Uputa za korištenje aplikacije

Web e-Potpis

Ver. dok. 1.6
Aplikacija v4.2.2
Zagreb, siječanj, 2024.

Sadržaj:

1. UVOD

Elektronički potpis predstavlja generički pojam koji podrazumijeva čitav niz različitih vrsta digitalno prikazanih podataka pomoću kojih se vrši identifikacija korisnika i provjera vjerodostojnosti potpisanoga elektroničkog dokumenata. Njegovim se korištenjem osigurava autentičnost[1], integritet[2] i neporecivost[3] dokumenta.

1.1. Cilj i svrha

Aplikacija *Web e-Potpis* je napravljena u svrhu zaštite elektroničkih dokumenata i podataka. Cilj aplikacije *Web e-Potpis* je izrada i validacija elektroničkog potpisa za bilo koji tip ulazne datoteke (npr. PDF dokumenti, Microsoft Office dokumenti - Word, Excel, PowerPoint, Notepad, itd.).
Aplikacija ima mogućnost ugradnje vremenskog žiga[4], te brojanjem obavljenih akcija omogućuje naplatu po ostvarenim radnjama za određenog krajnjeg korisnika.

1.2. Područje primjene

Aplikacija *Web e-Potpis* je namijenjena korisnicima koji imaju osobne[5], poslovne[6] ili TDU[7] certifikate[8], a datoteke se potpisuju pojedinačnim odabirom od strane korisnika.

Korisniku je omogućen pristup aplikaciji preko web preglednika putem digitalnih certifikata na kripto uređaju (USB token/smart kartica)[9] i *Fininim* certifikatom. Aplikacija može potpisati datoteke isključivo *Fininim* ***kvalificiranim***[10] i ***normaliziranim***[11] certifikatima.

2. POJMOVI I SKRAĆENICE

- **Fina** - Financijska agencija
- **Potpisni profil** - predložak koji popunjava standardne vrijednosti kod potpisivanja s upisanim vrijednostima trenutno odabranog profila
- **PKI modul** – rješenje koje se koristi za potpisivanje podataka elektroničkim potpisom, podrazumijeva komponentu za korištenje u Web aplikacijama za potpisivanje gdje

[1] Primatelju poruke garantira se da smo mi stvarno poslali sadržaj dokumenta, a ne netko drugi tko bi se lažno predstavio u naše ime.
[2] Sigurnost da podaci u prijenosu ili obradi nisu uništeni ili promijenjeni. Elektroničkim potpisom osigurava se cjelovitost i izvornost podataka.
[3] Onemogućavanje poricanja (negiranja) akcije koje je osoba poduzela ili autorizirala.
[4] Podatkovni objekt koji nedvojbeno i nerazdvojivo povezuje određene podatke s određenim vremenom, čime je omogućeno dokazivanje postojanja tih podatka prije tog vremena. Vremenski žig (timestamp) ovjerava elektronički potpisane podatke o pouzdanom vremenu postojanja podataka zajedno s *hash* prezentacijom tih podataka.
[5] Građani – fizičke osobe
[6] Fizičke osobe povezane s poslovnim subjektom/organizacijom, poslužitelj povezan s poslovnim subjektom/organizacijom, aplikacija/servis povezana s poslovnim subjektom/organizacijom, uređaj-VPN povezan s poslovnim subjektom/organizacijom
[7] Za tijela državne uprave (osobe /zaposlenici)
[8] Digitalni certifikat je skup podataka u elektroničkom obliku koji predstavlja svojevrsnu elektroničku iskaznicu kojom se može jedinstveno identificirati osoba, poslužitelj, aplikacija ili neki drugi uređaj.
[9] Kripto uređaj je uređaj u koji je ugrađen čip na kojemu su pohranjeni digitalni certifikati.
[10] Upotrebljava se za elektroničko potpisivanje dokumenata ili transakcija. Kvalificirani certifikat i uporaba ključa u elektroničkom poslovanju jamči autentičnost, cjelovitost, izvornost i neporecivost.
[11] Upotrebljava se za autentifikaciju odnosno enkripciju (zaštitu tajnosti podataka) te za njihovu kombinaciju. Taj certifikat i uporaba ključa od strana uključenih u e-poslovanje osigurava autentičnost, cjelovitost, izvornost i tajnost. Ne osigurava neporecivost.

potpisivanje elektroničkim potpisom vrše krajnji korisnici. Krajnji korisnik na svom računalu instalira .exe datoteku. Instalacija se vrši samo jednom, a svako sljedeće ažuriranje vrši se automatski. Osnovna je prednost ove komponente što korisnicima omogućuje rad u različitim preglednicima i nije ovisna o klijentskoj Javi što znači da korisnik ne mora voditi računa o verziji Jave i pregledniku koji koristi.

3. PREDUVJETI KORIŠTENJA

Za korištenje aplikacije *Web e-Potpis* potrebno je imati sljedeće:

- Osobno računalo
- Operativni sustav: Windows 8 ili noviji
- Pristup Internetu
- Internetski preglednici: Google Chrome, Opera, Mozilla Firefox, Microsoft Edge
- Fina USB token/kartica ili CoBranding USB token/kartica poslovnih banaka u kojoj je integriran odgovarajući Finin digitalni certifikat
- Program za upravljanje USB tokenima/karticama (npr.SafeNet Authentication Client, ActiveClient, verzija 7.x ili viša, middleware za USB tokene/kartice)[12]
- Čitač smart kartice za Fina karticu ili CoBranding karticu
- Preporuka je koristiti najnoviju verziju Adobe Reader-a
- Instalirana PKI datoteka

4. PREGLED APLIKACIJE

Funkcionalnosti aplikacije *Web e-Potpis* su sljedeće:

1. elektroničko potpisivanje
2. validacija potpisa
3. ugradnja vremenskog žiga od strane potpisnika
4. dugoročna validacija/valjanost potpisa
5. podešavanje korisničkih profila

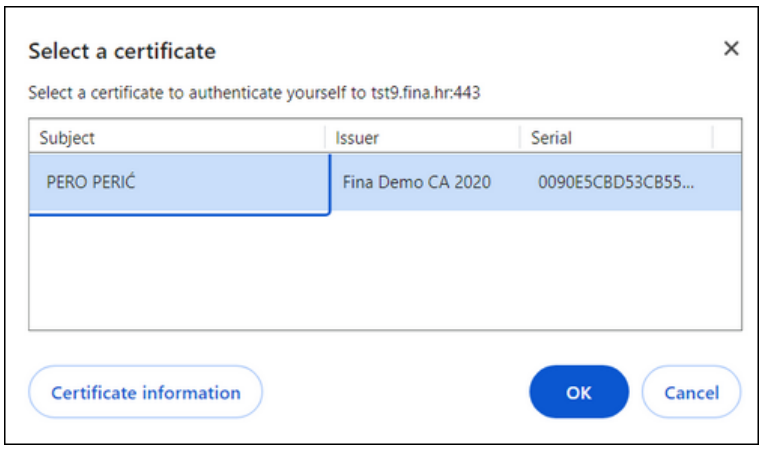
5. OPIS EKRANA

5.1. Početni ekran aplikacije – inicijalna prijava neregistriranog korisnika

Pristup aplikaciji ostvaruje se unosom adrese https://eposlovanje.fina.hr/WebEPotpis u internetski preglednik. Samim pristupom stranici otvara se pop-up prozor za odabir certifikata. Ako se pop-up prozor nije pojavio, potrebno je provjeriti je li kartica umetnuta u čitač (svjetlo na čitaču ne smije treperiti), ili USB token u računalo, kao i ispunjenost svih tehničkih preduvjeta za aplikaciju *Web e-Potpis* (poglavlje 3).

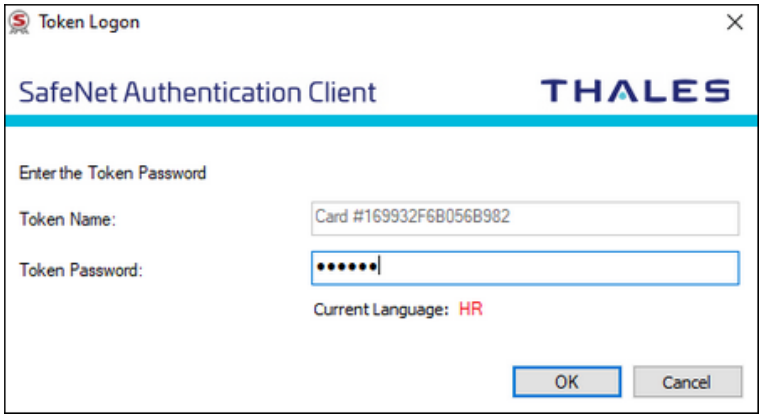
Ovisno o internetskom pregledniku, izgled ekrana može biti drugačiji, primjer za Google Chrome prikazuje Slika 1.

[12] Prilikom prijave na aplikaciju Web e-Potpis moguće je da internetski preglednici na operacijskom sustavu Microsoft Windows 8 uredno prepoznaju certifikat ako je verzija programa ActiveClient 7.x.



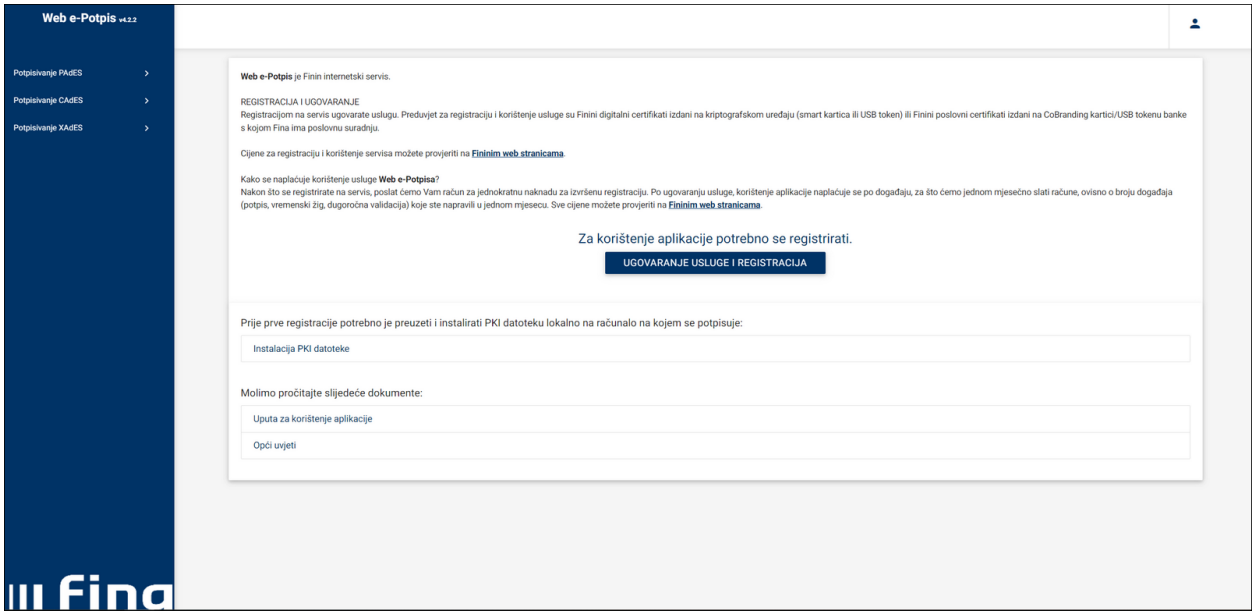
Slika 1. Odabir certifikata u internetskom pregledniku Google Chrome

NAPOMENA:
U pop-up prozoru bit će ponuđeni svi certifikati kojima se korisnik prijavljivao na računalu i kojim se trenutno koristi. Potrebno je odabrati odgovarajući certifikat za autentifikaciju.
Nakon odabira odgovarajućeg certifikata, otvara se prozor za unos PIN-a za korištenje odabranog certifikata (Slika 2).



Slika 2. Unos PIN-a

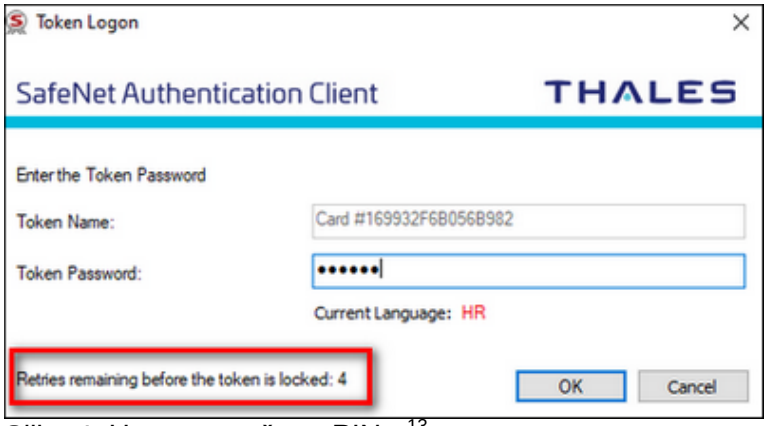
U slučaju da korisnik nije registriran otvara se ekran koji sadrži poveznicu za Web e-Potpis registraciju, poveznice na korisničke upute, opće uvjete, ali i instalacijske datoteke za PKI module (32-bit i 64-bit verzije) kao što prikazuje Slika 3.



