <i>OID</i> : 0.4.0.194112.1.3
qcStatements	НЕ	esi4-qcStatement-1	<i>OID</i> : 0.4.0.1862.1.1
		esi4-qcStatement-4	<i>OID</i> : 0.4.0.1862.1.4
		esi4-qcStatement-5	<i>OID</i> : 0.4.0.1862.1.5 <a href="https://ca.uino.gov.ba/pds/PDS-bs.pdf">https://ca.uino.gov.ba/pds/PDS-bs.pdf</a> , bs <a href="https://ca.uino.gov.ba/pds/PDS-sr.pdf">https://ca.uino.gov.ba/pds/PDS-sr.pdf</a> , sr <a href="https://ca.uino.gov.ba/pds/PDS-hr.pdf">https://ca.uino.gov.ba/pds/PDS-hr.pdf</a> , hr <a href="https://ca.uino.gov.ba/pds/PDS-en.pdf">https://ca.uino.gov.ba/pds/PDS-en.pdf</a> , en
		esi4-qcStatement-6	<i>OID</i> : 0.4.0.1862.1.6.2
subjectAltName	НЕ	rfc822Name	Опционално. Садржи <i>e-mail</i> адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: <a href="http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl">http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl</a> [2] URI: <a href="http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl">http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl</a>
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: <a href="http://ocsp.uino.gov.ba">http://ocsp.uino.gov.ba</a>
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: <a href="http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer">http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer</a>

## 2.15. УИО ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ МРЕЖНИХ СТРАНИЦА (SSL) ЗА ПРАВНА ЛИЦА

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 398 дана
Subject	commonName (CN)	Само један пуни квалификовани назив сервера (FQDN)
	organizationIdentifier (2.5.4.97)	VATBA-PIB (Порески идентификациони број ПИБ правног лица)
	organizationName (O)	Пуни регистровани скраћени назив правне особе или назив правне особе ако скраћени назив није регистрован
	localityName (L)	Мјесто сједишта правног лица
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
		keyEncipherment	Укључен <i>keyEncipherment</i> бит
extKeyUsage	НЕ	serverAuth	1.3.6.1.5.5.7.3.1
		clientAuth	1.3.6.1.5.5.7.3.2
certificatePolicies	НЕ	policyIdentifier	UIO 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	НЕ	dnsName	Пуни квалификовани назив послужитеља (FQDN)
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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. УИО АПЛИКАТИВНА ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ ЗА ПРАВНА ЛИЦА (NCP)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Назив апликације или информационог система
	organizationIdentifier (2.5.4.97)	VATVA-PIB (Порески идентификациони број ПИБ правног лица).
	organizationName (O)	Пуни регистровани скраћени назив правне особе или назив правне особе ако скраћени назив није регистрован
	localityName (L)	Мјесто сједишта правног лица
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
		nonRepudiation	Укључен <i>nonRepudiation</i> бит
extKeyUsage	НЕ	emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	НЕ	policyIdentifier	UIO 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	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UIINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UIINOIssuingCA1.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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/UIINOIssuingCA1.cer

## 2.17. УИО ПОТВРДА ЗА КВАЛИФИКОВАНИ ЕЛЕКТРОНСКИ ВРЕМЕНСКИ ЖИГ

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 4 године
Subject	commonName (CN)	UINO Q TSA 2020 <редни број издане потврде>
	organizationIdentifier (2.5.4.97)	VATBA-PIB UIO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Banja Luka
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ дужине 3072 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
		nonRepudiation	Укључен <i>nonRepudiation</i> бит
privateKeyUsage Period	НЕ	notBefore	Вријеме издавања потврде
		notAfter	Вријеме издавања потврде + 1 година
extKeyUsage	ДА	timeStamping	OID: 1.3.6.1.5.5.7.3.8
certificatePolicies	НЕ	policyIdentifier	UIO 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	НЕ	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/pds/PDS-bs.pdf, bs http://ca.uino.gov.ba/pds/PDS-sr.pdf, sr http://ca.uino.gov.ba/pds/PDS-hr.pdf, hr http://ca.uino.gov.ba/pds/PDS-en.pdf, en
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.2
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UIINOIssuingCA1.crl [2] URI: http://cdp.uinoca.ba/CRL/UIINOIssuingCA1.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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/UIINOIssuingCA1.cer

