Financijska Agencija
Zagreb, Koturaška 43

FINA PKI

PRAVILNIK O ADMINISTRIRANJU KORISNIKA I CERTIFIKATA

Verzija 1.0

Datum 31.03.2003.

FINA PKI

Pravilnik o administriranju korisnika i certifikata

AUTORSKA PRAVA

OSOBE ZA KONTAKTIRANJE U VEZI S FININOM PKI DOKUMENTACIJOM

Upiti u vezi s uvođenjem ovog Pravilnika te vođenjem administracije koja se na nj odnosi mogu se uputiti sljedećim osobama na njihove e-mail adrese:

Fanica.Beros@fina.hr

Leopold.Eke@fina.hr

PREGLED PROMJENA

Redni broj	Verzija	Točka	Opis promjene	Datum promjene

SADRŽAJ

1. UVOD

1.1. Cilj dokumenta

Cilj je ovog dokumenta:

1. Uputiti korisnika koje certifikate mogu dobiti, pod kojim uvjetima i kako zatražiti certifikat od FINA PKI
2. Opisati procedure po kojima će RA administrator, LRA zaposlenik i FINA HELP DESK obavljati operativne zadaće administriranja FINA PKI korisnika, što podrazumijeva upravljanje životnim ciklusom certifikata i održavanje informacija o korisniku FINA PKI.

1.2. Promjena dokumenta

1.2.1. Mehanizam upravljanja primjedbama

Napisane i potpisane primjedbe na ovaj dokument moraju biti upućene u PMA FINA PKI. Odluke o prihvaćanju primjedbi su diskreciono pravo PMA FINA PKI.

1.2.2. Obavijest o konačnim izmjenama

PMA FINA PKI će odrediti rok za obavijest o konačnim izmjenama.

1.3. Adresni podaci

Financijska agencija

Registar digitalnih certifikata

10000 Zagreb

Koturaška 43

Tel: ++385 (0)1-6304367

1.3.1. Osobe za kontaktiranje u vezi s Pravilnikom

Kontakt osobe za sva pitanja i objašnjenja u svezi sa sadržajem i načinom implementacije Pravilnika su sljedeće (njihove e-mail adrese):

Fanica.Beros@fina.hr

Leopold.Eke@fina.hr

1.3.2. Osobe za kontaktiranje u vezi s CP-om i PDS-om

Kontakt osobe za sva pitanja i objašnjenja u svezi sa sadržajem i načinom implementacije i ostvarenja pretpostavki iz CP-a i PDS-a su sljedeće (njihove e-mail adrese):

Fanica.Beros@fina.hr

Leopold.Eke@fina.hr

2. DEFINICIJE

2.1. Poslovni subjekt

Poslovni subjekti za potrebe ovog Pravilnika, su

- Pravne osobe,
- Dijelovi pravnih osoba,
- Tijela državne vlasti,
- Tijela državne uprave,
- Jedinice lokalne samouprave,
- Jedinice područne (regionalne) samouprave i
- Fizičke osobe koje obavljaju registriranu djelatnost u skladu s propisima.

2.2. Subjekti u certifikatima

U FINA PKI Subjekti certifikata svrstani su u slijedeće kategorije:

- Fizička osoba (građanin)
- Poslovni subjekt - fizička osoba
- Poslovni subjekt - poslužitelj
- Poslovni subjekt - uređaj
- Poslovni subjekt - aplikacija

2.3. DN - Jedinstveno ime subjekta

CA garantira Subjektima jedinstvenost njihovog DN u dijelu javnog imenika u kojem je FINA registrirana kao organizacija. Prilikom formiranja DN Subjekta CA primjenjuje dokumentirana pravila sukladna CP-u. CA samostalno kontrolira i dodjeljuje vrijednost atributa SerialNumber, kako bi ostvario jedinstvenost imena subjekata u dijelu svog prostora javnog imenika.

2.3.1. Procedure za rješavanje sporova o imenu

FINA CA će dosljedno provoditi pravila o formiranju DN prema točkama 3.1.2. i 3.1.2.1 CP-a. Korisniku je zabranjeno tražiti imena u DN, s kojima bi vrijeđao intelektualna ili autorska prava drugih korisnika. LRA neće provjeravati prava za upotrebu takvih imena i neće posredovati u svezi tih prava. FINA zadržava pravo u bilo koje vrijeme jednostrano ukinuti ili suspendirati certifikate s imenom subjekta koji uzrokuje takav spor.

2.3.2. Prepoznavanje, autentifikacija i uloga zaštitnih znakova

Razrješava se sukladno "Procedure za rješavanje sporova o imenu".

2.3.3. Prepoznavanje, autentifikacija i uloga zaštićenih znakova

Prema 3.1.2.4. CP-a.

2.4. Tipovi certifikata

Tražitelj certifikata sam odlučuje o izboru certifikata. Uvjeti izdavanja i uporaba regulirani su CP-om, PDS-om, ovim Pravilnikom i Ugovorom o certifikatu.

CA u FINA PKI će tražiteljima prema pripadajućem CP-u izdavati slijedeće operativne certifikate:

1. Osobni (građani – fizičke osobe)
2. Poslovni (fizičke osobe povezane s poslovnim subjektom/organizacijom)
3. Poslužitelj (poslužitelj povezan s poslovnim subjektom/organizacijom)
4. Uređaj – VPN (uređaj povezan s poslovnim subjektom/organizacijom)
5. Aplikacija/servis (aplikacija/servis povezana s poslovnim subjektom/organizacijom)

2.4.1. DEMO certifikati

Subjekt sam odlučuje o korištenju DEMO certifikata, uvjeti izdavanja i uporaba regulirani su u PDS-u. Subjektima izdavat će se slijedeći DEMO certifikati:

1. DEMO osobni (građani – fizičke osobe)
2. DEMO poslovni (fizičke osobe povezane s poslovnim subjektom/organizacijom)
3. DEMO poslužiteljski (poslužitelj povezan s poslovnim subjektom/organizacijom)
4. DEMO uređaj - VPN (uređaj povezan s poslovnim subjektom/organizacijom)
5. DEMO aplikacija/servis (aplikacija/servis povezana s poslovnim subjektom/organizacijom)

2.4.2. RDC certifikati

Subjekt sam odlučuje o izboru RDC certifikata. Uvjeti izdavanja i uporaba regulirani su u Ugovoru o certifikatu. CA u FINA PKI Subjektima prema pripadajućem CP-u izdavat će slijedeće operativne certifikate:

1. RDC osobni (građani – fizičke osobe)
2. RDC poslovni (fizičke osobe povezane s poslovnim subjektom/organizacijom)
3. RDC poslužitelj (poslužitelj povezan s poslovnim subjektom/organizacijom)
4. RDC uređaj - VPN (uređaj povezan s poslovnim subjektom/organizacijom)
5. RDC aplikativni (aplikacija/servis povezana s poslovnim subjektom/organizacijom)

2.5. Profili certifikata

Profili certifikata mogu biti:

- kvalificirani, i

- normalizirani

2.5.1. Uporaba certifikata i ključeva

Korištenje kvalificiranih certifikata i ključeva u tim certifikatima u elektroničkim komunikacijama znači **neporecivost** u elektroničkim komunikacijama – **napredni elektronički potpis** prema Zakonu o elektroničkom potpisu.

Normalizirani certifikati i ključevi u tim certifikatima mogu se koristiti za potrebe **identifikacije** strane u elektroničkim komunikacijama – **elektronički potpis** prema Zakonu o elektroničkom potpisu.

FINA će izdavati i normalizirane certifikate i ključeve u tim certifikatima koji će koristiti za **enkripciju** podataka.

2.6. Razine sigurnosti

Razine sigurnosti certifikata koje izdaje CA u FINA PKI navedene su u slijedećoj tablici, kao i kratki opis prijedloga primjene u aplikacijama koje odgovaraju svakoj razini.

