

HRVATSKI ZAVOD ZA ZDRAVSTVENO OSIGURANJE  
Direkcija - Služba za informatiku  
Zagreb, 27.09.13

## **Upute za AKDSH- aplikacija za digitalni potpis datoteka ver 1.2.1**

AKDSHCard Data Signer And Verifier ver 1.2

AKDSHCard utility ver. AKDSHCard DLL 1.22

Verzija uputa: 1.2.1

Datum izmjene: 27.09.2013

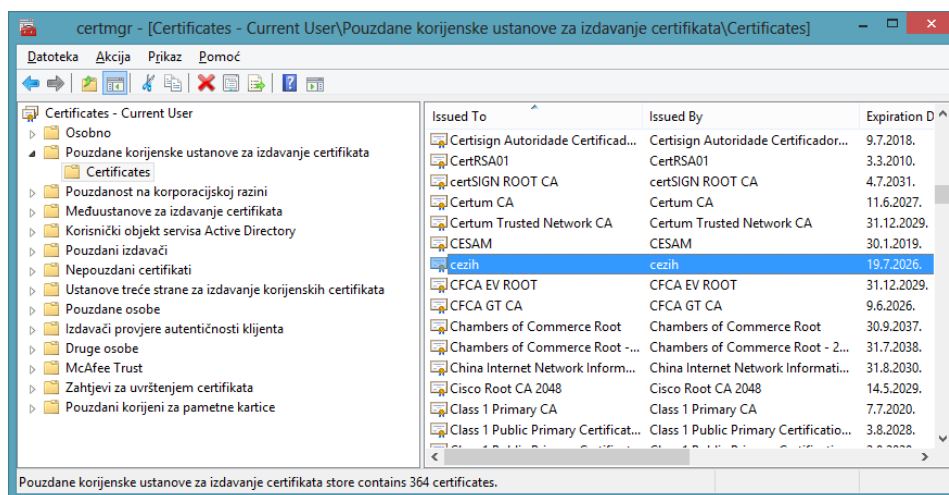
## 1. Instalacija programa

Jedna od novosti u odnosu na prethodnu verziju je i sama instalacijska procedura koja prije nije bila automatizirana.

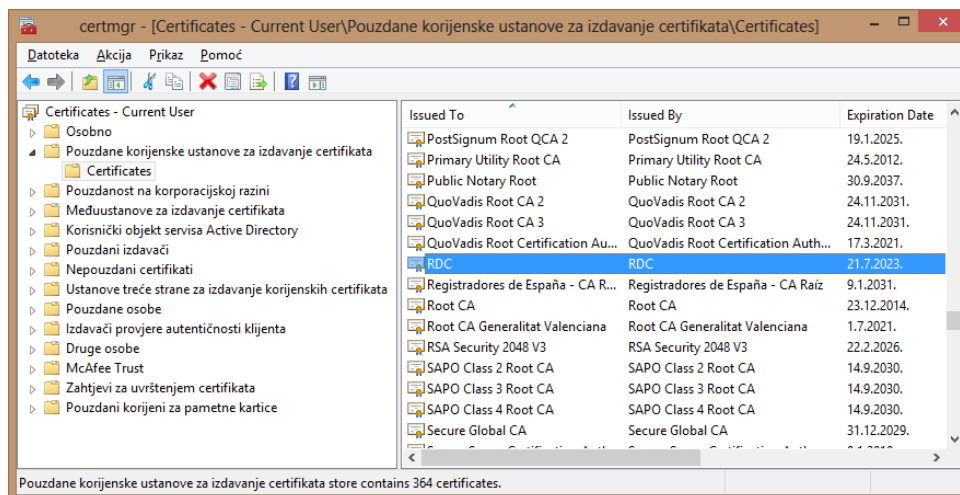
Postupak instalacije je uobičajeni pa ne navodimo detalje osim slijedeće što je potrebno:

- Prije instalacije, nužno je iz računala (čitača pametnih kartica) izvaditi pametnu karticu ukoliko je u čitaču.
- Pokretanje instalacije s administratorskim ovlastima
- U prvoj fazi program detektira prethodne verzije upravljačkih programa za HZZO pametnu karticu i deinstalira
- U jednom trenutku program traži da odlučite da li želite dodati prečace na radnu površinu – predlažemo da potvrdno odgovorite.
- Nakon završene instalacije predlažemo da se napravi restart računala.

