

FINA
PROFILI CERTIFIKATA ZA Demo FINA PKI ECC

Verzija 1.0

Povijest izmjena

Verzija	Datum	Razlog izmjene
1.0	26.05.2026.	Inicijalna verzija

SADRŽAJ

1.	Identifikacija kriptografskih algoritama i pripadajućih ključeva	4
2.	Profili certifikata	5
2.1.	Fina Demo Root CA G2 certifikat.....	5
2.2.	Demo certifikat za potpis odgovora OCSP servisa za Fina Demo Root CA G2.....	6
2.3.	Fina Demo Q-CA 2024 certifikat	7
2.4.	Demo certifikat za potpis odgovora OCSP servisa za Fina Demo Q-CA 2024	8
2.5.	Demo certifikat za kvalificirani elektronički vremenski žig	9
2.6.	Demo osobni EU kvalificirani certifikat za e-potpis (QCP-n-qscd).....	10
2.7.	Demo osobni EU kvalificirani certifikat za e-potpis (QCP-n).....	11
2.8.	Demo osobni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n-qscd)	12
2.9.	Demo osobni EU kvalificirani certifikat za automatizirani udaljeni e-potpis (QCP-n-qscd)....	13
2.10.	Demo poslovni EU kvalificirani certifikat za e-potpis (QCP-n-qscd)	14
2.11.	Demo poslovni EU kvalificirani certifikat za e-potpis (QCP-n).....	15
2.12.	Demo poslovni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n-qscd).....	16
2.13.	Demo poslovni EU kvalificirani certifikat za automatizirani udaljeni e-potpis (QCP-n-qscd) .	17
2.14.	Demo EU kvalificirani certifikat za e-pečat (QCP-l-qscd)	18
2.15.	Demo EU kvalificirani PSD2 certifikat za e-pečat (QCP-l).....	19
2.16.	Demo EU kvalificirani certifikat za udaljeni e-pečat (QCP-l-qscd).....	20
2.17.	Demo EU kvalificirani soft certifikat za e-pečat (QCP-l)	21
2.18.	Fina Demo Ad-CA 2024 certifikat	22
2.19.	Demo certifikat za potpis odgovora OCSP servisa za Fina Demo Ad-CA 2024.....	23
2.20.	Demo osobni autentikacijski certifikat (NCP+)	24
2.21.	Demo osobni udaljeni certifikat (NCP+).....	25
2.22.	Demo osobni soft certifikat (NCP).....	26
2.23.	Demo osobni udaljeni certifikat (LCP).....	27
2.24.	Demo poslovni autentikacijski certifikat (NCP+)	28
2.25.	Demo poslovni udaljeni certifikat (NCP+)	29
2.26.	Demo poslovni soft certifikat (NCP)	30
2.27.	Demo poslovni soft certifikat (LCP).....	31
2.28.	Demo aplikacijski certifikat razine 1 (NCP).....	32
2.29.	Demo aplikacijski certifikat razine 2 (NCP).....	33
2.30.	Demo aplikacijski certifikat razine 2 (NCP+)	34
2.31.	Demo aplikacijski certifikat razine 3 (NCP+).....	35
2.32.	Demo certifikat za e-pečat Trusted liste (NCP+)	36
2.33.	Demo administrativni certifikat (NCP+).....	37
2.34.	Fina Demo Root CA G2 TLS	38
2.35.	Demo certifikat za potpis odgovora OCSP servisa za Fina Demo Root CA G2 TLS	39
2.36.	Fina Demo TLS CA 2024	40
2.37.	Demo certifikat za potpis odgovora OCSP servisa za Fina Demo TLS CA 2024.....	41
2.38.	Demo EU QWAC certifikat (QCP-w).....	42
2.39.	Demo EU PSD2 QWAC certifikat (QCP-w-psd2)	43
2.40.	Demo SSL certifikat razine 2 (OVCP).....	45
3.	Profil CRL	46
4.	Profil OCSP odgovora	47
4.1.	Profil OCSP odgovora za certifikate koje izdaju Fina Demo Root CA G2, Fina Demo Q-CA 2024 i Fina Demo Ad-CA 2024	47
4.2.	Profil OCSP odgovora za certifikate koje izdaju Fina Demo Root CA G2 TLS i Fina Demo TLS CA 2024.....	48
5.	Profil Demo kvalificiranog elektroničkog vremenskog žiga	49

1. Identifikacija kriptografskih algoritama i pripadajućih ključeva

U sljedećoj tablici prikazani su nazivi kriptografskih algoritama i pripadajućih ključeva zajedno s OID-om koji ih jednoznačno identificira. U tablicama opisa profila certifikata u ovom su dokumentu korištene oznake koje se upotrebljavaju u dokumentu ETSI TS 119 312.

OID	ETSI	Microsoft	ASN.1 Editor	Dodatno	Značenje
2.16.840.1.101.3.4.2.1	SHA-256	sha256	sha256		Hash funkcija
2.16.840.1.101.3.4.2.2	SHA-384	sha384	sha384		Hash funkcija
2.16.840.1.101.3.4.2.3	SHA-512	sha512	sha512		Hash funkcija
1.2.840.10045.4.3.2	ecdsa-with-SHA256	sha256ECDSA	sha256ECDSA		ECDSA poezan s SHA256
1.2.840.10045.4.3.3	ecdsa-with-SHA384	sha384ECDSA	sha384ECDSA		ECDSA poezan s SHA384
1.2.840.10045.3.1.7	P-256	ECDSA P256	ECDSA P256	secp256r1	NIST EC sa 256 bita
1.3.132.0.34	P-384	ECDSA P384	ECDSA P384	secp384r1	NIST EC sa 384 bita
1.3.132.0.35	P-521	ECDSA P521	ECDSA P521	ansip521r1	NIST EC sa 521 bita
1.2.840.10045.2.1	id-ecPublicKey	ECC	ECC	-	EC javni ključ

Tablica 1. OID-ovi kriptografskih algoritama i duljine ključeva

2. Profili certifikata

2.1. Fina Demo Root CA G2 certifikat

Osnovna polja		
Polje	Atribut	Vrijednost
Version	Version	X.509 v3, (vrijednost="2")
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384
signatureValue		Potpis izdavatelja certifikata
Issuer	commonName	Fina Demo Root CA G2
	organizationIdentifier	VATHR-85821130368
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + 25 godina
Subject	commonName	Fina Demo Root CA G2
	organizationIdentifier	VATHR-85821130368
	organizationName	Financijska agencija
	countryName	HR
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey
	subjectPublicKey	P-384
Ekstenzije		
Polje	Kritično	Vrijednost
KeyUsage	DA	KeyCertSign, cRLSign
BasicConstraints	DA	cA=true pathLenConstraint=None
AuthorityKeyIdentifier	NE	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	Vrijednost duljine 160 bita