Razina sigurnosti	Klasa	Područje primjene
Standardna	**1**	Ova je razina je prikladna u okolinama u kojima postoje rizici i posljedice prouzrokovane kompromitiranjem podataka, ali nemaju veće značenje. To može biti pristup tajnim podacima gdje vjerojatnost zlonamjernog pristupa nije velika. U ovoj sigurnosnoj razini se podrazumijeva da je mala vjerojatnost da korisnici budu zlonamjerni.
Srednja	**2**	Ova razina je prikladna za okoline u kojima su rizici i posljedice kompromitiranja podataka umjereni. Može se koristiti u transakcijama koje imaju znatnu novčanu vrijednost ili rizik od krivotvorenja, ili u onim koje imaju pristup tajnim informacijama u kojima je vjerojatnost zlonamjernog pristupa znatna.
Visoka	**3**	Ova razina je prikladna za uporabu u transakcijama u kojima je ugroženost podataka visoka, ili su posljedice propusta u sustavu zaštite velike. To su transakcije vrlo visoke vrijednosti ili s velikim rizikom od krivotvorenja.

2.7. Temeljne karakteristike FINA PKI certifikata

OPIS KARAKTERISTIKE	Razina sigurnosti		
	Standardna	**Srednja**	**Visoka**
Period važenja (godine)	5	2	1
Osiguranje od poslovnih rizika	DA	DA	DA
SSCD	NE	DA	DA

OPIS KARAKTERISTIKE	Razina sigurnosti		
	Standardna	Srednja	Visoka
I&A			
Inicijalni I&A kod RA ili LRA	DA	DA	DA
Ponovni I&A kod RA ili LRA (godine)	5	4	3
Obnavljanje/opoziv			
Obnavljanje – automatski	DA	DA	NE
Obnavljanje – na zahtjev	DA	DA	DA
Opoziv i objava CRL-a (sati)	24	12	6

2.8. Konstrukcija OID-a za FINA PKI

Od BSI **(British Standars Institution**) ICD **(International Code Designator)** je dodjeljen OID za FINU. Za potrebe FINA PKI uvodi se slijedeća kontstrukcija OID-a:

OID polje	Atribut	Kod	Opis
FINA PKI	ISO	1	ISO
	ORG	3	ISO organizacija
	ICD	124	International Code Designator
	FINA	1104	ID za FINU prema ICD-u
	PKI	5	PKI objekti u FINI
Policy	Policy	XX	Kodiranje verzije politike 1X – RDC CP 2X – TDU CP 3X – DEMO PDS 4X – TSP
Tip	Tip certifikata	X	Kodiranje tipa certifikata
Profil	Profil	X	Kodiranje politike prema EU i korištenja SSCD
Limit	Razina sigurnosti (Preporučeni limit)	X	Kodiranje razine sigurnosti - preporučenog financijskog limita pouzdanja u certifikat

2.9. WEB i ID profili

CA sustav u FINA PKI omogućava izdavanje:

1. Standardnih certifikata koje se zovu WEB
2. ID certifikate s dva para asimetričnih ključeva (potpis i enkripciju)

EN označeni certifikati imaju KeyUsage oznaku**: Key Encipherment**, dok **DS** označeni certifikati imaju KeyUsage Oznaku: **Digital Signature**.

Profil	Namjena	Uporaba ključa		Osnovni profil	Specijalizirani profil	SSCD
		EN	DS			
WEB	Web user	X	X	RFC 2459	Promjenjivo	Izbor
	Web server	X	X	RFC 2459	Promjenjivo	Izbor
ID	Enterprise	X		RFC 2459	Promjenjivo	Izbor
			X	RFC 2459	Promjenjivo	Izbor
	Entrust aplikacija	X		RFC 2459	Entrust OID	Izbor
			X	RFC 2459	Entrust OID	
	Administration	X		RFC 2459	Entrust OID	Izbor
			X	RFC 2459	Entrust OID	
VPN	Uređaji	X		RFC 2459	IPSEC	Izbor
			X	RFC 2459	IPSEC	

2.9.1. WEB profil

2.9.1.1. Opis

Entrust sustav omogućava izdavanje standardnih certifikata koje se zovu WEB certifikati. Iz njihovog naziva proizlazi i njihova namjena, uporaba u standardnim INTERNET aplikacijama kao što su standardni pretraživači i poslužitelji:

- Microsoft Internet Explorer
- Microsoft Internet Information Server
- Netscape
- Netscape WEB server (iPlanet)
- Mozilla
- Apache WEB server (sa SSL podrškom).

U standardnoj Entrust postavi WEB certifikat je standardni X.509 v3 certifikat s Key Usage ekstenzijom Digital Signature i Key Encryption, formiran prema RFC 2459, čime se želi zadovoljiti sve PKI standardne aplikacije. Ekstenzije dodatno sadrže Subject Alternate Name potreban za podršku e-mail aplikacijama i Netscape ekstenzije koje su nužne za podršku Netscape PKI aplikacijama. Extended Key usage potreban za neke Microsoft PKI aplikacije nije definiran, ali ga je moguće jednostavno dodati.

WEB certifikati se mogu izdavati svim aplikacijama koje mogu zadati standardni PKCS#10 zahtjev za registraciju javnog ključa. Temeljem PKCS#10 WEB Enrollment server i Entrust Authority izdaju klijentu X.509 v3 certifikat.

PKCS#10 zahtjevi za izdavanje certifikata mogu se uputiti na više načina, putem sustava WEB Enrollment server ili za veliki broj slijednih zahtjeva pomoću Smart Card enrollment server-a, preko XML datoteke koja sadrži seriju PKCS#10 zahtjeva.

S obzirom da su WEB certifikati otvoreni za bilo koju PKI aplikaciju koja je poznata u današnjem PKI svijetu, zbog diverzije okruženja u kojima se PKI aplikacija može nalaziti, Entrust prepušta upravljanje ovom vrstom certifikata samoj aplikaciji. Aplikacija u srazu s Entrust sustavom treba biti u mogućnosti zatražiti certifikat pomoću PKCS#10 zahtjeva.

Dodatno treba napomenuti da Entrust sustav ne kontrolira i arhivira privatni ključ WEB certifikata, s obzirom da PKCS#10 zahtjev ne sadrži privatni ključ, nego samo javni ključ. U ovom modelu sustav ne arhivira enkripcijske ključeve za korisnika, tako da se taj model ne može koristiti za aplikacije koje izvode permanentnu enkripciju podataka u kojem treba podržati model koji bi omogućio pričuvu tajnog ključa za enkripciju.

2.9.1.2. Standardne aplikacije koje koriste Entrust WEB profil

Tip	Standardne aplikacije	Uporaba	dodatno	sučelje za registraciju
WEB klijent certifikati	MS Internet Explorer	SSL autentifikacija klijenta		PKCS#10
		S/MIME v2 zaštita E-mail-a		
	Nescape	SSL autentifikacija		PKCS#10
		S/MIME v2 zaštita E-mail-a		
	Mozilla	SSL autentifikacija		PKCS#10
		S/MIME v2 zaštita E-mail-a		
	MS Office XP	digitalni potpis Office XP datoteka i e-mail-a.		PKCS#10
	MS Crypto API aplikacije	digitalni potpis, enkripcija, autentifikacija PKCS#7		PKCS#10
	OpenSSL	sve funkcije OpenSSL uz registraciju ključeva preko PKCS#10		PKCS#10
	Općenito PKCS#10 PKI aplikacije i alati	sve aplikacije koje mogu registrirati svoje ključeve preko PKCS#10 upita		PKCS#10
	VPN klijenti (PKCS #10)	VPN klijenti	dodati OID-e za VPN	PKCS#10
	WAP klijenti	podrška za sve vrste WAP klijenata		PKCS#10

Tip	Standardne aplikacije	Uporaba	dodatno	sučelje za registraciju
WEB poslužitelj certifikati	MS ISS server	SSL autentifikacija klijenta i servera	RFC2459	PKCS#10
	Nescape (iPlanet)	SSL autentifikacija klijenta i servera	RFC2459	PKCS#10
	Apache (OpenSSL)	SSL autentifikacija klijenta i servera	RFC2459	PKCS#10
	Drugi WEB poslužitelji koji mogu registrirati svoj ključ prema PKCS#10	SSL autentifikacija klijenta i servera	RFC2459	PKCS#10

2.9.2. ID profil

2.9.2.1. Opis

Entrust ID profil čini skup sigurnosnih čimbenika koji omogućavaju korištenje dva para asimetričnih ključeva za sve vrste sigurnosnih servisa:

- Autentifikacija
- Cjelovitost
- Izvornost
- Tajnost

Korisnik upotrebljava Entrust Toolkit (aplikativni biblioteku programskih funkcija) ili Entrust Ready aplikacije kako bi na najkvalitetniji način koristio Entrust ID. Entrust ID osigurava:

1. *FIPS 140-1 level 1 konformnost programskog sustava,*
2. *automatsko održavanje životnog ciklusa kriptoloških čimbenika (transparentno za korisnika) preko PKIX-CMP protokola.*
3. *dva para asimetričnih ključeva, jedan za digitalni potpis i drugi za enkripciju,*
4. *uspostavu uniformne sigurnosne politike kod korisnika certifikata,*
5. *mogućnost sigurne enkripcije podataka temeljem sigurne središnje pohrane potpune povijesti korisničkih enkripcijskih ključeva (mogućnost key recovery-a).*

Entrust ID može omogućiti eksport svojih ključeva za Microsoft Crypto API aplikacije, međutim u tom slučaju uporaba ključeva više nije u domeni verificiranog Entrust toolkit-a i nije moguće zadovoljiti FIPS udruživost ukupnog PKI sustava. Eksport ključeva podrazumijeva napuštanje tajnog ključa izvan sigurne okoline. Novije implementacije SSCD omogućavaju paralelnu uporabu SSCD za CSP i PKCS#11 aplikacije, međutim to nije verificirano od Entrust-a pošto se sa SSCD-om rukuje u neverificiranoj programskoj okolini otpada FIPS verifikacija ukupnog PKI sustava.

2.9.2.2. Standardne aplikacije koje koriste Entrust ID profil

Tip	Standardne aplikacije	Uporaba	dodatno	sučelje za registraciju
Entrust ID	Entrust toolkit (C/C++, Visual Basic, Java) (Microsoft Windows, UNIX, OS/390)	Sve korisničke aplikacije u koje se može ugraditi funkcije iz Entrust toolkit-a.		PKIX
	Entrust Desktop aplikacije	Entelligence (S/MIME v3 funkcija na desktopu)		PKIX
		Entrust ICE (enkripcija cijelih folder-a)		PKIX
		Entrust Express (MS Outlook/Lotus Notes/Eudora) – email plug in		
		Entrust GINA Logon (PKI SSO na MS Windows stanice)		
	Entrust TruePass/ GetAccess	Entrust WEB sigurnosne aplikacije		PKIX
	Entrust Ready aplikacije	Checkpoint VPN		PKIX
		Druge Entrust Ready aplikacije (vidjeti popis na Entrust-ovom WEB-site-u)		
	Microsoft Windows 2000/XP PKI aplikacije	MS Windows 2000 PKI aplikacije podržane su temeljem "exporta" ključeva iz Entrust ID-a u Crypto API, ili registracijom Entrust ID ključeva sa smart kartice preko CSP provider-a proizvođača smart karice.		PKIX
VPN certifikati				
VPN jedan par ključeva	CISCO VPN	VPN		SCEP
	Drugi SCEP udruživi uređaji	VPN		SCEP
VPN certifikati	Uređaji koji zadaju PKCS#10 zahtjev	VPN		PKCS#10

3. OPĆI UVJETI ZA IZDAVANJE CERTIFIKATA

Način procesiranja Zahtjeva za izdavanje certifikata (u daljnjem tekstu Zahtjev) i pripadajuće dokumentacije ovisit će o vrsti traženog certifikata.

3.1. Dokumentacija

Tražitelj certifikata, fizika osoba – građanin ili poslovni subjekt za dobivanje certifikata od FINA PKI mora podnijeti slijedeću dokumentaciju:

1. Zahtjev za izdavanje certifikata
2. Potpisani ugovor o certifikatu ili izjava o prihvaćanju uvjeta u PDS-u za DEMO certifikate
3. ID dokument i/ili dokumentaciju za utvrđivanje:
   - identiteta fizičke osobe – građanina, ili
   - pravnog subjektiviteta / identiteta poslovnog subjekta

3.2. Korisnički računi

Otvaranje korisničkog računa je dio registracijskog procesa novog tražitelja certifikata ili subjekta u certifikatu u FINA PKI.

3.2.1. Fizičke osobe - građani

3.2.1.1. Korisnički računi

Korisnički računi koji se otvaraju fizičkim osobama – građanima sadrže slijedeće skupine podataka:

1. Opći podaci o korisničkom računu
2. ID organizacijske jedinice LRA i LRA zaposlenika
3. Podaci o korisniku
4. Način bezgotovinskog plaćanja izvršenih usluga

3.2.2. Poslovni subjekti

3.2.2.1. Korisnički računi

Korisnički računi koji se otvaraju poslovnim subjektima sadrže slijedeće skupine podataka:

1. Opći podaci o korisničkom računu
2. ID organizacijske jedinice LRA i LRA zaposlenika
3. Podaci o poslovnom subjektu
4. Način bezgotovinskog plaćanja izvršenih usluga

3.2.2.2. Korisnički podračuni

Krajnji korisnici certifikata koji se izdaju poslovnim subjektima su:

1. Zaposlenici poslovnog subjekta/pripadajuće osobe ovlašteni za potpisivanje
2. Aplikacije, poslužitelji i uređaji (VPN)

Za potrebe evidentiranja ovih subjekata otvaraju se korisnički podračuni tipa 1 i 2.

3.3. Identifikacija tražitelja certifikata

3.3.1. Fizičke osobe - građani

Državljani RH kao identifikacijski dokument mogu koristiti osobnu iskaznicu ili putovnicu. Ako je osoba strani državljanin, identifikacija se vrši putovnicom ili Europskom iskaznicom (Europskom identifikacijskom karticom). Prilikom identifikacije provjerava se sljedeće:

- država izdavanja dokumenta,
- broj dokumenta,
- datum i mjesto izdavanja, i
- rok važenja

3.3.2. Poslovni subjekti

Poslovni subjekti ovisno o zakonima i propisima u RH koje reguliraju obavljanje određenih aktivnosti prilažu slijedeću dokumentaciju za utvrđivanje pravnog subjektiviteta i identiteta:

1. ***Registracija poslovne djelatnost (upis u registar sukladno zakonima i propisima u RH)***
2. ***Obavijest Državnog zavoda za statistiku o razvrstavanju po NKD radi preuzimanja šifre djelatnosti i matičnog broja***

3.4. Dodatna provjera točnosti identifikacijskih podataka

FINA zadržava diskreciono pravo da dodatno provjeri točnost identifikacijskih podataka koji su prezentirani i upisani u Zahtjev. Provjera će se izvršiti temeljem rezidentnih podatka o fizičkoj osobi i/ili poslovnom subjektu koje posjeduje FINA ili neka druga organizacija.

4. CERTIFIKATI ZA FIZIČKE OSOBE

4.1. Zahtjev za izdavanje osobnog certifikata

Zahtjev za izdavanje osobnog certifikata (dalje u tekstu: Zahtjev) je pisani zahtjev fizičke osobe – građanina, i podnosi se na propisanom obrascu u dva primjerka (nalazi se na WEB stranicama FINE na adresi: **http://demo-pki.fina.hr/**.... OBRASCI). Tražitelju se vraća jedan primjerak Zahtjeva s potvrdom datuma primitka. Fizičke osobe – građani podnose Zahtjev u podružnici FINE na čijem je području prebivalište fizičke osobe. Specifikacija traženog certifikata je sastavni dio Zahtjeva.

Građanin Zahtjev i specifikaciju traženog certifikata vlastoručno potpisuje i time potvrđuje istinitost podataka u Zahtjevu i specifikaciji.

LRA zaposlenik FINE zadužen za ove poslove, zaprima Zahtjev i provjerava ispravnost Zahtjeva i potpunost priložene dokumentacije.

4.2. Ugovor o certifikatu

NAPOMENA:

Odnosi se samo na izdavanje RDC certifikata.

Na tipski Ugovor o RDC certifikatu (nalazi se na WEB stranicama FINE na adresi: **http://demo-pki.fina.hr/**.... UGOVORI), fizička osoba - građanin stavlja samo vlastoručni potpis.

4.3. Dokumentacija za utvrđivanje identiteta

Vjerodostojnost podataka iz Zahtjeva podnositelj zahtjeva fizička osoba – građanin dokazuje identifikacijskom ispravom. Podaci iz identifikacijske isprave moraju u potpunosti odgovarati podacima iz Zahtjeva.