Za potpisivanje HZZO pametnom karticom, osim osobnog certifikata koji je na HZZO pametnoj kartici potrebno je imati instaliran i korijenski certifikat kojeg možete skinuti sa ovog linka: <http://www.cezih.hr/certifikat/cacert.crt>. Certifikat mora biti instaliran kao na slici:



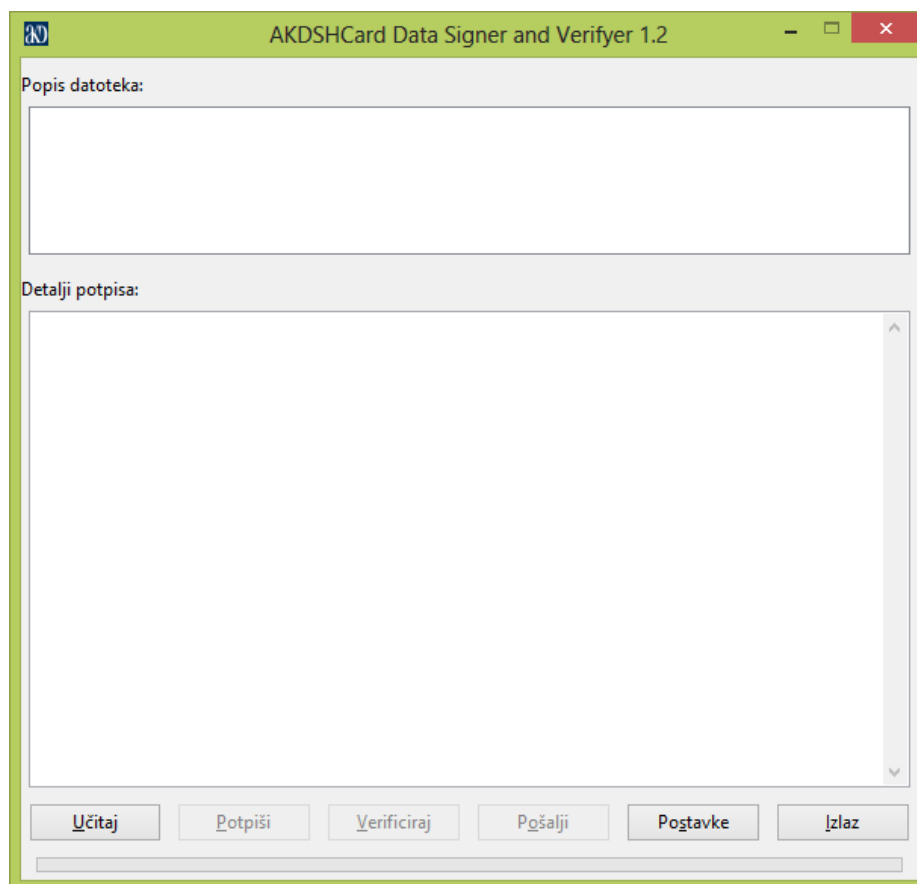
Ukoliko trebate verificirati potpisi dokumenata koji su načinjeni FINA pametnom karticom tada trebate imati instalirani FINA root certifikat kojeg možete skinuti sa <http://rdc.fina.hr/CA/RDCca.cer>. Certifikat mora biti instaliran kako je na slici.



Učitavanje osobnog certifikata trebalo bi se izvršiti kod samog umetanja pametne kartice u čitač kartica. Naravno, preduvjet je ispravna instalacija čitača kartica na operativni sustava. Moguće rješenje problema koji se pojavljuju pročitajte u [Dodatku A](#), na kraju uputa.