Slika 3. Prijava u aplikaciju neregistriranog korisnika

5.1.1. Neuspješna prijava u aplikaciju

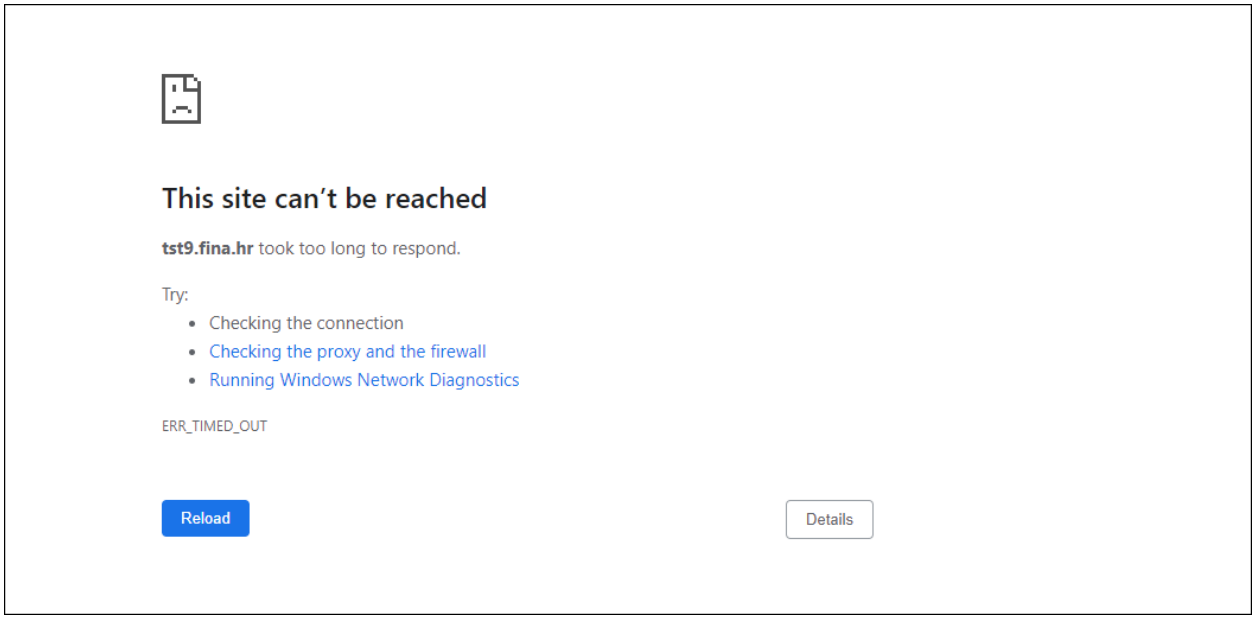
Ako korisnik nije unio ispravan PIN na ekranu će se pojaviti sljedeća poruka (Slika 4).



Slika 4. Unos pogrešnog PIN-a[13]

Ako prijava nije uspjela, može se pojaviti ovakav ekran (Slika 5).

[13] USB token/kartica će se zaključati ako se pet puta unese pogrešan PIN.
U slučaju da se USB token/kartica zaključa, ovisno o vrsti kripto uređaja potrebno je kod sigurnog kripto uređaja doći na šalter Fine kako bi se izvršilo otključavanje istog, pod uvjetom da je navedeno moguće. Kod QSCD kripto uređaja potrebno je postupiti prema uputi za otključavanje QSCD kripto uređaja koja se nalazi na sljedećoj poveznici https://rdc.fina.hr/upute/Aktivacija_i_otkljucavanje_QSCD_uredjaja.pdf .
Pokušaj otključavanja sa proizvoljnim pogrešnim upisivanjem unlock code-a rezultira nepovratnim zaključavanjem USB tokena/kartice, što konačno ima za posljedicu opoziv certifikata i izdavanje novog (naplaćuje se).
Ako se radi o CoBrending USB tokenu/kartici, korisnik se treba obratiti službi korisničke podrške same banke.



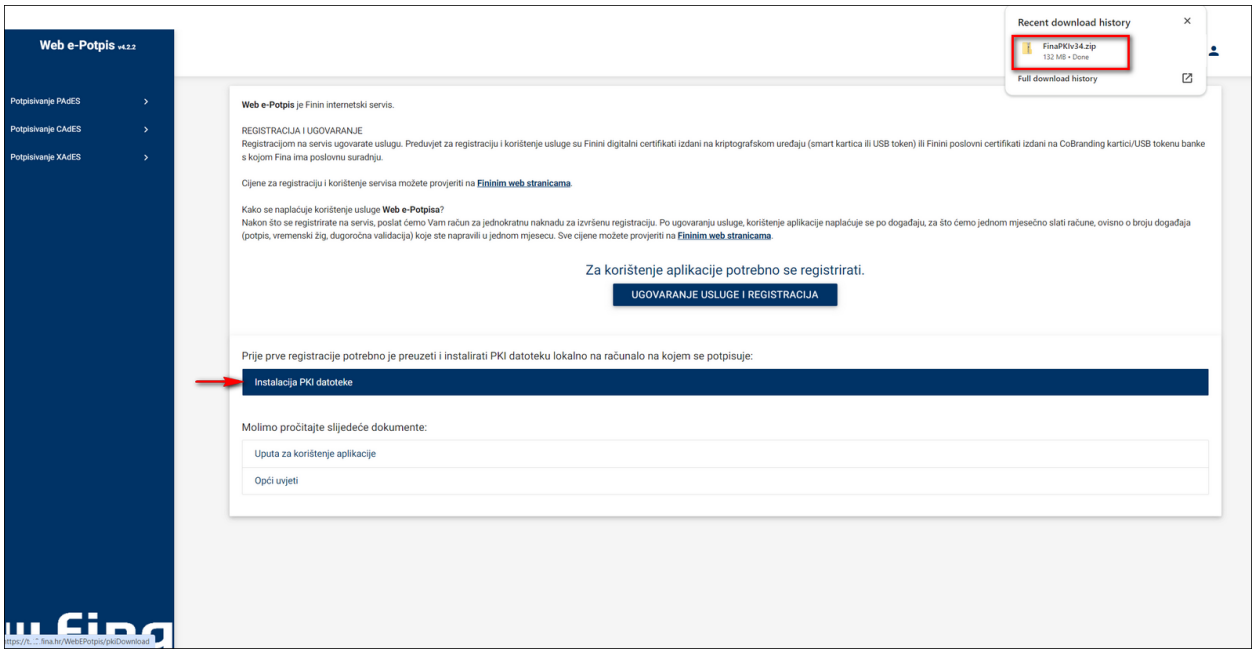
Slika 5. Neuspješna prijava u aplikaciju

5.2. Instalacija PKI modula

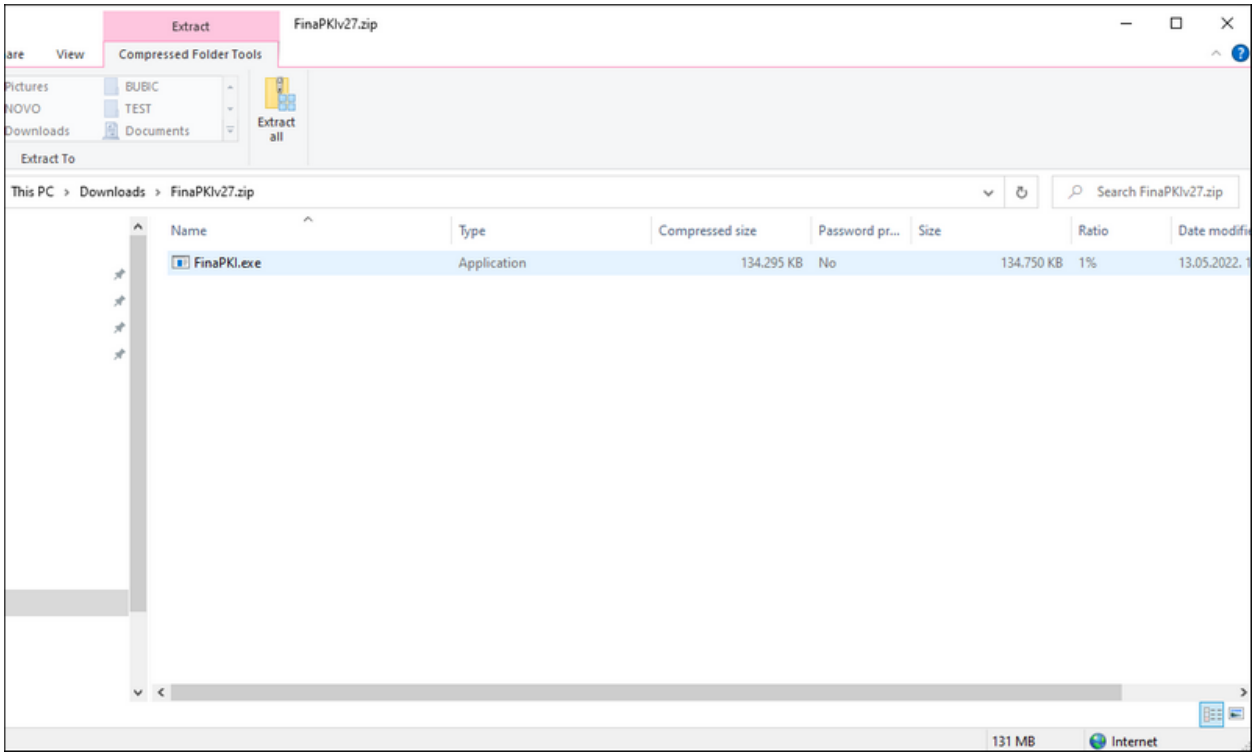
Prije prvog potpisivanja te registracije potrebno je preuzeti i instalirati PKI datoteku lokalno na računalo na kojem se potpisuje.

Instalacija se pokreće klikom na poveznicu ***Instalacija PKI datoteke***.

Datoteku je potrebno spremiti lokalno na računalo te pokrenuti instalaciju sa računala (Slika 6, Slika 7).

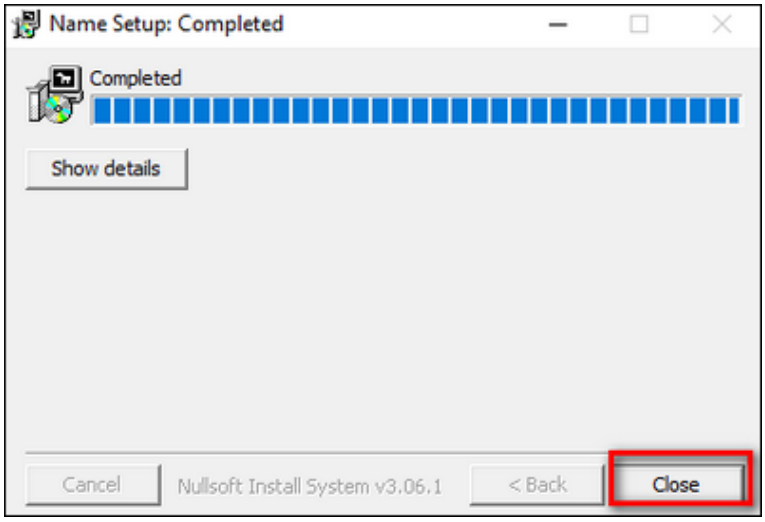


Slika 6. Preuzimanje Instalacije PKI datoteke



Slika 7. Pohranjivanje Instalacije PKI datoteke

Klikom na instalacijsku datoteku automatski se pokreće instalacija te u slučaju uspjeha korisnik dobiva ekran kojeg prikazuje Slika 8[14].

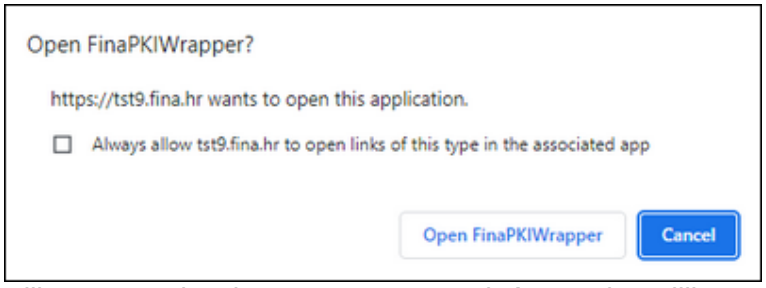


Slika 8. Uspješna instalacija PKI modula

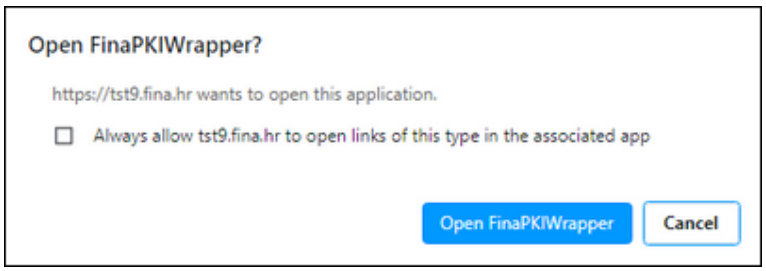
[14] Ako računalo ima postavljene pojačane postavke sigurnosti, kod instalacije se mogu pojaviti upozoravajuće poruke kod kojih je potrebno potvrditi instalaciju.

5.2.1. Upozoravajuće poruke kod pokretanja potpisnog modula

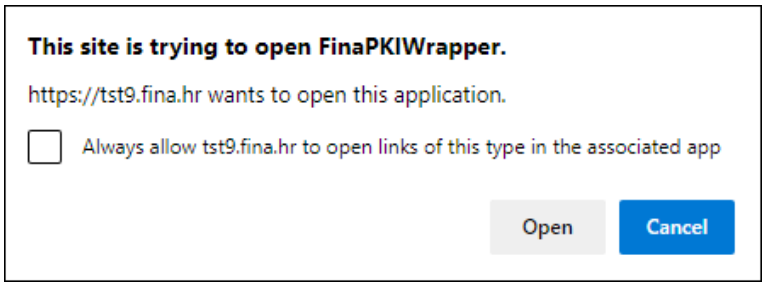
Prilikom pokretanja potpisnog modula tijekom procesa potpisivanja, registracije i sl. internetski preglednik će javiti upozoravajuću poruku o pokretanju vanjske aplikacije gdje je potrebno potvrditi pokretanje. Na svakom pregledniku poruka ima malo drugačiji izgled, ali moguće je postaviti kvačicu koja će isključiti pojavljivanje poruke u budućnosti. Navedene poruke prikazuju Slika 9., Slika 10., Slika 11. i Slika 12.



