Упатство за користење

iBank Enrollment Волшебник

Содржина

1. Вовед

iBank Enrollment Wizard е апликација која овозможува едноставно ракување со iBank клучевите и сертификатите на корисиците со smart-картички.

Во iBank системот, за автентикација на корисникот и за криптирање на чувствителни пораки се користи RSA алгоритмот. Секој корисник на iBank системот треба да поседува пар клучеви (јавен и приватен клуч), како и сертификат кој одговара на неговиот клуч. Овие клучеви и сертификати се чуваат на smart-картичката.

Ракувањето со клучевите и сертификатите опфаќа неколку акции кои што корисиците можат да ги извршат сами, со помош на iBank Enrollment Волшебникот:

- Генерирање на нови клучеви и пријава за сертификат
- Вчитување (импорт) на издадениот сертификат на смарт картичката
- Обнова на сертификат (барање за нов сертификат и за пар на клучеви)

iBank Enrollment Волшебникот ги поедноставува овие активности. Така што корисник кој што добил бланко смарт картичка (без клучеви) може за неколку минути да генерира свој пар на клучеви и да се пријави за сертификат, истиот потоа и да го добие и да започне со работа во iBank системот, без потреба непосредно да се обраќа на соодветното тело за издавање на сертификат (certificate authority).

2. Цел

Целта на документов е практично запознавање на корисникот со iBank Enrollment Волшебникот (во понатамошниот текст: Волшебникот). Читајќи го овој документ, корисникот ќе се запознае со корисничката спрега на Волшебникот. Исто така детално ќе се запознае со постапките кои што треба да ги изврши за да ги користи опциите на Волшебникот.

Документов ќе се обиде на јасен јазик, повеќе преку слики, да го изложи редоследот на акциите кои му се потребни на корисникот при работа со Enrollment Wizardot:

- Креирал нов пар на клучеви и се пријавил за нов сертификат
- Креирал (Импортирал) сертификат откако истиот му бил издаден
- Се пријавил за нов сертификат врз база на постоечките клучеви откако ќе се приближи истекот на претходниот сертификат ("обнова на сертификат")

Корисникот на iBank системот кој што поседува smart-картичка, со помош на Волшебникот, може самиот, од својата фирма или од дома, имајќи при тоа конекција кон Интернет, да ги изведе овие акции. Корисникот кој при пријавата на iBank ситемот добил картичка накоја веќе постојат клучеви и сертификат, веројатно ќе ги користи услугите на Волшебникот дури при првото истекување на сертификатот. Од друга страна, оној што добил бланко картичка (без клучеви и сертификат) може да генерира

свој пар клучеви и да побара сертификат. Оваа, последната услуга ќе ја користат и корисниците кои веќе имаат клучеви, преку соодветен одговор од техничката поддршка доколку сака неговиот пар клучеви да се промени.

3. Целна Група

Документов е наменет за корисниците на iBank системот кои поседуваат smart-картичка со која се пријавуваат на системот. Постојат барем две категории на корисници:

- Корисници кои имаат добиено празна ("бланко") картичка. Оваа картичка е само персонализирана, т.е. има зададено корисничко име и лозинка, но на неа не постојат пар клучеви на корисникот ниту соодветен сертификат. Како таква, истата сеуште е неупотреблива во iBank системот.
- Корисници кои ја добиле својата картичка на која постојат клучеви и сертификат

Првата група на корисници ќе го користат iBank Enrollment Волшебникот за да:

- Генерираат нов клучеви на картичката и да се пријават за сертификат, а потоа (откако сертификатот ќе биде издаден)
- Да се пријават (го импортираат) сертификатот и го сместат на картичката

Со тоа овие корисници стануваат рамноправни со другата група на корисници, со таа предност што нивните клучеви се генерирани локално, на самата картичка, во опкружувањето кое што корисникот го има во својата фирма. Тие клучеви се случајно генерирани и единствен примерок од клучевите е сместен на картичката.

Обете групи ќе го користат iBank Enrollment Волшебникот кога ќе дојде до моментот за истекување на сертификатот. Бидејќи сертификатите се издаваат со одреден рок на важење, пред истекот на тој рок, корисниците ќе мораат да се пријават за обнова на сертификатот. iBank Enrollment Волшебникот му овозможува на корисникот и да види колку уште време му важи неговиот сертификат, и ако е периодот на важење пред крај, да:

- Генерира ново барање за нов сертификат (истоветен со постоечкиот сертификат само со продолжен рок на важење), а потоа (кога сертификатот ќе биде издаден)
- Го превзема (импортира) издадениот сертификат и го сместува на картичката.

4. Сродни (поврзани документи)

Како додатни информации, можете да ги погледнете и другите документи во склоп на документацијата за iBank Enrollment Волшебникот:

- iBank Enrollment Волшебникот: Упатство за инсталација
- iBank Enrollment Волшебник: Мали пауки од криптографија

5. Почеток на работа со апликацијата

5.1. Активирање на Волшебникот

Корисничката спрега на Волшебникот е како и кај другите (“волшебници”) – замислена е така да го "води" корисникот од една страница на друга, по ред до конечното завршување на акцијата која корисникот сака да ја изведе, со можност за враќање наназад на секој чекор.

Откако ќе биде успешно инсталиран, Волшебникот се активира од Start менито или со двоен клик на соодветната икона “Enrollment Wizard” на работната површина (desktop-от). Откако ќе се подигне, се прикажува поздравната страница:

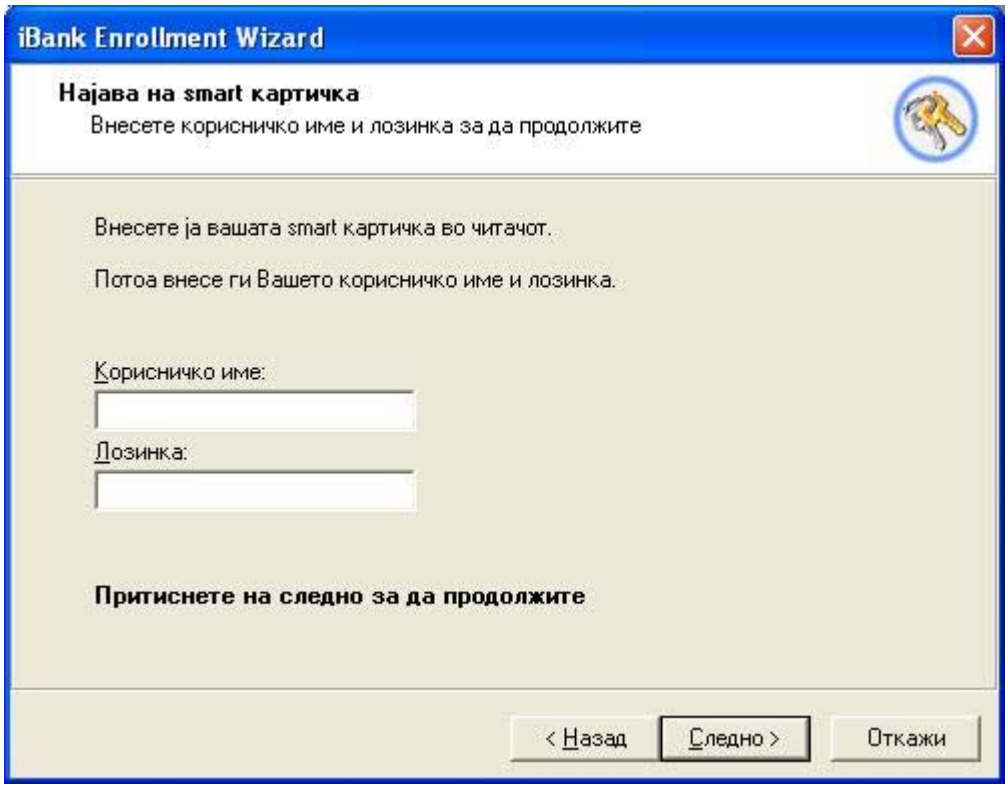
Не секоја од страните, при дното постојат, три копчиња:

- **Назад**: Овозможува враќање на претходната страница. Кориснкот при секој чекор (освен првиот и последниот) може да се врати на претходниот чекор и да ги измени подесувањата кои ги внел во тој чекор.
- **Следно**: Преоѓа на следната страница и воедно ги памти подесувањата кои што корисникот, евентуално ги внел на соодветната страница
- **Крај**: Прекинување на работата со Волшебникот. Волшебникот може да прекине со работа во било кој момент пред да започне со извршување на соодветната акција.

