

	Opis promjene vezane uz izdavanje TLS/SSL certifikata na Fina RDC 2020 CA	klasifikacija:	
		strana:	1/7

FINA

Opis promjena vezanih uz izdavanje TLS/SSL certifikata na Fina RDC 2020 CA

Datum izrade: 05.11.2024.

	Opis promjene vezane uz izdavanje TLS/SSL certifikata na Fina RDC 2020 CA	klasifikacija:	
		strana:	2/7

SADRŽAJ

1.	Uvod	3
2.	Razlozi uvođenja promjena	3
3.	Promjene u certifikatima	3
4.	Profili TLS/SSL certifikata	4
	SSL certifikat razine 2 (OVCP)	4
	EU QWAC certifikat (QCP-w)	5
	EU PSD2 QWAC certifikat (QCP-w-psd2)	6

	Opis promjene vezane uz izdavanje TLS/SSL certifikata na Fina RDC 2020 CA	klasifikacija:	
		strana:	3/7

1. Uvod

Fina priprema promjenu u izdavanju TLS/SSL certifikata koje će umjesto dosadašnjeg subordiniranog Fina RDC 2015 s danom 25.11.2024. započeti izdavati subordinirani Fina RDC 2020 CA.

Svi ostali tipovi certifikata čiji je izdavatelj Fina već se izdaju na Fina RDC 2020 CA i u tom dijelu nema promjena. Isto tako nema promjena vezanih uz korijensko certifikacijsko tijelo Fina Root CA koje je izdavatelj Fina RDC 2020 CA certifikata.

2. Razlozi uvođenja promjena

S obzirom na činjenicu da certifikat Fina RDC 2015 CA ističe 25.11.2025. godine, ovaj subordinirani CA nakon 25.11.2024. više ne može izdavati TLS/SSL certifikate na period valjanosti od godine dana.

U cilju nastavka izdavanja TLS/SSL certifikata na period valjanosti od godine dana (bez potrebe za skraćivanjem vremenskog perioda važenja certifikata), od 25.11.2024. navedene certifikate započinje izdavati Fina RDC 2020 CA.

3. Promjene u certifikatima

Promjene u TLS/SSL certifikatima su minimalne, a neophodne su zbog promjene CA koji će izdavati navedene certifikate (Fina RDC 2020).

Promjene u profilima certifikata su sljedeće:

- Vrijednost atributa **commonName (CN)** u polju **Issuer** se mijenja na način da će umjesto vrijednosti „Fina RDC 2015“ imati vrijednost „Fina RDC 2020“.
- Fina OID u certificatePolicies ekstenziji** mijenja se tako da se šesta komponenta OID-a mijenja u „13“, npr. Fina OID „1.3.124.1104.5.12.14.2“ mijenja se u Fina OID „1.3.124.1104.5.13.14.2“.

U Tablici 1. ovog poglavlja kao i u opisu profila TLS/SSL certifikata u poglavlju 4. „Profili TLS/SSL certifikata“ naveden je Fina OID za pojedini tip certifikata.

- URL u ekstenziji CRLDistributionPoints** koji opisuje lokaciju CRL liste se mijenja i biti će: „[1] URI: <http://rdc.fina.hr/RDC2020/FinaRDCCA2020partX.crl>“
- URL CA certifikata izdavatelja u ekstenziji Authority Information Access** se mijenja i biti će <http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer>.

Tablica 1. u ovom dokumentu prikazuje popis **tipova TLS/SSL certifikata** koje će Fina RDC 2020 CA započeti izdavati s datumom 25.11.2024.

NAZIV TIPRA CERTIFIKATA	FINA OID
SSL certifikat razine 2 (OVCP)	1.3.124.1104.5.13.14.2
EU QWAC certifikat (QCP-w)	1.3.124.1104.5.13.14.1.2
EU PSD2 QWAC certifikat (QCP-w-psd2)	1.3.124.1104.5.13.14.1.4

Tablica 1.: Popis tipova TLS/ SSL certifikata - Fina RDC 2020 CA

	Opis promjene vezane uz izdavanje TLS/SSL certifikata na Fina RDC 2020 CA	klasifikacija:	
		strana:	4/7

4. Profili TLS/SSL certifikata

Vrijednost u pojedinom profilu TLS/SSL certifikata kod koje došlo do promjene sukladno podacima navedenim u poglavlju 3. „Promjene u certifikatima“ u sljedećim je tablicama označena crvenkastom bojom.

