OPIS PLANIRANIH PROMJENA U PROFILIMA

FINA RDC CERTIFIKATA

Profili FINA RDC certifikata će se izmijeniti zbog uvođenja OIB-a osobe, odnosno OIB-a poslovnog subjekta u certifikate, tako da se u odnosu na dosadašnje profile certifikata uvode niže opisane promjene.

Polje subject

Najveće promjene uvode se u polju subject koje sadrži distinguished name (DN) subjekta.

Polje subject za poslovne certifikate za osobu imat će oblik::

CN = *IME PREZIME*

SERIALNUMBER = HR*OIBOSOBE.W.Z*

L = *SJEDIŠTE_POSLOVNOG_SUBJEKTA*

O = *IME_POSLOVNOG_SUBJEKTA* HR*OIBPS*

C = HR

Polje subject za osobne certifikate imat će oblik::

CN = *IME PREZIME*

SERIALNUMBER = HR*OIBOSOBE.W.Z*

L = *PREBIVALIŠTE*

O = OSOBNI

C = HR

W i *Z* su pozitivni cijeli brojevi i imaju interno značenje u FINI. *OIBOSOBE* je osobni identifikacijski broj fizičke osobe, a *OIBPS* je osobni identifikacijski broj poslovnog subjekta.

U nastavku su navedene promjene u atributima polja.subject.

Atribut serialNumber

U polju subject koji sadrži DN subjekta uvodi se zaseban atribut serialNumber, a koji sadržava serijski broj subjekta. Vrijednost ovog serijskog broja je u dosadašnjim certifikatima bila sastavni dio atributa commonName, upisana nakon imena i prezimena osobe.

Format serijskog broja subjekta se mijenja te će se serijski broj sastojati od tri komponente odijeljene točkom, od kojih prva komponenta sadrži prefiks HR i OIB fizičke osobe, dok druga i treća komponenta imaju interno značenje. Primjer novog izgleda serijskog broja je: HR12345678901.1.1

Atribut organizationalUnitName

Dosadašnji atributi organizationalUnitName se ukidaju.za FINA RDC certifikate.

Atribut organizationName

Atribut organizationName za poslovne certifikate sadrži skraćeni naziv i OIB poslovnog subjekta, a za osobne certifikate sadrži vrijednost OSOBNI.

Vrijednosti ovog atributa za poslovne certifikate se upisuju na način da se lijeve strane upisuje službeni skraćeni naziv poslovnog subjekta do najviše 50 znakova. Ukoliko skraćeni naziv poslovnog subjekta sadrži preko 50 znakova, skraćeni naziv se dodatno skraćuje na 50 znakova. Nakon zadnjeg upisanog znaka skraćenog naziva poslovnog subjekta s desne strane se dodaje znak za razmak te se nakon njega dodaje OIB poslovnog subjekta u formi HROIB, tj. ispred znamenki OIB-a se dodaju slova HR.

Atribut organizationName slijedi neposredno ispred atributa countryName.

Atribut localityName

U polje subject uvodi se atribut localityName. Ovaj atribut u poslovnim certifikatima sadrži naziv mjesta sjedišta poslovnog subjekta. U osobnim certifikatima localityName sadrži prebivalište odnosno boravište osobe.

Atribut countryName

Atribut countryName sadrži oznaku države sukladno standardu ISO 3166.

Ekstenzija QCStatements

Za kvalificirane certifikate uvodi se dodatna ekstenzija QCStatements (izjave kvalificiranog certifikata) u koju se upisuje izjava id-etsi-qcs-QcCompliance koja označava da je certifikat izdan kao kvalificirani certifikat.

Opisi profila FINA RDC certifikata

U nastavku je dan detaljniji opis profila FINA RDC certifikata te su žutom bojom označeni dijelovi profila certifikata koji će se mijenjati.