На оваа поздравна страница, со притискање на **Следно**, Волшебникот започнува со работа

5.2. Пријавување на smart-картичката

Првата страница која што Волшебникот ја прикажува е **Пријава на smart-картичка**:



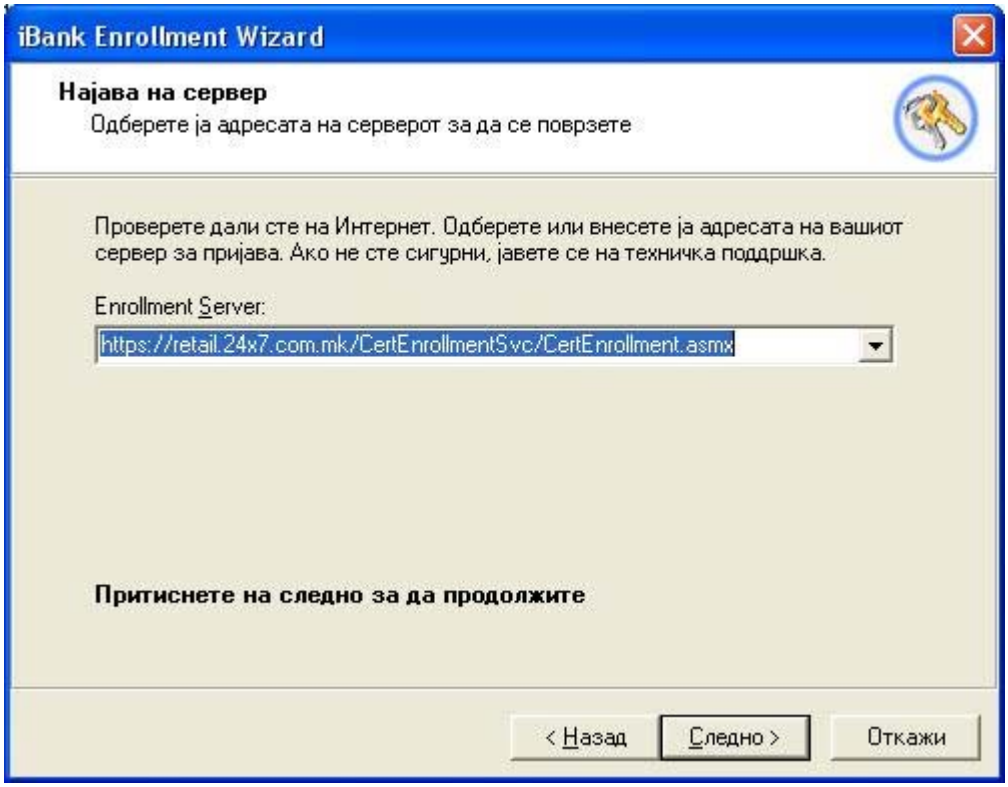
Корисникот треба да ја уфрли својата smart-картичка во читачот на картички и да го внесе своето корисничко име и лозинка. Ова корисничко име и лозинка корисникот ги добива заедно со смарт картичката.

Со притискање на **Следно**, Волшебникот ќе се обиде да се пријави на smart-картичката. Во случај пријавувањето да не успее, Волшебникот ќе пријави соодветна грешка и нема да помине на следниот чекор. Треба да се биде внимателен при внесувањето на корисничкоти име и лозинка, бидејќи при три последователни погрешни пријавувања smart-картичката се блокира.

Доколку корисничкото име и лозинката се исправни, Волшебникот ќе помине на следната страница – **Пријава на сервер**.

5.3. Пријава на сервер

Пријавувањето на сервер е следната страница која се прикажува откако Волшебникот се пријавил на smart-картичката:



Во полето **Сервер за издавање на сертификати** треба да се внесе Web адресата на серверот на кој што се наоѓа поддршката за издавање на сертификати. Оваа адреса корисникот ќе ја добие заедно со smart-картичката, или може да ја добие ако се јави во техничка поддршка.

Со пирискање на **Следно**, треба да се обезбеди врска со интернет, со оглед на тоа дека Волшебникот ќе се обиде да се поврзе со серверот. Во случај да врската со Интернет не е воспоставена, Волшебникот ќе пријави грешка и не поминува на следниот чекор.

Ако се биде во ред, Волшебникот преминува на следните страници по ред:

- **Детектиран статус на smart–картичката,** каде што корисникот може да ја види актуелната состојба на smart-картичката и својот account на серверот за издавањена сертификати
- **Изберете опција**, каде што корисникот може да избере една од опциите врзани за издавањето на сертификати
- **Ваш избор**, каде корисникот уште еднаш потврдува која опција ја избрал, а потоа се извршува и самата избрана акција, и
- **Комплетирање на работата со Волшебникот**, која го прикажува резултатот на извршената акција.

5.4. Излез од волшебникот

Работата со Волшебникот нормално се прекинува кога ќе се изврши соодветната акција и се преоѓа на страната **Комплетирање на работата на Enrollment**

Волшебникот, а потоа се притиска копчето **Крај** (кое што го заменува копчето **Следно**).

Во случај кога корисникот во текот на работата со Волшебникот се предомислил, и во момент кога се наоѓа пред последната страна, може да притисне на копчето **Откажи**. Волшебникот ќе побара од корисникот потврда за напуштање на работата, а потоа (ако корисникот потврди) ќе ја прекине работата без никакви измени на smart-картичката. Корисникот може да го активира Волшебникот во било кое време подоцна и да ја доврши започната работа.

6. Запознавање со корисничката спрега

6.1. Како да генерирам клучеви да се пријавам за сертификат?

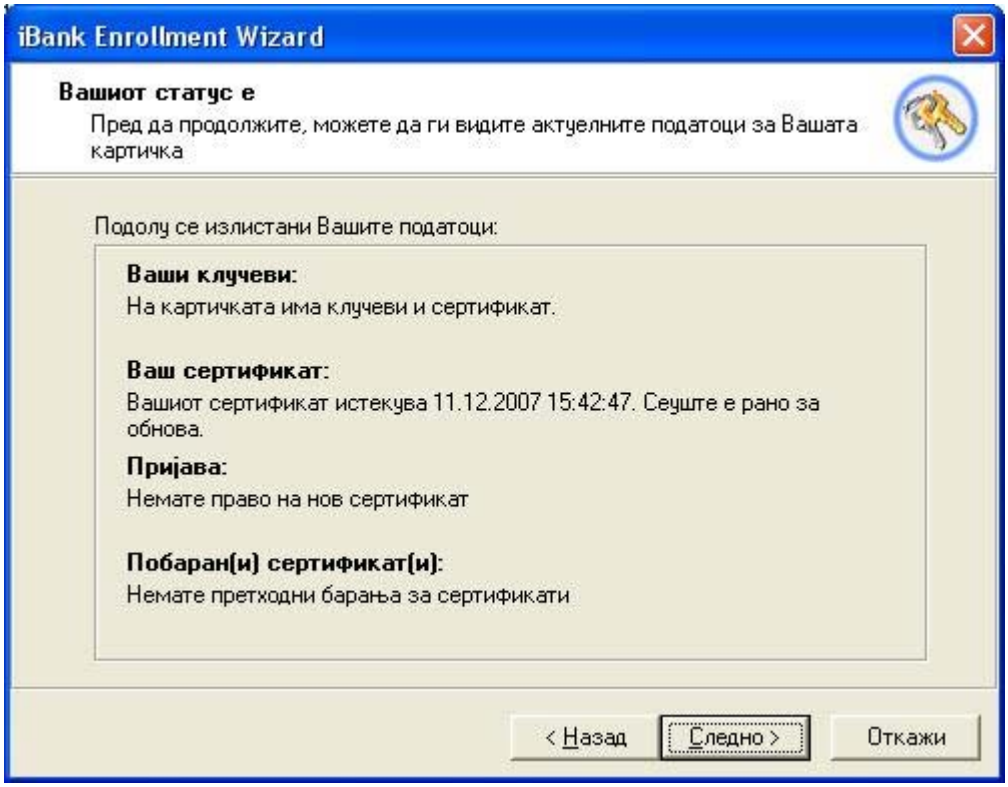
Следете ги упатствата од §7.2 , каде што детално е објаснета оваа процедура.