Tablica 2. Osnovna polja i ekstenzije profila Fina Demo Root CA G2 certifikata

2.2. Demo certifikat za potpis odgovora OCSP servisa za Fina Demo Root CA G2

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, (vrijednost="2")
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue	Potpis izdavatelja certifikata		
Issuer	commonName (CN)	Fina Demo Root CA G2	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 13 mjeseci	
Subject	commonName (CN)	Fina Demo Root G2 OCSP	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-384	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
extKeyUsage	NE	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9 (<i>id-kp-OCSPSigning</i>)
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5 (<i>id-pkix-ocsp-nocheck</i>)
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	DA		cA=FALSE pathLenConstraint=None

Tablica 3. Osnovna polja i ekstenzije profila Certifikata za potpis odgovora OCSP servisa za Fina Demo Root CA G2

2.3. Fina Demo Q-CA 2024 certifikat

Osnovna polja			
Polje	Atribut	Vrijednost	
Version	Version	X.509 v3, (vrijednost="2")	
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta	
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384	
signatureValue		Potpis izdavatelja certifikata	
Issuer	commonName	Fina Demo Root CA G2	
	organizationIdentifier	VATHR-85821130368	
	organizationName	Financijska agencija	
	countryName	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 17 godina.	
Subject	commonName	Fina Demo Q-CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName	Financijska agencija	
	countryName	HR	
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-384	
Ekstenzije			
Polje	Kritično	Vrijednost	
KeyUsage	DA	KeyCertSign, cRLSign	
BasicConstraints	DA	cA=true pathLenConstraint=None	
AuthorityKeyIdentifier	NE	Vrijednost duljine 160 bita	
SubjectKeyIdentifier	NE	Vrijednost duljine 160 bita	
certificatePolicies	NE	policyIdentifier	All issuance policies (Any policy – OID: 2.5.29.32.0) policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyQualifiers	
Authority Information Access	NE	id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoRootCAG2.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoRootCAG2.crl

Tablica 4. Osnovna polja i ekstenzije profila Fina Demo Q-CA 2024 certifikata

2.4. Demo certifikat za potpis odgovora OCSP servisa za Fina Demo Q-CA 2024

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdatelja certifikata
Issuer	commonName (CN)		Fina Demo Q-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 13 mjeseci
Subject	commonName (CN)		Fina Demo Q 2024 OCSP
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
extKeyUsage	NE	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9 (<i>id-kp-OCSPSigning</i>)
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5 (<i>id-pkix-ocsp-nocheck</i>)
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	DA		cA=FALSE pathLenConstraint=None

Tablica 5. Osnovna polja i ekstenzije profila Demo certifikata za potpis odgovora OCSP servisa za Fina Demo Q-CA 2024

2.5. Demo certifikat za kvalificirani elektronički vremenski žig

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue	Potpis izdavatelja certifikata		
Issuer	commonName (CN)		Fina Demo Q-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 61 mjesec
Subject	commonName (CN)		Fina Demo QTSA 2024 <redni broj izdanog certifikata>
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		nonRepudiation	Uključen nonRepudiation bit
privateKeyUsage Period	NE	notBefore	Vrijeme izdavanja certifikata
		notAfter	Vrijeme izdavanja certifikata + 13 mjeseci (od toga je 1 mjesec <i>grace period</i>)
extKeyUsage	DA	timeStamping	OID: 1.3.6.1.5.5.7.3.8
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
qCStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 https://demo-pki.fina.hr/pds/PDSqts-en.pdf , en https://demo-pki.fina.hr/pds/PDSqts-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.2
CRLDistributionPoints	NE	DistributionPoint	[1]URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoRootCAG2.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 6. Osnovna polja i ekstenzije profila Demo certifikata za kvalificirani elektronički vremenski žig

2.6. Demo osobni EU kvalificirani certifikat za e-potpis (QCP-n-qscd)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue	Potpis izdatelja certifikata		
Issuer	commonName (CN)		Fina Demo Q-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 37 mjeseci
Subject	serialNumber		HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=32
	commonName (CN)		Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	givenName		Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)		Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationName (O)		OSOBNI
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-256
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.11.8.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		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 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoQCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 7. Osnovna polja i ekstenzije profila Demo osobnog EU kvalificiranog certifikata za e-potpis (QCP-n-qscd)

2.7. Demo osobni EU kvalificirani certifikat za e-potpis (QCP-n)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue	Potpis izdavatelja certifikata		
Issuer	commonName (CN)		Fina Demo Q-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 37 mjeseci
Subject	serialNumber		HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=23
	commonName (CN)		Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	givenName		Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)		Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationName (O)		OSOBNI
	countryName (C)		Dvoslovni ISO kod države izdavatelja identifikacijske isprave potpisnika.
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-256
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.11.2.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	qcp-natural (0), OID: 0.4.0.194112.1.0
qcStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoQCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 8. Osnovna polja i ekstenzije profila Demo osobnog EU kvalificiranog certifikata za e-potpis (QCP-n)

2.8. Demo osobni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n-qscd)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdavatelja certifikata
Issuer	commonName (CN)		Fina Demo Q-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 37 mjeseci
Subject	serialNumber		HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=47
	commonName (CN)		Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	givenName		Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)		Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationName (O)		OSOBNi
	countryName (C)		Dvoslovni ISO kod države izdavatelja identifikacijske isprave potpisnika.
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.11.7.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		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 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoQCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 9. Osnovna polja i ekstenzije profila Demo osobnog EU kvalificiranog certifikata za udaljeni e-potpis (QCP-n-qscd)

	Profili certifikata za Demo Fina PKI ECC	klasifikacija:	
		strana:	13/49

2.9. Demo osobni EU kvalificirani certifikat za automatizirani udaljeni e-potpis (QCP-n-qscd)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdavatelja certifikata
Issuer	commonName (CN)		Fina Demo Q-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 37 mjeseci
Subject	serialNumber		HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=50
	commonName (CN)		Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	givenName		Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)		Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationName (O)		OSOBNI
	countryName (C)		Dvoslovni ISO kod države izdavatelja identifikacijske isprave potpisnika.
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.11.7.12
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	qcp-natural (0), OID: 0.4.0.194112.1.0
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 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoQCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 10. Osnovna polja i ekstenzije profila Demo osobnog EU kvalificiranog certifikata za automatizirani udaljeni e-potpis (QCP-n-qscd)

2.10. Demo poslovni EU kvalificirani certifikat za e-potpis (QCP-n-qscd)

Osnovna polja			
Polje	Atribut	Vrijednost	
Version	Version	X.509 v3, vrijednost="2"	
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta	
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384	
signatureValue		Potpis izdatelja certifikata	
Issuer	commonName (CN)	Fina Demo Q-CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 37 mjeseci	
Subject	serialNumber	HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=34	
	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi	
	givenName	Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	surname (SN)	Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	organizationalUnit (OU)	Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 2. razine.	
	organizationalUnit (OU)	Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 1. razine.	
	organizationIdentifier	Dvoslovni ISO kod države registracije poslovnog subjekta te jedanaesteroznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj i za TDU: HR<OIB_vrijednost>. Za ostale poslovne subjekte jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.	
organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili TDU, ili naziv poslovnog subjekta ili TDU ako skraćeni naziv nije registriran.		
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-256	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.12.8.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		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 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoint	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoQCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 11. Osnovna polja i ekstenzije profila Demo poslovnog EU kvalificiranog certifikata za e-potpis (QCP-n-qscd)