FINA RDC Poslovni autentifikacijski i enkripcijski certifikat

FINA RDC Poslovni autentifikacijski i enkripcijski certifikat			
Atributi osnovnih politika		**vrijednost/sadržaj**	**opis/komentar**
Namjena		Autentifikacija, elektronički potpis i enkripcija	
Razina sigurnosti		Srednja	
X.509 - CERTIFIKAT		**vrijednost/sadržaj**	**opis/komentar**
1. Version		X.509 verzija 3.	Format; cijeli broj
2. serialNumber		10. znamenkasti neponovljivi cijeli broj	format; cijeli broj (2^{32}) - bez vodećih nula
3. signatureAlgorithm		1.2.840.113549.1.1.5.	sha1RSA
4. issuer			
organizationalUnit		RDC	ovjerovitelj (CA)
organizationName		FINA	naziv poslovnog subjekta koji pruža usluge certificiranja (CSP)
countryName		HR	zemlja sjedišta poslovnog subjekta koji pruža usluge certificiranja (CSP)
5. validity			
Valid from (not before)		vrijeme izdavanja	format; YYMMDDhhmmssZ (UTCTime)
Valid to (not after)		vrijeme izdavanja+24 mjeseci	format; YYMMDDhhmmssZ (UTCTime)
6. subject		X.500 DN fizičke osobe u poslovnom subjektu	format; niz znakova UTF8
commonName		ime i prezime korisnika	
serialNumber		serijski broj	Serijski broj u formatu HROIB.W.1 (W je cijeli broj)
localityName		naziv mjesta sjedišta poslovnog subjekta	
organizationName		Skraćeni naziv poslovnog subjekta i OIB poslovnog subjekta	Format: skraćeni_naziv HROIB skraćeni naziv max. 50 znakova
countryName		oznaka države prema ISO 3166	
7. Public key		RSA-1024 javni ključ subjekta	prema RFC 3279
X.509 - OBAVEZNE EKSTENZIJE	**kritično**	**vrijednost/sadržaj**	**opis/komentar**
8. authorityKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
9. subjectKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
10. keyUsage	DA	digitalSignature&keyEncihperment	
11. certificatePolicies	NE		
PolicyIdentifier=		1.3.124.1104.5.11.2.4.2	FINA RDC poslovni autentifikacijski certifikat (srednja razina sigurnosti)

URL na CP		http://rdc.fina.hr/cp/	
12. basicConstrains	NE		
subjectType=		End Entity	
pathLengthConstraint=		None	
13. CRL Distribution Point	NE		
(1) CRL distribuirana; LDAP		CRLn	
ou=		RDC	
o=		FINA	
c=		HR	
(2) CRL kombinirana; LDAP		ldap://rdc-ldap.fina.hr/ou=RDC,o=FINA, c=HR?certificateRevocationList%3Bbinary	
(3) CRL kombinirana; HTTP		URL=http://rdc.fina.hr/crls/rdc.crl	
X.509 - OPCIONALNE EKSTENZIJE	**Kritično**	**vrijednost/sadržaj**	**opis/komentar**
14. subjectAltName	NE	e-mail adresa subjekta	format; RFC 822 Name
15. Private Key Usage Period	NE	100 %	Relativni period valjanosti privatnog ključa subjekta u odnosu na certifikat

FINA RDC Poslovni potpisni certifikat

FINA RDC Poslovni potpisni certifikat			
Atributi osnovnih politika		**vrijednost/sadržaj**	**opis/komentar**
Namjena		Napredni elektronički potpis	
Razinama sigurnosti		Srednja	
X.509 – CERTIFIKAT		**vrijednost/sadržaj**	**opis/komentar**
1. Version		X.509 verzija 3.	Format; cijeli broj
2. serialNumber		10. znamenkasti neponovljivi cijeli broj	format; cijeli broj (2^{32}) - bez vodećih nula
3. signatureAlgorithm		1.2.840.113549.1.1.5.	sha1RSA
4. issuer			
organizationalUnit		RDC	ovjerovitelj (CA)
organizationName		FINA	naziv poslovnog subjekta koji pruža usluge certificiranja (CSP)
countryName		HR	zemlja sjedišta poslovnog subjekta koji pruža usluge certificiranja (CSP)
5. validity			
Valid from (not before)		vrijeme izdavanja	format; YYMMDDhhmmssZ (UTCTime)
Valid to (not after)		vrijeme izdavanja+24 mjeseci	format; YYMMDDhhmmssZ (UTCTime)
6. subject		X.500 DN fizičke osobe u poslovnom subjektu	format; niz znakova UTF8
commonName		ime i prezime potpisnika	
serialNumber		serijski broj	Serijski broj u formatu HROIB.W.5 (W je cijeli broj)
localityName		naziv mjesta sjedišta poslovnog subjekta	
organizationName		Skraćeni naziv poslovnog subjekta i OIB poslovnog subjekta	Format: skraćeni_naziv HROIB skraćeni naziv max. 50 znakova
countryName		Oznaka države prema ISO 3166	
7. Public key		RSA-1024 javni ključ subjekta	prema RFC 3279
X.509 – OBAVEZNE EKSTENZIJE	**kritično**	**vrijednost/sadržaj**	**opis/komentar**
8. authorityKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
9. subjectKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
10. keyUsage	DA	Non Repudiation	
11. certificatePolicies	NE		
PolicyIdentifier=		1.3.124.1104.5.11.2.2.2	FINA RDC poslovni potpisni certifikat (srednja razina sigurnosti)
URL na CP		http://rdc.fina.hr/cp/	
12. basicConstrains	NE		
subjectType=		End Entity	
pathLengthConstraint=		None	