6.2. Како да обновам сертификат?

Процедурата за формирање на барање е дефинирана во §7.2.

6.3. Како да проверам дали ми е сертификатот е издаден?

Активирајте го Волшебникот како што е тоа опишано во §5.1. Откако ќе се пријавите на smart-картичката (§ 5.2) и на серверот за издавање на сертификати (§5.3), се прикажува страница **Детектиран статус на smart-картичката**, слична како на следнава слика:



Додека сертификатот не биде издаден, во полето **Барање(а) за сертификат** ќе пишува "Вашиот сертификат сеуште не е издаден". Оној момент кога натписот ќе се промени во "Новиот сертификат е во меѓувреме издаден и можете да го превземете", Вашиот сертификат е спремен за вчитување. Во тој случај, продолжете со процедурата како што е опишано во §7.3.

Процедурате за издавање на сертификати обично треа од неколку часа до еден ден.

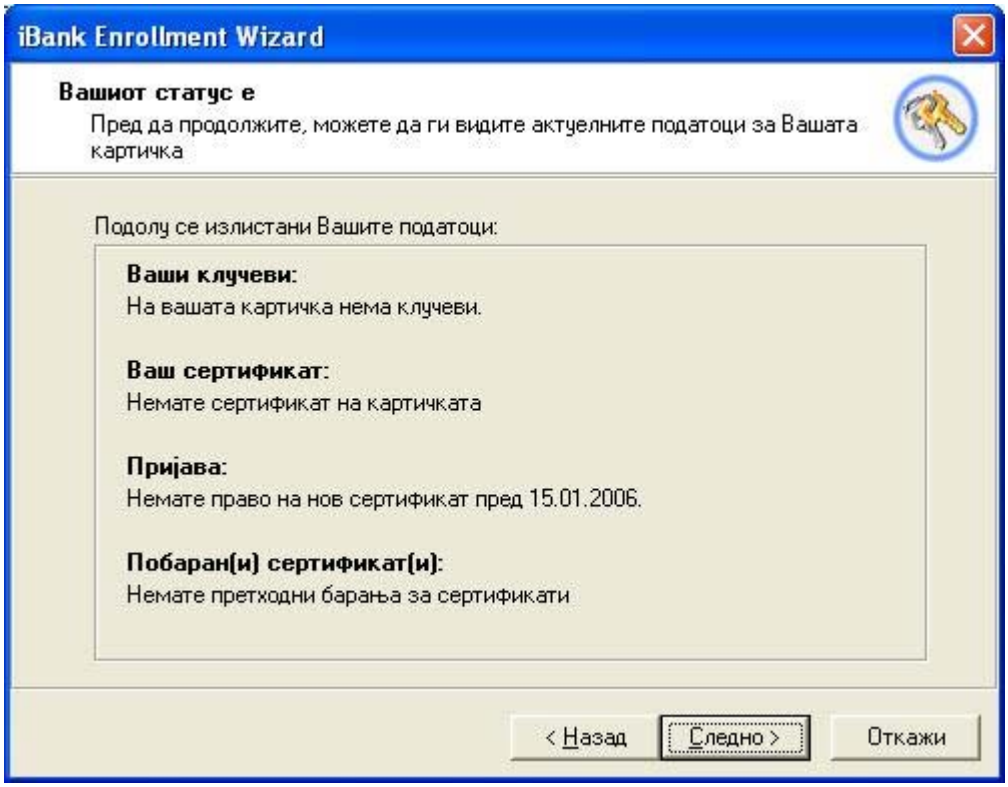
6.4. Како да го вчитам сертификатот кој ми е веќе издаден?

Процедурата за вчитување на сертификат, ако е веќе издаден, опишана е во §7.3.

7. Работа со програмот

7.1. Генерирање на клучеви и пријава за сертификат

Активирајте го Волшебникот како што е тоа опишано во §5.1. Откако ќе се пријавите на smart-картичката (§ 5.2) и на серверот за издавње на сертификати (§5.3), се прикажува страната **Детектиран статус на smart-картичката**, слично како на следнава слика:

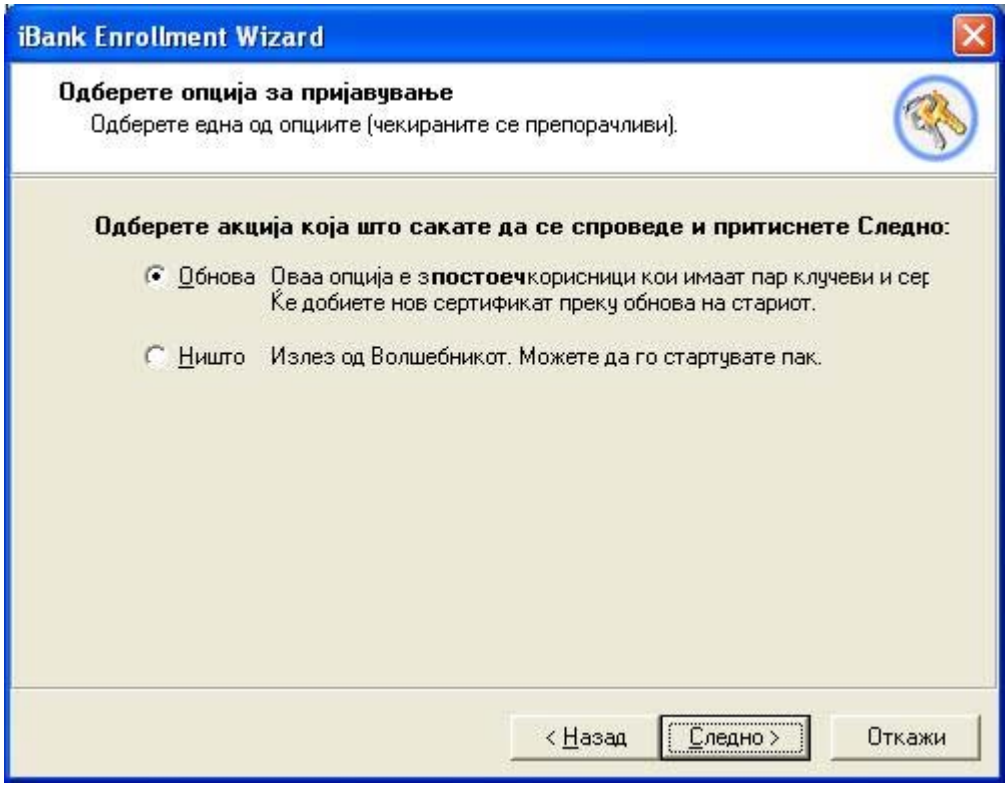


Битните полиња се заокружени со црвена боја.