2.11. Demo poslovni EU kvalificirani certifikat za e-potpis (QCP-n)

Osnovna polja			
Polje	Atribut	Vrijednost	
Version	Version	X.509 v3, vrijednost="2"	
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta	
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384	
signatureValue		Potpis izdavatelja certifikata	
Issuer	commonName (CN)	Fina Demo Q-CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 37 mjeseci	
Subject	serialNumber	HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=25	
	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi	
	givenName	Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	surname (SN)	Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	organizationalUnit (OU)	Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 2. razine.	
	organizationalUnit (OU)	Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 1. razine.	
	organizationIdentifier	Dvoslovni ISO kod države registracije poslovnog subjekta te jedanaesteroznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj i za TDU: HR<OIB_vrijednost>. Za ostale poslovne subjekte jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.	
subjectPublic KeyInfo	organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili TDU, ili naziv poslovnog subjekta ili TDU ako skraćeni naziv nije registriran.	
	countryName (C)	Dvoslovni ISO kod države registracije poslovnog subjekta	
	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-256	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.12.2.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	qcp-natural (0), OID: 0.4.0.194112.1.0
qcStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoQCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 12. Osnovna polja i ekstenzije profila Demo poslovnog EU kvalificiranog certifikata za e-potpis (QCP-n)

	Profili certifikata za Demo Fina PKI ECC	klasifikacija:	
		strana:	16/49

2.12. Demo poslovni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n-qscd)

Osnovna polja			
Polje	Atribut	Vrijednost	
Version	Version	X.509 v3, vrijednost="2"	
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta	
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384	
signatureValue		Potpis izdavatelja certifikata	
Issuer	commonName (CN)	Fina Demo Q-CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 37 mjeseci	
Subject	serialNumber	HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=48	
	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi	
	givenName	Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	surname (SN)	Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	organizationalUnit (OU)	Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 2. razine.	
	organizationalUnit (OU)	Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 1. razine.	
	organizationIdentifier	Dvoslovni ISO kod države registracije poslovnog subjekta te jedanaesteroznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj i za TDU: HR<OIB_vrijednost>. Za ostale poslovne subjekte jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.	
	organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili TDU, ili naziv poslovnog subjekta ili TDU ako skraćeni naziv nije registriran.	
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-384	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.12.7.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		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 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoQCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 13. Osnovna polja i ekstenzije profila Demo poslovnog EU kvalificiranog certifikata za udaljeni e-potpis (QCP-n-qscd)

	Profili certifikata za Demo Fina PKI ECC	klasifikacija:	
		strana:	17/49

2.13. Demo poslovni EU kvalificirani certifikat za automatizirani udaljeni e-potpis (QCP-n-qscd)

Osnovna polja			
Polje	Atribut	Vrijednost	
Version	Version	X.509 v3, vrijednost="2"	
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta	
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384	
signatureValue		Potpis izdavatelja certifikata	
Issuer	commonName (CN)	Fina Demo Q-CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 37 mjeseci	
Subject	serialNumber	HR<O/B_<i>vrijednost</i> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=49	
	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi	
	givenName	Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	surname (SN)	Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	organizationalUnit (OU)	Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 2. razine.	
	organizationalUnit (OU)	Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 1. razine.	
	organizationIdentifier	Dvoslovni ISO kod države registracije poslovnog subjekta te jedanaesteroznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj i za TDU: HR<O/B_<i>vrijednost</i>. Za ostale poslovne subjekte jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.	
	organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili TDU, ili naziv poslovnog subjekta ili TDU ako skraćeni naziv nije registriran.	
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-384	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.12.7.12
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	qcp-natural (0), OID: 0.4.0.194112.1.0
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 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.1
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoQCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 14. Osnovna polja i ekstenzije profila Demo poslovnog EU kvalificiranog certifikata za automatizirani udaljeni e-potpis (QCP-n-qscd)

2.14. Demo EU kvalificirani certifikat za e-pečat (QCP-I-qscd)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdavatelja certifikata
Issuer	commonName (CN)		Fina Demo Q-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 37 mjeseci
Subject	serialNumber		Jedinstveni jedanaesteroznamenasti broj (za pravne osobe kojima je dodijeljen OIB u Republici Hrvatskoj i za TDU: OIB, za ostale pravne osobe jedanaesteroznamenasti broj je jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB), te dva broja W i Z koji predstavljaju Finine interne oznake, Z=36
	commonName (CN)		Naziv kojeg subjekt obično koristi za svoje predstavljanje.
	organizationIdentifier		„VAT“, dvoslovni ISO kod države, "-", VAT broj (OIB za pravne osobe registrirane u Republici Hrvatskoj i za TDU)
	organizationName (O)		Puni registrirani skraćeni naziv pravne osobe ili TDU, ili naziv pravne osobe ili TDU ako skraćeni naziv nije registriran.
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-256
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.13.8.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		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 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.2
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa autora pečata u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoQCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 15. Osnovna polja i ekstenzije profila Demo EU kvalificiranog certifikata za e-pečat (QCP-I-qscd)

2.15. Demo EU kvalificirani PSD2 certifikat za e-pečat (QCP-I)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdavatelja certifikata
Issuer	commonName (CN)		Fina Demo Q-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 37 mjeseci
Subject	serialNumber		OIB koji je u Republici Hrvatskoj dodijeljen pružatelju platnih usluga te dva broja W i Z odijeljena točkama koji predstavljaju Finine interne oznake, Z=39
	commonName (CN)		Naziv kojeg pružatelj platnih usluga obično koristi za svoje predstavljanje.
	organizationIdentifier		Identifikator pružatelja platnih usluga kojeg određuje ili dodjeljuje nadležno tijelo matične države članice EU.
	organizationName (O)		Puni registrirani skraćeni naziv pružatelja platnih usluga ili puni naziv pružatelja platnih usluga ako skraćeni naziv nije registriran.
subjectPublic KeyInfo	countryName (C)		Dvoslovni ISO kod države registracije pravne osobe.
	AlgorithmIdentifier		id-ecPublicKey
subjectPublicKey			P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.13.1.4
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	qcp-legal(1), OID: 0.4.0.194112.1.1
qCStatements	NE	id-qcs-pkixQCSyntax-v2	id-etsi-qcs-SemanticsId-Legal
		esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.2
etsi-psd2-qcStatement	Uloge dodijeljene pružatelju platnih usluga: 0.4.0.19495.1.1 (id-psd2-role-ppsp-as), PSP_AS) i/ili 0.4.0.19495.1.2 (id-psd2-role-ppsp-pi), PSP_PI) i/ili 0.4.0.19495.1.3 (id-psd2-role-ppsp-ai), PSP_AI) i/ili 0.4.0.19495.1.4 (id-psd2-role-ppsp-ic), PSP_IC)} Naziv nadležnog tijela matične države članice: NCAName (UTF8String (SIZE (1..256))) Identifikator nadležnog tijela matične države članice NCAId: dvoslovni ISO kod države, "-", NCA identifikator (2-8 znakova (A-Z)).		
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa autora pečata u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoQCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 16. Osnovna polja i ekstenzije profila Demo EU kvalificiranog PSD2 certifikata za e-pečat (QCP-I)