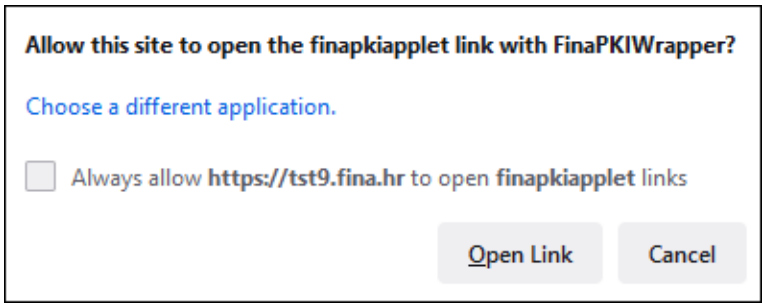
Slika 9. Google Chrome – upozoravajuća poruka prilikom pokretanja modula



Slika 10. Opera – upozoravajuća poruka prilikom pokretanja modula

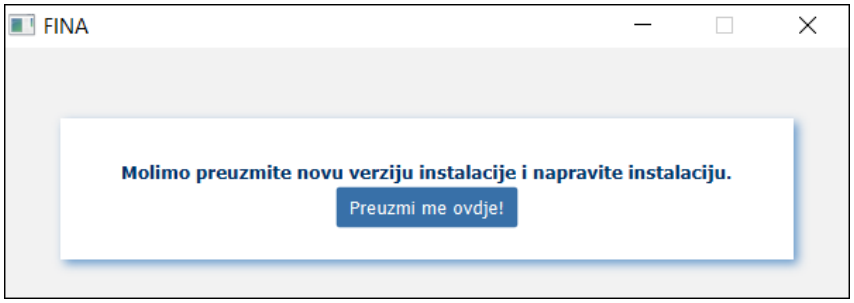


Slika 11. Microsoft Edge – upozoravajuća poruka prilikom pokretanja modula



Slika 12. Mozilla Firefox – upozoravajuća poruka prilikom pokretanja modula

U slučaju da se korisniku prilikom pokretanja PKI modula pojavi ekran sa obavijesti da mora preuzeti novu verziju instalacije PKI datoteke (Slika 13) instalaciju je potrebno pokrenuti klikom na gumb **Preuzmi me ovdje!**

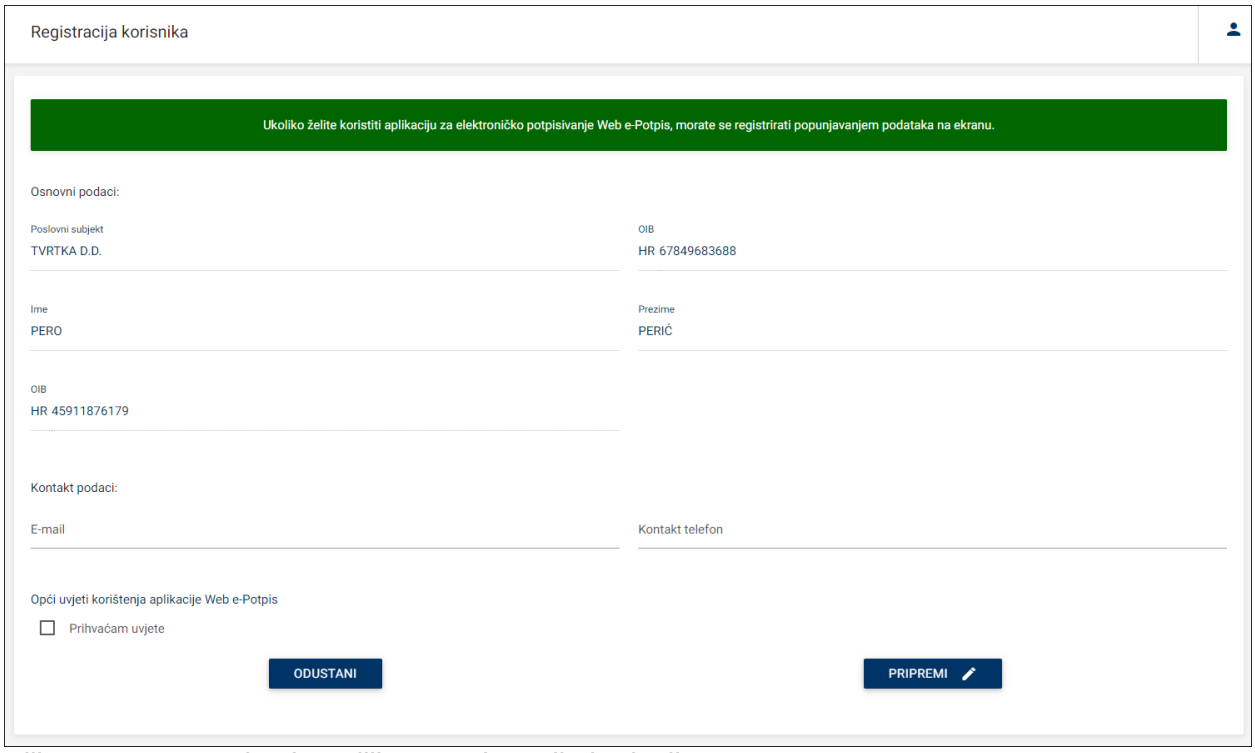


Slika 13. Preuzimanje Instalacije PKI datoteke

5.3. Registracija

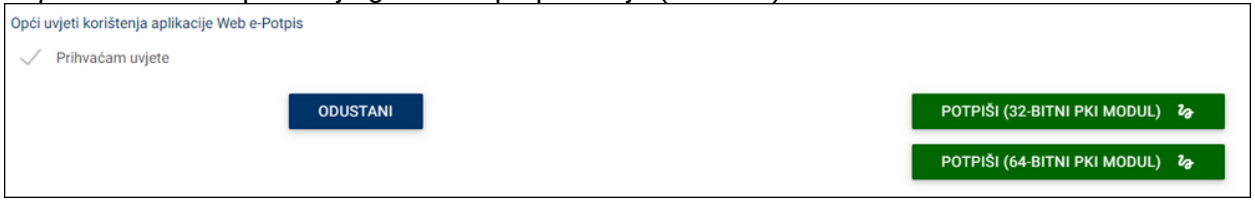
U slučaju da korisnik nije registriran, može izvršiti registraciju klikom na gumb „**UGOVARANJE USLUGE I REGISTRACIJA**“ kojeg prikazuje Slika 3.

Klikom na gumb se otvara forma za registraciju korisnika. Osnovni podaci se čitaju direktno sa certifikata s kojim je korisnik pristupio aplikaciji, a korisnik mora sam unijeti kontakt podatke u pripadajuća polja.



Slika 14. Unos podataka prilikom registracije korisnika

Nakon obavezne oznake prihvaćanja uvjeta korištenja aplikacije korisnik radi klik na gumb *Pripremi* te mu se prikazuju gumbi za potpisivanje (Slika 15).



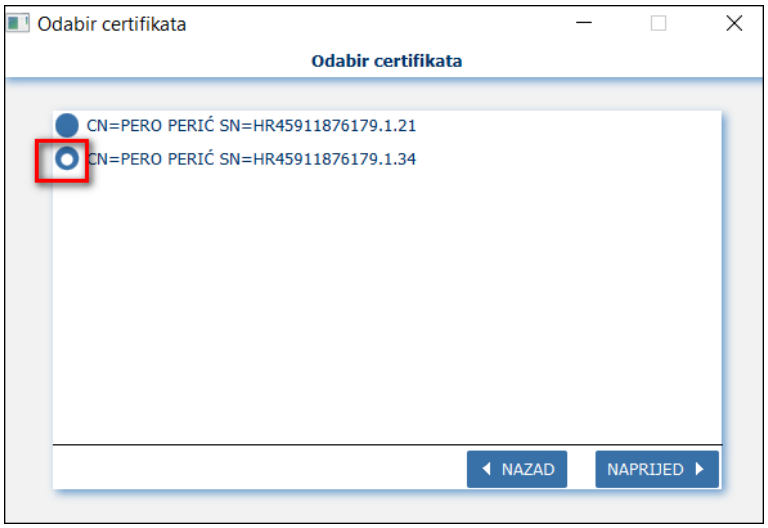
Slika 15. Odabir potpisivanja sa 32-bit ili 64-bit modulom

U slučaju korištenja 32-bitnog operacijskog sustava odabire se opcija „POTPIŠI (32-BITNI PKI MODUL)“, dok se u slučaju 64-bitnog operacijskog sustava odabire opcija „POTPIŠI (64-BITNI PKI MODUL)“ kojom se pokreće 64-bitna verzija PKI modula. Korisnici 64-bitnog operacijskog sustava mogu potpisivati datoteke i putem gumba „POTPIŠI (32-BITNI PKI MODUL)“, ali prije toga moraju izvršiti instalaciju 32-bitnog PKI modula.

Prilikom pokretanja potpisnog modula internetski preglednik će javiti upozoravajuću poruku o pokretanju vanjske aplikacije gdje je potrebno potvrditi pokretanje (detalji opisani u poglavlju 5.2.1).

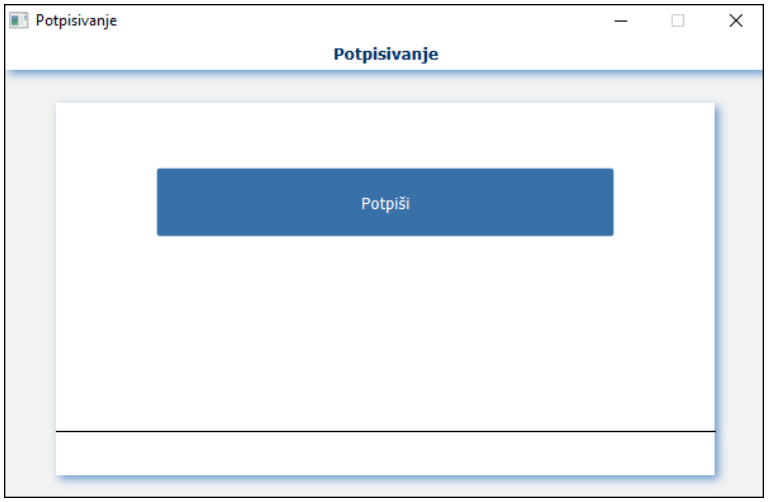
Za registraciju na aplikaciju Web e-Potpis potrebno je odabrati certifikat s kojim se prihvaćaju Opći uvjeti i završava proces registracije. Za prihvat Općih uvjeta i dovršenje procesa registracije može se odabrati jedan od ponuđenih certifikata. Na kripto uređaju se uobičajeno nalaze dva certifikata:

- Normalizirani certifikat za autentifikaciju i elektronički potpis (primjer: HR45911876179.1.21.)
- Kvalificirani certifikat za elektronički potpis (primjer: HR45911876179.1.25. ili HR45911876179.1.34., ovisno o vrsti kripto uređaja)



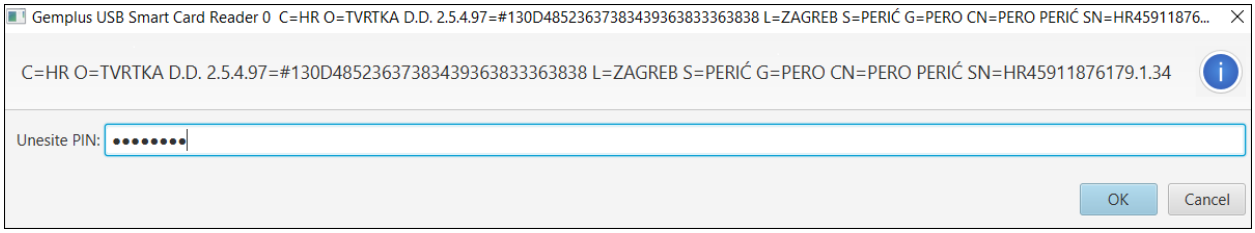
Slika 16. Odabir ponuđenih certifikata – na slici je odabran kvalificirani certifikat

Nakon odabira certifikata potrebno je kliknuti na gumb ***NAPRIJED*** i nakon toga ***Potpiši.***



Slika 17. Potpisivanje u tijeku

Prilikom potpisivanja potrebno je unijeti PIN certifikata (Slika 18).

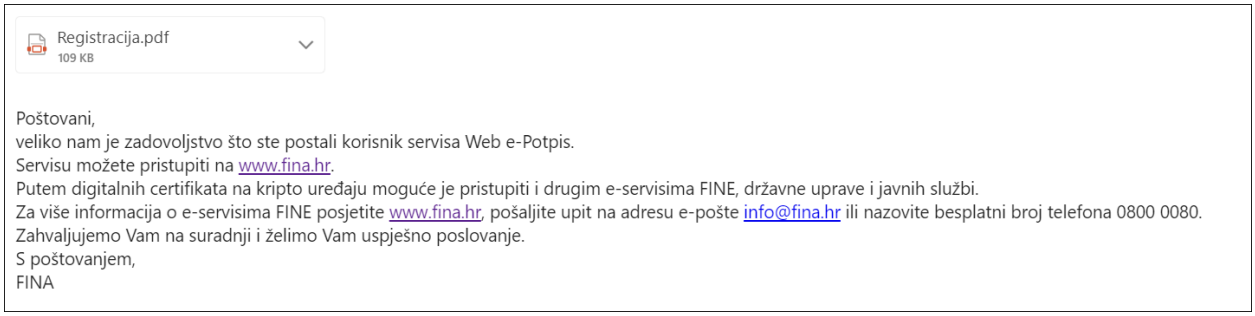


Slika 18. Unos PIN-a

Po uspješno odrađenoj registraciji korisniku će se prikazati ekran sa potvrdom o registraciji na aplikaciju Web e-potpis (Slika 19).