4.4. Odbijanje Zahtjeva

Utvrdi li se da nisu ispunjeni uvjeti za izdavanje certifikata, Zahtjev s priloženom dokumentacijom vraća se podnositelju uz usmeno obrazloženje. Razlozi za odbijanje zahtjeva mogu biti:

- nepotpunost ili neispravnost priložene dokumentacije
- neslaganje podataka o tražitelju s podacima iz dokumentacije Zahtjeva, ili
- drugi razlozi

5. I&A I DN - OSOBNI CERTIFIKATI

5.1. I&A

I&A procedure za osobne certifikate, mogu biti:

1. **Licem u lice**: Ova se metoda preferira u FINA PKI i biti će upotrebljavana u najvećem broju slučajeva. LRA zaposlenik će provjeriti identifikacijski dokument fizičke osobe - građanina. Državljani RH kao dokument za identifikaciju mogu koristiti osobnu iskaznicu ili putovnicu. Ako je osoba strani državljanin, identifikacijski dokument može biti putovnica ili Europska iskaznica (Europska identifikacijska kartica).

ALTERNATIVA – primjenjuje se samo po odobrenju PMA FINA PKI

2. **Shared secret** (zajednička tajna): Ova metoda će biti upotrebljavana u slučajevima kada je tražitelj na udaljenoj lokaciji i LRA zaposlenik je već ranije uspostavio poslovni odnos s tražiteljem. LRA zaposlenik će autentificirati tražitelja zahtijevajući od njega neku neobjavljenu informaciju (npr. broj korisničkog računa u registru korisnika FINA PKI, JMBG ili neki drugi ID broj), koju će LRA zaposlenik nakon toga provjeriti.
3. **Treća strana sa valjanim PKI ključem**: Ova metoda će se koristi u slučaju kada je tražitelj na udaljenoj lokaciji i LRA zaposlenik nema ranije uspostavljen poslovni odnos sa tražiteljem, ali ima ranije uspostavljeni poslovni odnos sa autoritetom kojem se tražitelj obraća. LRA zaposlenik će autentificirati tražitelja jer je treća strana provela identifikaciju tražitelja **"licem u lice"**.

5.2. DN

Jedinstveno ime subjekta (DN)

1. Prezime i ime
2. Serijski broj

6. CERTIFIKATI ZA POSLOVNE SUBJEKTE

6.1. Zahtjev za izdavanje certifikata

Zahtjev je pisani zahtjev tražitelja (poslovnog subjekta) i podnosi se na propisanom obrascu (nalazi se na WEB stranicama FINE na adresi: **http://demo-pki.fina.hr/**.... OBRASCI) u dva primjerka. Tražitelju se vraća jedan primjerak Zahtjeva s potvrdom datuma primitka. Poslovni subjekti i njihovi dijelovi podnose Zahtjev u podružnici FINE na čijem je području sjedište poslovnog subjekta ili dijela poslovnog subjekta. Specifikacija traženog certifikata je sastavni dio Zahtjeva. Zahtjev uz pečat potpisuje osoba ovlaštena za zastupanje i time potvrđuje istinitost podataka u Zahtjevu.

6.1.1. Fizičke osobe koje obavljaju registriranu djelatnost za koji nije potreban poslovni prostor

Ukoliko za obavljanje registriranog obrta odnosno registrirane djelatnosti nije potreban poslovni prostor, fizička osoba podnosi Zahtjev u podružnici FINE na čijem području je prebivalište fizičke osobe. Vjerodostojnost podataka o prebivalištu podnositelj Zahtjeva dokazuje davanjem na uvid identifikacijske isprave. Podaci iz identifikacijske isprave moraju u potpunosti odgovarati podacima iz Zahtjeva i dokumentacije priložene zahtjevu.

6.1.2. Osoba ovlaštena za zastupanje

Na Zahtjev i specifikaciju traženih certifikata uz pečat potpisuje se osoba ovlaštena za zastupanje i time potvrđuje istinitost podataka u obrascu. Ako je rješenjem o upisu poslovnog subjekta u nadležni registar više osoba određeno za samostalno i pojedinačno zastupanje, specifikaciju traženih certifikata potpisuje osoba ovlaštena za takvo zastupanje. Ako je više osoba određeno za zajedničko zastupanje, Zahtjev i specifikaciju traženih certifikata potpisuje jedna od njih uz pisanu suglasnost ostalih ovlaštenika. Ako je više osoba određeno za zastupanje od kojih neke samostalno i pojedinačno, a druge zajednički, Zahtjev i specifikaciju traženih certifikata može potpisati:

- osoba određena za samostalno i pojedinačno zastupanje ili
- jedna od osoba određenih za zajedničko zastupanje uz pisanu suglasnost ostalih ovlaštenika.

Tekst pečata mora biti istovjetan tekstu naziva tražitelja upisanog u registar u punom ili skraćenom nazivu.

Zaposlenik FINE iz rješenja o upisu u registar odnosno drugog akta ako upis u registar nije propisan utvrđuje da li je osoba koja je uz pečat potpisala Zahtjev i specifikaciju traženih certifikata osoba ovlaštena za zastupanje.

6.2. Ugovor o certifikatu

NAPOMENA:

Odnosi se samo na izdavanje RDC certifikata.

Tipski Ugovor o RDC certifikatu (nalazi se na WEB stranicama FINE na adresi: **http://demo-pki.fina.hr/**.... UGOVORI), uz pečat potpisuje osoba ovlaštena za zastupanje.

6.3. Dokumentacija za utvrđivanje pravnog subjektiviteta (identiteta) poslovnog subjekta

Dokumentacijom potrebnom za utvrđivanje pravnog subjektiviteta utvrdit će se valjanost identiteta podnositelja Zahtjeva i ocijeniti da li tražitelj ispunjavanja sve zakonske i ostale uvjete za dobivanje traženog certifikata.

Uz Zahtjev tražitelj – poslovni subjekt prilaže dokumentaciju:

- rješenje o upisu u nadležni registar, ako je upis u registar propisan, ili
- zakon odnosno drugi propis temeljem kojeg je tražitelj osnovan ako nije određeno da se upisuje u registar;
- Obavijest Državnog zavoda za statistiku o razvrstavanju prema Nacionalnoj klasifikaciji djelatnosti (NKD) i o matičnom broju

6.3.1. Rješenje o upisu u registar

Pod rješenjem o upisu u registar razumijeva se rješenje o upisu u registar kojega vodi sud ili organ odnosno tijelo uprave (u daljnjem tekstu: Rješenje o upisu u registar).

Rješenje o upisu u registar podnose uz Zahtjev svi tražitelji koji su prema propisima dužni upisati se u registar.

Ako je tražitelj organizacijski dio poslovnog subjekta, prilaže rješenje o upisu u registar dijela poslovnog subjekta.

Rješenje se podnosi u izvorniku ili preslici ovjerenoj od nadležnog organa na zakonom propisani način (javnobilježnička ovjera ili ovjera mjerodavnog tijela države sjedišta poslovnog subjekta).

6.3.2. Zakon ili drugi propis temeljem kojeg je korisnik osnovan

Tražitelj koji je osnovan po zakonu ili drugom propisu uz Zahtjev prilaže presliku zakona ili drugog propisa objavljenog u Narodnim novinama ako nije određeno da se upisuje u registar.

6.3.3. Obavijest o razvrstavanju i matični broj

Državni zavod za statistiku daje Obavijest o razvrstavanju prema Nacionalnoj klasifikaciji djelatnosti i dodjeljuje matični broj.

Fizičkim osobama koje obavljaju registriranu djelatnost sukladno propisima, uključujući i osobe koje obavljaju registriranu djelatnost kao slobodno zanimanje (liječnici, stomatolozi, ljekarnici i drugi koji se upisuju u registar ili imenik strukovne komore), Državni zavod za statistiku posredstvom mjerodavnog tijela dodjeljuje matični broj.