	Profili certifikata za Demo Fina PKI ECC	klasifikacija:	
		strana:	20/49

2.16. Demo EU kvalificirani certifikat za udaljeni e-pečat (QCP-I-qscd)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdavatelja certifikata
Issuer	commonName (CN)		Fina Demo Q-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 37 mjeseci
Subject	serialNumber		Jedinstveni jedanaesteroznamenasti broj (za pravne osobe kojima je dodijeljen OIB u Republici Hrvatskoj: OIB, za ostale pravne osobe jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB), te dva broja W i Z koji predstavljaju Finine interne oznake, Z=51
	commonName (CN)		Naziv kojeg subjekt obično koristi za svoje predstavljanje.
	organizationIdentifier		„VAT“, dvoslovni ISO kod države, „“, VAT broj (OIB za pravne osobe registrirane u Republici Hrvatskoj ili TDU)
	organizationName (O)		Puni registrirani skraćeni naziv pravne osobe ili TDU, ili naziv pravne osobe ili TDU ako skraćeni naziv nije registriran.
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.13.7.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		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 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.2
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa autora pečata u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoQCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 17. Osnovna polja i ekstenzije profila Demo EU kvalificiranog certifikata za udaljeni e-pečat (QCP-I-qscd)

2.17. Demo EU kvalificirani soft certifikat za e-pečat (QCP-I)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdavatelja certifikata
Issuer	commonName (CN)		Fina Demo Q-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 61 mjesec
Subject	serialNumber		Jedinstveni jedanaesteroznamenasti broj (za pravne osobe kojima je dodijeljen OIB u Republici Hrvatskoj i TDU: OIB, za ostale pravne osobe jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB), te dva broja W i Z koji predstavljaju Finine interne oznake, Z=37
	commonName (CN)		Naziv kojeg subjekt obično koristi za svoje predstavljanje.
	organizationIdentifier		„VAT“, dvoslovni ISO kod države, "-", VAT broj (OIB za pravne osobe registrirane u Republici Hrvatskoj)
	organizationName (O)		Puni registrirani skraćeni naziv pravne osobe ili TDU, ili naziv pravne osobe ili TDU ako skraćeni naziv nije registriran.
	countryName (C)		Dvoslovni ISO kod države registracije pravne osobe.
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.701.13.1.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	qcp-legal (1), OID: 0.4.0.194112.1.1
qCStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.2
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa autora pečata u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoQCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoQCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 18. Osnovna polja i ekstenzije profila Demo EU kvalificiranog soft certifikata za e-pečat (QCP-I)

2.18. Fina Demo Ad-CA 2024 certifikat

Osnovna polja			
Polje	Atribut	Vrijednost	
Version	Version	X.509 v3, (vrijednost="2")	
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta	
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384	
signatureValue		Potpis izdavatelja certifikata	
Issuer	commonName	Fina Demo Root CA G2	
	organizationIdentifier	VATHR-85821130368	
	organizationName	Financijska agencija	
	countryName	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 17 godina.	
Subject	commonName	Fina Demo Ad-CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName	Financijska agencija	
	countryName	HR	
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-384	
Ekstenzije			
Polje	Kritično	Vrijednost	
KeyUsage	DA	KeyCertSign, cRLSign	
BasicConstraints	DA	cA=true pathLenConstraint=None	
AuthorityKeyIdentifier	NE	Vrijednost duljine 160 bita	
SubjectKeyIdentifier	NE	Vrijednost duljine 160 bita	
certificatePolicies	NE	policyIdentifier	All issuance policies (Any policy – OID: 2.5.29.32.0)
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
Authority Information Access	NE	id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoRootCAG2.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoRootCAG2.crl

Tablica 19. Osnovna polja i ekstenzije profila Fina Demo Ad-CA 2024 certifikata

2.19. Demo certifikat za potpis odgovora OCSP servisa za Fina Demo Ad-CA 2024

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdatelja certifikata
Issuer	commonName (CN)		Fina Demo Ad-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 13 mjeseci
Subject	commonName (CN)		Fina Demo Ad 2024 OCSP
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
extKeyUsage	NE	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9 (<i>id-kp-OCSPSigning</i>)
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5 (<i>id-pkix-ocsp-nocheck</i>)
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	DA		cA=FALSE pathLenConstraint=None

Tablica 20. Osnovna polja i ekstenzije profila Demo Certifikata za potpis odgovora OCSP servisa za Fina Demo Ad-CA 2024

2.20. Demo osobni autentikacijski certifikat (NCP+)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdavatelja certifikata
Issuer	commonName (CN)		Fina Demo Ad-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 37 mjeseci
Subject	serialNumber		HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaestoznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=22
	commonName (CN)		Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	givenName		Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)		Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationName (O)		OSOBNI
	countryName (C)		Dvoslovni ISO kod države izdavatelja identifikacijske isprave potpisnika.
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-256
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.11.4.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	ncplusplus (2), OID: 0.4.0.2042.1.2
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 21. Osnovna polja i ekstenzije profila Demo osobnog autentikacijskog certifikata (NCP+)

2.21. Demo osobni udaljeni certifikat (NCP+)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue	Potpis izdavatelja certifikata		
Issuer	commonName (CN)	Fina Demo Ad-CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 37 mjeseci	
Subject	serialNumber	HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=42	
	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi	
	givenName	Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	surname (SN)	Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	organizationName (O)	OSOBNi	
	countryName (C)	Dvoslovni ISO kod države izdavatelja identifikacijske isprave potpisnika.	
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-384	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.11.10.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	nccplus (2) OID: 0.4.0.2042.1.2
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 22. Osnovna polja i ekstenzije profila Demo osobnog udaljenog certifikata (NCP+)

2.22. Demo osobni soft certifikat (NCP)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdatelja certifikata
Issuer	commonName (CN)		Fina Demo Ad-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 61 mjeseci
Subject	serialNumber		HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=29
	commonName (CN)		Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	givenName		Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)		Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationName (O)		OSOBNi
	countryName (C)		Dvoslovni ISO kod države izdatelja identifikacijske isprave potpisnika.
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.11.3.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	ncp (1), OID: 0.4.0.2042.1.1
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 23. Osnovna polja i ekstenzije profila Demo osobnog soft certifikata (NCP)

2.23. Demo osobni udaljeni certifikat (LCP)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdavatelja certifikata
Issuer	commonName (CN)		Fina Demo Ad-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 61 mjeseci
Subject	serialNumber		HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=44
	commonName (CN)		Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	givenName		Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)		Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationName (O)		OSOBNi
	countryName (C)		Dvoslovni ISO kod države izdavatelja identifikacijske isprave potpisnika.
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.11.9.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	lcp (3), OID: 0.4.0.2042.1.3
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 24. Osnovna polja i ekstenzije profila Demo osobnog udaljenog certifikata (LCP)