13. CRL Distribution Point	NE		
(1) CRL distribuirana; LDAP		CRLn	
ou=		RDC	
o=		FINA	
c=		HR	
(2) CRL kombinirana; LDAP		ldap://rdc-ldap.fina.hr/ou=RDC,o=FINA, c=HR?certificateRevocationList %3Bbinary	
(3) CRL kombinirana; HTTP		URL=http://rdc.fina.hr/crls/rdc.crl	
14. qCStatements	NE	id-etsi-qcs-QcCompliance	
X.509 - OPCIONALNE EKSTENZIJE	**Kritično**	**vrijednost/sadržaj**	**opis/komentar**
15. subjectAltName	NE	e-mail adresa subjekta	format; RFC 822 Name
16. Private Key Usage Period	NE	100 %	Relativni period valjanosti privatnog ključa subjekta u odnosu na certifikat

FINA RDC Osobni autentifikacijski i enkripcijski certifikat

FINA RDC Osobni autentifikacijski i enkripcijski certifikat			
Atributi osnovnih politika		**vrijednost/sadržaj**	**opis/komentar**
Namjena		Autentifikacija, elektronički potpis i enkripcija	
Razina sigurnosti		Srednja	
X.509 - CERTIFIKAT		**vrijednost/sadržaj**	**opis/komentar**
1. Version		X.509 verzija 3.	Format; cijeli broj
2. serialNumber		10. znamenkasti neponovljivi cijeli broj	format; cijeli broj (232) - bez vodećih nula
3. signatureAlgorithm		1.2.840.113549.1.1.5.	sha1RSA
4. issuer			
organizationalUnit		RDC	ovjerovitelj (CA)
organizationName		FINA	naziv poslovnog subjekta koji pruža usluge certificiranja (CSP)
countryName		HR	zemlja sjedišta poslovnog subjekta koji pruža usluge certificiranja (CSP)
5. validity			
Valid from (not before)		vrijeme izdavanja	format; YYMMDDhhmmssZ (UTCTime)
Valid to (not after)		vrijeme izdavanja+24 mjeseci	format; YYMMDDhhmmssZ (UTCTime)
6. subject		X.500 DN fizičke osobe	format; niz znakova UTF8
commonName		ime i prezime korisnika	
serialNumber		serijski broj	Serijski broj u formatu HROIB.W.2 (W je cijeli broj)
localityName		mjesto prebivališta korisnika	
organizationName		OSOBNI	
countryName		oznaka države prema ISO 3166	
7. Public key		RSA-1024 javni ključ subjekta	prema RFC 3279
X.509 - OBAVEZNE EKSTENZIJE	**kritično**	**vrijednost/sadržaj**	**opis/komentar**
8. authorityKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
9. subjectKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
10. keyUsage	DA	digitalSignature&keyEncihperment	
11. certificatePolicies	NE		
PolicyIdentifier=		1.3.124.1104.5.11.1.4.2	FINA RDC osobni autentifikacijski certifikat (srednja razina sigurnosti)
URL na CP		http://rdc.fina.hr/cp/	
12. basicConstrains	NE		
subjectType=		End Entity	
pathLengthConstraint=		None	

13. CRL Distribution Point	NE		
(1) CRL distribuirana; LDAP		CRLn	
ou=		RDC	
o=		FINA	
c=		HR	
(2) CRL kombinirana; LDAP		ldap://rdc-ldap.fina.hr/ou=RDC,o=FINA, c=HR?certificateRevocationList%3Bbinary	
(3) CRL kombinirana; HTTP		URL=http://rdc.fina.hr/crls/rdc.crl	
X.509 - OPCIONALNE EKSTENZIJE	**Kritično**	**vrijednost/sadržaj**	**opis/komentar**
14. subjectAltName	NE	e-mail adresa subjekta	format; RFC 822 Name
15. Private Key Usage Period	NE	100 %	Relativni period valjanosti privatnog ključa subjekta u odnosu na certifikat