## 2.18. УИО ПОТВРДА ЗА ПОТПИС ОДГОВОРА OCSP СЕРВИСА ЗА UINO ISSUING CA1

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 12 мјесеци
Subject	commonName (CN)	UINO Issuing CA1 OCSP
	organizationIdentifier (2.5.4.97)	VATBA-PIB UIO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Banja Luka
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
		nonRepudiation	Укључен <i>nonRepudiation</i> бит
extKeyUsage	НЕ	ocspSigning	OID: 1.3.6.1.5.5.7.3.9
ocsp-nocheck	НЕ		OID: 1.3.6.1.5.5.7.48.1.5
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.2.1.16.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: <a href="http://ca.uino.gov.ba/bs/dokumenti">http://ca.uino.gov.ba/bs/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/sr/dokumenti">http://ca.uino.gov.ba/sr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/hr/dokumenti">http://ca.uino.gov.ba/hr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/en/documents">http://ca.uino.gov.ba/en/documents</a>
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: <a href="http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl">http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl</a> [2] URI: <a href="http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl">http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl</a>
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: <a href="http://ocsp.uino.gov.ba">http://ocsp.uino.gov.ba</a>
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: <a href="http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer">http://cdp.uino.gov.ba/AIA/UINOIssuingCA1.cer</a>

## 2.19. УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ЗАПОСЛЕНЕ (QSP-n-qscd)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	CA:BA-JIP, гдје је JIP (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификационој исправи
	organizationIdentifier (2.5.4.97)	VATBA-PIB UIO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Мјесто сједишта УИО или регионалног центра.
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	nonRepudiation	Укључен nonRepudiation бит
certificatePolicies	НЕ	policyIdentifier	UIO 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	НЕ	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/pds/PDS-bs.pdf, bs http://ca.uino.gov.ba/pds/PDS-sr.pdf, sr http://ca.uino.gov.ba/pds/PDS-hr.pdf, hr http://ca.uino.gov.ba/pds/PDS-en.pdf, en
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	НЕ	rfc822Name	Опционално. Садржи e-mail адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UIINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UIINOIssuingCA2.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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/UIINOIssuingCA2.cer



## 2.20. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ ЗА ЗАПОСЛЕНЕ (NCP+)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivaње
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	CA:BA-JIP, гдје је JIP (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификационој исправи
	organizationIdentifier (2.5.4.97)	VATBA-PIB UIO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Мјесто сједишта УИО или регионалног центра.
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	Digital Signature	Укључен <i>digitalSignature</i> бит
		keyEncipherment	Укључен <i>keyEncipherment</i> бит
extKeyUsage	НЕ	clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.2.2.11.2.1 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	ncplus (2), OID: 0.4.0.2042.1.2
subjectAltName	НЕ	rfc822Name	Опционално. Садржи е-mail адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UIINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UIINOIssuingCA2.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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/UIINOIssuingCA2.cer

**2.21. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И АУТЕНТИФИКАЦИЈУ ЗА ЗАПОСЛЕНЕ (NCP+)**

**ОСНОВНА ПОЉА**

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	CA:BA-JIP, гдје је JIP (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификационој исправи
	organizationIdentifier (2.5.4.97)	VATBA-PIB UIO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Мјесто сједишта УИО или регионалног центра.
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2014 бита

**EKSTENZIJE**

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	ДА	Digital Signature	Укључен <i>digitalSignature</i> бит
		keyEncipherment	Укључен <i>keyEncipherment</i> бит
extKeyUsage	НЕ	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	НЕ	policyIdentifier	UIO 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	ncrplus (2), OID: 0.4.0.2042.1.2
subjectAltName	НЕ	rfc822Name	Опционално. Садржи е-маил адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UIINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UIINOIssuingCA2.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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/UIINOIssuingCA2.cer