2.24. Demo poslovni autentikacijski certifikat (NCP+)

Osnovna polja			
Polje	Atribut	Vrijednost	
Version	Version	X.509 v3, vrijednost="2"	
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta	
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384	
signatureValue		Potpis izdavatelja certifikata	
Issuer	commonName (CN)	Fina Demo Ad-CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 37 mjeseci	
Subject	serialNumber	HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=21	
	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi	
	givenName	Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	surname (SN)	Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	organizationalUnit (OU)	Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 2. razine.	
	organizationalUnit (OU)	Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 1. razine.	
	organizationIdentifier	Dvoslovni ISO kod države registracije poslovnog Subjekta te jedanaesteroznamenasti broj. Za poslovne subjekte i za TDU kojima je dodijeljen OIB u Republici Hrvatskoj: HR<OIB_vrijednost>. Za ostale poslovne subjekte jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.	
organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili TDU, ili naziv poslovnog subjekta ili TDU ako skraćeni naziv nije registriran.		
subjectPublic KeyInfo	countryName (C)	Dvoslovni ISO kod države registracije poslovnog subjekta	
	AlgorithmIdentifier	id-ecPublicKey	
subjectPublicKey		P-256	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.12.4.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	ncplusplus (2), OID: 0.4.0.2042.1.2
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 25. Osnovna polja i ekstenzije profila Demo poslovnog autentikacijskog certifikata (NCP+)

2.25. Demo poslovni udaljeni certifikat (NCP+)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdavatelja certifikata
Issuer	commonName (CN)		Fina Demo Ad-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 37 mjeseci
Subject	serialNumber		HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=41
	commonName (CN)		Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi
	givenName		Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	surname (SN)		Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi
	organizationIdentifier		Dvoslovni ISO kod države registracije poslovnog subjekta te jedanaesteroznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: HR<OIB_vrijednost>. Za ostale poslovne subjekte jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.
	organizationName (O)		Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.
subjectPublic KeyInfo	countryName (C)		Dvoslovni ISO kod države registracije poslovnog subjekta
	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.12.10.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	ncplusplus (2) OID: 0.4.0.2042.1.2
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caissuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 26. Osnovna polja i ekstenzije profila Demo poslovnog udaljenog certifikata (NCP+)

2.26. Demo poslovni soft certifikat (NCP)

Osnovna polja			
Polje	Atribut	Vrijednost	
Version	Version	X.509 v3, vrijednost="2"	
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta	
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384	
signatureValue		Potpis izdavatelja certifikata	
Issuer	commonName (CN)	Fina Demo Ad-CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 61 mjeseci	
Subject	serialNumber	HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=30	
	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi	
	givenName	Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	surname (SN)	Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	organizationIdentifier	Dvoslovni ISO kod države registracije poslovnog subjekta te jedanaesteroznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: HR<OIB_vrijednost>. Za ostale poslovne subjekte jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.	
	organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.	
subjectPublic KeyInfo	countryName (C)	Dvoslovni ISO kod države registracije poslovnog subjekta	
	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-384	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.12.3.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	nep (1), OID: 0.4.0.2042.1.1
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 27. Osnovna polja i ekstenzije profila Demo poslovnog soft certifikata (NCP)

2.27. Demo poslovni soft certifikat (LCP)

Osnovna polja			
Polje	Atribut	Vrijednost	
Version	Version	X.509 v3, vrijednost="2"	
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta	
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384	
signatureValue		Potpis izdavatelja certifikata	
Issuer	commonName (CN)	Fina Demo Ad-CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 61 mjeseci	
Subject	serialNumber	HR<OIB_vrijednost> ili dvoslovni ISO kod države izdavanja identifikacijske isprave potpisnika i jedanaesteroznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=28	
	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi	
	surname (SN)	Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	organizationIdentifier	Dvoslovnii ISO kod države registracije poslovnog subjekta te jedanaesteroznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: HR<OIB_vrijednost>. Za ostale poslovne subjekte jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.	
	organizationName (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.	
	countryName (C)	Dvoslovni ISO kod države registracije poslovnog subjekta.	
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-384	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.12.5.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	lcp (3), OID: 0.4.0.2042.1.3
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 28. Osnovna polja i ekstenzije profila Demo poslovnog soft certifikata (LCP)

2.28. Demo aplikacijski certifikat razine 1 (NCP)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdatelja certifikata
Issuer	commonName (CN)		Fina Demo Ad-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 61 mjeseci
Subject	commonName (CN)		Naziv aplikacije
	organizationIdentifier		Dvoslovni ISO kod države registracije poslovnog subjekta te jedanaesteroznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: HR<OIB_vrijednost>. Za ostale poslovne subjekte jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB. Ovaj atribut se ne primjenjuje u certifikatima koji se izdaju za potrebe fiskalizacije.
	organizationName (O)		Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran. Nakon ovog naziva za certifikate koji se izdaju za potrebe fiskalizacije dodaje se razmak i „HR“ i OIB poslovnog subjekta.
	countryName (C)		Dvoslovni ISO kod države registracije poslovnog subjekta
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa subjekta u rfc822Name.
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.15.3.1
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	nep (1), OID: 0.4.0.2042.1.1
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 29. Osnovna polja i ekstenzije profila Demo aplikacijskog certifikata razine 1 (NCP)

2.29. Demo aplikacijski certifikat razine 2 (NCP)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdatelja certifikata
Issuer	commonName (CN)		Fina Demo Ad-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 37 mjeseci
Subject	commonName (CN)		Naziv aplikacije
	organizationIdentifier		Dvoslovni ISO kod države registracije poslovnog subjekta te jedanaestoznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: HR<OIB_vrijednost>. Za ostale poslovne subjekte jedanaestoznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.
	organizationName (O)		Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.
	countryName (C)		Dvoslovni ISO kod države registracije poslovnog subjekta
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa subjekta u rfc822Name.
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.15.3.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	ncp (1), OID: 0.4.0.2042.1.1
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 30. Osnovna polja i ekstenzije profila Demo aplikacijskog certifikata razine 2 (NCP)

	Profili certifikata za Demo Fina PKI ECC	klasifikacija:	
		strana:	34/49

2.30. Demo aplikacijski certifikat razine 2 (NCP+)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdatelja certifikata
Issuer	commonName (CN)		Fina Demo Ad-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 37 mjeseci
Subject	commonName (CN)		Naziv aplikacije
	organizationIdentifier		Dvoslovni ISO kod države registracije poslovnog subjekta te jedanaesteroznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: HR<OIB_vrijednost>. Za ostale poslovne subjekte jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.
	organizationName (O)		Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.
	countryName (C)		Dvoslovni ISO kod države registracije poslovnog subjekta
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-256
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa subjekta u rfc822Name.
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.15.4.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	ncplusplus (2), OID: 0.4.0.2042.1.2
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 31. Osnovna polja i ekstenzije profila Demo aplikacijskog certifikata razine 2 (NCP+)