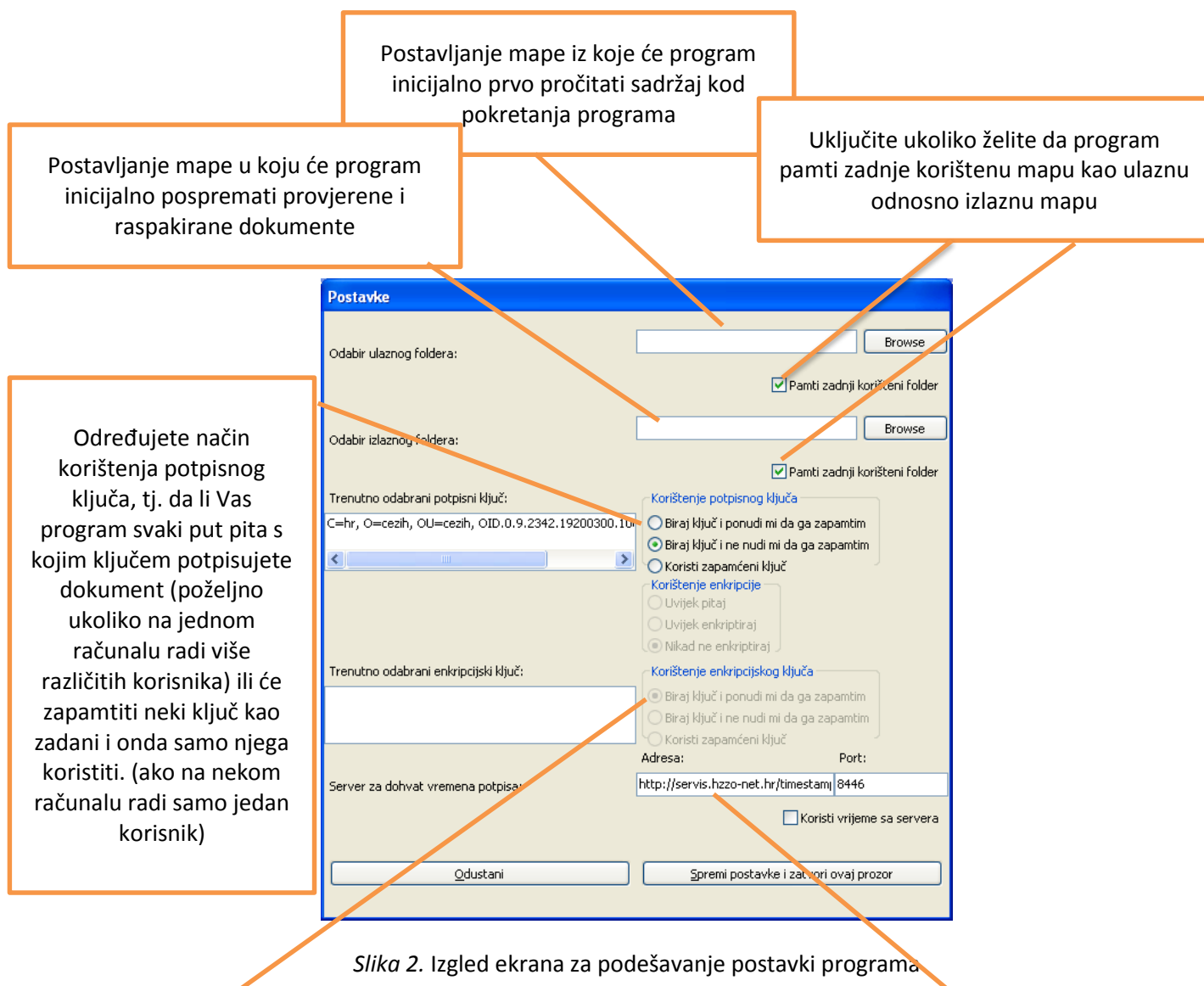
## 2. Pokretanje i podešavanje parametara programa

Nakon pokretanja programa dobije se ekranska slika kako je to na slici 1.



Slika 1. Izgled programa

Parametre programa podešavamo na opciji „Postavke“. Odabirom navedene opcije otvara se slijedeći ekran sl.2.



Slika 2. Izgled ekrana za podešavanje postavki programa

Trenutno nije omogućeno, ali program može i enkriptirati dokument koji se potpisuje. Biti će raspoloživo u nekoj budućoj verziji

Adresa servisa s kojeg program dobiva službenu informaciju o vremenu potpisa:

<http://servis.hzzo-net.hr/timestamp-1/rest/timestamp>

Port je 8446.

Ukoliko ISKLJUČIVO želite to vrijeme onda treba uključiti opciju ispod „Koristi vrijeme sa servera“. Vremenski server HZZO-o je trenutno van funkcije pa se predlaže ne uključivanje te opcije.