Во случај кога под **Ваши клучеви** пишува нешто друго, а не "На картичката нема ниту клучеви ни сертификат", тоа значи дека на картичката веќе постојат клучеви. Во тој случај, добро размислете дали сакате да генерирате нови клучеви, бидејќи истите ќе го завземат местото на старите, кои што пак при оваа постапка ќе бидат уништени. Ако пак на картичката нема клучеви и сертификат, новите клучеви можат да се генрираат без никаков страв.

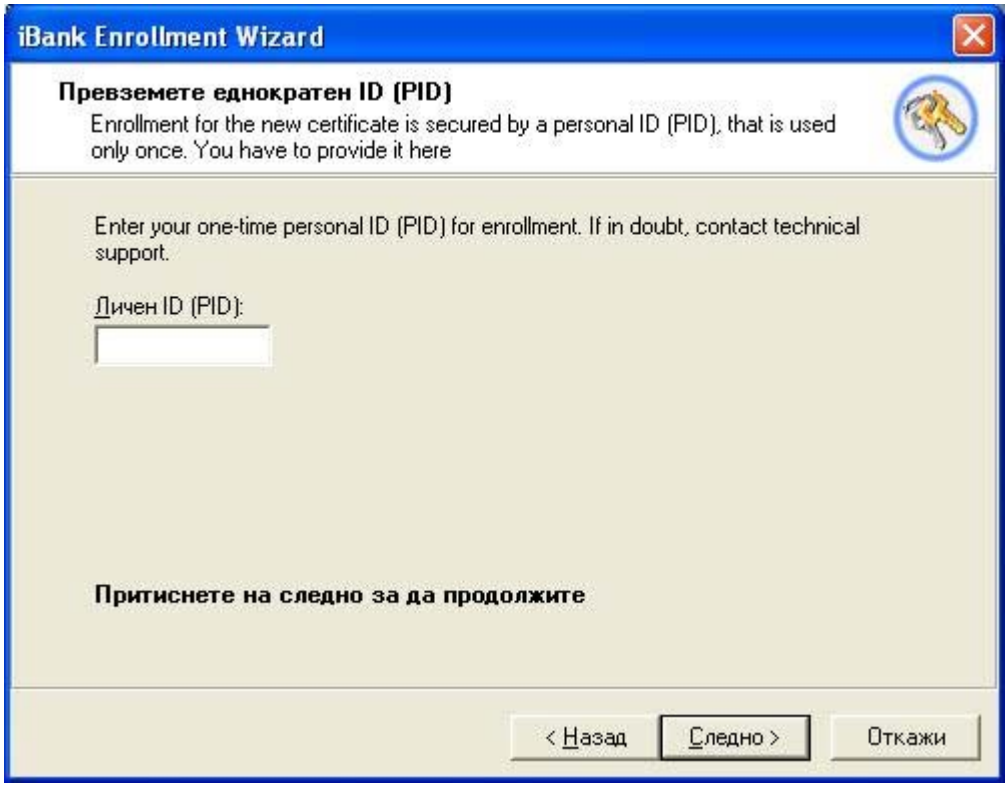
Освен тоа, во полето **Пријава за сертификат** треба да биде испишан рокот за пријавување за нов сертификат. Ако овде пишува нешто друго (на пр. "Во моментов немате право да се пријавите за нов сертификат"), тоа значи дека на серверот за издавање на сертификати е е дозволено издавње на сертификат за даденот корисник. Во тој случај, генерирањето на клучевите и пријавата за сертификат нема да бидат возможни – јавете се во техничка поддршка за да се договорите да Ви се овозможи оваа опција.

Со притискање на **Следно**, Волшебникот му ги нуди на корисникот соодветните опции:



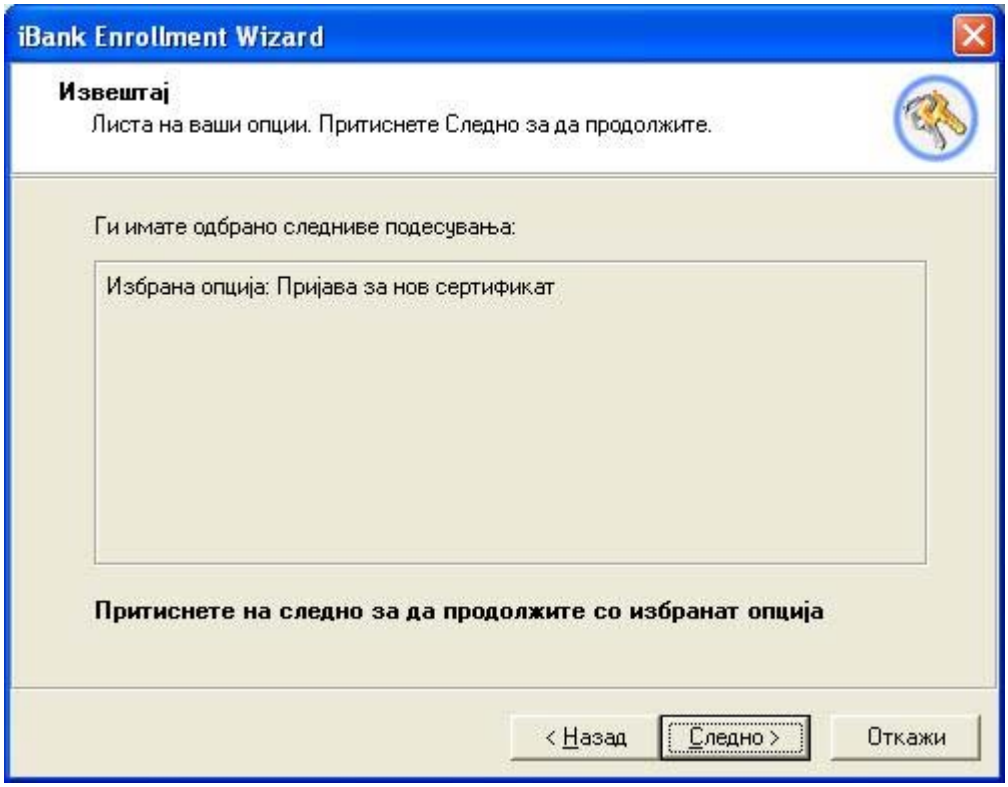
Треба да се одбере опцијата **Пријава** и да се притисне на **Следно**. Оваа опција нема да биде овозможена во случај како што беше опишано погоре (издавањето на сертификат не е дозволено), во тој случај единствено можете да ја одберете опцијата **Ништо** и да го напуштите Волшебнникот. Доколку на картичката веќе постојат клучеви, опцијата **Пријава** ќе биде содржана во "Напредни опции".

Волшебникот во следниот чекор ќе го прикаже прозорец за внес на еднократен личен ID (PID):



Еднократниот PID го добива тогаш кога ќе добие smart-картичка на која нема клучеви. Како што самото име кажува, еднократниот PID се користи само еднаш, после кој корисникот треба да бара нов PID ако сака повторно да креира клучеви и да се пријави за сертификат. Во тој случај, овој PID корисникот или го знае однапред, или ќе го добие од техничка поддршка.