2.31. Demo aplikacijski certifikat razine 3 (NCP+)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdatelja certifikata
Issuer	commonName (CN)		Fina Demo Ad-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 13 mjeseci
Subject	commonName (CN)		Naziv aplikacije
	organizationIdentifier		Dvoslovni ISO kod države registracije poslovnog subjekta te jedanaesteroznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: HR<OIB_vrijednost>. Za ostale poslovne subjekte jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.
	organizationName (O)		Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.
	countryName (C)		Dvoslovni ISO kod države registracije poslovnog subjekta
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-384
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa subjekta u rfc822Name.
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.15.4.3
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	ncplusplus (2), OID: 0.4.0.2042.1.2
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 32. Osnovna polja i ekstenzije profila Demo aplikacijskog certifikata razine 3 (NCP+)

2.32. Demo certifikat za e-pečat Trusted liste (NCP+)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue	Potpis izdatelja certifikata		
Issuer	commonName (CN)		Fina Demo Ad-CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata +25 mjeseci
Subject	serialNumber		„P“, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=31
	commonName (CN)		Naziv kojeg određuje središnje tijelo državne uprave nadležno za poslove gospodarstva
	organizationIdentifier		„VATHR-“ OIB središnjeg tijela državne uprave nadležnog za poslove gospodarstva
	organizationName (O)		Naziv središnjeg tijela državne uprave nadležnog za poslove gospodarstva
	countryName (C)		HR
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		P-256
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	nonRepudiation	Uključen nonRepudiation bit
extKeyUsage	NE	id-tsl-kp-tslSigning	OID: 0.4.0.2231.3.0
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.17.4.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	ncplusplus (2), OID: 0.4.0.2042.1.2
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 33. Osnovna polja i ekstenzije profila Demo certifikata za e-pečat Trusted liste (NCP+)

2.33. Demo administrativni certifikat (NCP+)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue	Potpis izdavatelja certifikata		
Issuer	commonName (CN)	Fina Demo Ad-CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 37 mjeseca	
Subject	serialNumber	HR<OIB_vrijednost> te dva broja W i Z koji predstavljaju Finine interne oznake, Z=24	
	commonName (CN)	Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi	
	givenName	Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	surname (SN)	Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi	
	organizationIdentifier	Dvoslovni ISO kod države za Hrvatsku i OIB Fine: HR85821130368	
	organizationName (O)	FINA	
subjectPublic KeyInfo	countryName (C)	HR	
	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-256	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	emailProtection	OID: 1.3.6.1.5.5.7.3.4
		clientAuth	OID: 1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.801.16.4.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	ncpplus (2), OID: 0.4.0.2042.1.2
subjectAltName	NE	rfc822Name	Opcionalno. E-mail adresa potpisnika u rfc822Name.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoAdCA2024.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoAdCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 34. Osnovna polja i ekstenzije profila Demo administrativnog certifikata (NCP+)

2.34. Fina Demo Root CA G2 TLS

Osnovna polja		
Polje	Atribut	Vrijednost
Version	Version	X.509 v3, (vrijednost="2")
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384
signatureValue		Potpis izdavatelja certifikata
Issuer	commonName	Fina Demo Root CA G2 TLS
	organizationIdentifier	VATHR-85821130368
	organizationName	Financijska agencija
	countryName	HR
Validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + 25 godina
Subject	commonName	Fina Demo Root CA G2 TLS
	organizationIdentifier	VATHR-85821130368
	organizationName	Financijska agencija
	countryName	HR
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey
	subjectPublicKey	P-384
Ekstenzije		
Polje	Kritično	Vrijednost
KeyUsage	DA	KeyCertSign, cRLSign
BasicConstraints	DA	cA=true pathLenConstraint=None
AuthorityKeyIdentifier	NE	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	Vrijednost duljine 160 bita

Tablica 35. Osnovna polja i ekstenzije profila Fina Demo Root CA G2 TLS certifikata

	Profili certifikata za Demo Fina PKI ECC	klasifikacija:	
		strana:	39/49

2.35. Demo certifikat za potpis odgovora OCSP servisa za Fina Demo Root CA G2 TLS

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version	X.509 v3, vrijednost="2"	
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta	
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384	
signatureValue	Potpis izdavatelja certifikata		
Issuer	commonName (CN)	Fina Demo Root CA G2 TLS	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 13 mjeseci	
Subject	commonName (CN)	Fina Demo Root G2 TLS OCSP	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-384	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
extKeyUsage	NE	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9 (<i>id-kp-OCSPSigning</i>)
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5 (<i>id-pkix-ocsp-nocheck</i>)
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	DA		cA=FALSE pathLenConstraint=None

Tablica 36. Osnovna polja i ekstenzije profila Certifikata za potpis odgovora OCSP servisa za Fina Demo Root CA G2 TLS

2.36. Fina Demo TLS CA 2024

Osnovna polja			
Polje	Atribut	Vrijednost	
Version	Version	X.509 v3, vrijednost="2"	
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta	
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384	
signatureValue		Potpis izdavatelja certifikata	
Issuer	commonName (CN)	Fina Demo Root CA G2 TLS	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 12 godina.	
Subject	commonName (CN)	Fina Demo TLS CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-384	
Ekstenzije			
Polje	Kritično	Vrijednost	
KeyUsage	DA	KeyCertSign, cRLSign	
extKeyUsage	NE	id-kp-serverAuth (OID: 1.3.6.1.5.5.7.3.1)	
		id-kp-clientAuth (OID: 1.3.6.1.5.5.7.3.2)	
BasicConstraints	DA	cA=true pathLenConstraint=None	
AuthorityKeyIdentifier	NE	Vrijednost duljine 160 bita	
SubjectKeyIdentifier	NE	Vrijednost duljine 160 bita	
certificatePolicies	NE	policyIdentifier	All issuance policies (Any policy – OID: 2.5.29.32.0)
Authority Information Access	NE	id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoRootCAG2TLS.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoRootCAG2TLS.crl

Tablica 37. Osnovna polja i ekstenzije profila Fina Demo TLS CA 2024 certifikata

2.37. Demo certifikat za potpis odgovora OCSP servisa za Fina Demo TLS CA 2024

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue	Potpis izdavatelja certifikata		
Issuer	commonName (CN)	Fina Demo TLS CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 13 mjeseci	
Subject	commonName (CN)	Fina Demo TLS 2024 OCSP	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	P-384	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
extKeyUsage	NE	OCSPSigning	OID: 1.3.6.1.5.5.7.3.9 (<i>id-kp-OCSPSigning</i>)
ocsp-nocheck	NE		OID: 1.3.6.1.5.5.7.48.1.5 (<i>id-pkix-ocsp-nocheck</i>)
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	DA		cA=FALSE pathLenConstraint=None

Tablica 38. Osnovna polja i ekstenzije profila Certifikata za potpis odgovora OCSP servisa za Fina Demo TLS CA 2024

