

Uputstvo za korišćenje

iBank Enrollment Wizard

Saržaj

1. UVOD	3
2. CILJ	3
3. CILJNA GRUPA	4
4. SRODNA (POVEZANA) DOKUMENTA	4
5. POČETAK RADA SA APLIKACIJOM	4
5.1. POKRETANJE WIZARDA	4
5.2. PRIJAVA NA SMART-KARTICU	5
5.3. PRIJAVA NA SERVER	6
5.4. IZLAZ IZ WIZARDA	7
6. UPOZNAVANJE SA KORISNIČKOM SPREGOM	8
6.1. KAKO DA GENERIŠEM KLJUČEVE I PRIJAVIM SE ZA SERTIFIKAT?.....	8
6.2. KAKO DA ZANOVIM SERTIFIKAT?.....	8
6.3. KAKO DA PROVERIM DA LI MI JE SERTIFIKAT IZDAT?.....	8
6.4. KAKO DA UČITAM SERTIFIKAT KOJI MI JE IZDAT?.....	9
7. RAD SA PROGRAMOM	9
7.1. GENERISANJE KLJUČEVA I PRIJAVA ZA SERTIFIKAT.....	9
7.2. GENERISANJE ZAHTEVA ZA ZANAVLJANJE SERTIFIKATA	13
7.3. IMPORT IZDATOG SERTIFIKATA NA KARTICU	17
8. REČNIK POJMOVA	19
9. INDEKS	20

1. Uvod

iBank Enrollment Wizard je aplikacija koja omogućava jednostavno rukovanje iBank ključevima i sertifikatima korisnika na smart-karticama.

U iBank sistemu, za autentikaciju korisnika i za kriptovanje osjetljivih poruka koristi se RSA algoritam. Svaki korisnik iBank sistema treba da poseduje par ključeva (javni i privatni ključ), kao i sertifikat koji odgovara njegovom javnom ključu. Ovi ključevi i sertifikat se čuvaju na smart-kartici ili drugom medijumu.

Rukovanje ključevima i sertifikatima obuhvata nekoliko akcija koje korisnici mogu da izvrše sami, uz pomoć iBank Enrollment Wizarda:

- Generisanje novih ključeva i prijava za sertifikat
- Učitavanje (import) izdatog sertifikata na smart-karticu
- Zanavljanje sertifikata (zahtev novog sertifikata za postojeći par ključeva) i

iBank Enrollment Wizard veoma pojednostavljuje ove akcije. Tako, korisnik koji je dobio blanko smart-karticu (bez ključeva), može za nekoliko minuta da generiše svoj par ključeva i da se prijavi za sertifikat, i da ga zatim dobije i počne rad u iBank sistemu, bez potrebe da se neposredno obraća odgovarajućem telu za izdavanje sertifikata (certificate authority).

2. Cilj

Svrha dokumenta je praktično upoznavanje korisnika sa iBank Enrollment Wizardom (u daljem tekstu: Wizardom). Čitajući ovaj dokument, korisnik će se upoznati sa korisničkom spregom Wizarda. Takođe, detaljno će se upoznati sa postupcima koje treba da izvrši kako bi obavio jednu od akcija koje Wizard podržava.

Dokument će pokušati da jasnim jezikom, sa dosta slika, pruži redosled poteza koji su potrebni sa strane korisnika da bi, uz pomoć Wizarda:

- Kreirao novi par ključeva i prijavio se za odgovarajući sertifikat
- Učitao (importovao) sertifikat kada mu bude izdat
- Prijavio se za novi sertifikat na bazi postojećih ključeva kada se približi istek prethodnog sertifikata ("zanavljanje sertifikata"), ili

Korisnik iBank sistema koji poseduje smart-karticu, uz pomoć Wizarda, može sam, u svojoj organizaciji ili kod kuće, koristeći konekciju na Internet, da obavlja ove akcije. Korisnik koji je pri prijavi za iBank sistem dobio karticu na kojoj već postoje ključevi i sertifikat verovatno će koristiti usluge Wizarda tek prilikom prvog zanavljanja sertifikata. S druge strane, korisnik koji je dobio blanko karticu (bez ključeva i sertifikata) može da generiše svoje ključeve na kartici i da zahteva novi sertifikat. Ovu poslednju uslugu će koristiti i korisnik koji već ima ključeve, uz odgovarajući dogovor sa tehničkom podrškom, u slučaju da želi da se njegov par ključeva promeni.

3. Ciljna grupa

Dokument je namenjen korisnicima iBank sistema koji poseduju smart-karticu kojom se prijavljuju na sistem. Postoje bar dve kategorije ovih korisnika:

- Korisnici koji su dobili praznu ("blanko") karticu. Ovakva kartica je samo personalizovana, tj. ima zadato korisničko ime i lozinku, ali na njoj nema ključeva korisnika niti odgovarajućeg sertifikata. Kao takva, ona (još) nije upotrebljiva za iBank sistem.
- Korisnici koji su dobili smart-karticu na kojoj postoje ključevi i sertifikat

Prva grupa korisnika će koristiti iBank Enrollment Wizard kako bi:

- Generisali nove ključeve na kartici i prijavili se za sertifikat, a zatim (kada sertifikat bude izdat)
- Preuzeli (importovali) izdati sertifikat i smestili ga na karticu

Time ovi korisnici postaju ravnopravni sa drugom grupom korisnika, uz prednost da su njihovi ključevi generisani lokalno, na smart kartici, u okruženju koje taj korisnik ima u svojoj organizaciji. Ti ključevi su slučajno generisani i jedini primerak tih ključeva je smešten na kartici.