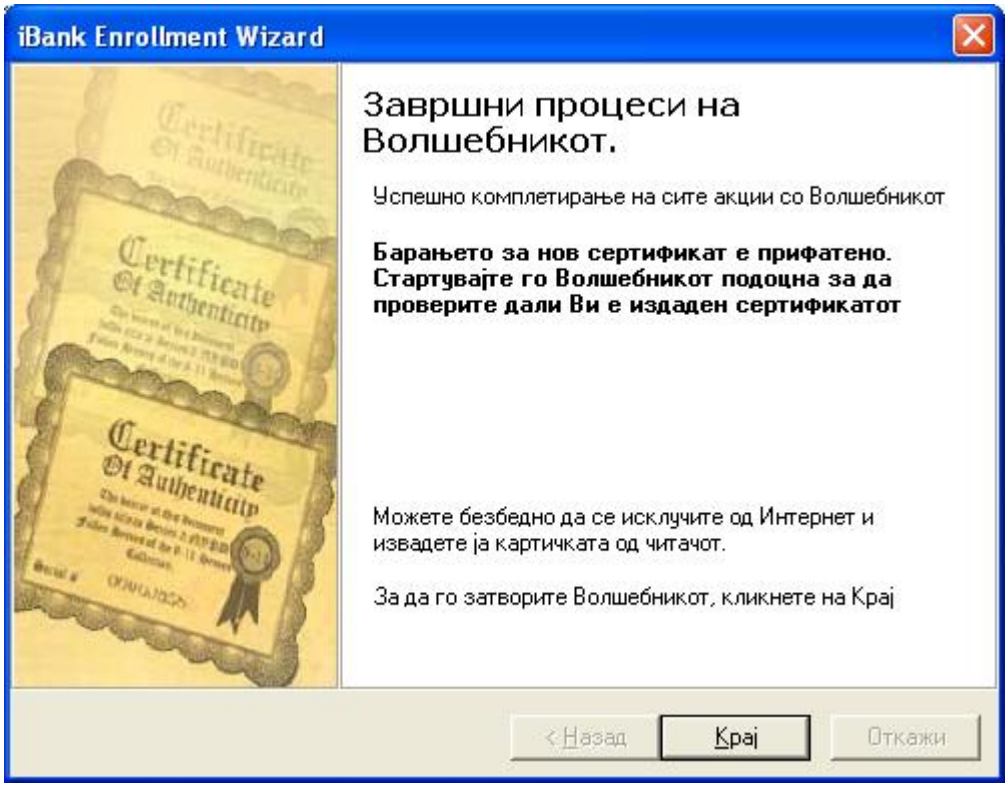
Со притискање на **Следно**, Волшебникот го проверува PID-от. Во случај да е тој погрешен, ќе пријави соодветна грешка, а во спротивно Волшебникот преоѓа на страница на која потрвдува дека е избрана опцијата **Пријава**:



Со притискање на **Следно**, Волшебникот:

- Генерира јавен и приватен клуч на картичката, со бришење на евентуално постоечките клучеви (доколку постоеле)
- Го испраќа *јавниот* клуч на потпишување на серверот за издавање на сертификати (приватниот клуч останува на картичката – не ја напушта)

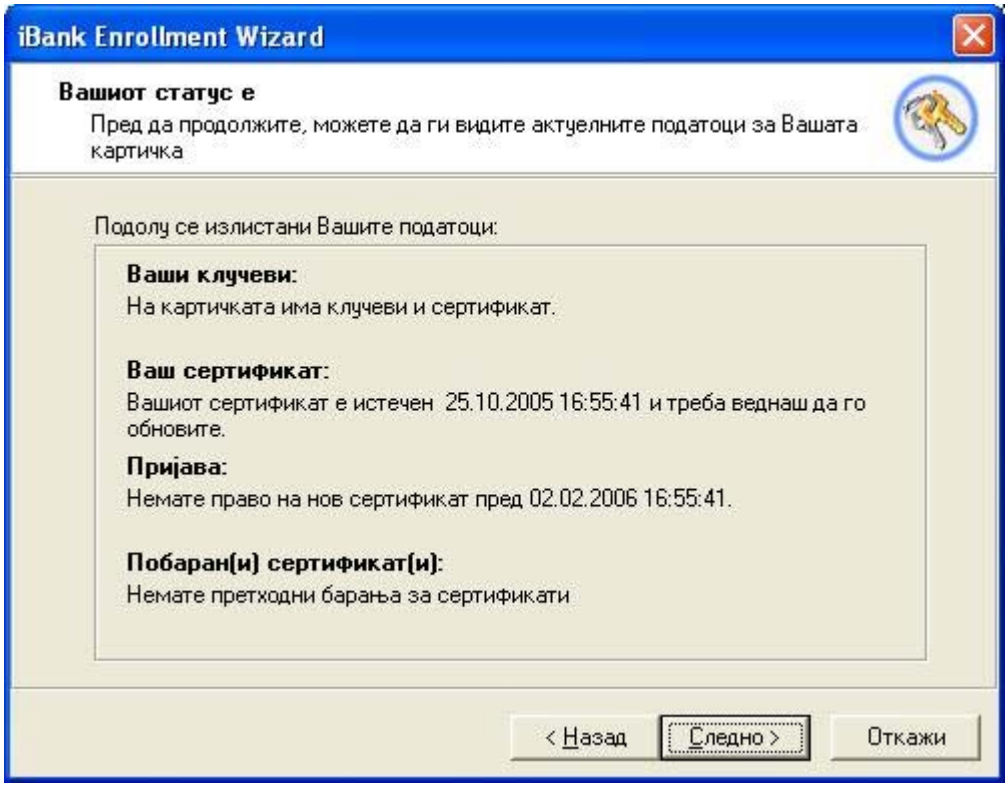
Се прикажува страната **Комплетирање на работата на iBank Enrollment Волшебникот**:



Со притискање на **Крај**, Волшебникот ја завршува работата. За да го превземете својот издаден сертификат, треба повторно да го активирате Волшебникот: видете §7.3 за повеќе информации во врска со ова.

7.2. Генерирање на барање за обнова на сертификат

Активирајте го волшебникот како што е тоа опишано во §5.1. Откако ќе се пријавите на smart-картичката (§ 5.2) и на серверот за издавање на сертификати (§5.3), се прикажува страната **Детектиран статус на smart-картичката**, слична како на следнава слика:



Во полето **Ваш сертификат** би требало да го пишува датумот на истекување на сертификатот, како и препорака дали сертификатот треба да се обновува. Ова не е само препорака: серверот за издавање сертификати навистина ќе издаде сертификат ако Волшебникот тоа го препорачал.

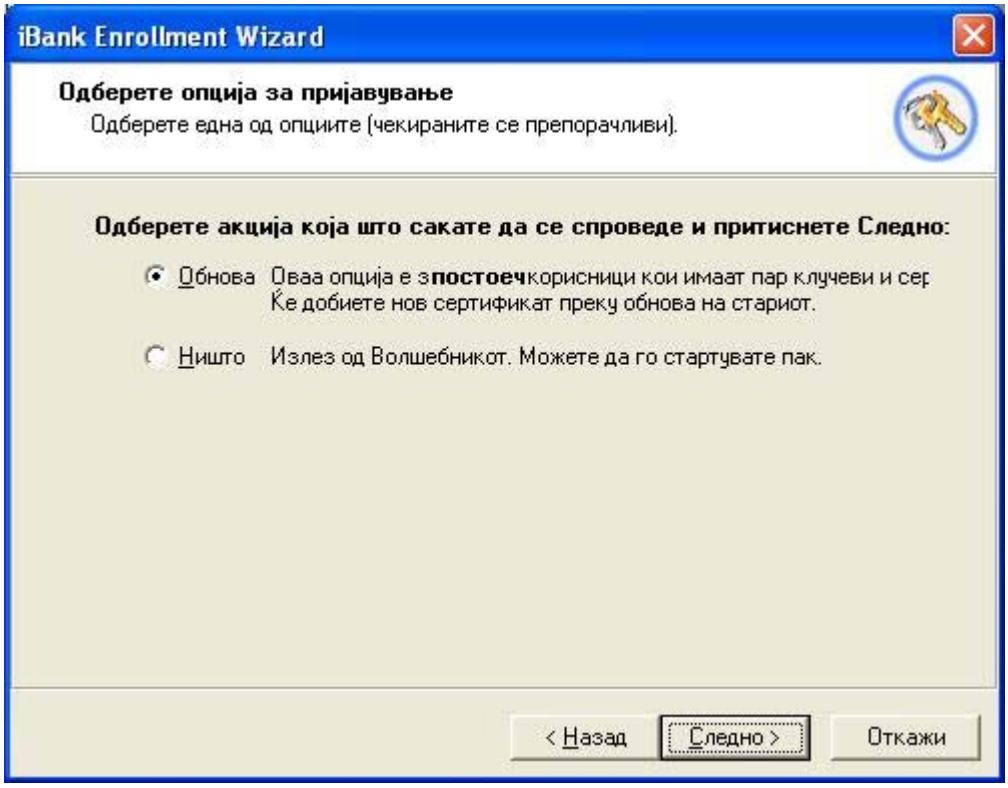
Во ова поле може да се наоѓа една од следниве информации:

- "На smart-картичката нема сертификат": доколку сертификатот навистина го нема. Во овој случај обновата не е возможна
- "Вашиот сертификат истекува… и сеуште е рано за негова обнова": времето на престанок на важност на сертификатот не е доволно скоро за да серверот за издавање на сертификати може да дозволи обнова
- "Вашиот сертификат ќе истече …и треба да го обновите": времето на престанок на важење на Вашиот сертификат е бкиску и можна е негова обнова.
- "Вашиот сертификат е истечен …и би требало итно да го обновите": сертификатот неодамна истекол, но серверот за обнова на сертификати сеуште овозможува негова обнова
- "Вашиот сертификат е истечен …и доцна е за негова обнова": сертификатот е истечен релативно поодамна и не е возможна негова обнова.

Обновата е возможна во третиот и четвртиот случај. Во останатите случаи не е: во приот обновувањето нема смисла, во вториот нема потреба за истото, а во петтиот случај е веќе прекасно. Доколку Ви се случи овој последниот случај, контактирајте ја техничката поддршка за да Ви се овозможи накнадно обновување.

Доколку обновувањето на сертификатот е возможно, во полето **Пријава за сертификат** ќе биде даден рокот во кој е можна обновата на сертификатот.

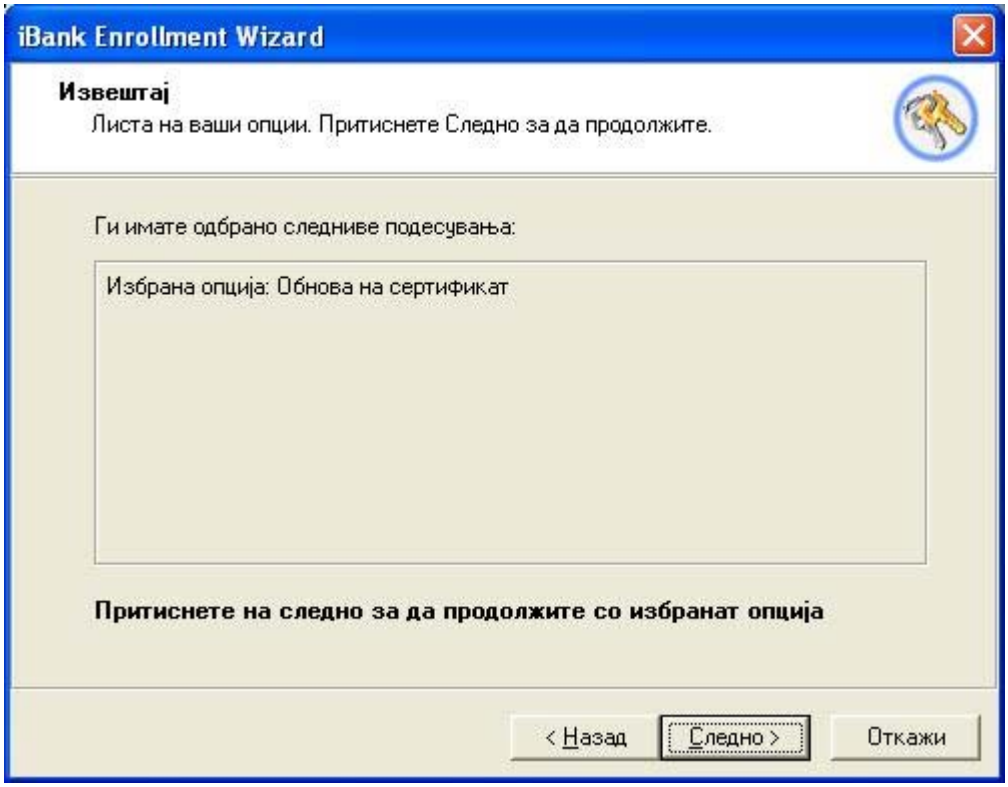
Доколку е обновата можна, со притискање на **Следно**, Волшебникот ќе прикаже страница слична како следнава слика:



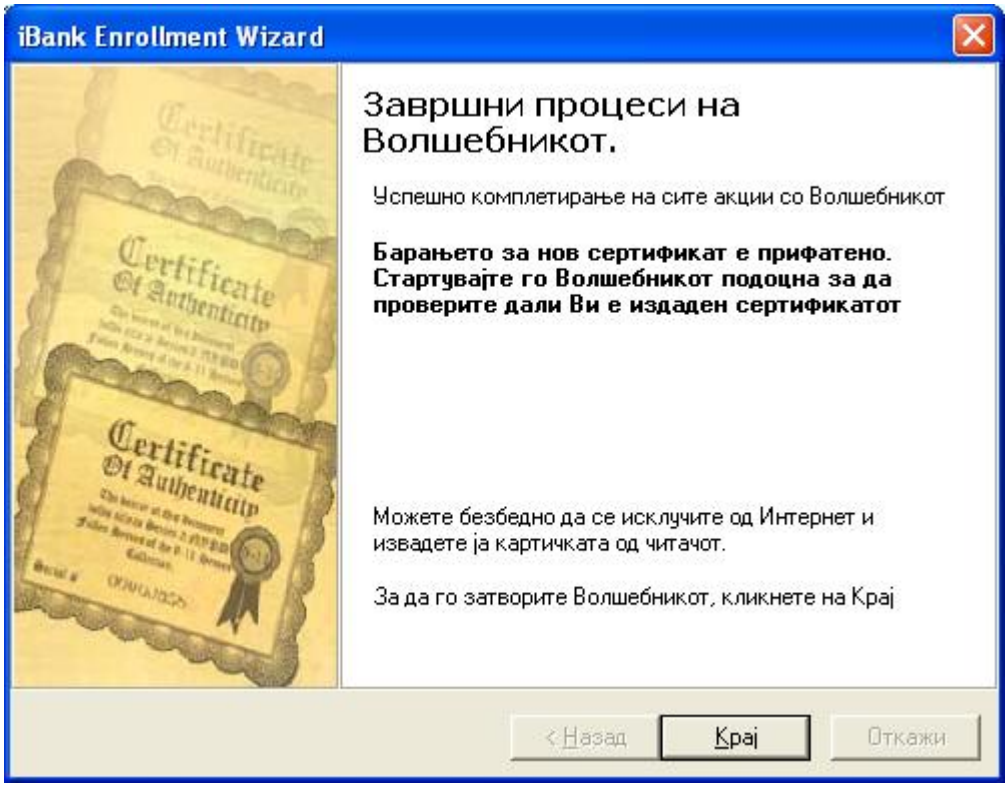
Волшебникот секогаш ги прикажува акциите кои имаат смисла за дадениот корисник, а помеѓу истите **Обновата** ќе биде меѓу препорачаните опции ако сертификатот е близу до истекување или е веќе истечен.