6.4. Odbijanje Zahtjeva

Utvrdi li se da nisu ispunjeni uvjeti za izdavanje certifikata, Zahtjev s priloženom dokumentacijom vraća se tražitelju uz usmeno obrazloženje. Razlozi za vraćanje zahtjeva mogu biti:

- nepotpunost ili neispravnost priložene dokumentacije
- neslaganje podataka o tražitelju s podacima iz dokumentacije Zahtjeva
- da osoba koja je potpisala Zahtjev i specifikaciju traženih certifikata nije ovlaštena za zastupanje, i
- drugi razlozi

7. I&A I DN - CERTIFIKATI ZA POSLOVNE SUBJEKTE

7.1. Poslovni certifikati - I&A i DN

7.1.1. I&A - Korak 1.

Poslovni subjekti ovisno o zakonima i propisima u RH koje reguliraju registraciju poslovne aktivnosti uz zahtjev za izdavanje certifikata prilažu dokumentaciju o pravnom subjektivitetu i identitetu.

7.1.1.1. I&A za poslovne subjekte koji se upisuju u trgovački registar

Zahtjev potpisuje osoba ovlaštena za zastupanje. Uz zahtjev se prilaže:

- rješenje o upisu u registar
- obavijest o razvrstavanju poslovnog subjekta

Dijelovi poslovnog subjekta koji se upisuju u trgovački registar

Zahtjev potpisuje osoba ovlaštena za zastupanje. Uz zahtjev se prilaže:

- rješenje o upisu dijela pravne osobe u registar
- obavijest o razvrstavanju poslovnog subjekta

7.1.1.2. I&A za poslovne subjekte koji su osnovani temeljem propisa

Tijela državne uprave i tijela jedinice lokalne samouprave i uprave i udruge

Zahtjev potpisuje osoba ovlaštena za zastupanje. Uz zahtjev se prilaže:

- akt nadležnog organa o osnivanju poslovnog subjekta odnosno dijela poslovnog subjekta odnosno rješenje o upisu u registar ili presliku propisa po kojem je poslovni subjekt osnovan;
- obavijest o razvrstavanju

Fond osnovan zakonom

Zahtjev potpisuje osoba ovlaštena za zastupanje. Uz Zahtjev se prilaže:

- akt o osnivanju, ugovor odnosno presliku propisa kojim je fond osnovan;
- obavijest o razvrstavanju

7.1.1.3. I&A za poslovne subjekte koji se upisuju u registar organa uprave

Zahtjev potpisuje osoba ovlaštena za zastupanje. Uz Zahtjev se prilaže:

- rješenje o upisu u registar
- obavijest o razvrstavanju

Dijelovi poslovnog subjekta koji se upisuju u registar organa uprave

Zahtjev potpisuje osoba ovlaštena za zastupanje. Uz Zahtjev se prilaže:

- akt o upisu dijela organizacije u registar, i
- obavijest o razvrstavanju poslovnog subjekta

7.1.1.4. I&A za organizacije koje se ne upisuju u registar

Zahtjev potpisuje osoba ovlaštena za zastupanje, uz koji se prilaže:

- obavijest o razvrstavanju (za vjerske zajednice)

7.1.1.5. I&A za fizičke osobe koji imaju registrirani obrt odnosno obavljaju registriranu djelatnost

Zahtjev potpisuje fizička osoba koja ima registrirani obrt odnosno obavlja registriranu djelatnost. Uz Zahtjev se prilaže:

- rješenje o upisu u registar nadležnog organa ili
- ugovor o kooperativnoj suradnji;

Ako je navedeno da više osoba obavlja registrirani obrt odnosno registriranu djelatnost, zahtjev potpisuje jedna od njih koju odrede ugovorom ili izjavom o zajedničkom obavljanju obrta odnosno djelatnosti koju svi vlastoručno potpisuju..

7.1.1.6. I&A za javnog bilježnika

Zahtjev potpisuje fizička osoba – javni bilježnik i prilaže:

- rješenje Ministarstva pravosuđa RH o imenovanju javnog bilježnika

Zahtjev potpisuje javni bilježnik uz otisak službenog pečata. U **DN** upisuje se prezime i ime javnog bilježnika i naziv "**javni bilježnik**".

7.1.2. I&A - Korak 2.

Fizičke osobe u kvalificiranom poslovnom certifikatu su osobe ovlaštene za potpisivanje. I&A za osobu u kvalificiranom poslovnom certifikatu može se obaviti na jedan od sljedećih načina:

1. **Licem u lice**: Ova se metoda preferira u FINA PKI i biti će upotrebljavana u najvećem broju slučajeva. LRA zaposlenik će provjeriti identifikacijski dokument fizičke osobe - građanina. Državljani RH kao dokument za identifikaciju mogu koristiti osobnu iskaznicu ili putovnicu. Ako je osoba strani državljanin, identifikacijski dokument može biti putovnica ili Europska iskaznica (Europska identifikacijska kartica).

ALTERNATIVA – primjenjuje se samo po odobrenju PMA FINA PKI

2. **Shared secret** (zajednička tajna): Ova metoda će biti upotrebljavana u slučajevima kada je tražitelj na udaljenoj lokaciji i LRA zaposlenik je već ranije uspostavio poslovni odnos s tražiteljem. LRA zaposlenik će autentificirati tražitelja zahtijevajući od njega neku neobjavljenu informaciju (npr. broj korisničkog računa u registru korisnika FINA PKI, JMBG ili neki drugi ID broj), koju će LRA zaposlenik nakon toga provjeriti.

3. **Treća strana sa valjanim PKI ključem**: Ova metoda će se koristi u slučaju kada je tražitelj na udaljenoj lokaciji i LRA zaposlenik nema ranije uspostavljen poslovni odnos sa tražiteljem, ali ima ranije uspostavljeni poslovni odnos sa autoritetom kojem se tražitelj obraća. LRA zaposlenik će autentificirati tražitelja jer je treća strana provela identifikaciju tražitelja **"licem u lice"**.

7.1.3. DN

Jedinstveno ime subjekta (DN)

1. Naziv poslovnog subjekta i naziv dijela poslovnog subjekta
2. Matični broj
3. Prezime i ime osobe
4. Serijski broj

7.2. Certifikati za poslužitelje, uređaje (VPN) ili aplikacije – I&A i DN

Zahtjev za certifikat u kojem je subjekt poslovni subjekt i poslužitelj, uređaj (VPN) ili aplikacija može podnijeti samo osoba ovlaštena za zastupanje.

7.2.1. I&A - Korak 1.

Jednako kao i za poslovni certifikat.

7.2.2. I&A - Korak 2.

7.2.2.1. I&A skrbnika

Skrbnik je fizička osoba koju je osoba ovlaštena za zastupanje poslovnog subjekta ovlastila za upravljanje certifikatima za poslužitelje, uređaje (VPN) ili aplikacije tog poslovnog subjekta. I&A za osobe u ulozi skrbnika se može obaviti na jedan od sljedećih načina:

1. **Licem u lice**: Ova se metoda preferira u FINA PKI i biti će upotrebljavana u najvećem broju slučajeva. LRA zaposlenik će provjeriti identifikacijski dokument fizičke osobe - građanina. Državljani RH kao dokument za identifikaciju mogu koristiti osobnu iskaznicu ili putovnicu. Ako je osoba strani državljanin, identifikacijski dokument može biti putovnica ili Europska iskaznica (Europska identifikacijska kartica).

ALTERNATIVA – primjenjuje se samo po odobrenju PMA FINA PKI

2. **Shared secret** (zajednička tajna): Ova metoda će biti upotrebljavana u slučajevima kada je tražitelj na udaljenoj lokaciji i LRA zaposlenik je već ranije uspostavio poslovni odnos s tražiteljem. LRA zaposlenik će autentificirati tražitelja zahtijevajući od njega neku neobjavljenu informaciju (npr. broj korisničkog računa u registru korisnika FINA PKI, JMBG ili neki drugi ID broj), koju će LRA zaposlenik nakon toga provjeriti.
3. **Treća strana sa valjanim PKI ključem**: Ova metoda će se koristi u slučaju kada je tražitelj na udaljenoj lokaciji i LRA zaposlenik nema ranije uspostavljen poslovni odnos sa

tražiteljem, ali ima ranije uspostavljeni poslovni odnos sa autoritetom kojem se tražitelj obraća. LRA zaposlenik će autentificirati tražitelja jer je treća strana provela identifikaciju tražitelja **"licem u lice"**.

7.2.3. I&A - Korak 3.

7.2.3.1. I&A za poslužitelje, uređaje (VPN) ili aplikacije

Poslovni subjekt mora imati pravo na IP adresu, domenu ili aplikaciju za koje zahtjeva izdavanje certifikata. CA to neće provjeravati niti posredovati u mogućim sporovima. CA će opozvati ili suspendirati certifikat koji je predmet spora.