Obe grupe korisnika će koristiti iBank Enrollment Wizard kada dođe trenutak isteka sertifikata. Pošto se sertifikati izdaju sa određenim rokom važenja, pred kraj tog roka, korisnici će morati da se prijave za nove sertifikate. iBank Enrollment Wizard omogućava korisniku da vidi koliko još vremena će njegov sertifikat važiti, i ako je period važenja pri kraju, da:

- Generiše novi zahtev za sertifikat (istovetan postojećem sertifikatu, samo sa produženim rokom važenja), a zatim (kada sertifikat bude izdat)
- Preuzme (importuje) izdati sertifikat i smesti ga na karticu.

4. Srodna (povezana) dokumenta

Radi dodatnih informacija, trebalo bi pogledati i druge dokumente u sklopu dokumentacije iBank Enrollment Wizarda:

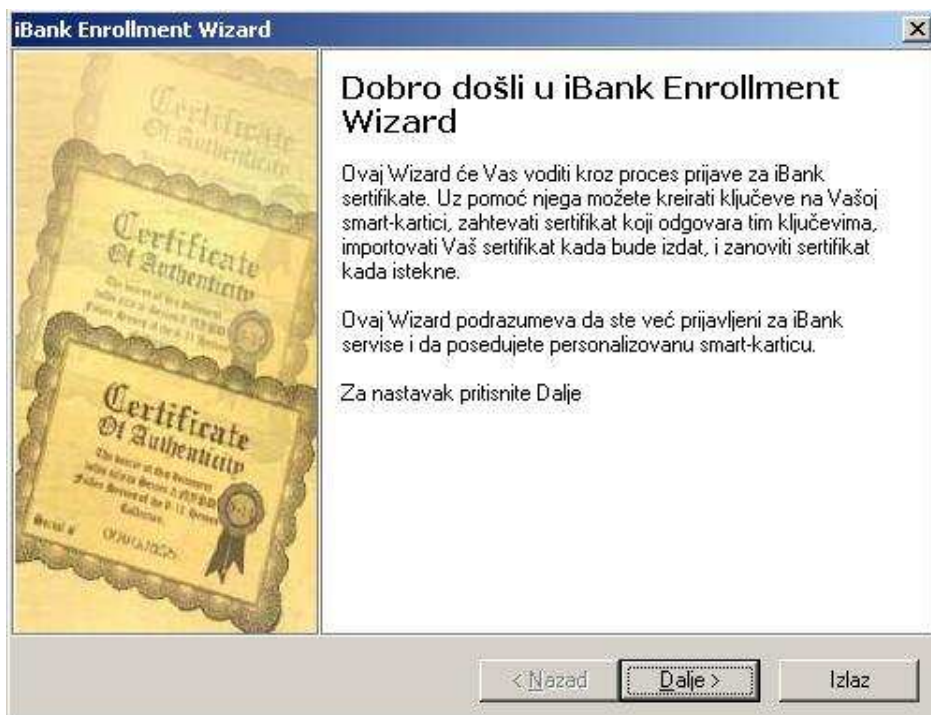
- iBank Enrollment Wizard: Uputstvo za instalaciju
- iBank Enrollment Wizard: Mala pouka iz kriptografije

5. Početak rada sa aplikacijom

5.1. Pokretanje Wizarda

Wizardova korisnička sprega je nalik drugim wizardima ("čarobnjacima") – zamišljena je tako da "vodi" korisnika sa jedne na drugu stranicu, redom do konačnog izvršenja akcije koju korisnik želi, uz mogućnost povratka unazad na svakom koraku.

Pošto je uspešno instaliran, Wizard se pokreće iz Start menija ili dvostrukim klikom na odgovarajuću ikonu "Enrollment Wizard" na radnoj površini (desktopu). Kada se pokrene, prikazuje se pozdravna stranica:



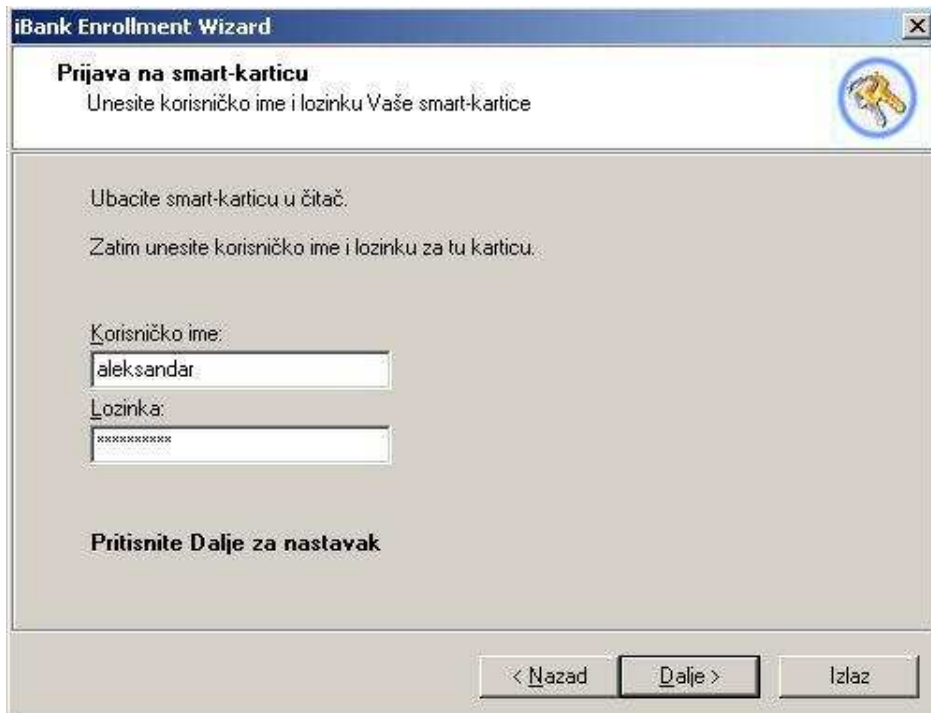
Na svakoj od stranica, u dnu, postoje tri dugmeta:

- **Nazad:** Omogućava povratak na prethodnu stranicu. Korisnik u svakom koraku (sem prvog i poslednjeg) može da se vrati na prethodni korak i da ispravi podešavanja koja je uneo u tom koraku
- **Dalje:** Prelazi na sledeću stranicu i ujedno pamti podešavanja koja je korisnik, eventualno, uneo na datoj stranici
- **Izlaz:** Prekida rad Wizarda. Wizard može prekinuti rad u ma kom trenutku pre nego što započne efektivno izvršavanje odgovarajuće akcije.

Na ovoj pozdravnoj stranici, pritiskom na **Dalje**, Wizard počinje sa radom.

5.2. Prijava na smart-karticu

Prva stranica koju Wizard prikazuje jeste **Prijava na smart-karticu**:



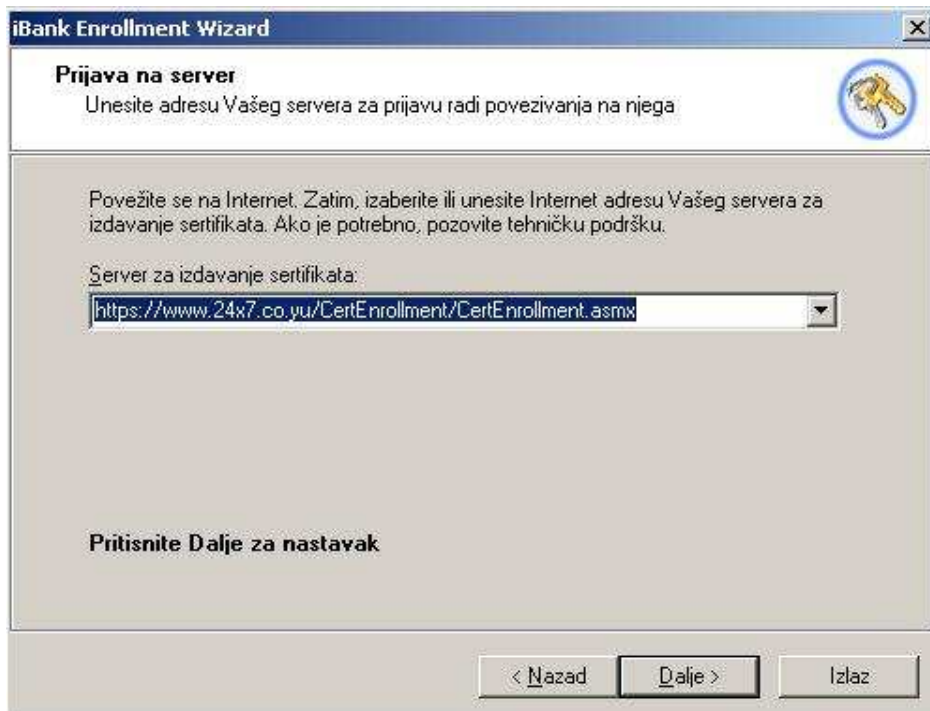
Korisnik treba da ubaci svoju smart-karticu u čitač kartica i da unese svoje korisničko ime i lozinku. Ovo korisničko ime i lozinku korisnik je dobio zajedno sa smart-karticom.

Pritiskom na **Dalje**, Wizard pokušava prijavu na smart-karticu. U slučaju da prijava ne uspe, Wizard će prijaviti odgovarajuću grešku i neće preći na sledeći korak. Treba biti pažljiv prilikom unosa korisničkog imena i lozinke, budući da posle tri pogrešne prijave dolazi do blokiranja smart-kartice.

Ako su korisničko ime i lozinka ispravni, Wizard će preći na sledeću stranicu - **Prijava na server**.