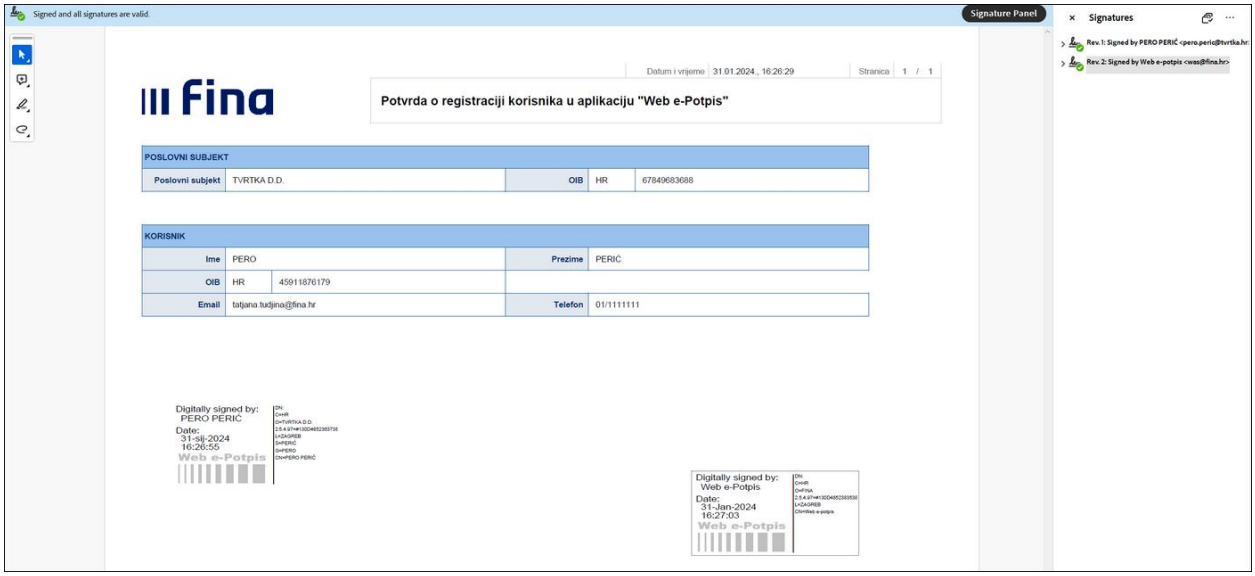
Slika 19. Početni ekran nakon registracije

Nakon uspješne registracije sustav dostavlja poruku na e-mail adresu koju je korisnik upisao prilikom registracije.



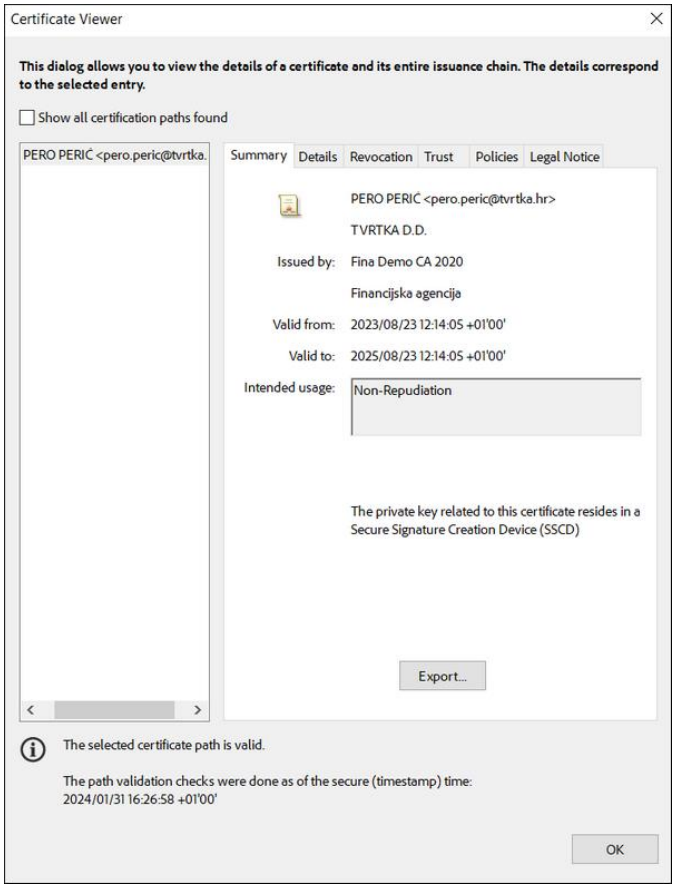
Slika 20. *Poruka nakon uspješne registracije*

i datoteku s nazivom Registracija.pdf (Slika 21).

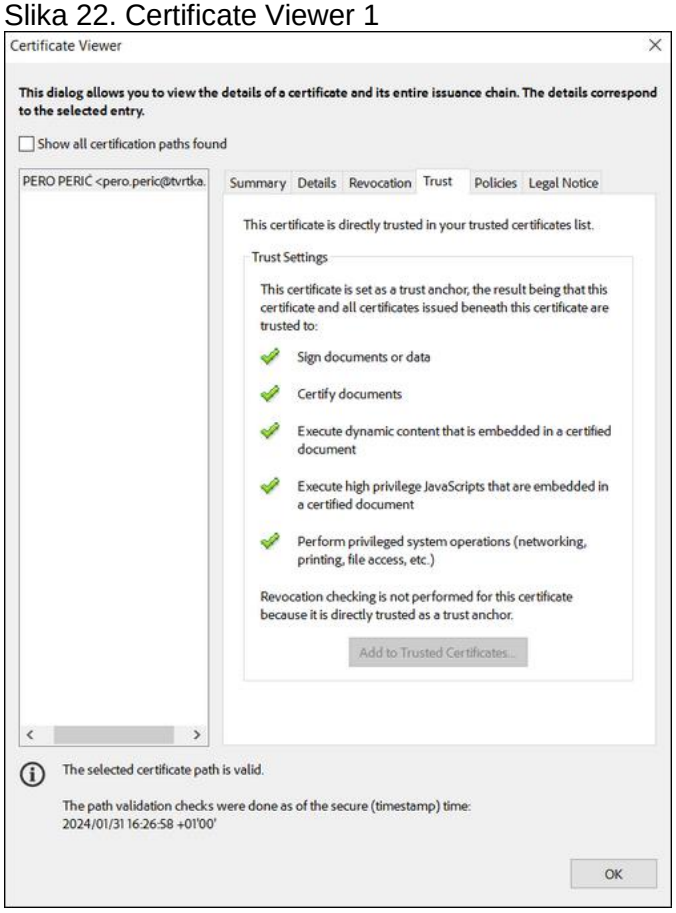


Slika 21. Registracija.pdf

Za provjeru detalja potpisa potrebno je desnim klikom miša na mjesto potpisa odabrati opciju *Show signature Properties*. Nakon toga odabrati *Show Signer`s* Certificates (Slika 22).



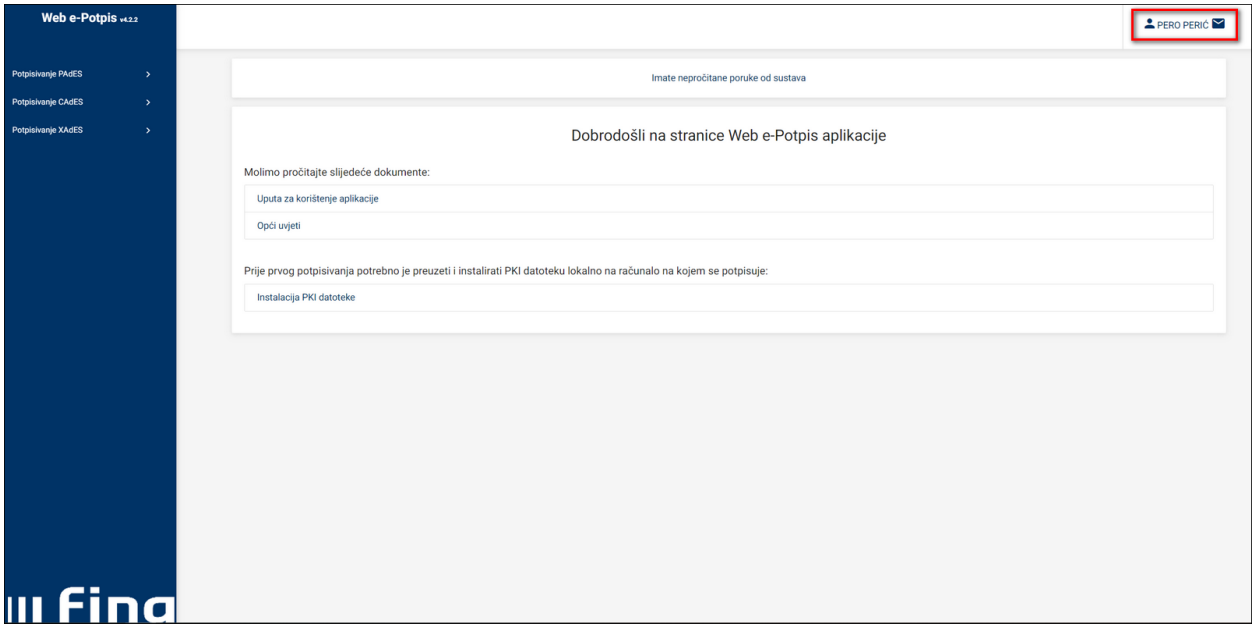
Slika 22. Certificate Viewer 1



Slika 23. Certificate Viewer 2

5.4. Uspješna prijava u aplikaciju registriranog korisnika

Prilikom uspješne prijave u aplikaciju registriranom korisniku se prikazuje početna stranica koju prikazuje Slika 24.



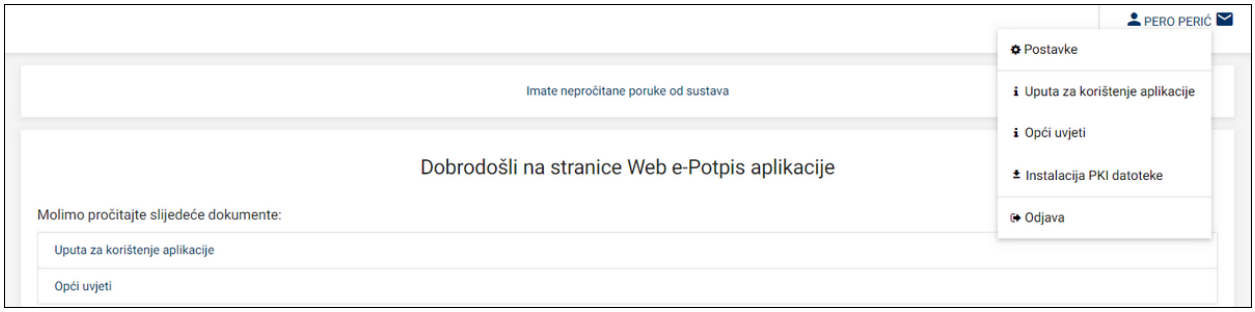
Slika 24. Početna stranica aplikacije

Na početnoj stranici nalaze se poveznice na korisničke upute, opće uvjete i instalacijske datoteke za PKI modul.