FINA RDC Osobni potpisni certifikat

FINA RDC Osobni potpisni certifikat			
Atributi osnovnih politika		**vrijednost/sadržaj**	**opis/komentar**
Namjena		Napredni elektronički potpis	
Razina sigurnosti		Srednja	
X.509 – CERTIFIKAT		**vrijednost/sadržaj**	**opis/komentar**
1. Version		X.509 verzija 3.	Format; cijeli broj
2. serialNumber		10. znamenkasti neponovljivi cijeli broj	format; cijeli broj (232) - bez vodećih nula
3. signatureAlgorithm		1.2.840.113549.1.1.5.	sha1RSA
4. issuer			
organizationalUnit		RDC	ovjerovitelj (CA)
organizationName		FINA	naziv poslovnog subjekta koji pruža usluge certificiranja (CSP)
countryName		HR	zemlja sjedišta poslovnog subjekta koji pruža usluge certificiranja (CSP)
5. validity			
Valid from (not before)		vrijeme izdavanja	format; YYMMDDhhmmssZ (UTCTime)
Valid to (not after)		vrijeme izdavanja+24 mjeseci	format; YYMMDDhhmmssZ (UTCTime)
6. subject		X.500 DN fizičke osobe	format; niz znakova UTF8
commonName		ime i prezime potpisnika	
serialNumber		serijski broj	Serijski broj u formatu HROIB.W.3 (W je cijeli broj)
localityName		mjesto prebivališta potpisnika	
organizationName		OSOBNI	
countryName		oznaka države prema ISO 3166	
7. Public key		RSA-1024 javni ključ subjekta	prema RFC 3279
X.509 - OBAVEZNE EKSTENZIJE	**kritično**	**vrijednost/sadržaj**	**opis/komentar**
8. authorityKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
9. subjectKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
10. keyUsage	DA	digitalSignature&keyEncihperment	
11. certificatePolicies	NE		
PolicyIdentifier=		1.3.124.1104.5.11.1.4.2	FINA RDC osobni autentifikacijski certifikat (srednja razina sigurnosti)
URL na CP		http://rdc.fina.hr/cp/	
12. basicConstrains	NE		
subjectType=		End Entity	

pathLengthConstraint=		None	
13. CRL Distribution Point	NE		
(1) CRL distribuirana; LDAP		CRLn	
ou=		RDC	
o=		FINA	
c=		HR	
(2) CRL kombinirana; LDAP		ldap://rdc-ldap.fina.hr/ou=RDC,o=FINA,c=HR?certificateRevocationList%3Bbinary	
(3) CRL kombinirana; HTTP		URL=http://rdc.fina.hr/crls/rdc.crl	
14. qCStatements	NE	id-etsi-qcs-QcCompliance	
X.509 - OPCIONALNE EKSTENZIJE	**Kritično**	**vrijednost/sadržaj**	**opis/komentar**
15. subjectAltName	NE	e-mail adresa subjekta	format; RFC 822 Name
16. Private Key Usage Period	NE	100 %	Relativni period valjanosti privatnog ključa subjekta u odnosu na certifikat

FINA RDC Poslovni certifikat za poslužitelj

FINA RDC Poslovni certifikat za poslužitelj			
Atributi osnovnih politika		**vrijednost/sadržaj**	**opis/komentar**
Namjena		Certifikat za poslužitelj	
Razina sigurnosti		Srednja	
X.509 - CERTIFIKAT		**vrijednost/sadržaj**	**opis/komentar**
1. Version		X.509 verzija 3.	Format; cijeli broj
2. serialNumber		10. znamenkasti neponovljivi cijeli broj	format; cijeli broj (2^{32}) - bez vodećih nula
3. signatureAlgorithm		1.2.840.113549.1.1.5.	sha1RSA
4. issuer			
organizationalUnit		RDC	ovjerovitelj (CA)
organizationName		FINA	naziv poslovnog subjekta koji pruža usluge certificiranja (CSP)
countryName		HR	zemlja sjedišta poslovnog subjekta koji pruža usluge certificiranja (CSP)
5. validity			
Valid from (not before)		vrijeme izdavanja	format; YYMMDDhhmmssZ (UTCTime)
Valid to (not after)		vrijeme izdavanja+24 mjeseci	format; YYMMDDhhmmssZ (UTCTime)
6. subject		X.500 DN poslužitelja u poslovnom subjektu	format; niz znakova UTF8
commonName		naziv poslužitelja	
localityName		naziv mjesta sjedišta poslovnog subjekta	
organizationName		skraćeni naziv poslovnog subjekta i OIB poslovnog subjekta	Format: skraćeni_naziv HROIB skraćeni naziv max. 50 znakova
countryName		oznaka države prema ISO 3166	
7. Public key		RSA-1024 javni ključ subjekta	prema RFC 3279
X.509 - OBAVEZNE EKSTENZIJE	**kritično**	**vrijednost/sadržaj**	**opis/komentar**
8. authorityKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
9. subjectKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
10. keyUsage	DA	digitalSignature&keyEncihperment	
11. certificatePolicies	NE		
PolicyIdentifier=		1.3.124.1104.5.11.3.4.2	FINA RDC poslovni autentifikacijski certifikat (srednja razina sigurnosti)
URL na CP		http://rdc.fina.hr/cp/	
12. basicConstrains	NE		
subjectType=		End Entity	
pathLengthConstraint=		None	
13. CRL Distribution Point	NE		