Opcije podešavanja dovoljno je postaviti prvi put prilikom pokretanja aplikacije ili naknadno ukoliko želimo promijeniti određene funkcionalnosti

### 3. Postupak potpisivanja dokumenta

Program se može koristiti za potpisivanje određene vrste datoteka pohranjenih u digitalnom obliku na Vašem računalu. Popis dozvoljenih vrsta datoteka definiran je u dokumentu: *whiteList.wt*. Ukoliko imate potrebu da se neka Vaša vrsta dokumenta uvrsti na popis dozvoljenih za potpis ([Dodatak B](#)) - pošaljite zahtjev na elektronsku poštu [helpdesek@hzzo.hr](mailto:helpdesek@hzzo.hr) u kojem će te objasniti razloge zašto Vam to treba. Vaš zahtjev će biti analiziran i ukoliko je opravdan nova datoteka *whiteList.wt* biti će objavljena na portalu od kuda će te je moći skinuti.

Ovisno o vrsti datoteke koju potpisujete pokreće se i program koji Vam prije samog potpisivanja prikazuje „što potpisuje“. Ukoliko na svom računalu nemate standardni program za tu vrstu dokumenta – program će Vas pitati kojim programom želite prikazati dokument. Potpisivanje je moguće raditi s HZZO pametnom karticom.

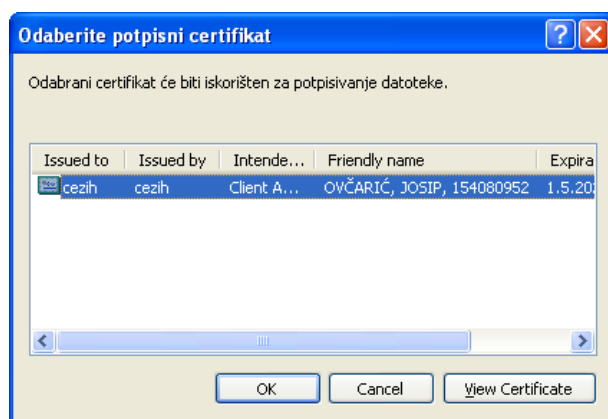
Postupak potpisivanja datoteke provodi se u dva koraka:

#### 3.1. Odabir (datoteka) dokumenata za potpis

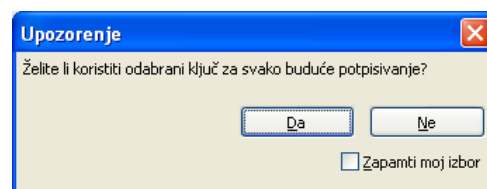
Na početnom ekranu se izabere opcija „Učitaj“. Treba napomenuti da program može odjednom potpisati više različitih datoteka. Popis svih odabranih datoteka prikazati će se u gornjem dijelu početnog ekrana (Slika 1.). Postupak odabira datoteka podrazumijeva označavanje datoteka na Vašem računalu koje želite potpisati, te ga nije potrebno dodatno objašnjavati.

#### 3.2. Potpisivanje i spremanje potpisanih dokumenata (datoteka)

Ako smo uspješno završili prethodni korak tada kliknemo na gumbić „Potpiši“ i program nas prvo pita s kojim ključem potpisujemo (slika 3.). Ukoliko nismo u „Postavkama“ programa prethodno ništa postavili – pitanje na koje je potrebno odgovoriti je da li želimo odabrani ključ koristiti za buduća potpisivanja? Ono što odgovorite sprema se u „Postavke“ programa. (Slika 4)