5.5. Postavke

U desnom gornjem kutu aplikacije nalazi se ime prijavljenog korisnika te se u pripadajućem padajućem meniju može odabrati nekoliko opcija (*Slika 25*):

- Postavke – pristup do postavki prijavljenog korisnika
- Uputa za korištenje aplikacije – poveznica do uputa za korištenje aplikacije
- Opći uvjeti – poveznica do općih uvjeta
- Instalacija PKI datoteke
- Odjava – poveznica za odjavu iz aplikacije, za potpunu odjavu iz aplikacije potrebno je ugasiti prozor preglednika

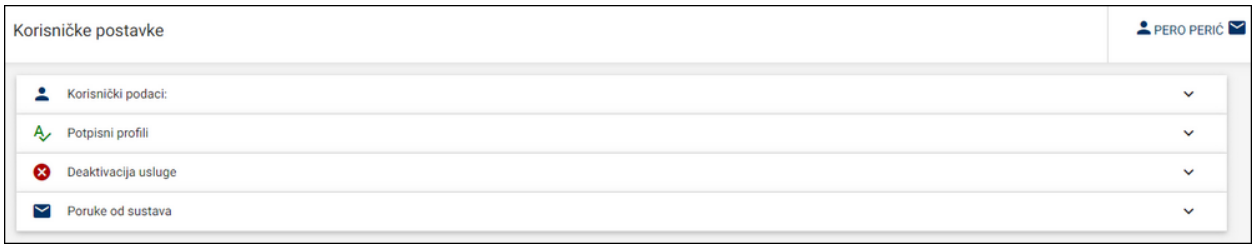


Slika 25. Pristupanje korisničkim postavkama

Klikom na opciju izbornika Postavke, otvara se ekran sa četiri dodatne opcije (Slika 26):

- Korisnički podaci
- Potpisni profili

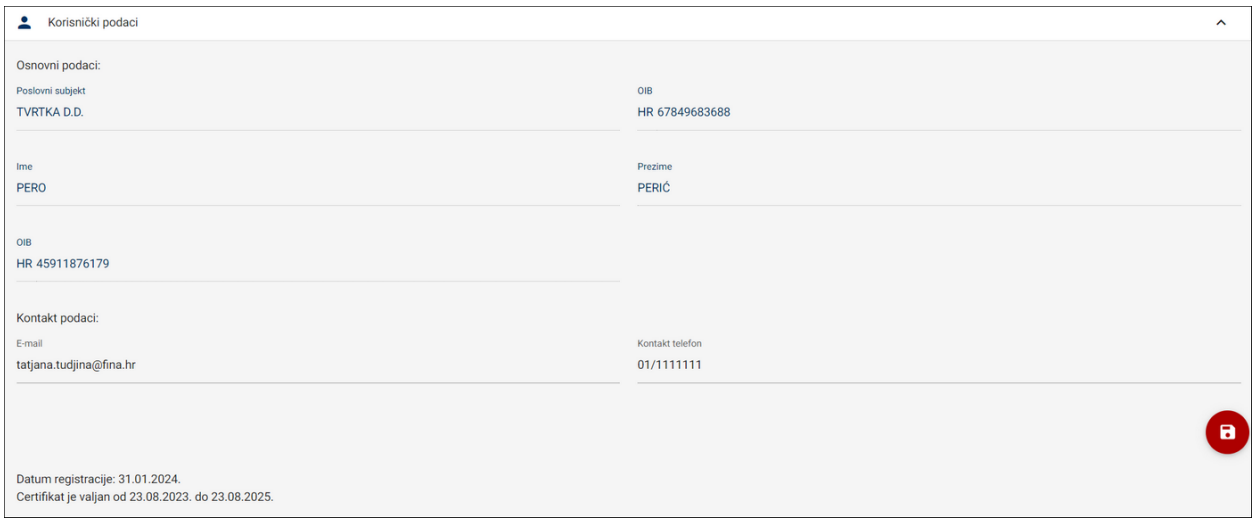
- Deaktivacija usluge
- Poruke od sustava



Slika 26. Opcije korisničkih postavki

5.5.1. Korisnički podaci

Klikom na opciju *Korisnički podaci* korisniku se otvara ekran gdje može pregledati svoje postojeće korisničke podatke, ali i urediti kontakt podatke. Klikom na crveni gumb u desnom kutu podaci se spremaju.



Slika 27. Korisnički podaci

5.5.2. Potpisni profili

Ulaskom na ekran korisničkih postavki korisniku se pojavljuje popis potpisnih profila koje je prethodno izradio. Prelaskom kursora miša preko ikone plusa pojavljuju se ikonice profila za svaki tip potpisa (Slika 28).

Slika 28. Dodavanje korisničkog profila

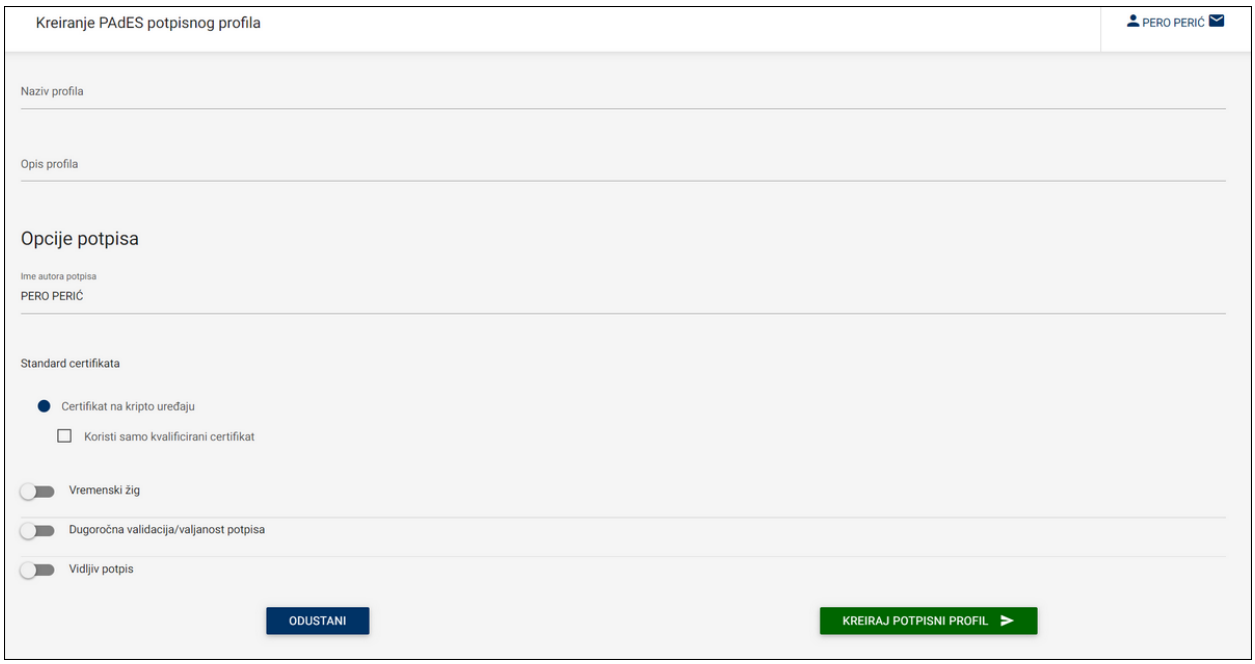
5.5.2.1. PAdES

Klikom na ikonu PAdES profila (ikona *PDF*) otvara se forma za unos postavki (Slika 29).

Kod ispunjavanja novog potpisnog profila prvo je potrebno ispuniti naziv i opis profila. Ime autora potpisa se automatski popunjava, no korisnik ga može promijeniti.

Kao standard certifikata korisnik može odabrati

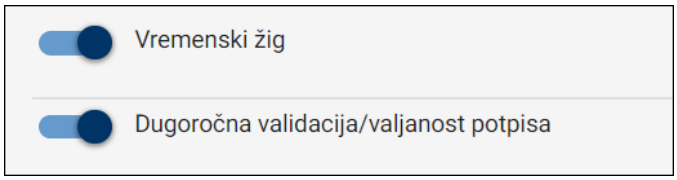
- Certifikat na kripto uređaju – uz dodatnu mogućnost odabira samo kvalificiranih certifikata



Slika 29. Kreiranje PAdES potpisnog profila

Dvije dodatne opcije koje korisnik može uključiti su:

- Vremenski žig
- Dugoročna validacija/valjanost potpisa – uključivanjem ove opcije automatski se primjenjuje i vremenski žig.

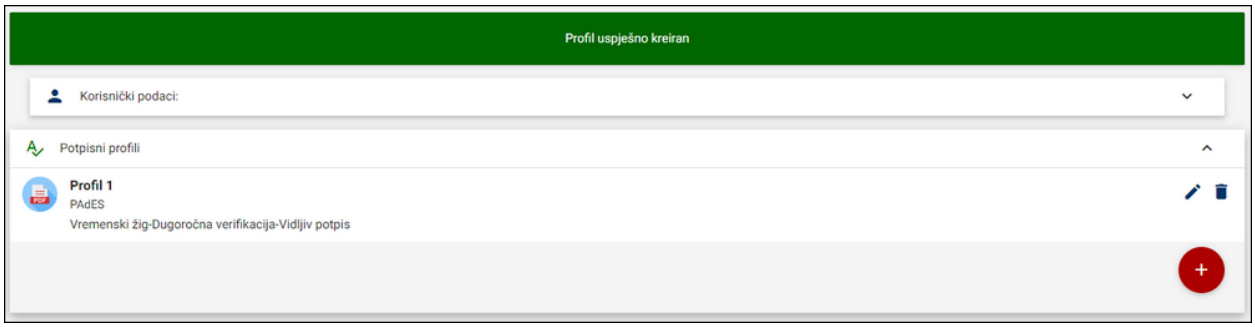


Slika 30. Opcije vremenskog žiga i dugoročne validacije/valjanosti potpisa

Korisnik također ima opciju podešavanja vidljivosti potpisa. U slučaju da je potpis vidljiv može se definirati stranica u dokumentu na kojoj će se prikazati potpis. Ujedno je moguće definirati točnu poziciju potpisa na stranici kroz pomicanje kvadratića oznake „Digital signature“ u pojednostavljenoj skici stranice PDF dokumenta.

Slika 31. Podešavanje pozicije potpisa

Klikom na gumb „Kreiraj potpisni profil“ spremaju se podaci te se ispisuje potvrdna poruka (Slika 32). Novi profil se pojavljuje u popisu te ga je klikom na ikonu olovke moguće ažurirati.



Slika 32. Pregled potpisnih profila

5.5.2.2. CAdES

Klikom na ikonu CAdES profila (ikona *CMS*) otvara se forma za unos postavki (Slika 33).

Kod ispunjavanja novog potpisnog profila prvo je potrebno ispuniti naziv i opis profila.

Korisnik dalje ispunjava opcije potpisa gdje ima nekoliko različitih mogućnosti.

Tip potpisa:

- Prilikom potpisivanja spremi izvornu datoteku zajedno s potpisom (Attached) – podrazumijeva spremanje datoteke u .p7m formatu koja se može samostalno validirati.
- Prilikom potpisivanja spremi izvornu datoteku odvojeno od potpisa (Detached) – podrazumijeva spremanje potpisa u izdvojenu .p7s datoteku, za validaciju se koristi i originalna datoteka i potpis u izdvojenoj datoteci.

Korisnik zatim može definirati tri dodatna polja:

- Napomena uz potpis – proizvoljna napomena
- Mjesto potpisivanja
  - Država
  - Oznaka države
- Uloga potpisnika – moguć odabir iz skupa predefiniranih uloga (npr. direktor, prokurist, odvjetnik itd.)

Za algoritam potpisa dostupne su dvije vrijednosti:

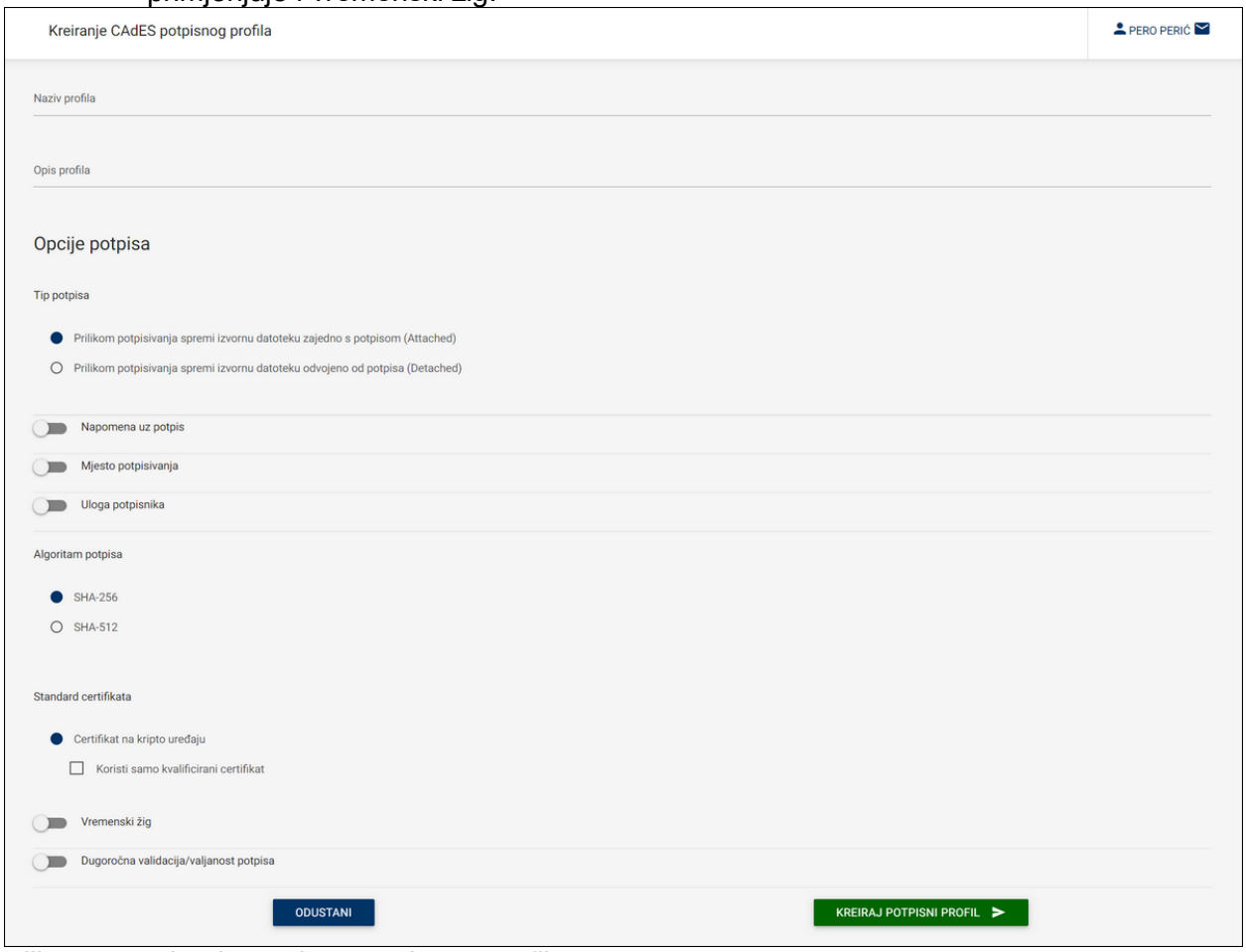
- SHA-256 – algoritam izračuna sažetka u dužini 256 bitova
- SHA-512 - algoritam izračuna sažetka u dužini 512 bitova

Kao standard certifikata korisnik može odabrati

- Certifikat na kripto uređaju – uz dodatnu mogućnost odabira samo kvalificiranih certifikata

Dvije dodatne opcije koje korisnik može uključiti:

- Vremenski žig
- Dugoročna validacija/valjanost potpisa – uključivanjem ove opcije automatski se primjenjuje i vremenski žig.