(1) CRL distribuirana; LDAP		CRLn	
ou=		RDC	
o=		FINA	
c=		HR	
(2) CRL kombinirana; LDAP		ldap://rdc-ldap.fina.hr/ou=RDC,o=FINA, c=HR?certificateRevocationList%3Bbinary	
(3) CRL kombinirana; HTTP		URL=http://rdc.fina.hr/crls/rdc.crl	
X.509 - OPCIONALNE EKSTENZIJE	**Kritično**	**vrijednost/sadržaj**	**opis/komentar**
14. Private Key Usage Period	NE	100 %	Relativni period valjanosti privatnog ključa subjekta u odnosu na certifikat

FINA RDC Poslovni certifikat za aplikaciju

FINA RDC Poslovni certifikat za aplikaciju			
Atributi osnovnih politika		**vrijednost/sadržaj**	**opis/komentar**
Namjena		Certifikat za aplikaciju	
Razina sigurnosti		Srednja	
X.509 - CERTIFIKAT		**vrijednost/sadržaj**	**opis/komentar**
1. Version		X.509 verzija 3.	Format; cijeli broj
2. serialNumber		10. znamenkasti neponovljivi cijeli broj	format; cijeli broj (2^{32}) - bez vodećih nula
3. signatureAlgorithm		1.2.840.113549.1.1.5.	sha1RSA
4. issuer			
organizationalUnit		RDC	ovjerovitelj (CA)
organizationName		FINA	naziv poslovnog subjekta koji pruža usluge certificiranja (CSP)
countryName		HR	zemlja sjedišta poslovnog subjekta koji pruža usluge certificiranja (CSP)
5. validity			
Valid from (not before)		vrijeme izdavanja	format; YYMMDDhhmmssZ (UTCTime)
Valid to (not after)		vrijeme izdavanja+24 mjeseci	format; YYMMDDhhmmssZ (UTCTime)
6. subject		X.500 DN aplikacije u poslovnom subjektu	format; niz znakova UTF8
commonName		ime aplikacije	
localityName		naziv mjesta sjedišta poslovnog subjekta	
organizationName		skraćeni naziv poslovnog subjekta i OIB poslovnog subjekta	Format: skraćeni_naziv HROIB skraćeni naziv max. 50 znakova
countryName		oznaka države prema ISO 3166	
7. Public key		RSA-1024 javni ključ subjekta	prema RFC 3279
X.509 - OBAVEZNE EKSTENZIJE	**kritično**	**vrijednost/sadržaj**	**opis/komentar**
8. authorityKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
9. subjectKeyIdentifier	NE	60-bit SHA-1 hash vrijednost ključa	
10. keyUsage	DA	digitalSignature&keyEncihperment	
11. certificatePolicies	NE		
PolicyIdentifier=		1.3.124.1104.5.11.5.4.2	FINA RDC poslovni autentifikacijski certifikat (srednja razina sigurnosti)
URL na CP		http://rdc.fina.hr/cp/	
12. basicConstrains	NE		
subjectType=		End Entity	
pathLengthConstraint=		None	
13. CRL Distribution Point	NE		

(1) CRL distribuirana; LDAP		CRLn	
ou=		RDC	
o=		FINA	
c=		HR	
(4) CRL kombinirana; LDAP		ldap://rdc-ldap.fina.hr/ou=RDC,o=FINA, c=HR?certificateRevocationList%3Bbinary	
(5) CRL kombinirana; HTTP		URL=http://rdc.fina.hr/crls/rdc.crl	
X.509 - OPCIONALNE EKSTENZIJE	**Kritično**	**vrijednost/sadržaj**	**opis/komentar**
14. Private Key Usage Period	NE	100 %	Relativni period valjanosti privatnog ključa subjekta u odnosu na certifikat