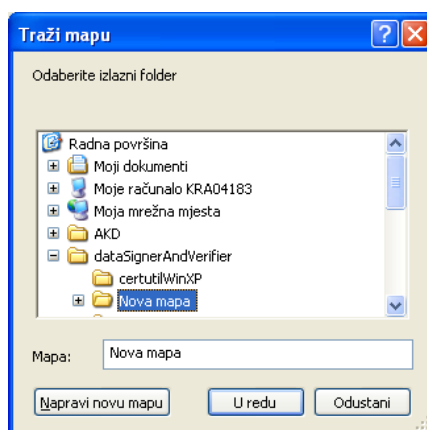


Slika 3. Odabir ključa za potpis

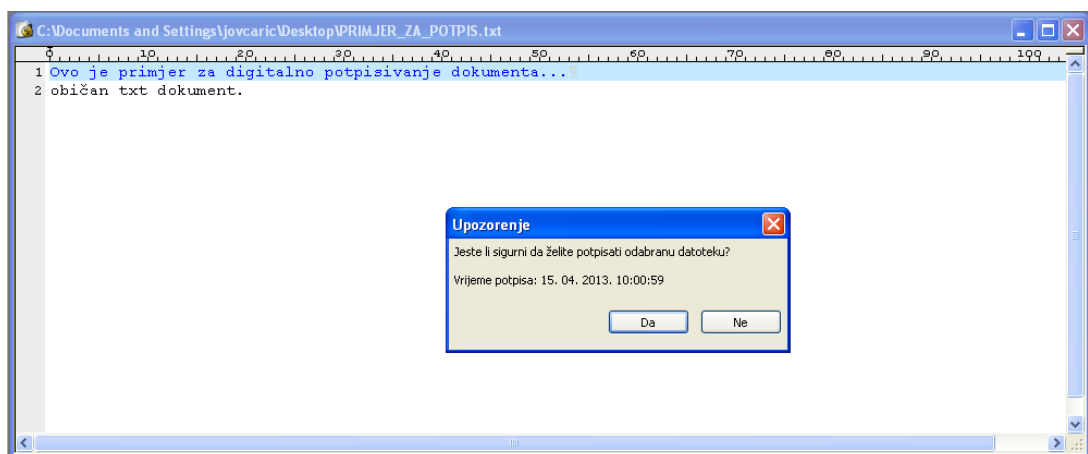


Slika 4. Potvrda

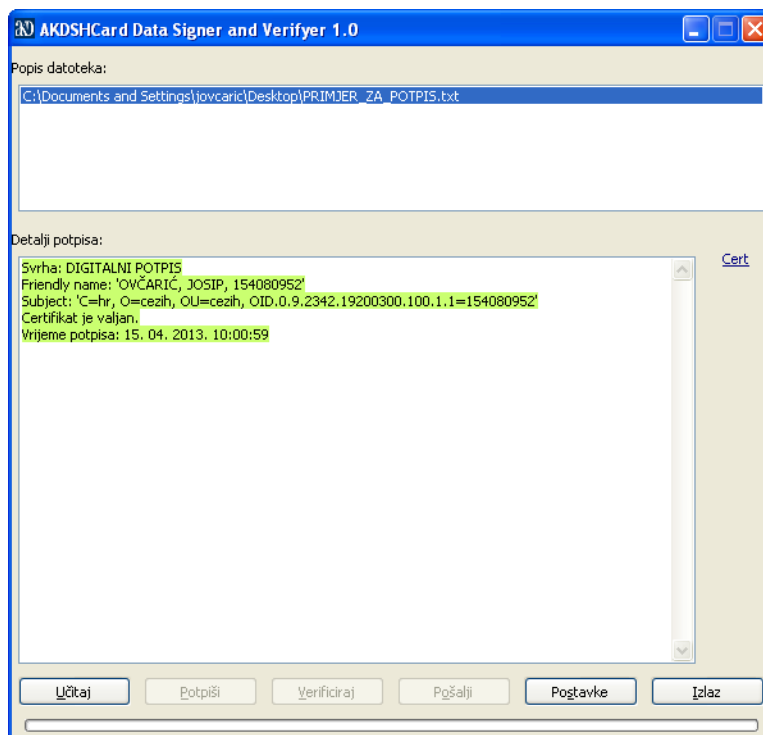
Nakon toga potrebno je odabrati lokaciju spremanja potpisane datoteke (slika 5.)



*Slika 5.* Odabir mape gdje će se pospremiti digitalno potpisani dokument (datoteka)  
Prije samog potpisa korisniku je na ekranu vidljiv sadržaj dokumenta kojeg potpisuje, te se još jednom traži potvrda potpisivanja. (Slika 6.). Ukoliko pritisnete gumbić „Da“ program Vas još pita za PIN te ukoiko je s Vašim ključem sve u redu prikazuje ze konačan rezultat potpisa – Slika 7., a digitalno potpisani dokument možete preuzeti u mapi koju ste odredili na slici 5.