Slika 33. Kreiranje CAdES potpisnog profila

Klikom na gumb „Kreiraj potpisni profil“ spremaju se podaci te se ispisuje potvrdna poruka.

5.5.2.3. XAdES

Klikom na ikonu XAdES profila (ikona *XML*) otvara se forma za unos postavki (Slika 34).

Kod ispunjavanja novog potpisnog profila prvo je potrebno ispuniti naziv i opis profila.

Korisnik dalje ispunjava opcije potpisa gdje ima nekoliko različitih mogućnosti.

Tip potpisa:

- Prilikom potpisivanja spremi izvornu datoteku zajedno s potpisom (Attached) – podrazumijeva spremanje potpisa na kraj XML datoteke
- Prilikom potpisivanja spremi izvornu datoteku odvojeno od potpisa (Detached) – podrazumijeva spremanje potpisa u izdvojenu XML datoteku, za validaciju se koristi i originalna datoteka i potpis u izdvojenoj datoteci.

Korisnik zatim može definirati par dodatnih polja:

- Mjesto potpisivanja
  - Država
  - Oznaka države
- Uloga potpisnika – moguć odabir iz skupa predefiniranih uloga (npr. direktor, prokurist, odvjetnik itd.)

Za algoritam potpisa dostupne su dvije vrijednosti:

- SHA-256 – algoritam izračuna sažetka u dužini 256 bitova
- SHA-512 - algoritam izračuna sažetka u dužini 512 bitova

Sljedeća sekcija odnosi se na format potpisnog dokumenta gdje korisnik definira elemente koji se zapisuju unutar *SignedDataObjectProperties* segmenta potpisa:

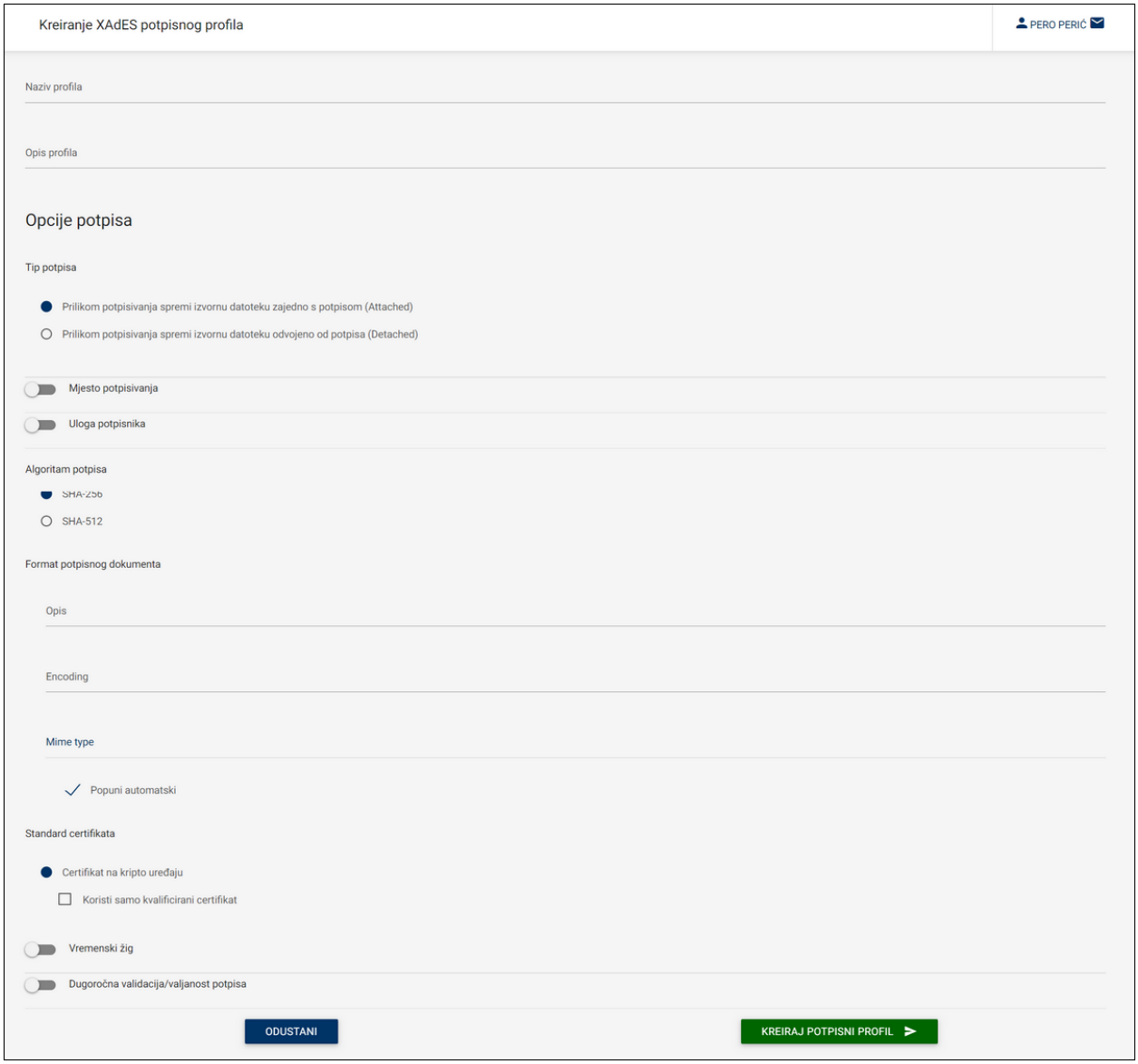
- Opis – proizvoljan opis koji se zapisuje u *xades:Description* element
- Encoding – oznaka encodinga koja se zapisuje u *xades:Encoding* element
- Mime type – moguće automatsko popunjavanje, a moguć i unos od strane korisnika koji se zapisuje u *xades:MimeType* element

Kao standard certifikata korisnik može odabrati

- Certifikat na kripto uređaju – uz dodatnu mogućnost odabira samo kvalificiranih certifikata

Dvije dodatne opcije koje korisnik može uključiti su

- Vremenski žig
- Dugoročna validacija/valjanost potpisa – uključivanjem ove opcije automatski se primjenjuje i vremenski žig.



Slika 34. Kreiranje XAdES potpisnog profila

Klikom na gumb „Kreiraj potpisni profil“ spremaju se podaci te se ispisuje potvrdna poruka.

5.5.3. Deaktivacija usluge

Korisnik ima mogućnost deaktivacije usluge kroz aplikaciju, najraniji datum deaktivacije je sutrašnji datum.

Slika 35. Deaktivacija usluge – odabir datuma

Klikom na gumb *Pripremi* pojavljuju se gumbi za potpisivanje zahtjeva za deaktivaciju usluge (Slika 36).

Slika 36. Odabir potpisivanja sa 32-bit ili 64-bit modulom

U slučaju korištenja 32-bitnog operacijskog sustava odabire se opcija „*POTPIŠI (32-BITNI PKI MODUL)*“, dok se u slučaju 64-bitnog operacijskog sustava odabire opcija „*POTPIŠI (64-BITNI PKI MODUL)*“ kojom se pokreće 64-bitna verzija PKI modula. Korisnici 64-bitnog operacijskog sustava mogu potpisivati datoteke i putem gumba „*POTPIŠI (32-BITNI PKI MODUL)*“, ali prije toga moraju izvršiti instalaciju 32-bitnog PKI modula.

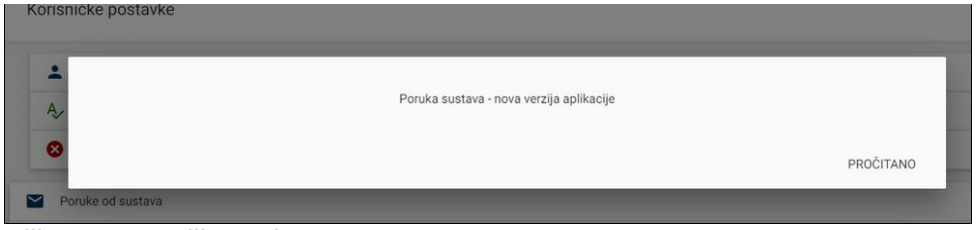
Odabirom certifikata te klikom na gumb za potpisivanje pokreće se deaktivacija usluge sa odabranim datumom. Datum deaktivacije se može i promijeniti istovjetnim postupkom.

5.5.4. Poruke sustava

Sljedeća stavka se odnosi na poruke sustava koje korisnici mogu pregledavati otvaranjem sekcije Poruke od sustava (Slika 37).

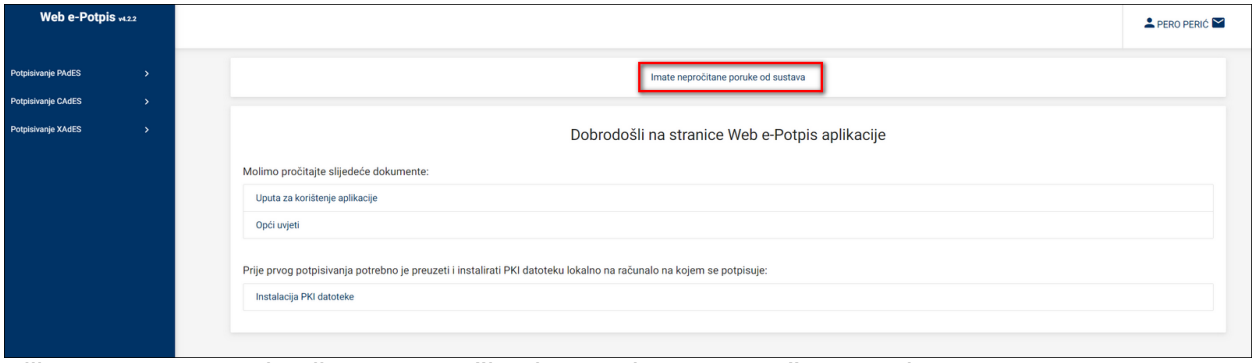
Slika 37. Pristigle poruke korisnika

Svaka pojedinačna poruka se može detaljno pregledavati te označiti kao pročitana (Slika 38).



Slika 38. Detalji poruke

Porukama sustava može se pristupiti i putem početnog ekrana aplikacije gdje se korisniku prikazuje statusna obavijest „Imate nepročitane poruke od sustava“ (Slika 39).

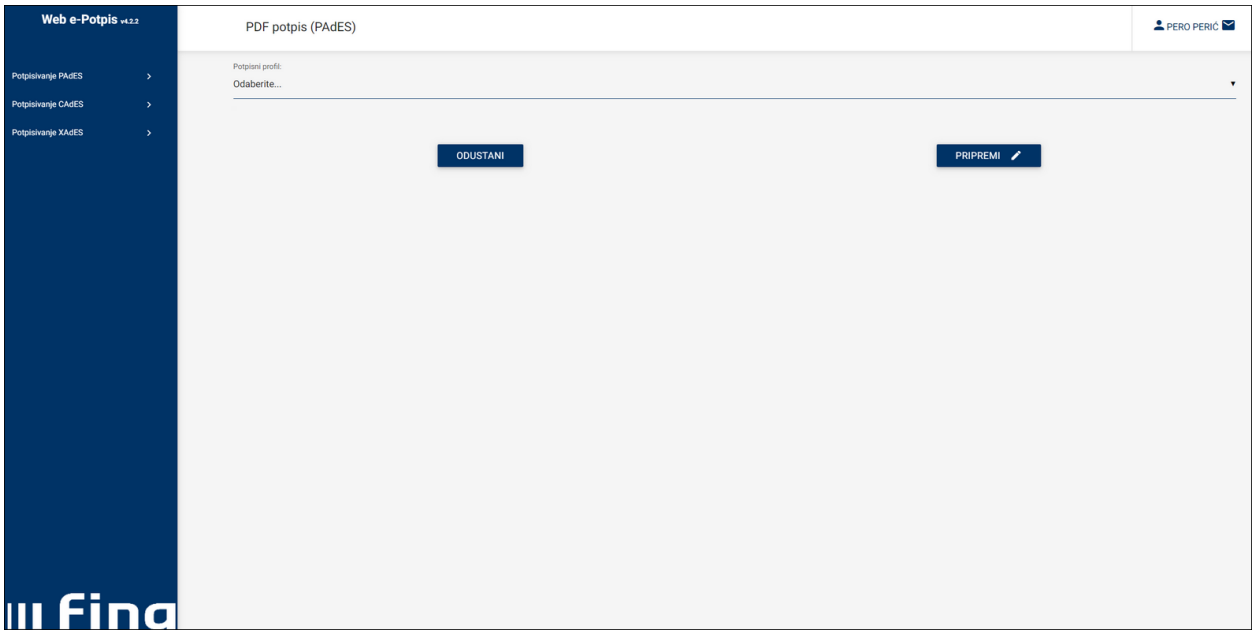


Slika 39. Statusna obavijest o nepročitanim porukama na početnom ekranu

5.6. Potpisivanje

5.6.1. PAdES

Za potpisivanje PDF dokumenata potrebno je odabrati stavku menija *Potpisivanje PAdES* → *Potpis*. Klikom na nju otvara se početni ekran za potpisivanje dokumenata kojeg prikazuje Slika 40.