Кога корисникот ќе ја одбвере опцијата **Обнова** и ќе притисне **Следно**, Волшебникот во некои ситуации може да ја прикаже страната за внес на еднократниот личен ID (PID), како во §7.1. Оваа страница Волшебникот ја прикажува доколку политиката на iBank системот е подесена така што за обнова на сертификатот е потребен PID. Доколку е тоа случај, корисниот треба за оваа фаза да обезбеди PID кој што ќе го користи за обнова.

Во секој случај, без разлика дали страната за внес на PID била прикажана или не, со притискање на **Следно**, Волшебникот ја прикажува страната за потврда за избраната опција:



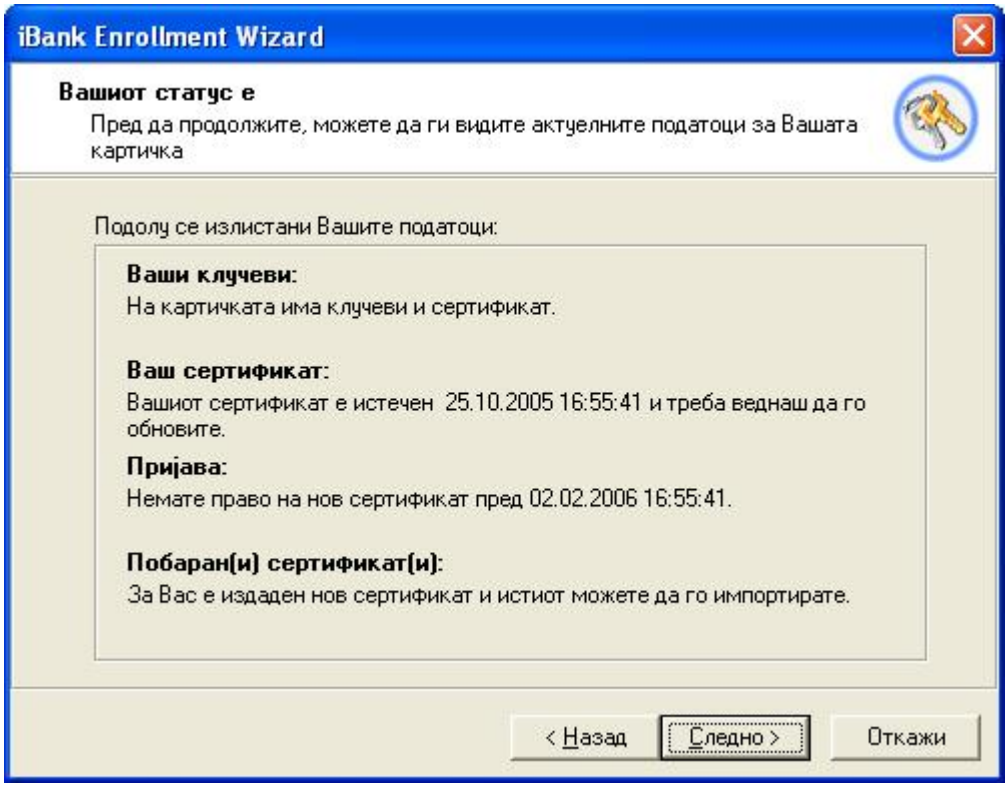
Со притискање на **Следно**, Волшебникот ги превезма податоците за корисникот од постоечкиот сертификат, прави барање за обнова на сертификат за постоечкиот јавен клуч, го праќа ова барање кон серверот за обнова на сертификат, а потоа ја прикажува страната **Комплетирање на работата на iBank Enrollment Волшебникот**:



Со притискање на **Крај**, Волшебникот ја завршува работата. За да го превземете Вашиот обновен сертификат, треба повторно да го активирате Волшебникот: Видете §7.3 за повеќе информации во врска со ова.

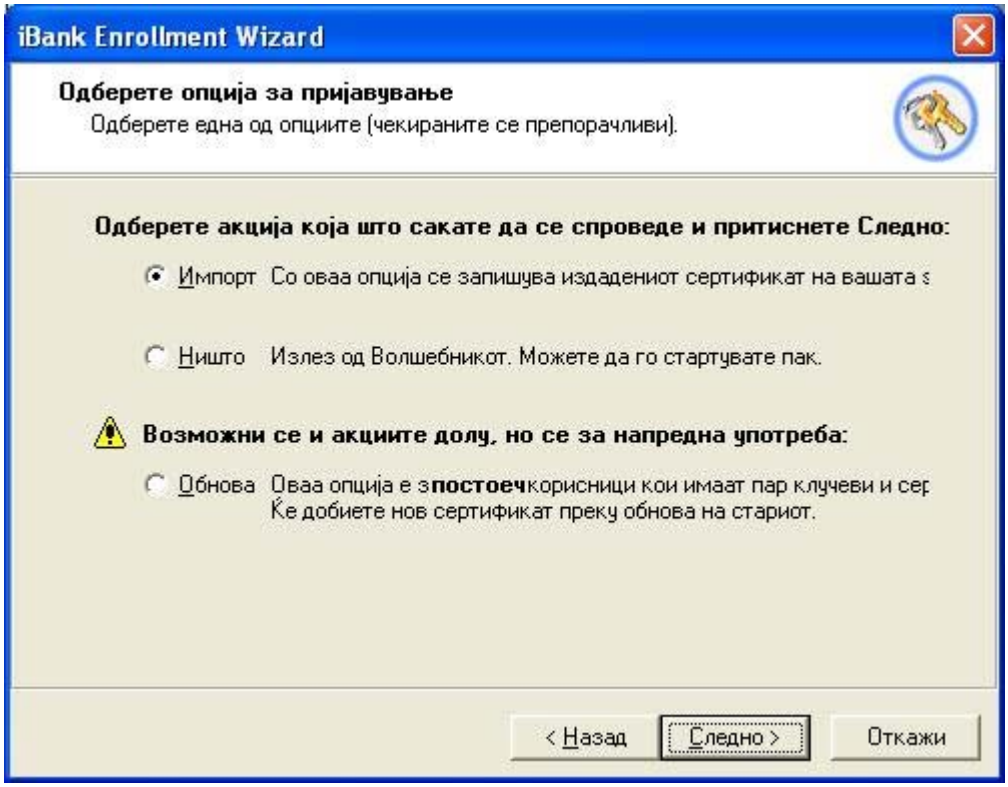
7.3. Импорт на издадениот сертификат на картичка

Активирајте го волшебникот како што е тоа опишано во §5.1. Откако ќе се пријавите на smart-картичката (§ 5.2) и на серверот за издавање на сертификати (§5.3), се прикажува страната **Детектиран статус на smart-картичката**, слична како на следнава слика:

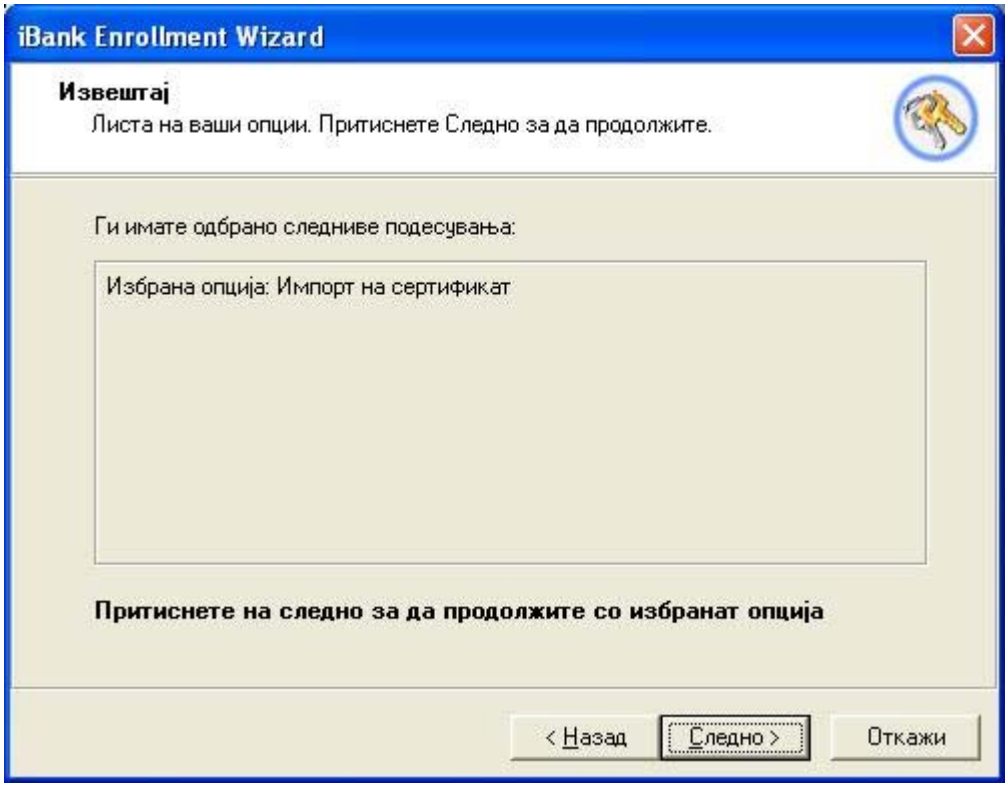


Доколку во полето **Барање(а) за сертификат** стои "новиот сертификат е во меѓувреме издадени можете да го превземете", би требало да го превземете вашиот сертификат. Ако во ова поле стои "Последниот издаден сертификат веќе сте го превзеле", тоа значи дека вашиот сертификат е веќе превземен, но Вас ништо не ве спречува да го превземете повторно, со тоа што во тој случај опцијата за превземање ќе биде сместена во "напредни" опции. Во останатите случаи, превземањето на сертификати не е можно.

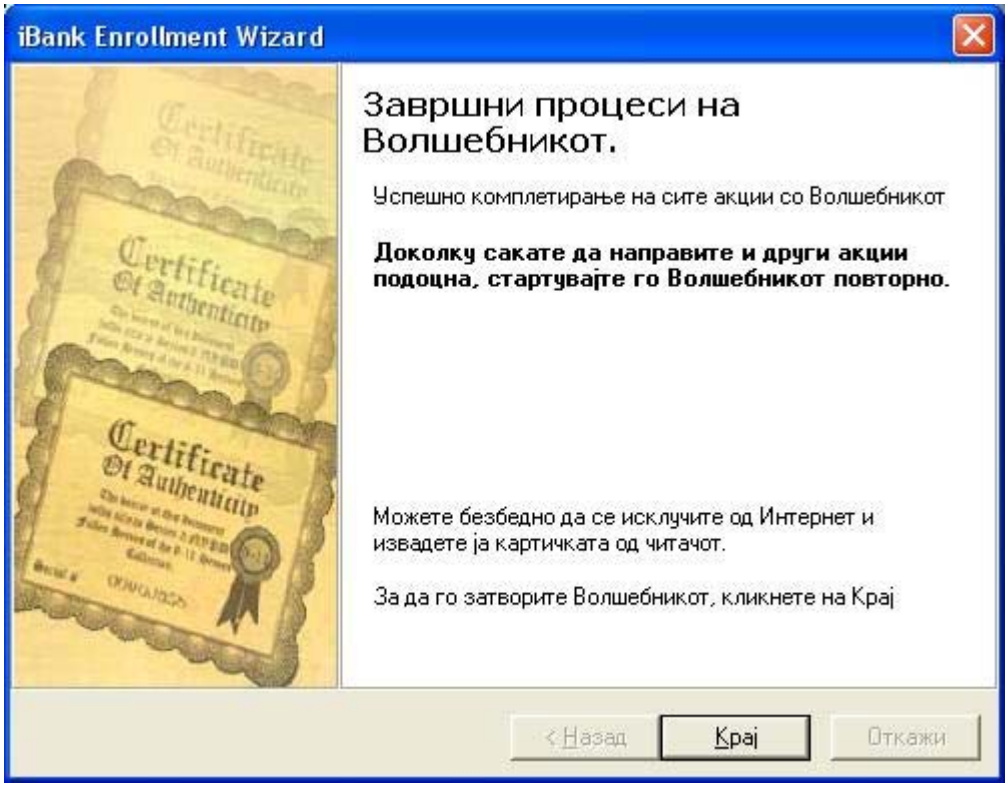
Со притискање на **Следно**, се прикажува страница како на следнава слика:



Со притискање на **Следно**, Волшебникот уште еднаш ја потврдува избраната опција:



Со наредно притискање на **Следно**, Волшебникот воспоставува врска со серверот за издавње на сертификати, го превзема сертификатот и го сместува на smart-картичка, после кое го прикажува резултатот од акцијата:



Со притискање на **Крај** Волшебникот се затвора, а smart-картичката е сега повторно спремна за користење во iBank системот.

8. Речник на поими

сертификат.....в. сертификат

čarobnjak .....в. волшебник

дигитален потпис....податок иваден од одреден документ со користење на приватниот клуч на корисникот. Со јавниот клуч може да се верификува валидноста на потписот.

enrollment .....англ. "пријава", "пријавување". Ова е вообичаен термин кој се користи за да се означи процесот на пријавување на корисникот за сертификат (в.)

јавен клуч.....*клуч* (в.) кој сочини пар со *приватниот клуч* (в.). За разлика од приватниот клуч, поправило не се држи во тајност. Од него е невозможно да се изведе приватниот клуч. Секој корисник на iBank има свој приватени јавен клуч. Јавниот клуч накорисникот се

користи за верификација на дигиталниот потпис (в.) на тој корисник и за енкрипција на податоци.

клуч .....податок во криптографијата кој се користи за трансформација на други податоци. На пример, клучот може да се користи за да се криптира одреден податок, или од одредена соџина да се добие дигитален потпис.

Приватен клуч....клуч (в.) кој сочинува пар со *јавниот клуч* (в.). приватниот клуч се држи во тајност за секој корисник (на smart-картичка (в.) или на друг медиум), и не може да се открие без разлика на тоа што соодветниот јавен клуч е публикуван. Секој корисник на iBank има свој приватен и соодветен јавен клуч. Приватниот клуч служи за потпишување од страна на тој корисник, како и за декриптирање на податоци кои му се испратени на тој корисник.

сертификат.....јавен клуч (в.) потпишан од страна на тело овластено за потпишување. Служи за да се обезбеди автентичност на јавните клучеви. Секој корисник, за да го користи iBank системот, мора да ги поседува не само својот јаван и приватен (в.) клуч, туку и соодветен сертификат. Улогата на iBank Enrollment Волшебникот е да ја олесни постапката на добивање клучеви за корисниците.

smart-картичка ...(некаде ја нарекуваат "паметна картичка"): уред со големина на кредитна картичка кои што има неколку функции кои го чинат идеален за чување на чувствителни криптографски податоци: физичка заштита на податоци, логичка заштита (преку систем на лозинка), одвивање на чувствителните криптографски податоци на самата картичка.

обнова .....процедура со која корисникот кој веќе има сертификат кој одговара на неговиот јавен клуч добива нов сертификат кој одговара на неговиот јавен клуч, но со продолжено времетраење.

9. Индекс