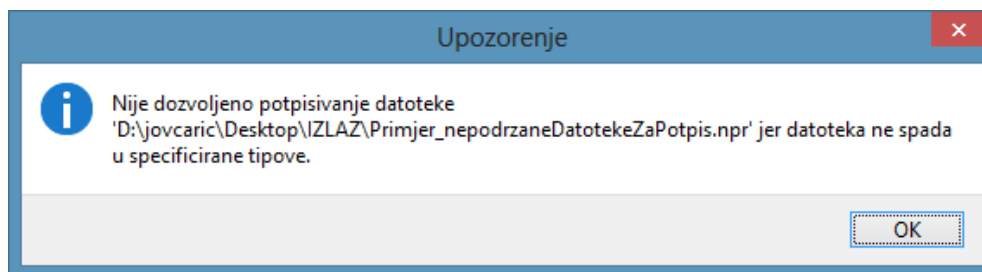


*Slika 6.* Prikaz i samo potpisivanje dokumenta



Slika 7. Uspješno izvršeno potpisivanje

Ukoliko ste za potpisivanje odabrali vrstu datoteke koja nije definirana u *whiteList.wt* ([Dodatak B](#)) npr. „Primjer\_nepodrzaneDatotekeZaPotpis.npr“ tada kod pokušaja potpisivanja takve datoteke javlja se slijedeća poruka:





#### 4. Postupak provjera digitalno potpisanih dokumenata

Slično postupku potpisivanja i ovaj postupak ide u dva koraka. Treba napomenuti da sam korisnik programa korištenjem „Postavki“ programa može prilagoditi program njegovim navikama i željama. Mogući su slijedeći osnovni scenariji:

- na nekoj ulaznoj mapi se nalaze svi digitalno potpisani dokumenti koje treba verificirati te će se isti spremati na jednu izlaznu mapu
- program svaki put pita s koje lokacije da učitati ulazni dokument, ali pri tome može i ne mora zapamtiti gdje je zadnje učitavao
- program uvijek gleda istu ulaznu mapu (npr. slovnu oznaku CD/DVD uređaja ili sl.)

Mjesto gdje će pospremati verificirane dokumente – ovisno o navici korisnika – bilo bi poželjno da svaki put odredi sam korisnik ili da se koristi opcija „zadnje zapamćene lokacije spremanja“ (preporuka)

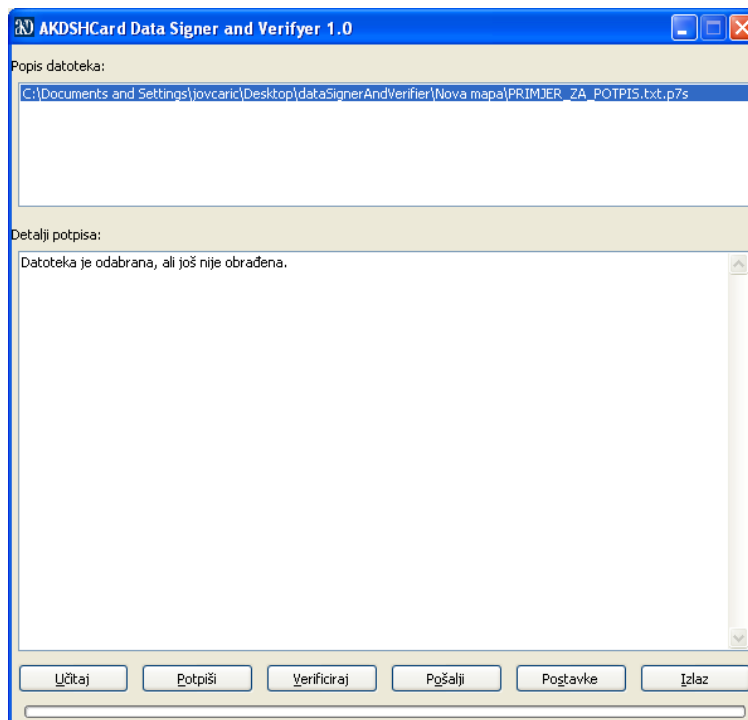
Moguće je vršiti provjeru dokumenata koji su potpisani bilo FINA pametnom karticom ili HZZO pametnom karticom.

##### 4.1. Odabir dokumenata za verifikaciju

Na početnom ekranu se klikne gumbić : „Učitaj“. Treba napomenuti da program može sekvencijalno odjednom provjeriti više različitih datoteka. Popis svih odabranih prikazati će se u gornjem dijelu početnog ekrana (Slika 1.). Postupak odabira je uobičajen i klasičan te nema potrebe ga ovdje posebno pojašnjavati.