SSL certifikat razine 2 (OVCP)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version	V3, vrijednost="2"	
serialNumber	CertificateSerialNumber	16 ili 17 okteta, 64 bita entropije	
signatureAlgorithm	AlgorithmIdentifier	sha256WithRSAEncryption	
signatureValue		Potpis izdavatelja certifikata	
Issuer	commonName (CN)	Fina RDC 2020	
	organizationName (O)	Financijska agencija	
	countryName (C)	HR	
Validity	notBefore	Vrijeme izdavanja certifikata	
	notAfter	Vrijeme izdavanja certifikata + 12 mjeseci	
Subject	serialNumber	Identifikator pravne osobe sastavljen na način koji pokazuje značenje njegovog sadržaja: VAT, dvoslovčani 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)	
	localityName (L)	Mjesto sjedišta pravne osobe	
	organizationName (O)	Puni registrirani skraćeni naziv pravne osobe ili naziv pravne osobe ako skraćeni naziv nije registriran.	
	countryName (C)	HR	
subjectPublic KeyInfo	AlgorithmIdentifier	rsaEncryption	
	subjectPublicKey	Javni ključ subjekta, podržane duljineRSA ključa: 2048, 3072 i 4096 bita.	
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	serverAuth	1.3.6.1.5.5.7.3.1
		clientAuth	1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.13.14.2
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti cPSuri: https://www.fina.hr/en/legislation-documents-and-conformance-certificates
		policyIdentifier	ovcp (7), OID: 0.4.0.2042.1.7
		policyIdentifier	organization-validated (2), OID: 2.23.140.1.2.2
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://rdc.fina.hr/RDC2020/FinaRDCCA2020partX.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.fina.hr
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer
Signed Certificate Timestamps	NE	SignedCertificateTimestampList	Lista potpisanih vremenskih žigova certifikata sukladno RFC 6962.

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

	Opis promjene vezane uz izdavanje TLS/SSL certifikata na Fina RDC 2020 CA	klasifikacija:	
		strana:	5/7

EU QWAC certifikat (QCP-w)

Osnovna polja				
Polje		Atribut	Vrijednost	
Version		Version	V3, vrijednost="2"	
serialNumber		CertificateSerialNumber	16 ili 17 okteta, 64 bita entropije	
signatureAlgorithm		AlgorithmIdentifier	sha256WithRSAEncryption	
signatureValue			Potpis izdavatelja certifikata	
Issuer		commonName (CN)	Fina RDC 2020	
		organizationName (O)	Financijska agencija	
		countryName (C)	HR	
Validity		notBefore	Vrijeme izdavanja certifikata	
		notAfter	Vrijeme izdavanja certifikata + 12 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".	
		localityName (L)	Mjesto poslovanja pravne osobe ili državnog tijela.	
		organizationName (O)	Puni registrirani skraćeni naziv pravne osobe ili državnog tijela, ili puni naziv pravne osobe ili državnog tijela ako skraćeni naziv nije registriran.	
		countryName (C)	HR	
subjectPublic KeyInfo		AlgorithmIdentifier	rsaEncryption	
		subjectPublicKey	Javni ključ subjekta, podržane duljine RSA ključa: 2048, 3072 i 4096 bita.	
Ekstenzije				
Polje		Kritično	Atribut	Vrijednost
KeyUsage		DA	digitalSignature	Uključen digitalSignature bit
			keyEncipherment	Uključen keyEncipherment bit
extKeyUsage		NE	serverAuth	1.3.6.1.5.5.7.3.1
			clientAuth	1.3.6.1.5.5.7.3.2
certificatePolicies		NE	policyIdentifier	FINA OID: 1.3.124.1104.5.13.14.1.2
			policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti cPSuri: https://www.fina.hr/en/legislation-documents-and-conformance-certificates
			policyIdentifier	QCP-w, OID: 0.4.0.194112.1.4
			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://rdc.fina.hr/pds/PDSQWAC-en.pdf , en https://rdc.fina.hr/pds/PDSQWAC-hr.pdf , hr
			esi4-qcStatement-6	OID: 0.4.0.1862.1.6.3
subjectAltName		NE	dNSName	Puni kvalificirani naziv poslužitelja (FQDN) u dNSName obliku. Najmanje jedan zapis/stavak.
CRLDistributionPoints		NE	DistributionPoint	[1] URI: http://rdc.fina.hr/RDC2020/FinaRDCCA2020partX.crl
AuthorityKeyIdentifier		NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier		NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints		NE		cA=FALSE pathLenConstraint=None
Authority Information Access		NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.fina.hr
			id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer
Signed Certificate Timestamps		NE	SignedCertificateTimestampList	Lista potpisanih vremenskih žigova certifikata sukladno RFC 6962.