5.3. Prijava na server

Prijava na server je sledeća stranica koja se prikazuje pošto je Wizard završio prijavljivanje na smart-karticu:



U polje **Server za izdavanje sertifikata** treba uneti Web adresu servera na kome se nalazi podrška za izdavanje sertifikata. Ovu adresu će korisnik dobiti zajedno sa smart-karticom, ili je može dobiti ako pozove tehničku podršku

Pre pritiska na **Dalje**, treba obezbediti vezu sa Internetom, obzirom da će Wizard pokušati da kontaktira sa serverom. U slučaju da veza sa Internetom nije uspostavljena, Wizard prijavljuje grešku i ne prelazi na sledeći korak.

Ako sve bude u redu, Wizard prelazi na nove stranice, redom:

- **Detektovani status smart-kartice**, gde korisnik može da vidi trenutno stanje smart-kartice i svog naloga na serveru za izdavanje sertifikata
- **Izaberite opciju**, gde korisnik može da izabere jednu od akcija vezanih za izdavanje sertifikata
- **Vaš izbor**, gde korisnik još jednom potvrđuje opciju koju je izabrao, i posle koje se obavlja i sama izabrana akcija, i
- **Završetak rada iBank Enrollment Wizarda**, koja prikazuje rezultat izvršene akcije.

5.4. Izlaz iz Wizarda

Rad sa Wizardom se normalno prekida tako što se izvrši odgovarajuća akcija i pređe na stranicu **Završetak rada iBank Enrollment Wizarda**, a zatim pritisne dugme **Kraj** (koje zamenjuje dugme **Dalje**).

U slučaju da se korisnik tokom rada sa Wizardom predomisli, ma kada pre ove poslednje stranice može da pritisne dugme **Izlaz**. Wizard će upitati korisnika za potvrdu izlaska, a zatim će (ako korisnik potvrdi) prekinuti rad bez ikakve izvršene akcije na smart-kartici.

Korisnik može ponovo da pokrene Wizarda u ma kom trenutku kasnije da dovrši započeti posao.

6. Upoznavanje sa korisničkom spregom

6.1. Kako da generišem ključeve i prijavim se za sertifikat?

Sledite uputstva iz §7.1, gde je detaljno objašnjena ova procedura.

6.2. Kako da zanovim sertifikat?

Procedura generisanja zahteva za znavljanje objašnjena je u §7.2.

6.3. Kako da proverim da li mi je sertifikat izdat?

Pokrenite Wizarda kako je to opisano u §5.1. Pošto se prijavite na smart-karticu (§ 5.2) i na server za izdavanje sertifikata (§5.3), prikazuje se stranica **Detektovani status smart-kartice**, slična kao na sledećoj slici:



Dok sertifikat ne bude izdat, u polju **Zahtev(i) za sertifikatom** pišaće “Vaš sertifikat još nije izdat”. Onog momenta kada se natpis promeni u “Novi sertifikat je u međuvremenu izdat i možete ga preuzeti”, Vaš novi sertifikat je spreman za učitavanje. U tom slučaju, nastavite proceduru kako je opisano u §7.3.

Procedura izdavanja sertifikata obično traje od nekoliko sati do 1 dan. Korisnicima se u tom periodu može jedino preporučiti malo strpljenja.

6.4. Kako da učitam sertifikat koji mi je izdat?

Procedura učitavanja sertifikata, ako je izdat, opisana je u §7.3.

7. Rad sa programom

7.1. Generisanje ključeva i prijava za sertifikat

Pokrenite Wizarda kako je to opisano u §5.1. Pošto se prijavite na smart-karticu (§ 5.2) i na server za izdavanje sertifikata (§5.3), prikazuje se stranica **Detektovani status smart-kartice**, slična kao na sledećoj slici:



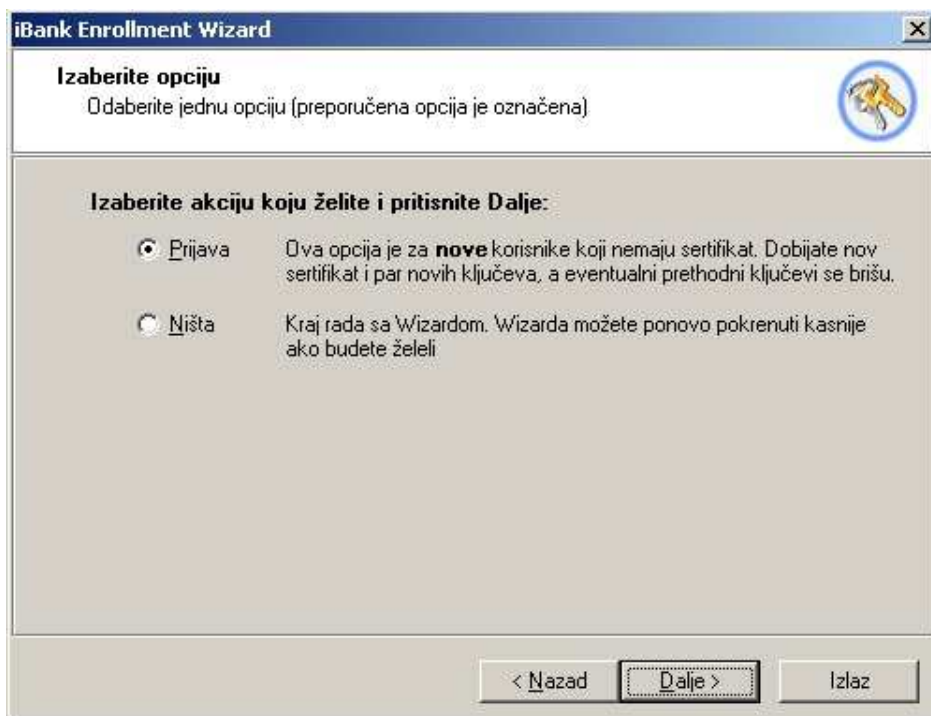
Značajna polja su zaokružena crvenom bojom.