2.38. Demo EU QWAC certifikat (QCP-w)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta.
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue			Potpis izdatelja certifikata
Issuer	commonName (CN)		Fina Demo TLS CA 2024
	organizationIdentifier		VATHR-85821130368
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 6 mjeseci
Subject	commonName (CN)		Samo jedan puni kvalificirani naziv poslužitelja (FQDN)
	serialNumber		OIB koji je u Republici Hrvatskoj dodijeljen pravnoj osobi ili državnom tijelu.
	jurisdictionOfIncorporationCountryName		HR
	businessCategory		Sadrži jedan od sljedećih niza znakova: "Private Organization" ili "Government Entity".
	organizationName (O)		Puni registrirani skraćeni naziv pravne osobe ili državnog tijela, ili puni naziv pravne osobe ili državnog tijela ako skraćeni naziv nije registriran.
	localityName (L)		Mjesto sjedišta pravne osobe
subjectPublic KeyInfo	AlgorithmIdentifier		id-ecPublicKey
	subjectPublicKey		Javni ključ subjekta, podržane duljine ECC ključa: P-256, P-384 i P-521.
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	FINA OID: 1.3.124.1104.5.901.14.1.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	QCP-w, OID: 0.4.0.194112.1.4
qCStatements	NE	policyIdentifier	extended-validation (1), OID: 2.23.140.1.1
		id-qcs-pkixQCSyntax-v2	id-etsi-qcs-SemanticsId-Legal
		esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
subjectAltName	NE	esi4-qcStatement-6	OID: 0.4.0.1862.1.6.3
		dNSName	Puni kvalificirani naziv poslužitelja (FQDN) u dNSName obliku. Najmanje jedan zapis/stavak.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoTLSCA2024partX.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	DA		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoTLSCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr
Signed Certificate Timestamps	NE	SignedCertificateTimestamp List	Lista potpisanih vremenskih žigova certifikata sukladno RFC 6962.

Tablica 39. Osnovna polja i ekstenzije profila Demo EU QWAC certifikata (QCP-w)

2.39. Demo EU PSD2 QWAC certifikat (QCP-w-psd2)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		X.509 v3, vrijednost="2"
serialNumber	CertificateSerialNumber		Broj veći od nule (0), duljine 16 okteta
signatureAlgorithm	AlgorithmIdentifier		ecdsa-with-SHA384
signatureValue	Potpis izdavatelja certifikata		
Issuer	commonName (CN)	Fina Demo TLS CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 6 mjeseci	
Subject	commonName (CN)	Samo jedan puni kvalificirani naziv poslužitelja (FQDN)	
	serialNumber	OIB koji je u Republici Hrvatskoj dodijeljen pružatelju platnih usluga.	
	jurisdictionOfIncorporationCountryName	HR	
	businessCategory	Sadrži jedan od sljedećih niza znakova: "Private Organization" ili "Government Entity".	
	organizationIdentifier	Identifikator pružatelja platnih usluga kojeg određuje ili dodjeljuje nadležno tijelo matične države članice EU.	
	organizationName (O)	Puni registrirani skraćeni naziv pružatelja platnih usluga ili puni naziv pružatelja platnih usluga ako skraćeni naziv nije registriran.	
	localityName (L)	Mjesto sjedišta pravne osobe	
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	Javni ključ subjekta, podržane duljine ECC ključa: P-256, P-384 i P-521.	
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	FINA OID: 1.3.124.1104.5.901.14.1.4
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	QCP-w-psd2, OID: 0.4.0.19495.3.1
		policyIdentifier	extended-validation (1), OID: 2.23.140.1.1
qCStatements	NE	id-qcs-pkixQCSyntax-v2	id-etsi-qcs-SemanticsId-Legal
		esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 https://demo-pki.fina.hr/pds/PDSQC1-0-en.pdf , en https://demo-pki.fina.hr/pds/PDSQC1-0-hr.pdf , hr
		esi4-qcStatement-6	OID: 0.4.0.1862.1.6.3
		etsi-psd2-qcStatement	Uloge dodijeljene pružatelju platnih usluga: 0.4.0.19495.1.1 (id-psd2-role-pp-as), PSP_AS) i/ili 0.4.0.19495.1.2 (id-psd2-role-pp-pi), PSP_PI) i/ili 0.4.0.19495.1.3 (id-psd2-role-pp-ai), PSP_AI) i/ili 0.4.0.19495.1.4 (id-psd2-role-pp-ic), PSP_IC)} Naziv nadležnog tijela matične države članice: NCAName (UTF8String (SIZE (1..256))) Identifikator nadležnog tijela matične države članice NCAId: dvoslovni ISO kod države, "-", NCA identifikator (2-8 znakova (A-Z)).

Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
cabfOrganizationIdentifier	NE	registrationSchemedentifier	Identifikator registracijske sheme.
		registrationCountry	Dvoslovni ISO kod države nadležnog tijela.
		registrationReference	Registracijska referenca dodijeljena u skladu s pravilima registracijske sheme.
subjectAltName	NE	dNSName	Puni kvalificirani naziv poslužitelja (FQDN) u dNSName obliku. Najmanje jedan zapis/stavak.
CRLDistributionPoints	NE	DistributionPoint	[1]URI: http://demo-pki.fina.hr/crl/DemoTLSCA2024partX.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	DA		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-calssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoTLSCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr

Tablica 40. Osnovna polja i ekstenzije profila Demo EU PSD2 QWAC certifikata (QCP-w-psd2)

2.40. Demo SSL certifikat razine 2 (OVCP)

Osnovna polja			
Polje	Atribut	Vrijednost	
Version	Version	X.509 v3, vrijednost="2"	
serialNumber	CertificateSerialNumber	Broj veći od nule (0), duljine 16 okteta	
signatureAlgorithm	AlgorithmIdentifier	ecdsa-with-SHA384	
signatureValue		Potpis izdavatelja certifikata	
Issuer	commonName (CN)	Fina Demo TLS CA 2024	
	organizationIdentifier	VATHR-85821130368	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 6 mjeseci	
Subject	serialNumber	Identifikator pravne osobe sastavljen na način koji pokazuje značenje njegovog sadržaja: VAT, dvoslovni ISO kod države sjedišta pravne osobe, „-“, OIB pravne osobe te točkom odijeljeni broj W koji predstavlja Fininu internu oznaku, npr. VATHR-12345678901.1	
	commonName (CN)	Samo jedna od vrijednosti upisanih u ekstenziju certifikata <i>Subject Alternative Name</i> (puni kvalificirani naziv poslužitelja (FQDN) ili Wildcard naziv domene ili IP adresa poslužitelja)	
	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)	HR	
subjectPublic KeyInfo	AlgorithmIdentifier	id-ecPublicKey	
	subjectPublicKey	Javni ključ subjekta, podržane duljine ECC ključa: P-256, P-384 i P-521.	
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	FINA OID: 1.3.124.1104.5.901.14.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/finadigicert/certifikati-za-testiranje-i-demonstraciju/fina-demo-okolina cPSuri: https://www.fina.hr/certificates-for-testing-and-demonstration/fina-demo-environment
		policyIdentifier	ovcp (7), OID: 0.4.0.2042.1.7
subjectAltName	NE	dNSName ili iPAddress	Puni kvalificirani naziv poslužitelja (FQDN) ili Wildcard naziv domene u dNSName obliku, ili IP adresa poslužitelja u iPAddress obliku. Najmanje jedan zapis/stavak.
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://demo-pki.fina.hr/crl/DemoTLSCA2024partX.crl
AuthorityKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	Vrijednost duljine 160 bita
BasicConstraints	DA		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://demo-pki.fina.hr/certifikati/DemoTLSCA2024.cer
		id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://demo-ocsp.fina.hr
Signed Certificate Timestamps	NE	SignedCertificateTimestampList	Lista potpisanih vremenskih žigova certifikata sukladno RFC 6962.