Tablica 3. Osnovna polja i ekstenzije profila EU QWAC certifikata (QCP-w)

EU PSD2 QWAC certifikat (QCP-w-psd2)

Osnovna polja			
Polje	Atribut		Vrijednost
Version	Version		V3, vrijednost="2"
serialNumber	CertificateSerialNumber		16 ili 17 okteta, 64 bita entropije
signatureAlgorithm	AlgorithmIdentifier		sha256WithRSAEncryption
signatureValue			Potpis izdavatelja certifikata
Issuer	commonName (CN)		Fina RDC 2020
	organizationName (O)		Financijska agencija
	countryName (C)		HR
Validity	notBefore		Vrijeme izdavanja certifikata
	notAfter		Vrijeme izdavanja certifikata + 12 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".
	localityName (L)		Mjesto poslovanja pružatelja platnih usluga.
	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.
	countryName (C)		HR
subjectPublic KeyInfo	AlgorithmIdentifier		rsaEncryption
	subjectPublicKey		Javni ključ subjekta, podržane duljine RSA ključa: 2048, 3072 i 4096 bita.
Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
KeyUsage	DA	digitalSignature	Uključen digitalSignature bit
		keyEncipherment	Uključen keyEncipherment bit
extKeyUsage	NE	serverAuth	1.3.6.1.5.5.7.3.1
		clientAuth	1.3.6.1.5.5.7.3.2
certificatePolicies	NE	policyIdentifier	FINA OID: 1.3.124.1104.5.13.14.1.4
		policyQualifiers	policyQualifierId: id-qt-cps { id-qt 1 } cPSuri: https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti cPSuri: https://www.fina.hr/en/legislation-documents-and-conformance-certificates
		policyIdentifier	QCP-w-psd2, OID: 0.4.0.19495.3.1
		policyIdentifier	extended-validation (1), OID: 2.23.140.1.1
		id-qcs-pkixQCSyntax-v2	id-etsi-qcs-SemanticsId-Legal
qCStatements	NE	esi4-qcStatement-1	OID: 0.4.0.1862.1.1
		esi4-qcStatement-5	OID: 0.4.0.1862.1.5 https://rdc.fina.hr/pds/PDSQWAC-en.pdf , en https://rdc.fina.hr/pds/PDSQWAC-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-psp-as), PSP_AS) i/ili 0.4.0.19495.1.2 (id-psd2-role-psp-pi), PSP_PI) i/ili 0.4.0.19495.1.3 (id-psd2-role-psp-ai), PSP_AI) i/ili 0.4.0.19495.1.4 (id-psd2-role-psp-ic), PSP_IC)} Naziv nadležnog tijela matične države članice: NCAName (UTF8String (SIZE (1..256))) Identifikator nadležnog tijela matične države članice NCAId: dvoslovčani ISO kod države, "-", NCA identifikator (2-8 znakova (A-Z)).
			Puni kvalificirani naziv poslužitelja (FQDN) u
			dNSName obliku. Najmanje jedan zapis/stavak.
subjectAltName	NE	dNSName	Puni kvalificirani naziv poslužitelja (FQDN) u dNSName obliku. Najmanje jedan zapis/stavak.

	Opis promjene vezane uz izdavanje TLS/SSL certifikata na Fina RDC 2020 CA	klasifikacija:	
		strana:	7/7

Ekstenzije			
Polje	Kritično	Atribut	Vrijednost
CRLDistributionPoints	NE	DistributionPoint	[1] URI: http://rdc.fina.hr/RDC2020/FinaRDCCA2020partX.crl
AuthorityKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
SubjectKeyIdentifier	NE	keyIdentifier	SHA-1 sažetak duljine 160 bita
BasicConstraints	NE		cA=FALSE pathLenConstraint=None
Authority Information Access	NE	id-ad-ocsp	Access Method=On-line Certificate Status Protocol accessLocation: http://ocsp.fina.hr
		id-ad-caIssuers	Access Method=Certification Authority Issuer accessLocation: http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer

Tablica 4. Osnovna polja i ekstenzije profila EU PSD2 QWAC certifikata (QCP-w-psd2)