U slučaju da u polju **Vaši ključevi** piše nešto drugo, a ne "Na kartici nema ni ključeva ni sertifikata", to znači da na kartici već postoje ključevi. U tom slučaju, dobro razmislite da li zaista želite da generišete nove ključeve, jer će oni zauzeti mesto starih ključeva, koji moraju tom prilikom da budu uništeni. Ako, pak, na kartici nema ključeva i sertifikata, novi ključevi mogu da se generišu bez ikakve bojazni.

Sem toga, u polju **Prijava za sertifikat** trebalo bi da piše rok do koga je moguća prijava za novi sertifikat. Ako je ovde napisano nešto drugo (npr. "Trenutno nemate prava da se prijavite za novi sertifikat"), to znači da na serveru za izdavanje sertifikata nije dozvoljeno

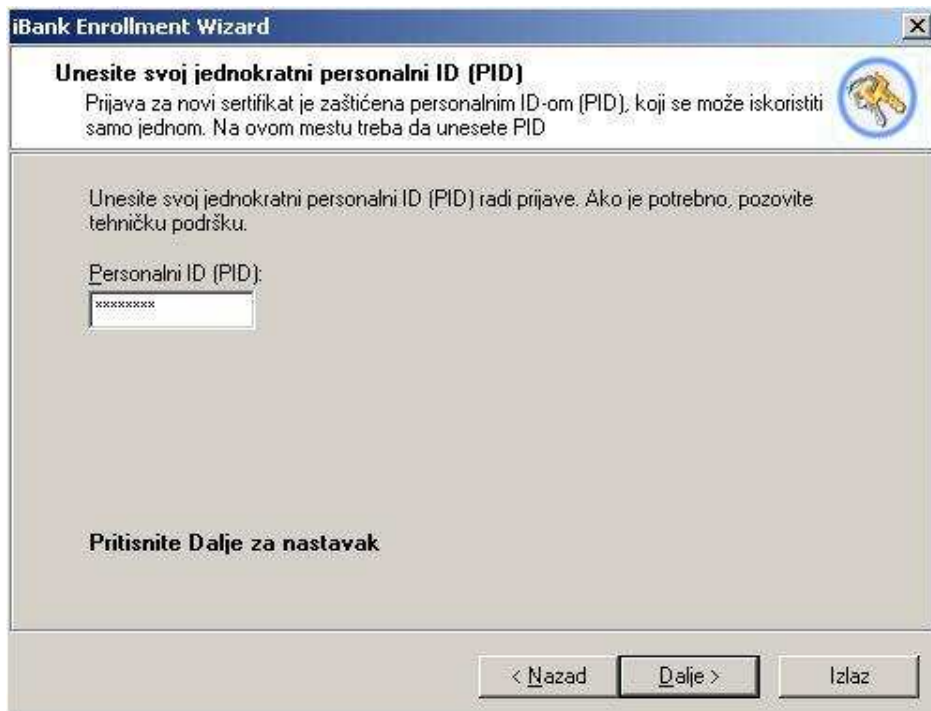
izdavanje sertifikata za datog korisnika. U tom slučaju, generisanje ključeva i prijava za sertifikat neće biti mogući – pozovite tehničku podršku radi dogovora o tome da Vam se ta funkcija omogući.

Pritiskom na **Dalje**, Wizard nudi korisniku odgovarajuće opcije:



Treba izabrati opciju **Prijava** i pritisnuti **Dalje**. Ova opcija nije omogućena u slučaju opisanom gore (izdavanje sertifikata nije dozvoljeno), u kom slučaju jedino možete odabrati opciju **Ništa** i napustiti Wizard. Ako su na kartici već postojali ključevi, opcija **Prijava** biće svrstana u "napredne" opcije.

Wizard u sledećem koraku prikazuje prozor za unos jednokratnog personalnog ID-a (PID):



Jednokratni PID korisnik dobija onda kada dobija smart-karticu na kojoj nema ključeva. Kao što mu i ime kaže, jednokratni PID se koristi samo jednom, posle čega korisnik treba da traži novi jednokratni PID ako mu bude potrebno da ponovo kreira ključeve i prijavljuje se za sertifikat. U svakom slučaju, ovaj PID korisnik ili zna unapred, ili će ga dobiti od tehničke podrške.