Tablica 41. Osnovna polja i ekstenzije profila Demo SSL certifikat razine 2 (OVCP)

	Profili certifikata za Demo Fina PKI ECC	klasifikacija:	
		strana:	46/49

3. Profil CRL

U sljedećoj tablici prikazan je profil CRL listi koje izdaju root i subordirani CA-ovi.

Osnovna polja i ekstenzije		
Polje	Vrijednost	
Version	v2, vrijednost="1"	
AlgorithmIdentifier	ecdsa-with-SHA384	
Issuer	Issuer DN, identično polju Subject izdavateljskog CA	
This Update	Vrijeme izdavanja CRL	
Next Update	Za CRL koju izdaje: <ul style="list-style-type: none"> Fina Demo Root CA G2: 12 mjeseci od vremena upisanog u polju This Update. Za Fina Demo Q-CA 2024: 24 sata od vremena upisanog u polju This Update. Za Fina Demo Ad-CA 2024: 24 sata od vremena upisanog u polju This Update. Za Fina Demo Root CA G2 TLS: 12 mjeseci od vremena upisanog u polju This Update. Za Fina Demo TLS CA 2024: 24 sata od vremena upisanom u polju This Update. 	
Revoked Certificates	Lista opozvanih/suspendiranih certifikata	
Ekstenzija	Kritično	Vrijednost
CRL Number	NE	Jednolično rastući cijeli broj
AuthorityKeyIdentifier	NE	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey
Issuing Distribution Point*	DA	Sadrži DistributionPoint vrijednost u kojoj je fullName s vrijednošću CRL Distribution Points ekstenzije certifikata, a polja onlyContainsUserCerts i onlyContainsCACerts u toj ekstenziji imaju vrijednost postavljenu na FALSE.
ExpiredCertsOnCRL	NE	Vrijedost ekstenzije: datum i vrijeme od kada CA u CRL trajno zadržava zapise o opozvanim certifikatima.

Tablica 42. Osnovna polja i ekstenzije profila CRL liste koje izdaju root i subordirani CA-ovi

* Ekstenzija IssuingDistributionPoint je sadržana samo u segmentiranim (particioniranim) CRL listama. Segmentirane (particionirane) CRL liste izdaje samo Fina Demo TLS CA 2024.

	Profili certifikata za Demo Fina PKI ECC	klasifikacija:	
		strana:	47/49

4. Profil OCSP odgovora

Profil OCSP odgovora sukladan je s ITF RFC 6960 dokumentom.

4.1. Profil OCSP odgovora za certifikate koje izdaju Fina Demo Root CA G2, Fina Demo Q-CA 2024 i Fina Demo Ad-CA 2024

Osnovna polja i ekstenzije	
Polje	Vrijednost
Version	v1(0)
AlgorithmIdentifier	ecdsa-with-SHA384
Signature:	Potpisni privatni ključ kojim je potpisan OCSP odgovor: P-384
responderID	Subject DN OCSP certifikata
thisUpdate	Vrijeme izrade OCSP odgovora.
nextUpdate	Nema
nonce	Vrijednost Nonce iz zahtjeva za status certifikata.
CertStatus	<ul style="list-style-type: none"> • good • revoked <ul style="list-style-type: none"> ○ revocationTime • unknown
CRLreason	Kodovi razloga za opoziv End-User certifikata su (0, 1, 3, 4, 5, 6 i 9).
ArchiveCutoff	Vrijednost polja mora biti postavljena na vrijednost koju ima polje "notBefore" pripadajućeg CA certifikata.

Tablica 43. Osnovna polja i ekstenzije OCSP profila koji izdaju Fina Demo Root CA G2, Fina Demo Q-CA 2024 i Fina Demo Ad-CA 2024

	Profili certifikata za Demo Fina PKI ECC	klasifikacija:	
		strana:	48/49

4.2. Profil OCSP odgovora za certifikate koje izdaju Fina Demo Root CA G2 TLS i Fina Demo TLS CA 2024

Osnovna polja i ekstenzije	
Polje	Vrijednost
Version	v1(0)
AlgorithmIdentifier	ecdsa-with-SHA256
Signature:	Potpisni privatni ključ kojim je potpisan OCSP odgovor za certifikate koje izdaje: <ul style="list-style-type: none"> • Fina Demo Root CA G2 TLS: P-256 • Fina Demo TLS CA 2024: P-256
responderID	Subject DN OCSP certifikata
thisUpdate	Vrijeme izrade OCSP odgovora.
nonce	Vrijednost Nonce iz zahtjeva za status certifikata.
CertStatus	<ul style="list-style-type: none"> • good • revoked <ul style="list-style-type: none"> ○ revocationTime • unknown
CRLreason	Kodovi razloga za opoziv End-User certifikata su (1, 3, 4, 5, i 9). U slučaju potrebe da bi CRLreason imao vrijednost „unspecified“ (0) ova ekstenzija se ne smije pojaviti.
ArchiveCutoff	Vrijednost polja je postavljena na vrijednost koju ima polje "notBefore" pripadajućeg CA certifikata.

Tablica 44. Osnovna polja i ekstenzije OCSP profila koji izdaju Fina Demo Root CA G2 TLS i Fina Demo TLS CA 2024

	Profili certifikata za Demo Fina PKI ECC	klasifikacija:	
		strana:	49/49

5. Profil Demo kvalificiranog elektroničkog vremenskog žiga

Polje	Vrijednosti za kvalificirani elektronički vremenski žig kojeg izdaje Fina Demo QTSA 2024 servis
version	V1, vrijednost="1"
policy	Fina OID: 1.3.124.1104.3.4.1.1.0
messageImprint	Podržani hash algoritmi <ul style="list-style-type: none"> • SHA-256 (OID: 2.16.840.1.101.3.4.2.1) • SHA-384 (OID: 2.16.840.1.101.3.4.2.2) • SHA-512 (OID: 2.16.840.1.101.3.4.2.3)
serialNumber	Cijeli broj (do 160 bita)
genTime	UTC vrijeme
accuracy	1 s
Nonce	Podržano, cijeli broj.
tsa	Subject DN Fina Demo QTSA 2024 certifikata
Ekstenzija	Vrijednost
qcStatements	QcStatements ekstenzija koja sadrži izjavu „esi4-qtstStatement-1”
signatureAlgorithm	ecdsa-with-SHA384

Tablica 45. Osnovna polja i ekstenzije profila „kvalificiranog“ vremenskog žiga koji izdaje Fina Demo QTSA 2024 servis