7.2.4. DN

Za imena javno dostupnih poslužitelja ili uređaja, DN se formira iz njihovog registriranog DNS imena, koje se smatra jedinstvenim s obzirom na INTERNET DNS ime. Za uređaj koji nema registrirano DNS ime, za DN će se uzeti javno registrirana (INTERNET) IP adresa.

Za imena poslužitelja ili uređaja koji se registriraju u lokalnim i privatnim mrežama, DN se formira prema dogovorenom obrascu, koji mora sadržavati naziv poslovnog subjekta u DN.

7.2.4.1. Poslužitelj

1. Naziv poslovnog subjekta i naziv dijela poslovnog subjekta
2. Matični broj
3. Registrirano ime domene

7.2.4.2. Uređaj

1. Naziv poslovnog subjekta i naziv dijela poslovnog subjekta
2. Matični broj
3. Registrirana IP adresa

7.2.4.3. Aplikacija

1. Naziv poslovnog subjekta i naziv dijela poslovnog subjekta
2. Matični broj
3. Naziv aplikacije
4. Serijski broj

8. OPĆA PRAVILA O ODRŽAVANJU INFORMACIJA O KORISNIKU

Korisnici FINA PKI, fizičke osobe - građani i poslovni subjekti imaju obvezu prema Zakonu o elektroničkom potpisu, prijaviti sve nastale statusne i druge promjene, koje utječu na već izdani certifikat i o tome priložiti propisanu dokumentaciju radi ažuriranja tih promjena u Registru korisnika i certifikata FINA PKI.

8.1. Zahtjev za promjenu

Korisnici FINA PKI, promjene dostavljaju u LRA, HELP DESK ili RA, nakon ispunjavanja obrasca **"Zahtjev za promjenu" (**nalazi se na WEB stranicama FINA PKI na adresi: **http://demo-pki.fina.hr/**.... OBRASCI).

Ako je **Zahtjev za promjenu** zaprimio LRA, nakon provjere valjanosti zahtjeva prosljeđuje ga standardnim kanalima u RA.

Ako je **Zahtjev za promjenu** zaprimio HELP DESK, nakon provjere valjanosti zahtjeva prosljeđuje ga standardnim kanalima u RA.

Ako je **Zahtjev za promjenu** zaprimio RA, nakon provjere valjanosti zahtjeva provodi instrukcije u zahtjevu.

8.2. Održavanje informacija o korisnicima osobnih certifikata

Za ažurno vođenje informacija u Registru korisnika FINA PKI, potrebno je da korisnici osobnih certifikata dostave informacije o promjeni:

1. Prezimena i/ili imena
2. Prebivališta i/ili kontakt informacija

8.2.1. Promjena prezimena i/ili imena

Promjenu prezimena i/ili imena fizička osoba dokazuje podnošenjem na uvid identifikacijskog dokumenta, odnosno drugog dokumenta u koji je nadležni organ unio takve podatke.

Promjena prezimena i/ili imena, ima za posljedicu opoziv izdanog osobnog certifikata i izdavanje novog osobnog certifikata.

8.2.2. Promjena prebivališta i/ili kontakt informacija

8.2.2.1. Promjena prebivališta

Promjenu prebivališta fizička osoba dokazuje podnošenjem na uvid identifikacijskog dokumenta, odnosno drugog dokumenta, u koju je nadležni organ unio takve podatke.

Promjena prebivališta nema za posljedicu opoziv izdanog osobnog certifikata.

8.2.2.2. Promjena kontakt informacija

Promjena kontakt informacija odnose na promjenu:

1. Broja telefona i/ili
2. Broja telefaksa-a i/ili
3. e-mail adrese

Promjena kontakt informacija nema za posljedicu opoziv izdanog osobnog certifikata.

8.3. Održavanje informacija o korisnicima poslovnih, poslužiteljskih, VPN i aplikativnih certifikata

Za ažurno vođenje informacija u Registru FINA PKI, potrebno je da korisnici - poslovni subjekti dostave informacije o promjeni:

1. U organizaciji odnosno pravnom statusu;
2. Tvrtke odnosno naziva;
3. Sjedišta;
4. Djelatnosti;
5. Osobe ovlaštene za zastupanje;
6. Osobe ovlaštene za potpisivanje;
7. Osobe u ulozi skrbnika;
8. Atributa identifikacije poslužitelja, uređaja (VPN) ili aplikacije
   - Ime domene
   - IP adresa
   - Naziv i e-mail adresa aplikacije
9. Kontakt informacija.

8.3.1. Promjena organizacije odnosno pravnog statusa

Promjenu organizacije odnosno pravnog statusa poslovni subjekt dokazuje rješenjem o upisu promjene u nadležni registar u koji je upisan. Ako se poslovni subjekt ne upisuje se u registar, promjena se dokazuje odlukom osnivača odnosno poslovnog subjekta.

Promjena organizacije odnosno pravnog statusa poslovnog subjekta ima za posljedicu opoziv izdanih certifikata i izdavanje novih.

8.3.2. Promjena tvrtke (naziva poslovnog subjekta)

Promjenu tvrtke poslovni subjekt dokazuje rješenjem o upisu promjene u nadležni registar. Ako se poslovni subjekt ne upisuje u registar, promjena se dokazuje odlukom osnivača odnosno poslovnog subjekta.

Promjena tvrtke (naziva poslovnog subjekta) ima za posljedicu opoziv izdanih certifikata i izdavanje novih.

8.3.3. Promjena sjedišta

Poslovni subjekt može tijekom rada promijeniti sjedište (mjesto i adresu). Promjenu sjedišta poslovni subjekt dokazuje rješenjem o upisu promjene u registar. Ako se poslovni subjekt ne upisuje u registar, promjena se dokazuje odlukom osnivača odnosno poslovnog subjekta. Zahtjev za promjenu potpisuje osoba ovlaštena za zastupanje.

Promjena sjedišta poslovnog subjekta nema za posljedicu opoziv izdanih certifikata.

8.3.4. Promjena djelatnosti

Poslovni subjekt može tijekom poslovanja promijeniti djelatnost. Upis nove djelatnosti poslovni subjekt dokazuje rješenjem o upisu u nadležni registar i Obaviješću Državnog zavoda za statistiku. Zahtjev za promjenu potpisuje osoba ovlaštena za zastupanje.

U slučaju promjene djelatnosti poslovnog subjekta potrebno je opozvati izdane certifikate i izdati nove certifikate.

8.3.5. Promjena osobe ovlaštene za zastupanje

Poslovni subjekt može tijekom poslovanja mijenjati osobe ovlaštene za zastupanje. Promjenu osobe ovlaštene za zastupanje poslovni subjekt dokazuje rješenjem o upisu promjene u nadležni registar. Ako se poslovni subjekt ne upisuje u registar, promjena osobe ovlaštene za zastupanje dokazuje se odlukom osnivača odnosno poslovnog subjekta. Zahtjev za promjenu potpisuje osoba koja je ovlaštena za zastupanje u času podnošenja Zahtjeva za promjenu.

Promjena osobe ovlaštene za zastupanje nema za posljedicu opoziv izdanih certifikata.

8.3.6. Promjena osobe ovlaštene za potpisivanje

Poslovni subjekt može tijekom poslovanja mijenjati osobe ovlaštene za potpisivanje. Zahtjev za promjenu potpisuje osoba ovlaštena za zastupanje.

U slučaju promjene osobe ovlaštene za potpisivanje potrebno je opozvati izdani poslovni certifikat.

8.3.7. Promjena skrbnika

Poslovni subjekt može mijenjati osobe u ulozi skrbnika. Zahtjev za promjenu potpisuje osoba ovlaštena za zastupanje.

Promjena osobe u ulozi skrbnika nema za posljedicu opoziv izdanih certifikata.

8.3.8. Promjena atributa za identifikaciju poslužitelja, uređaja (VPN) ili aplikacije

Poslovni subjekt može mijenjati slijedeće atribute identifikacije za poslužitelje, uređaje ili aplikacije:

1. Registrirano ime domene
2. Registrirana IP adresa
3. Naziv i e-mail adresa aplikacije

Zahtjev za promjenu potpisuje osoba ovlaštena za zastupanje.