Pritiskom na **Dalje**, Wizard proverava PID. U slučaju da je pogrešan, prijaviće odgovarajuću grešku, a u suprotnom Wizard prelazi na stranicu kojom potvrđuje da je izabrana opcija **Prijava**:



Pritiskom na **Dalje**, Wizard:

- Generiše javni i privatni ključ na kartici, uz brisanje eventualno postojećih ključeva sa kartice (ako ih je bilo)
- Šalje *javni* ključ na potpisivanje serveru za izdavanje sertifikata (privatni ključ ostaje na kartici – ne napušta je)

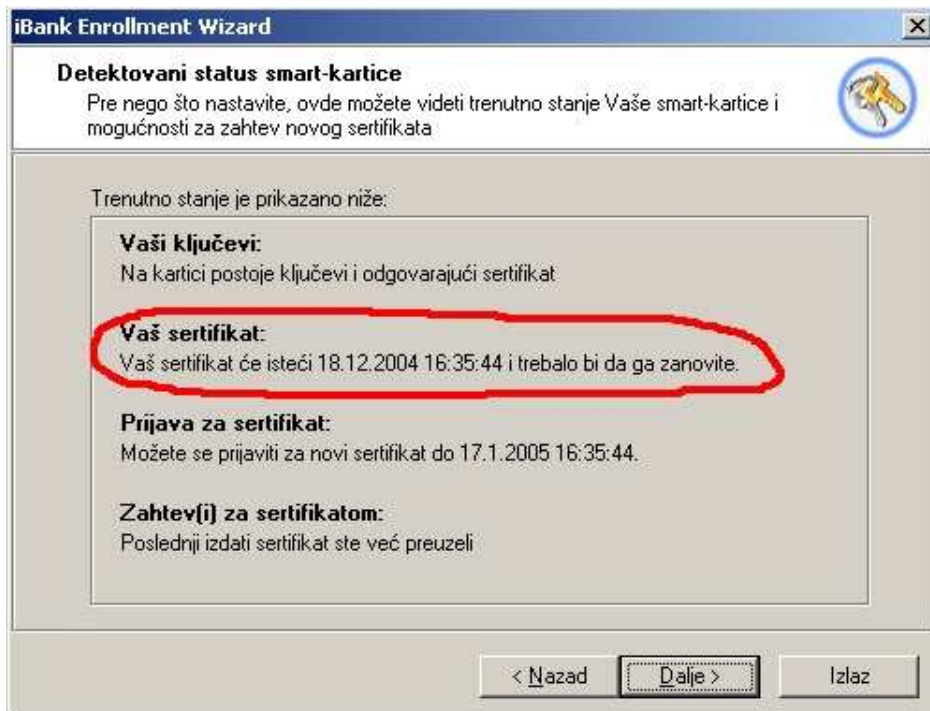
Prikazuje stranicu **Završetak rada iBank Enrollment Wizarda**:



Pritiskom na **Kraj**, Wizard završava rad. Da biste preuzeli svoj izdati sertifikat, treba ponovo da pokrenete Wizarda: vidi §7.3 radi više informacija o tome.

7.2. Generisanje zahteva za zanaavljanje sertifikata

Pokrenite Wizarda kako je to opisano u §5.1. Pošto se prijavite na smart-karticu (§ 5.2) i na server za izdavanje sertifikata (§5.3), prikazuje se stranica **Detektovani status smart-kartice**, slična kao na sledećoj slici:



U polju **Vaš sertifikat** trebalo bi da piše datum isteka sertifikata, kao i preporuka da li sertifikat treba zanavljati. Štaviše, ovo nije samo preporuka: server za izdavanje sertifikata će zaista izdati sertifikat samo ako je i Wizard to preporučio.

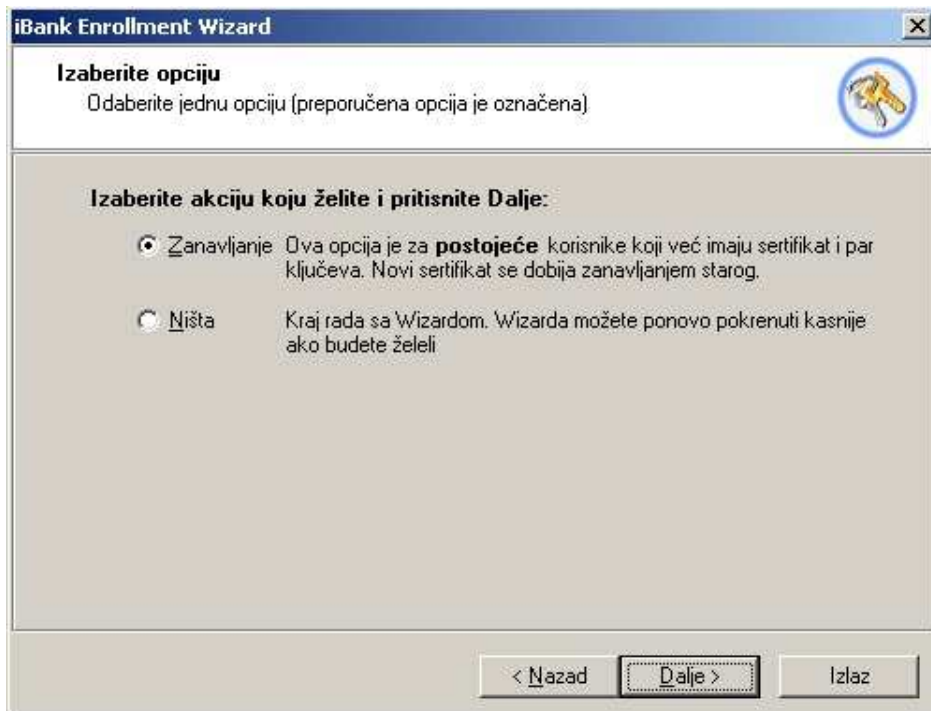
U ovom polju može da bude jedna od informacija:

- “Na smart-kartici nema sertifikata”: ako sertifikata zaista nema. U ovom slučaju zanavljanje nije moguće
- “Vaš sertifikat će isteći ... i još je rano za njegovo zanavljanje”: trenutak prestanka važenja sertifikata nije dovoljno blizu da bi server za izdavanje sertifikata dopustio zanavljanje
- “Vaš sertifikat će isteći ...i trebalo bi da ga zanovite”: trenutak prestanka važenja sertifikata je blizu i njegovo zanavljanje je već moguće.
- “Vaš sertifikat je istekao ...i trebalo bi da ga hitno zanovite”: sertifikat je skoro istekao, ali server za izdavanje sertifikata još dozvoljava njegovo zanavljanje
- “Vaš sertifikat je istekao ...i kasno je za njegovo zanavljanje”: sertifikat je istekao relativno odavno i zanavljanje više nije moguće.

U trećem i četvrtom slučaju, zanavljanje je moguće. U ostalim slučajevima nije: u prvom zanavljanje nema smisla, u drugom nema potrebe za njim, a u petom slučaju je prekasno. Ako Vam se desi ovaj poslednji slučaj, kontaktirajte tehničku podršku da bi Vam se naknadno zanavljanje omogućilo.

Ako je zanavljanje sertifikata moguće, u polju **Prijava za sertifikat** biće prikazan rok u kome je zanavljanje moguće.

Ako je zanavljanje moguće, pritiskom na Dalje, Wizard prikazuje stranicu sličnu kao na sledećoj slici:



Wizard uvek prikazuje sve akcije koje imaju smisla za datog korisnika, a među njima će **Zanavljanje** biti preporučena opcija ako je sertifikat blizu isteka ili je upravo istekao.

Kada korisnik izabere opciju **Zanavljanje** i pritisne **Dalje**, Wizard će u određenim situacijama prikazati stranicu za unos jednokratnog personalnog ID-a (PID), kao u §7.1. Ovu stranicu Wizard prikazuje ako je politika iBank sistema kao celine podešena tako da se za zanavljanje sertifikata zahteva PID. Ukoliko je to slučaj, korisnik treba za ovu fazu da obezbedi jednokratni PID koji će iskoristiti za zanavljanje.

U svakom slučaju, bilo da je stranica za unos PID-a prikazana ili ne, pritiskom na **Dalje**, Wizard prikazuje stranicu za potvrdu izabrane opcije:



Pritiskom na **Dalje**, Wizard preuzima podatke o korisniku iz postojećeg sertifikata, pravi zahtev za novi sertifikat za postojeći javni ključ, šalje ovaj zahtev serveru za izdavanje sertifikata, a zatim prikazuje stranicu **Završetak rada iBank Enrollment Wizarda**:



Pritiskom na **Kraj**, Wizard završava rad. Da biste preuzeli svoj izdati sertifikat, treba ponovo da pokrenete Wizarda: vidi §7.3 radi više informacija o tome.

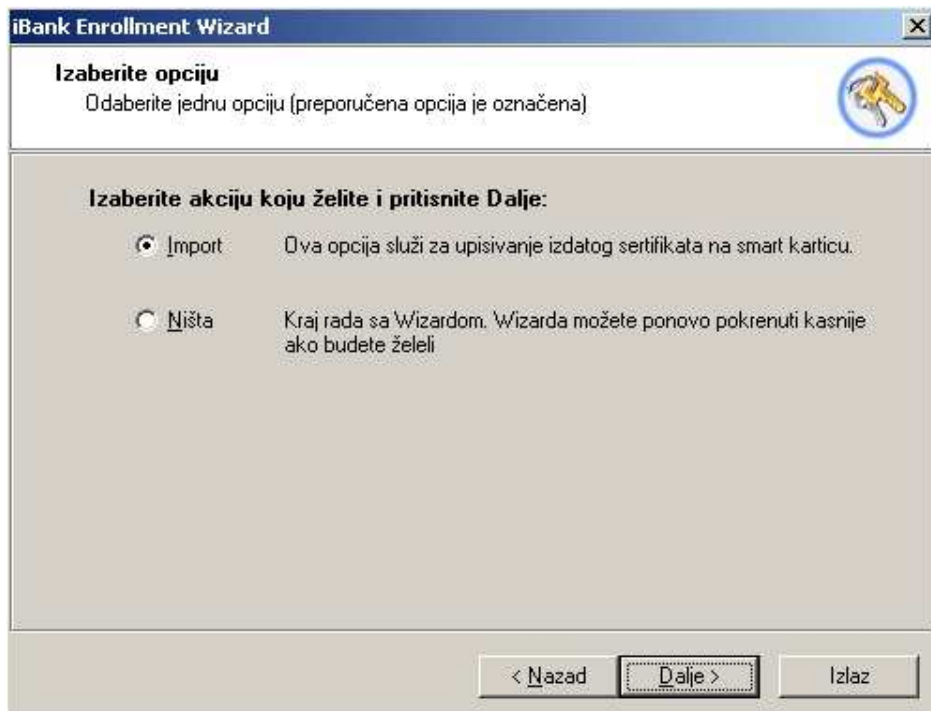
7.3. Import izdatog sertifikata na karticu