Slika 40. Početni ekran kod potpisivanja dokumenata

Prije pokretanja procesa potpisivanja potrebno je odabrati potpisni profil (Slika 40) sa spremljenim opcijama ili označiti stavku „*Bez profila*“ gdje se otvara prazna forma sa opcijama koje je potrebno ispuniti (to je isti set opcija koje se inače mogu spremiti u sklopu potpisnih profila).

Slika 41. Odabir profila za potpisivanje

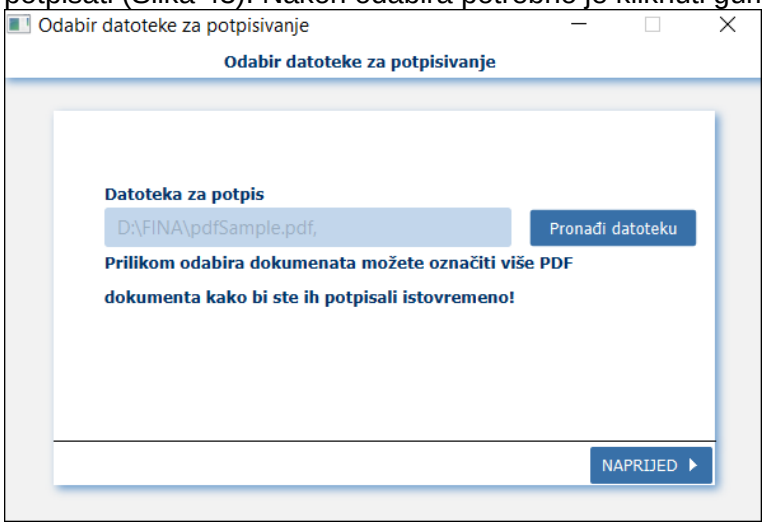
Jednom kada je odabran potpisni profil te korisnik klikne gumb *Pripremi* pojavljuju se opcije za pokretanje PKI modula (Slika 42). U slučaju korištenja 32-bitnog operacijskog sustava odabire se opcija „*POTPIŠI (32-BITNI PKI MODUL)*“, dok se u slučaju 64-bitnog operacijskog sustava odabire opcija „*POTPIŠI (64-BITNI PKI MODUL)*“ kojom se pokreće 64-bitna verzija PKI modula. Korisnici 64-bitnog operacijskog sustava mogu potpisivati datoteke i putem gumba „*POTPIŠI (32-BITNI PKI MODUL)*“, ali prije toga moraju izvršiti instalaciju 32-bitnog PKI modula.

Slika 42. Odabir potpisivanja sa 32-bit ili 64-bit modulom

VAŽNO

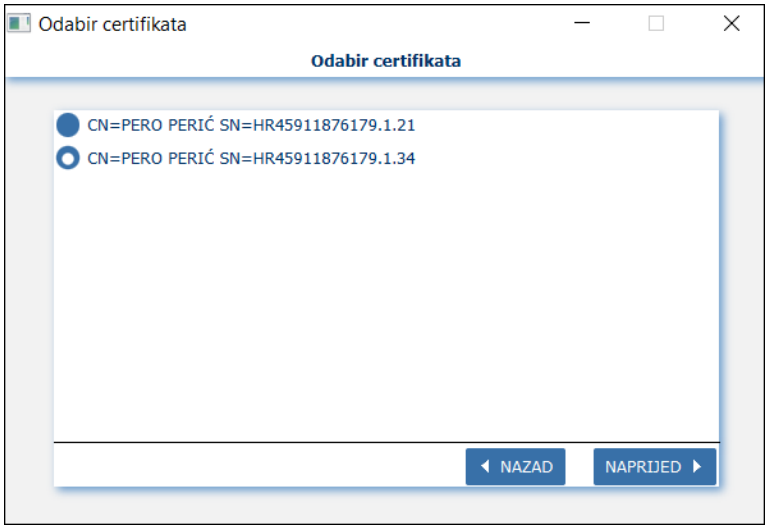
Kako bi potpisivanje bilo moguće korisnik prvo mora lokalno instalirati 32-bitni i/ili 64-bitni PKI modul, ovisno o njegovom operacijskom sustavu.

Prilikom pokretanja PKI modula prvo se otvara komponenta za odabir datoteke koju se želi potpisati (Slika 43). Nakon odabira potrebno je kliknuti gumb za nastavak.



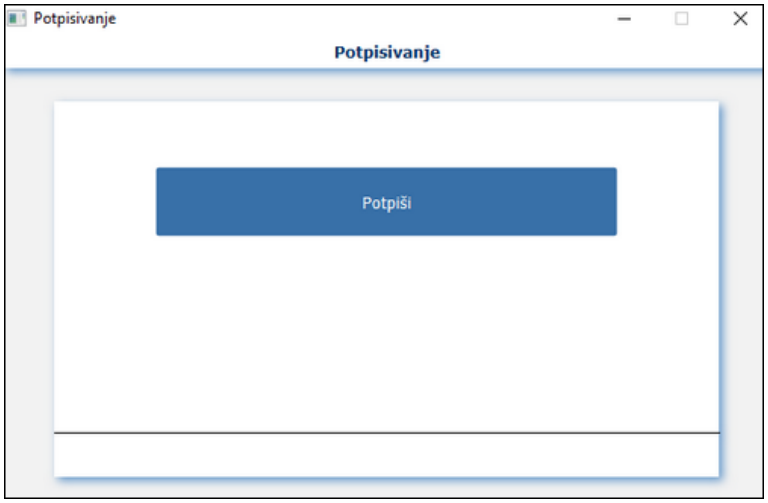
Slika 43. PKI modul - odabir datoteke za potpis

U slučaju da postoji više certifikata za odabir pojavit će se ekran za njihov odabir kao što prikazuje Slika 44.



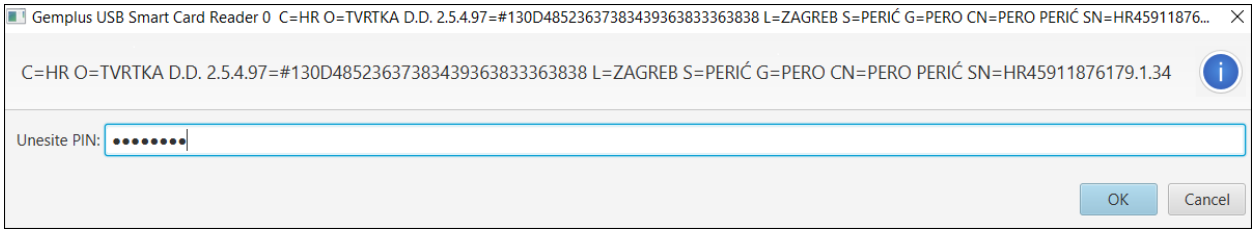
Slika 44. PKI modul – ekran odabira certifikata

Nakon izvršenog odabira pojavljuje se gumb *Potpiši* kojeg je potrebno kliknuti za završetak procesa potpisivanja (Slika 45).



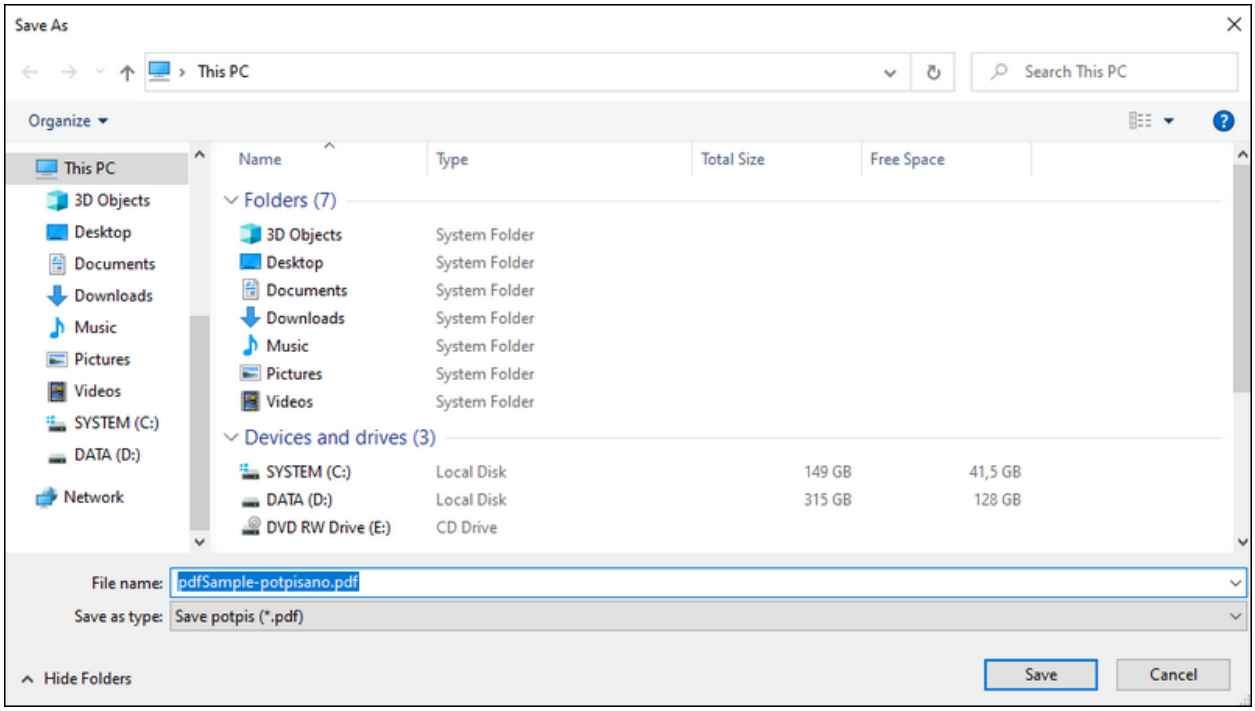
Slika 45. PKI modul – potpisivanje

Nakon klika na gumb *Potpiši* pojavljuje se polje za unos PIN-a (Slika 46).



Slika 46. PKI modul - unos PIN-a za potpisivanje dokumenta

Unosom PIN-a izvršava se potpisivanje te u slučaju uspjeha aplikacija traži korisnika da definira lokaciju na koju će pohraniti potpisanu datoteku (Slika 47).



Slika 47. PKI modul – odabir lokacije za spremanje potpisane datoteke

5.6.2. CAdES

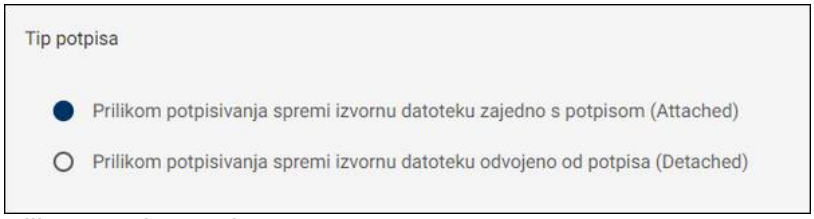
Za pristupanje ekranu CAdES potpisivanja korisnik treba odabrati stavku izbornika *Potpisivanje CAdES → Potpis.*

Prije pokretanja procesa potpisivanja potrebno je odabrati potpisni profil (Slika 48) sa spremljenim opcijama ili označiti stavku „*Bez profila*“ gdje se otvara prazna forma sa opcijama koje je potrebno ispuniti (to je isti set opcija koje se inače mogu spremiti u sklopu potpisnih profila kao što prikazuje Slika 33).

Slika 48. Odabir profila za potpisivanje

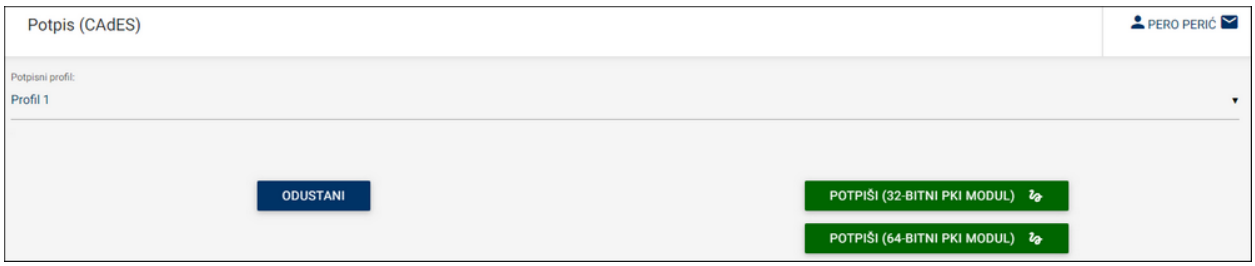
Jedna od ključnih postavki kod ove vrste potpisa je opcija **Tip potpisa**.

Ovisno o odabranoj opciji potpis će biti dio izvorne datoteka ili će biti u izdvojenoj datoteci:
- Prilikom potpisivanja spremi izvornu datoteku zajedno s potpisom (**Attached**) – podrazumijeva spremanje datoteke u .p7m formatu koja se može samostalno validirati.
- Prilikom potpisivanja spremi izvornu datoteku odvojeno od potpisa (**Detached**) – podrazumijeva spremanje potpisa u izdvojenu .p7s datoteku, za validaciju se koristi i originalna datoteka i potpis u izdvojenoj datoteci.



Slika 49. Tip potpisa

Jednom kada je odabran potpisni profil te korisnik klikne gumb *Pripremi* pojavljuju se opcije za pokretanje PKI modula (Slika 50). U slučaju korištenja 32-bitnog operacijskog sustava odabire se opcija „*POTPIŠI (32-BITNI PKI MODUL)*“, dok se u slučaju 64-bitnog operacijskog sustava odabire opcija „*POTPIŠI (64-BITNI PKI MODUL)*“ kojom se pokreće 64-bitna verzija PKI modula. Korisnici 64-bitnog operacijskog sustava mogu potpisivati datoteke i putem gumba „*POTPIŠI (32-BITNI PKI MODUL)*“, ali prije toga moraju izvršiti instalaciju 32-bitnog PKI modula.