U slučaju promjene ovih atributa potrebno je opozvati izdani certifikat i izdati novi.

8.3.9. Promjena kontakt informacija

Osobe za kontakt su:

1. Osobe ovlaštene za zastupanje
2. Osobe ovlaštene za potpisivanje, i
3. Osobe u ulozi skrbnika (poslužitelja, uređaja ili aplikacije)

Promjena kontakt informacija odnose na promjenu:

1. Broja telefona; i/ili
2. Broja telefax-a; i/ili
3. e-mail adrese

Zahtjev za promjenu potpisuje osoba ovlaštena za zastupanje.

Promjena kontakt informacija nema za posljedicu opoziv izdanog certifikata.

9. PROCEDURE UPRAVLJANJA ŽIVOTNIM CIKLUSOM CERTIFIKATA

NAPOMENA:

Postupci pod 2., 3., 4. i 5. se ne primjenjuju za DEMO certifikate.

Zadaće organizacijskih dijelova u FINA PKI po ovim poslovima su:

1. Inicijalno izdavanje certifikata
   - Varijanta I.
   - Varijanta II.
2. Obnova certifikata i ključeva
3. Vraćanje ključeva
4. Opoziv certifikata
5. Suspenzija certifikata

Točke koje slijede će opisati svaku od ovih aktivnosti i definirati postupke korisnika FINA PKI i postupke i odgovornosti LRA i RA u tim aktivnostima.

9.1. Inicijalno izdavanje certifikata

9.1.1. Varijanta I.

Postupci po ovoj varijanti inicijalnog izdavanja certifikata su:

1. Zaprimanje i obrada zahtjeva u LRA FINA PKI
2. I&A u LRA FINA PKI (i alternativna rješenja)
3. Upis tražitelja certifikata u Registar korisnika FINA PKI
4. Odobravanje zahtjeva i generiranje aktivacijskih (inicijalizacijskih) podataka
5. Distribucija aktivacijskih (inicijalizacijskih) podataka
6. Isporuka aktivacijskog koda
7. Generiranje certifikata i ključeva
8. Provedba sigurnosnih postupaka
9. Objava certifikata u imeniku

9.1.1.1. Korak 1. - Zaprimanje i obrada Zahtjeva

Zaprimanje i obrada Zahtjeva obavlja se prema točki 3., 4. ili 6. ovog Pravilnika.

9.1.1.2. Korak 2. - I&A

I&A ovisno o vrsti traženog certifikata obavlja se prema točki 5. ili 7. ovog Pravilnika.

9.1.1.3. Korak 3. - Upis tražitelja certifikata u Registar korisnika FINA PKI

Upis tražitelja certifikata u Registar korisnika FINA PKI je administrativni tehnički proces koji pokreće procese kreiranja digitalnog identiteta korisnika.

Informacije potrebne za upis u Registar korisnika FINA PKI (RKPKI) nalaze se u internom dokumentu "Uputa o Registru korisnika FINA PKI".

9.1.1.4. Korak 4. – Odobravanje zahtjeva i generiranje aktivacijskih (inicijalizacijskih) podataka

1. RA Administrator provjerava informacije o korisniku.
2. RA Administrator dodaje korisnika u X.500 imenik i kreira aktivacijske podatke.
3. Aktivacijski podaci se sastoje od referentnog broja i autorizacijskog koda. Oba su potrebna za generiranje certifikata i privatnog ključa korisnika:

9.1.1.5. Korak 5. – Distribucija aktivacijskih (inicijalizacijskih) podataka

1. Referentni broj se šalje elektroničkom poštom direktno korisniku
2. Autorizacijski kod se enkriptira i dostavlja se u LRA, ili
3. Autorizacijski kod se štampa u zatvorenu kovertu i šalje se preporučenom poštom na adresu korisnika

9.1.1.6. Korak 6. - Isporuka autorizacijskog koda u LRA

1. LRA prima dio aktivacijskih podataka (autorizacijski kod) za novog korisnika
2. LRA dekriptira autorizacijski kod za novog korisnika
3. LRA obavještava korisnika da može preuzeti autorizacijski kod
4. LRA mora identificirati korisnika prije predaje autorizacijskog koda. Za provjeru identiteta LRA zaposlenik koristi istu metodu koju je koristio pri koraku 2 "I&A PROCEDURE".
5. Nakon potvrde identiteta LRA zaposlenik predaje korisniku autorizacijski kod kojeg će korisnik koristiti kod generiranja ključeva i certifikata.
6. U slučaju da je treća strana izvršila provjeru identiteta korisnika, LRA zaposlenik će enkriptirati i poslati autorizacijski kod trećoj strani, koja će dekriptirati autorizacijski kod, ponovo identificirati korisnika i predati mu autorizacijski kod.

9.1.1.7. Korak 7. - Generiranje certifikata i ključeva

1. Upute za preuzimanje certifikata nalaze se na WEB stranicama FINE na adresi: http://demo-pki.fina.hr/.... **UPUTE O PREUZIMANJU CERTIFIKATA**. Korisnik također dobiva uputu putem elektroničke pošte, pri dostavi referentnog broja za preuzimanje certifikata. Upute su podložne promjenama u skladu sa promjenama FINA PKI sustava i nisu sastavni dio ovog Pravilnika. Za uspješno preuzimanje certifikata mjerodavna je zadnja verzija ovih uputa. Korisnicima se naglašava u ugovoru o certifikatu da ukoliko ne obavijeste CA/RA o problemima ili greškama u certifikatu u razumnom vremenu nakon prihvaćanja certifikata, oni prihvaćaju certifikat, jamče točnost njegovog sadržaja i suglasni su sa obvezama iz UGOVORA odnosno iz PDS-a za DEMO certifikate.

2. Korisnik koristi referentni broj koji je dobio od RA elektroničkom poštom i autorizacijski kod koji je dobio od LRA ili putem preporučene pošte od RA za generiranje ključeva. Da bi se to postiglo, Entrust klijent SW na njegovoj radnoj stanici mora biti na siguran način povezan s CA u FINA PKI. Referentni broj i autorizacijski kod se mogu koristiti samo jednom u roku od **pet radnih** dana.
3. Postupak preuzimanja certifikata ovisan je o tipu certifikata:
   - FINA ID (Enterprise) certifikati se preuzimaju i registriraju preko PKIX-CMP protokola i pomoću pripadajuće aplikacije i u skladu sa postupkom za preuzimanje Enterprise certifikata
   - FINA WEB certifikati se preuzimaju i registriraju pomoću WEB aplikacije u skladu s postupkom preuzimanja WEB certifikata

9.1.1.8. Korak 8 – Preporučeni sigurnosni postupci za korisnika

1. Fizičke kopije (tiskane na papiru) autorizacijskog koda moraju biti uništene.
2. Korisnik kopira svoje privatne ključeve i/ili svoje lozinke i osigurava ih prema svojoj sigurnosnoj politici.

9.1.1.9. Korak 9 – Objava certifikata

Po preuzimanju certifikata od korisnika, isti se objavljuje u javnom imeniku.

9.1.2. Varijanta II.

NAPOMENA:

Ovaj se postupak primjenjuje samo za osobne i poslovne certifikate.

Postupci po ovoj varijanti inicijalnog izdavanja certifikata su:

1. Zaprimanje i obrada zahtjeva u LRA FINA PKI (i alternativna rješenja)
2. I&A u LRA FINA PKI (i alternativna rješenja)
3. Upis tražitelja certifikata u Registar korisnika FINA PKI
4. Odobravanje zahtjeva i generiranje certifikata
5. Distribucija Smart kartica i PIN-ova

9.1.2.1. Korak 1. - Zaprimanje i obrada Zahtjeva

Kao i za varijantu I.

9.1.2.2. Korak 2. - I&A

Kao i za varijantu I.

9.1.2.3. Korak 3. - Upis tražitelja certifikata u Registar korisnika FINA PKI

Kao i za varijantu I.

9.1.2.4. Korak 4. – Odobravanje zahtjeva i generiranje certifikata

1. RA Administrator provjerava informacije o korisniku.
2. RA Administrator dodaje korisnika u X.500 imenik i kreira aktivacijske podatke.
3. Aktivacijske podatke preuzima CMS sustav i generira certifikat i ključeve na Smart karticu

9.1.2.5. Korak 5. – Distribucija Smart kartica i PIN-ova

Smart kartice i PIN-ovi se distribuiraju prema internim **Uputama o distribuciji i isporuci Smart kartica i PIN-ova**

9.2. Obnavljanje ključeva i certifikata

NAPOMENA:

Ovi se postupci ne primjenjuju za DEMO certifikate.