Pokrenite Wizarda kako je to opisano u §5.1. Pošto se prijavite na smart-karticu (§ 5.2) i na server za izdavanje sertifikata (§5.3), prikazuje se stranica **Detektovani status smart-kartice**, slična kao na sledećoj slici:



Ako u polju **Zahtev(i) za sertifikatom** stoji "Novi sertifikat je u međuvremenu izdat i možete ga preuzeti", trebalo bi da preuzmete svoj sertifikat. Ako u ovom polju stoji "Poslednji izdati sertifikat ste već preuzeli", to znači da je sertifikat već preuzet, ali Vas ništa ne sprečava da ga preuzmete ponovo, sem što će onda opcija za preuzimanje biti svrstana u "napredne" opcije. U ostalim slučajevima, preuzimanje sertifikata nije moguće.

Pritiskom na **Dalje**, prikazuje se stranica kao na sledećoj slici:



Po pritisku na **Dalje**, Wizard još jednom potvrđuje izabranu opciju:



Sledećim pritiskom na **Dalje**, Wizard uspostavlja vezu sa serverom za izdavanje sertifikata, preuzima sertifikat i smešta ga na smart-karticu, posle čega prikazuje rezultat izvršene akcije:



Pritisak na **Kraj** zatvara Wizarda, a smart-kartica je sada spremna za korišćenje u iBank sistemu.

8. Rečnik pojmova

certifikat v. sertifikat

čarobnjak..... v. wizard

digitalni potpis..... podatak izveden iz određenog dokumenta korišćenjem privatnog ključa korisnika. Javnim ključem se može verifikovati validnost potpisa.

enrollment..... engl. "prijava", "prijavlivanje". Ovo je uobičajeni termin koji se koristi da označi proces prijave korisnika za sertifikate (v.)

javni ključ *ključ* (v.) koji čini par sa *privatnim ključem* (v.). Za razliku od privatnog ključa, po pravilu se ne drži u tajnosti. Iz njega je nemoguće izvesti privatni ključ. Svaki korisnik iBank sistema ima svoj javni i privatni ključ. Javni ključ korisnika se koristi za verifikaciju digitalnog potpisa (v.) korisnika i za kriptovanje podataka za tog korisnika.

ključ..... podatak u kriptografiji koji se koristi za transformaciju drugih podataka. Na primer, ključ može da se koristi da bi se kriptovao određeni sadržaj, ili da bi se od određenog sadržaja dobio digitalni potpis.

privatni ključ..... *ključ* (v.) koji čini par sa *javnim ključem* (v.). Privatni ključ se drži u tajnosti za svakog korisnika (na smart-kartici (v.) ili drugom medijumu), i ne može se otkriti bez obzira na to što je odgovarajući javni ključ publikovan. Svaki korisnik iBank sistema ima svoj privatni i

odgovarajući javni ključ. Privatni ključ korisnika služi prilikom potpisivanja od strane tog korisnika, kao i za dekriptovanje podataka koji su tom korisniku poslani.

- sertifikat** javni ključ (v.) potpisan od strane tela ovlašćenog za potpisivanje. Služi da bi se osigurala autentičnost javnih ključeva. Svaki korisnik, da bi koristio iBank sistem, mora da poseduje ne samo svoj javni i privatni (v.) ključ, već i odgovarajući sertifikat. Uloga iBank Enrollment Wizarda i jeste olakšavanje postupka dobijanja sertifikata za korisnike.
- smart-kartica** (ponekad je zovu "pametna kartica"): uređaj veličine kreditne kartice koji ima nekoliko funkcija koje je čine idealnom za čuvanje osetljivih kriptografskih podataka: fizička zaštita podataka, logička zaštita (kroz sistem lozinke), obavljanje osetljivih kriptografskih operacija na samoj kartici.
- wizard** engl. "čarobnjak". Označava uslužni program koji je tako dizajniran da "vodi" korisnika korak po korak do rešenja problema. iBank Enrollment Wizard je primer wizarada.
- zanavljanje** procedura kojom korisnik koji već ima sertifikat koji odgovara njegovom javnom ključu dobija novi sertifikat koji odgovara istom javnom ključu, ali sa produženim periodom važenja.

9. Indeks

Generisanje ključeva.....	9	Provera izdavanja.....	8
Import sertifikata	17	Server	
Opcije		Prijava na server	6
Import.....	17	Smart-kartica	
Prijava.....	9	Prijava na karticu	5
Zanavljanje.....	13	Wizard	
Pokretanje Wizarda	4	Izlaz	7
Prijava na server	6	Pokretanje.....	4
Prijava na smart-karticu.....	5	Prijava na server	6
Prijava za sertifikat.....	9	Prijava na smart-karticu	5
Provera izdavanja sertifikata	8	Tipovi korisnika	4
Sertifikat		Uvod.....	3
Import.....	17	Zanavljanje sertifikata	13