## 2.22. УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И ДОМЕНСКУ АУТЕНТИФИКАЦИЈУ ЗА ЗАПОСЛЕНЕ (NCP+)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	СА:ВА-ЈИР, гдје је ЈИР (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname (SN)	Презиме потписника како је наведено у идентификационој исправи
	organizationIdentifier (2.5.4.97)	VATBA-PIB UIO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Мјесто сједишта УИО или регионалног центра.
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	ДА	Digital Signature	Укључен <i>digitalSignature</i> бит
		NonRepudiation	Укључен <i>NonRepudiation</i> бит
		keyEncipherment	Укључен <i>keyEncipherment</i> бит
extKeyUsage	НЕ	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	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.2.2.11.4.1 policyQualifierId: id-qt-cps { id-qt 1 }
		policyQualifiers	CPS uri: <a href="http://ca.uino.gov.ba/bs/dokumenti">http://ca.uino.gov.ba/bs/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/sr/dokumenti">http://ca.uino.gov.ba/sr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/hr/dokumenti">http://ca.uino.gov.ba/hr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/en/documents">http://ca.uino.gov.ba/en/documents</a>
		policyIdentifier	ncplus (2), OID: 0.4.0.2042.1.2
subjectAltName	НЕ	rfc822Name	Садржи <i>e-mail</i> адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: <a href="http://cdp.uino.gov.ba/CRL/UIINOIssuingCA2.crl">http://cdp.uino.gov.ba/CRL/UIINOIssuingCA2.crl</a> [2] URI: <a href="http://cdp.uinoca.ba/CRL/UIINOIssuingCA2.crl">http://cdp.uinoca.ba/CRL/UIINOIssuingCA2.crl</a>
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: <a href="http://ocsp.uino.gov.ba">http://ocsp.uino.gov.ba</a>
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: <a href="http://cdp.uino.gov.ba/AIA/UIINOIssuingCA2.cer">http://cdp.uino.gov.ba/AIA/UIINOIssuingCA2.cer</a>

## 2.23. УИО ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ И АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ PKCS #12 ФОРМАТА (NCP)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivaње
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 60 мјесеци
Subject	commonName (CN)	Име и презиме потписника како је наведено у идентификационој исправи
	serialNumber	CA:BA-JIP, гдје је JIP (Јединствени идентификатор потврде) псеудослучајно генерисан број
	givenName	Име потписника како је наведено у идентификационој исправи
	surname(SN)	Презиме потписника како је наведено у идентификационој исправи
	organizationIdentifier (2.5.4.97)	VATBA-PIB UIO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivaње
	localityName (L)	Мјесто сједишта УИО или регионалног центра.
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	Digital Signature	Укључен <i>digitalSignature</i> бит
		keyEncipherment	Укључен <i>keyEncipherment</i> бит
extKeyUsage	НЕ	clientAuth	OID: 1.3.6.1.5.5.7.3.2
		emailProtection	OID: 1.3.6.1.5.5.7.3.4
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.2.2.11.5.0 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	nep (1), OID: 0.4.0.2042.1.1
subjectAltName	НЕ	rfc822Name	Опционално. Садржи <i>e-mail</i> адресу потписника.
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UIINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UIINOIssuingCA2.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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/UIINOIssuingCA2.cer