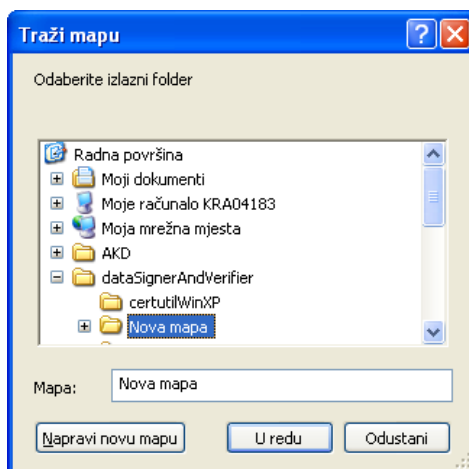
##### 4.2. Verifikacija i spremanje provjerenog dokumenta bez ključa

Nakon što smo odabrali dokument(e) koji želimo provjeriti kliknemo na gumbić „Verificiraj“ (Slika 8.)



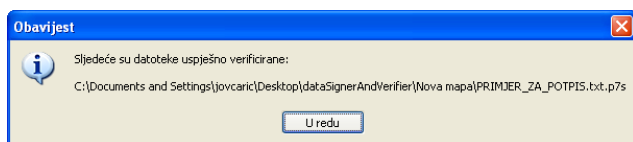
Slika 8. Provjera digitalno potpisanog dokumenta

U slijedećem koraku program traži da se odredi mjesto spremanja provjerenog dokumenta (slika 9.) gdje ovisno o „Postavkama“ program nudi lokaciju, uz napomenu da nakon pokretanja programa, kod prvog korištenja opcije „Verificiraj“ – uvijek nudi zadanu mapu u „Postavkama“

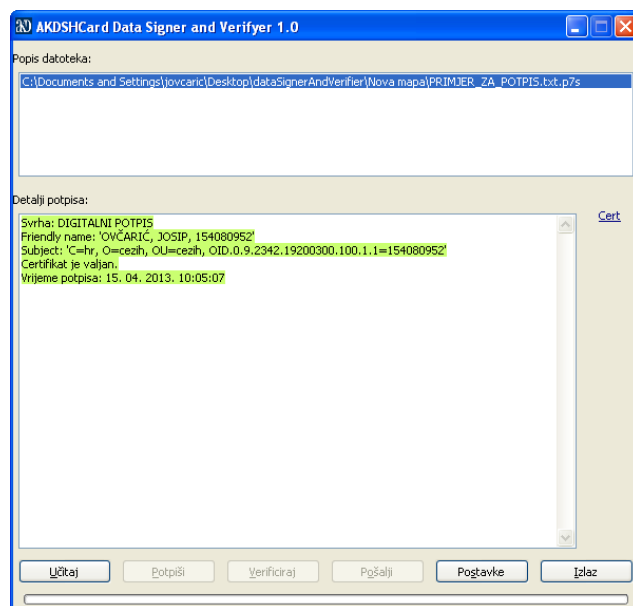


Slika 9. Određivanje mape gdje će biti pospremljen dokument nakon verifikacije

Ukoliko je sve u redu pojavljuje se ekran kao na slici 10. odnosno 11.



Slika 10. Informacija o rezultatu verifikacije



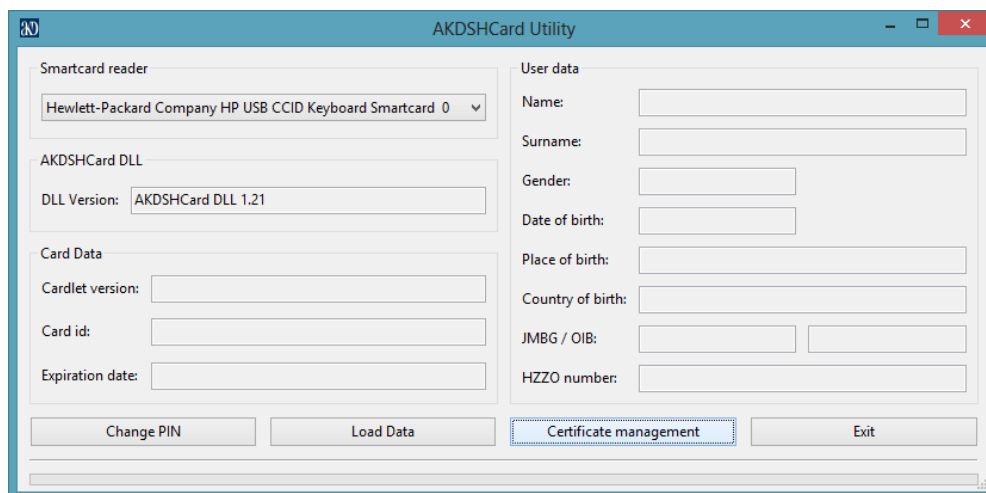
Slika 11. Informacija o rezultatu verifikacije