9.2.1. Obnavljanje ključeva

NAPOMENA:

Operacije obnove ključa koje se obavljaju nakon isteka ključa generiraju novi referentni broj i autorizacijski kod koji se šalje korisniku i LRA zaposleniku kao i kod inicijalnog izdavanja certifikata.

Ako certifikat nije opozvan, korisnik može u roku od tri mjeseca prije isteka roka valjanosti certifikata dostaviti zahtjev za izdavanje novog certifikata, sa pripadajućim parom ključeva. Takav zahtjev može biti poslan u LRA ili RA elektroničkom porukom potpisanom starim parom ključeva. RA izdaje novi identifikacijski broj i autorizacijski kod s kojima korisnik može registrirati svoj novi javni ključ i preuzeti svoj novi certifikat.

Za korisnike koji koriste FINA ID certifikate, obnova ključeva na CA provodi se automatski temeljem mrežnog PKIX-CMP protokola i uz pomoć SW instaliranog kod korisnika (u tu svrhu korisnik treba biti priključen na računalnu mrežu preko kojeg je dostupan FINA PKIX-CMP servis za obnovu certifikata). Korisnik vrši generiranje novih ključeva i njihovu registraciju prije njihovog isteka.

9.2.2. Obnavljanje certifikata

NAPOMENA:

Ako korisnik ne dostavi zahtjev, njegov će se RDC certifikat nakon isteka valjanosti smatrati poništenim, te će za dobivanje novog RDC certifikata biti podvrgnut svim procedurama inicijalne registracije.

Obnavljanje certifikata znači kreiranje novog certifikata sa istim imenom Subjekta, ali sa novim parom ključeva, rokom valjanosti i novim serijskim brojem.

Certifikat se može obnoviti ako:

- paru ključeva nije istekao rok valjanosti,
- privatni ključ nije kompromitiran, i
- informacije o Subjektu su ispravne.

FINA ID certifikati se automatski obnavljaju, ako je prethodni certifikat važeći i privatni ključ nije kompromitiran.

FINA Web certifikati se ne mogu automatski obnoviti, već korisnik šalje zahtjev za izdavanje novog certifikata.

9.3. Vraćanje ključeva

NAPOMENA:

Ovi se postupci ne primjenjuju za DEMO certifikate.

Vraćanje ključeva je servis za korisnike ID certifikata.

Da bi se izbjegle moguće zlouporabe, I&A korisnika jednak je onom kao kod inicijalne registracije korisnika.

Korisnik ili LRA zaposlenik popunjava **"Zahtjev za promjenu"** (kopija se nalazi na web stranici FINA PKI … pod nazivom OBRASCI).

9.4. Opoziv

NAPOMENA:

Ovi se postupci ne primjenjuju za DEMO certifikate.

Opoziv se zahtjeva kada korisnik više ne treba certifikat, ili kada je privatni ključ korisnika kompromitiran ili se sumnja u kompromitiranost.

Korisnik ili LRA zaposlenik će zahtijevati opoziv koristeći obrazac **"Zahtjev za promjenu"** koji se nalazi na web stranici FINA PKI ... pod nazivom OBRASCI.

Ako je **Zahtjev za promjenu** zaprimio HELP DESK, nakon provjere valjanosti zahtjeva prosljeđuje ga standardnim kanalima u RA.

9.4.1. Tko može zatražiti opoziv?

9.4.1.1. Opoziv na zahtjev korisnika

Korisnik (fizička osoba-građanin/poslovni subjekt) može zatražiti opoziv certifikata u bilo kojem trenutku zbog bilo kojeg razloga. Korisnik mora odmah uputiti zahtjev za opoziv certifikata, ako:

- neka od informacija u certifikatu promijeni ili zastari
- dođe do kompromitiranja privatnog ključa ili medija na kojem je spremljen

- osoba ovlaštena za potpisivanje više ne radi kod poslovnog subjekta ili više nema ovlasti za potpisivanje

Zahtjev potpisuje osoba ovlaštena za zastupanje.

9.4.1.2. Opoziv na zahtjev CA/RA

RA može opozvati certifikat iz slijedećih razloga:

- zahtjev suda ili nadležnog organa
- informacija u certifikatu je izmijenjena ili nije više valjana
- kompromitiranost ili sumnja na kompromitiranost privatnih ključeva, ili sadržaja na medijima
- propust korisnika u ispunjavanju obveza iz Ugovora o certifikatu, CP-a ili PDS-a za DEMO certifikate
- ako CA/RA smatra da certifikat nije izdan pravilno, odnosno u skladu sa navodima i obvezama iz Ugovora o certifikatu, CP-a ili PDS-a za DEMO certifikate

Zahtjev potpisuje voditelj CA ili RA.

9.4.1.3. Opoziv zbog prestanka ugovornog odnosa

Ako korisnik (fizička osoba – građanin ili poslovni subjekt) prekine ugovor o certifikatu prije isteka certifikata, RA će opozvati sve certifikate koji nisu istekli, a odnose se na taj ugovor.

Zahtjev potpisuje voditelj CA ili RA.

9.4.2. Procedure za opoziv certifikata

Zahtjev za opoziv certifikata treba u najkraćem roku biti predan izravno u RA ili putem LRA koji je autoriziran da prihvati takve zahtjeve u ime RA.

Zahtjev za opoziv može biti poslan elektroničkim kanalima ako je pritom potpisan privatnim ključem korisnika. Ako se zahtjev podnosi osobno, potrebno je na osnovu identifikacijskog dokumenta izvršiti I&A podnositelja zahtjeva kao i kod zaprimanja Zahtjeva za izdavanje certifikata.

Kada CA ili RA zahtjeva opoziv bez zahtjeva korisnika ili LRA zaposlenika, tada CA/RA mora dokumentirati razlog za opoziv. Svi autentificirani zahtjevi za opoziv i sve rezultirajuće akcije koje poduzima RA, biti će bilježeni i pohranjeni u skladu sa CP-om.

U slučaju da je certifikat opozvan, svi razlozi za opoziv će se pohraniti u RA podatkovnu osnovicu i čuvati u skladu sa CP-om.

9.5. Suspenzija

NAPOMENA:

Ovi se postupci ne primjenjuju za DEMO certifikate.

Korisnik ili LRA zaposlenik će zahtijevati suspenziju certifikata koristeći obrazac **"Zahtjev za promjenu"** koji se nalazi na web stranici FINA PKI ... pod nazivom OBRASCI.

Ako je **Zahtjev za promjenu** zaprimio HELP DESK, nakon provjere valjanosti zahtjeva prosljeđuje ga standardnim kanalima u RA.

Certifikat može biti postavljen u status suspenzije za vrijeme dok se provjerava zahtjev za opoziv.

9.5.1. Tko može zatražiti suspenziju ?

Zahtjev za suspenziju može poslati:

1. Korisnik za koga je certifikat izdan
2. Skrbnik za certifikat izdan za poslužitelja, uređaj ili aplikaciju
3. Poslovni subjekt
4. RA zaposlenici u ime poslovnog subjekta ili fizičke osobe - građanina
5. CA osoblje

9.5.2. Procedure za suspenziju certifikata

Procedure za traženje suspenzije razlikuju se ovisno od toga tko ih inicira. Kada zahtjev dolazi od korisnika, mora biti poslan u RA potpisanom mail porukom. Kada zahtjev dolazi od LRA zaposlenika, ona ga mora poslati izravno u RA u formi potpisane mail poruke.

Procedura za procesiranje zahtjeva za suspenziju sastoji se od slijedećeg:

1. Zahtjev se šalje u RA na način kako je gore navedeno
2. Potpis na zahtjevu se provjerava
3. Ako je zahtjev opravdan i prihvaćen, certifikat korisnika se suspendira i RA obavještava LRA zaposlenika, a LRA zaposlenik obavještava korisnika o suspenziji

9.5.2.1. Reaktiviranje certifikata

Korisnici se moraju osobno pojaviti kod LRA zaposlenika da bi zahtijevali reaktiviranje suspendiranih certifikata.