## 2.24. УИО ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ МРЕЖНИХ СТРАНИЦА (SSL)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	<i>Sha512RSA</i>
signatureValue		<i>Sha512</i>
Issuer	commonName (CN)	<i>UINO Issuing CA2</i>
	organizationName (O)	<i>Uprava za indirektno-neizravno oporezivaње</i>
	countryName (C)	<i>BA</i>
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 2 године
Subject	commonName (CN)	Само један пуни квалификовани назив послужитеља ( <i>FQDN</i> )
	organizationIdentifier (2.5.4.97)	<i>VATBA-PIB UIO VATBA-4401711930000</i>
	organizationName (O)	<i>Uprava za indirektno-neizravno oporezivanje</i>
	localityName (L)	Мјесто сједишта УИО или регионалног центра.
	countryName (C)	<i>BA</i>
subjectPublic KeyInfo	AlgorithmIdentifier	<i>rsaEncryption</i>
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
		keyEncipherment	Укључен <i>keyEncipherment</i> бит
extKeyUsage	НЕ	serverAuth	1.3.6.1.5.5.7.3.1
		clientAuth	1.3.6.1.5.5.7.3.2
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.2.2.13.1.0
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: <a href="http://ca.uino.gov.ba/bs/dokumenti">http://ca.uino.gov.ba/bs/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/sr/dokumenti">http://ca.uino.gov.ba/sr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/hr/dokumenti">http://ca.uino.gov.ba/hr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/en/documents">http://ca.uino.gov.ba/en/documents</a>
subjectAltName	НЕ	dnsName	Пуни квалификовани назив ( <i>FQDN</i> )
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: <a href="http://cdp.uino.gov.ba/CRL/UIINOIssuingCA2.crl">http://cdp.uino.gov.ba/CRL/UIINOIssuingCA2.crl</a> [2] URI: <a href="http://cdp.uinoca.ba/CRL/UIINOIssuingCA2.crl">http://cdp.uinoca.ba/CRL/UIINOIssuingCA2.crl</a>
AuthorityKeyIdentifier	НЕ	keyIdentifier	<i>SHA-1</i> сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	<i>SHA-1</i> сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: <a href="http://ocsp.uino.gov.ba">http://ocsp.uino.gov.ba</a>
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: <a href="http://cdp.uino.gov.ba/AIA/UIINOIssuingCA2.cer">http://cdp.uino.gov.ba/AIA/UIINOIssuingCA2.cer</a>

## 2.25. УИО КЕРБЕРОС ПОТВРДА ЗА ДОМЕН КОНТРОЛЕР (ДОМЕН КОНТРОЛЕР KDC)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 2 године
Subject	commonName (CN)	Само један пуни квалификовани назив послужитеља (FQDN)
	organizationIdentifier (2.5.4.97)	VATBA-PIB UIO VATBA-4401711930000
	organizationName (O)	Пуни регистровани скраћени назив правне особе или назив правне особе ако скраћени назив није регистрован (УИО)
	localityName (L)	Мјесто сједишта УИО или регионалног центра
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	ДА	digitalSignature	Укључен digitalSignature бит
		keyEncipherment	Укључен keyEncipherment бит
	НЕ	serverAuth	1.3.6.1.5.5.7.3.1
		clientAuth	1.3.6.1.5.5.7.3.2
extKeyUsage	НЕ	Smart card logon	1.3.6.1.4.1.311.20.2.2
		keyPurposeKdc	1.3.6.1.5.2.3.5
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.2.2.13.10.0 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
subjectAltName	НЕ	dnsName	Пуни квалификовани назив послужитеља (FQDN)
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UIINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UIINOIssuingCA2.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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/UIINOIssuingCA2.cer

## 2.26. УИО АПЛИКАТИВНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ PKCS #12 ФОРМАТА (NCP)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 24 мјесеца
Subject	commonName (CN)	Назив апликације, софтверског модула или информационог система
	organizationIdentifier (2.5.4.97)	VATBA-PIB UIO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Мјесто сједишта УИО или регионалног центра.
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

### ЕКСТЕНЗИЈЕ

ПОЉЕ	КРИТИЧНО	АТРИБУТ	ВРИЈЕДНОСТ
KeyUsage	ДА	Digital Signature	Укључен <i>digitalSignature</i> бит
		keyEncipherment	Укључен <i>keyEncipherment</i> бит
extKeyUsage	НЕ	clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	НЕ	policyIdentifier	UIO 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	nsp (1), OID: 0.4.0.2042.1.1
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UIINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UIINOIssuingCA2.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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/UIINOIssuingCA2.cer

## 2.27. УИО ПОТВРДА ЗА ВРЕМЕНСКИ ЖИГ

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivaње
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 4 године
Subject	commonName (CN)	UINO TSA 2020 <редни број издане потврде >
	organizationIdentifier (2.5.4.97)	VATBA-PIB UIO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Вања Лука
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 3072 бита

### ЕКСТЕНЗИЈЕ

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
		nonRepudiation	Укључен <i>nonRepudiation</i> бит
privateKeyUsage Period	НЕ	notBefore	Вријеме издавања потврде
		notAfter	Вријеме издавања потврде + 1 година
extKeyUsage	ДА	timeStamping	OID: 1.3.6.1.5.5.7.3.8
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.2.2.15.1.1
		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
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UIINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UIINOIssuingCA2.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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/UIINOIssuingCA2.cer