Napomene: Neki tipični ekrani/situacije nisu u ovim uputama jer se smatraju uobičajenim (npr. ukoliko na nekoj mapi već postoji dokument istog naziva, a mi tamo želimo kopirati neki drugi tog istog naziva – onda program daje ekrane upozorenje i sl.)

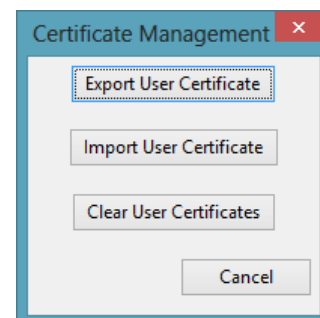
## DODATAK A: Problem kod ne učitavanja osobnog certifikata

Ukoliko se Vaš osobni certifikat ne učita kod prvog stavljanja pametne kartice u čitač pametnih kartica predlažemo da učitavanje izvršite ručno na način:

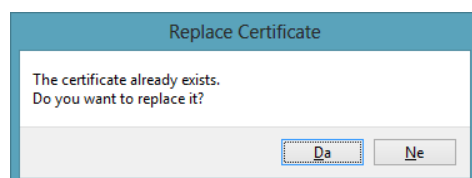
1. Pokrenite AKDSCard Utility i kliknite na gumb „Certificate management“



2. Na manjem ekranu koji se prikaže – odaberite „Import User Certificate“



3. Ukoliko osobni certifikat već postoji na računalu pojavit će se poruka kako je na slici ispod, a ako ne – certifikat će se učitati



DODATAK B: Popis vrsta datoteka dozvoljenih za digitalno potpisivanje (*whiteList.wt ver.1.0 od 12.06.2013.*)

<b>VRSTA DATOTEKE</b> <i>(gdje je X dekadaska znamenka)</i>	<b>NAČIN PRIKAZA</b>
<b>pXX</b>	Datoteka se otvara kao običan tekst
<b>XXX</b>	Datoteka se otvara kao običan tekst
<b>XXXX</b>	Datoteka se otvara kao običan tekst
<b>bXX</b>	Datoteka se otvara kao običan tekst
<b>lXX</b>	Datoteka se otvara kao običan tekst
<b>oXX</b>	Datoteka se otvara kao običan tekst
<b>unl</b>	Datoteka se otvara kao običan tekst
<b>npX</b>	Datoteka se otvara kao običan tekst
<b>npXX</b>	Datoteka se otvara kao običan tekst
<b>kXX</b>	Datoteka se otvara kao običan tekst
<b>eXX</b>	Datoteka se otvara kao običan tekst
<b>psXX</b>	Datoteka se otvara kao običan tekst
<b>txt</b>	Datoteka se otvara kao običan tekst
<b>tmp</b>	Datoteka se otvara kao običan tekst
<b>doc</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>docx</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>dot</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>dotx</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>rtf</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>xls</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>xlsx</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>ppt</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>pptx</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>pps</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>ppsx</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>pst</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>eml</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>odt</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>ods</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>jpg</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>bmp</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>tif</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>gif</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>wmf</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>png</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>avi</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>mp4</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>wmv</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>mpeg</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>mov</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>divx</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>mp3</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>ra</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>wav</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)

<b>VRSTA DATOTEKE</b> <i>(gdje je X dekadaska znamenka)</i>	<b>NAČIN PRIKAZA</b>
<b>wma</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>zip</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>rar</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>7z</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>gz</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>tar</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>arj</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>tgz</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)
<b>pdf</b>	Datoteka se otvara pomoću dedikirane aplikacije (native aplikacije)