2.28. УИО ПОТВРДА ЗА ПОТПИС ОДГОВОРА *OCSP* СЕРВИСА ЗА *UINO ISSUING CA2*

ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	<i>Sha512RSA</i>
signatureValue		<i>Sha512</i>
Issuer	commonName (CN)	<i>UINO Issuing CA2</i>
	organizationName (O)	<i>Uprava za indirektno-neizravno oporezivaње</i>
	countryName (C)	<i>BA</i>
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 12 мјесеци
Subject	commonName (CN)	<i>UINO Issuing CA2 OCSP</i>
	organizationIdentifier (2.5.4.97)	<i>VATBA-PIB UIO VATBA-4401711930000</i>
	organizationName (O)	<i>Uprava za indirektno-neizravno oporezivaње</i>
	localityName (L)	<i>Вања Лука</i>
	countryName (C)	<i>BA</i>
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ субјекта дужине 2048 бита

ЕКСТЕНЗИЈЕ

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
		nonRepudiation	Укључен <i>nonRepudiation</i> бит
extKeyUsage	НЕ	ocspSigning	OID: 1.3.6.1.5.5.7.3.9
ocsp-nocheck	НЕ		OID: 1.3.6.1.5.5.7.48.1.5
certificatePolicies	НЕ	policyIdentifier	UIO OID: 1.3.6.1.4.1.46134.10.2.2.16.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } CPS uri: <a href="http://ca.uino.gov.ba/bs/dokumenti">http://ca.uino.gov.ba/bs/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/sr/dokumenti">http://ca.uino.gov.ba/sr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/hr/dokumenti">http://ca.uino.gov.ba/hr/dokumenti</a> CPS uri: <a href="http://ca.uino.gov.ba/en/documents">http://ca.uino.gov.ba/en/documents</a>
CRLDistributionPoints	НЕ	DistributionPoint	[1] URI: <a href="http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl">http://cdp.uino.gov.ba/CRL/UINOIssuingCA1.crl</a> [2] URI: <a href="http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl">http://cdp.uinoca.ba/CRL/UINOIssuingCA1.crl</a>
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: <a href="http://ocsp.uino.gov.ba">http://ocsp.uino.gov.ba</a>
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: <a href="http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer">http://cdp.uino.gov.ba/AIA/UINOIssuingCA2.cer</a>

## 2.29. УИО ПОТВРДА ЗА ПОТПИСИВАЊЕ КОДА (NCP+)

### ОСНОВНА ПОЉА

ПОЉЕ	АТРИБУТ	ВРИЈЕДНОСТ
Version	Version	V3, вриједност="2"
serialNumber	CertificateSerialNumber	95 бита ентропије, што је 20 бајтова
signatureAlgorithm	AlgorithmIdentifier	Sha512RSA
signatureValue		Sha512
Issuer	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 36 мјесеци
Subject	commonName (CN)	Uprava za indirektno-neizravno oporezivanje
	organizationIdentifier (2.5.4.97)	VATBA-PIB UIO VATBA-4401711930000
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	localityName (L)	Вања Лука
	countryName (C)	BA
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption
	subjectPublicKey	Јавни кључ дужине 3072 бита

### ЕКСТЕНЗИЈЕ

POLJE	KRITIČNO	ATRIBUT	VRIJEDNOST
KeyUsage	ДА	digitalSignature	Укључен <i>digitalSignature</i> бит
extKeyUsage	НЕ	codeSigning	OID: 1.3.6.1.5.5.7.3.3
certificatePolicies	НЕ	policyIdentifier	UIO 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	НЕ	DistributionPoint	[1] URI: http://cdp.uino.gov.ba/CRL/UINOIssuingCA2.crl [2] URI: http://cdp.uinoca.ba/CRL/UINOIssuingCA2.crl
AuthorityKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
SubjectKeyIdentifier	НЕ	keyIdentifier	SHA-1 сажетак дужине 160 бита
BasicConstraints	НЕ		CA=FALSE pathLenConstraint=None
Authority Information Access	НЕ	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