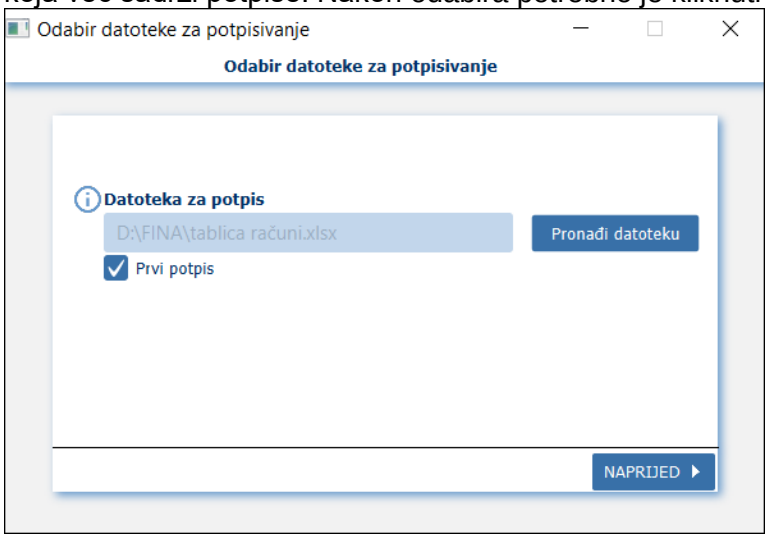


Slika 50. Odabir potpisivanja sa 32-bit ili 64-bit modulom

VAŽNO

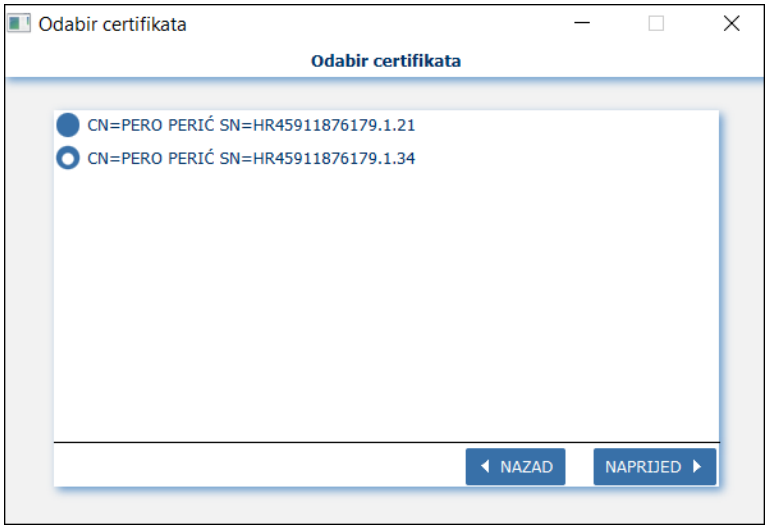
Kako bi potpisivanje bilo moguće korisnik prvo mora lokalno instalirati 32-bitni i/ili 64-bitni PKI modul, ovisno o njegovom operacijskom sustavu.

Prilikom pokretanja PKI modula prvo se otvara komponenta za odabir datoteke koju se želi potpisati (Slika 51). Tu postoji i kućica sa oznakom da li se radi o prvom potpisu.
Prvi potpisnik dokumenta označava opciju „Prvi potpis“. Kod svakog sljedećeg potpisa istog dokumenta navedena opcija treba biti isključena te je na tom mjestu potrebno pronaći datoteku koja već sadrži potpise. Nakon odabira potrebno je kliknuti gumb za nastavak.



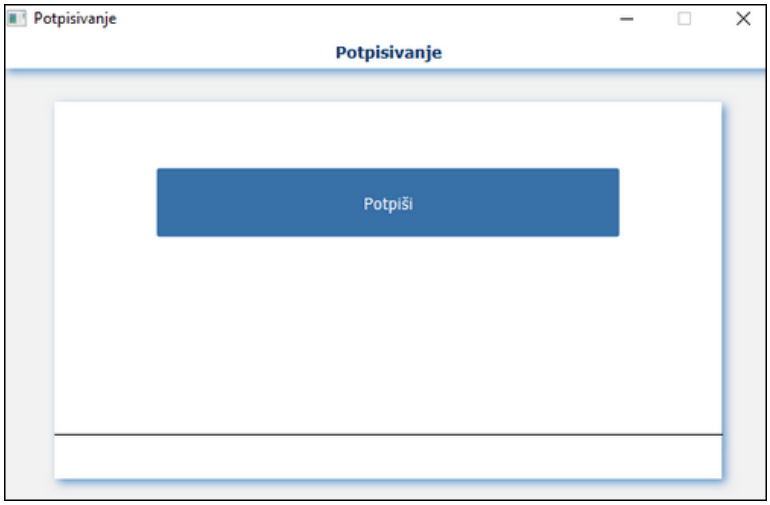
Slika 51. PKI modul - odabir datoteke za potpis

U slučaju da postoji više certifikata za odabir pojavit će se ekran za njihov odabir kao što prikazuje Slika 52.



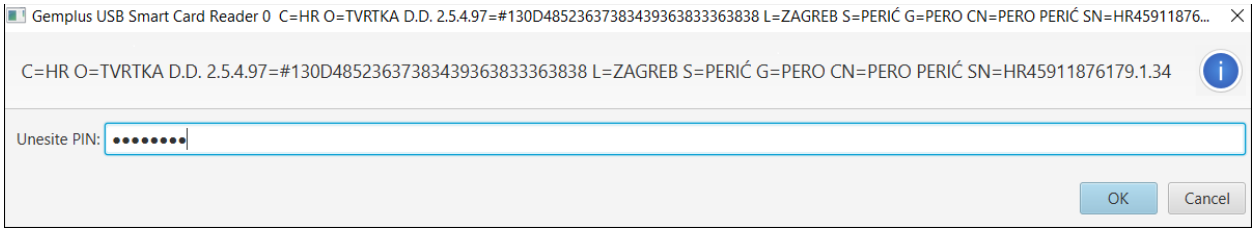
Slika 52. PKI modul – ekran odabira certifikata

Nakon izvršenog odabira pojavljuje se gumb *Potpiši* kojeg je potrebno kliknuti za završetak procesa potpisivanja (Slika 53).



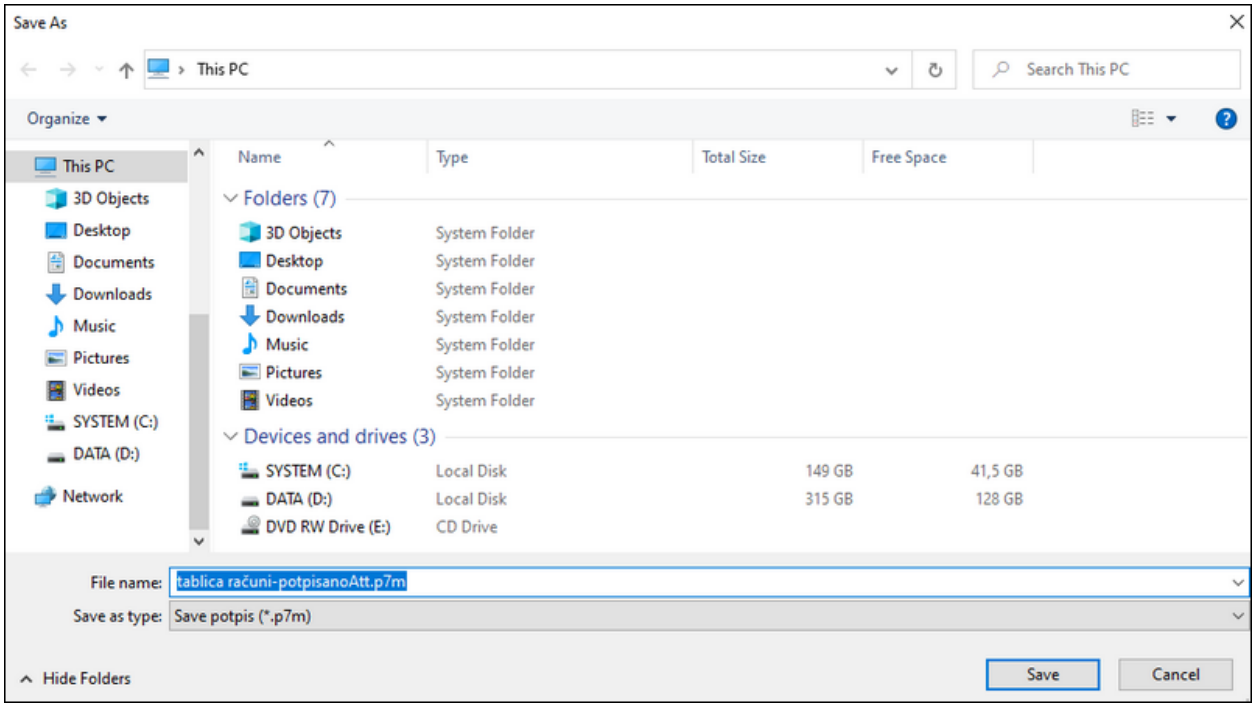
Slika 53. PKI modul – potpisivanje

Nakon klika na gumb *Potpiši* pojavljuje se polje za unos PIN-a (Slika 54).



Slika 54. PKI modul - unos PIN-a za potpisivanje dokumenta

Unosom PIN-a izvršava se potpisivanje te u slučaju uspjeha aplikacija traži korisnika da definira lokaciju na koju će pohraniti potpisanu datoteku (Slika 55).



Slika 55. Spremanje datoteke kod CAdES potpisa

5.6.3. XAdES

Za pristupanje ekranu XAdES potpisivanja korisnik treba odabrati stavku menija *Potpisivanje XAdES → Potpis.*

Prije pokretanja procesa potpisivanja potrebno je odabrati potpisni profil (Slika 56) sa spremljenim opcijama ili označiti stavku „*Bez profila*“ gdje se otvara prazna forma sa opcijama koje je potrebno ispuniti (to je isti set opcija koje se inače mogu spremiti u sklopu potpisnih profila kao što prikazuje Slika 34).

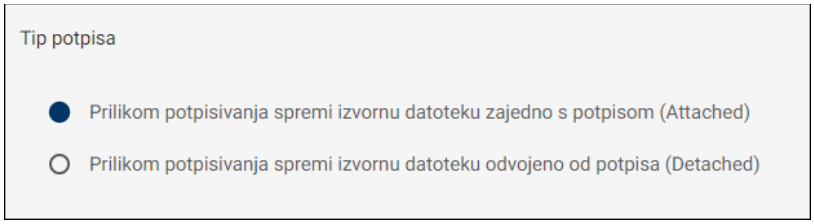
Slika 56. Odabir profila za potpisivanje

Jedna od ključnih postavki kod ove vrste potpisa je opcija **Tip potpisa**.

Ovisno o odabranoj opciji potpis će biti dio izvorne datoteka ili će biti u izdvojenoj datoteci:

- Prilikom potpisivanja spremi izvornu datoteku zajedno s potpisom (**Attached**) – podrazumijeva spremanje potpisa na kraj XML datoteke

- Prilikom potpisivanja spremi izvornu datoteku odvojeno od potpisa (**Detached**) – podrazumijeva spremanje potpisa u izdvojenu XML datoteku, za validaciju se koristi i originalna datoteka i potpis u izdvojenoj datoteci.



Slika 57. Tip potpisa

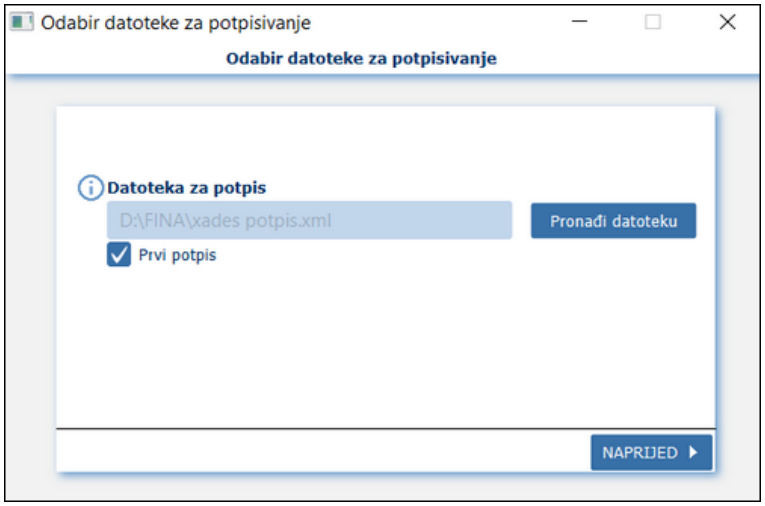
Jednom kada je odabran potpisni profil te korisnik klikne gumb *Pripremi* pojavljuju se opcije za pokretanje PKI modula (Slika 58). U slučaju korištenja 32-bitnog operacijskog sustava odabire se opcija „*POTPIŠI (32-BITNI PKI MODUL)*“, dok se u slučaju 64-bitnog operacijskog sustava odabire opcija „*POTPIŠI (64-BITNI PKI MODUL)*“ kojom se pokreće 64-bitna verzija PKI modula. Korisnici 64-bitnog operacijskog sustava mogu potpisivati datoteke i putem gumba „*POTPIŠI (32-BITNI PKI MODUL)*“, ali prije toga moraju izvršiti instalaciju 32-bitnog PKI modula.

Slika 58. Odabir potpisivanja sa 32-bit ili 64-bit modulom

VAŽNO

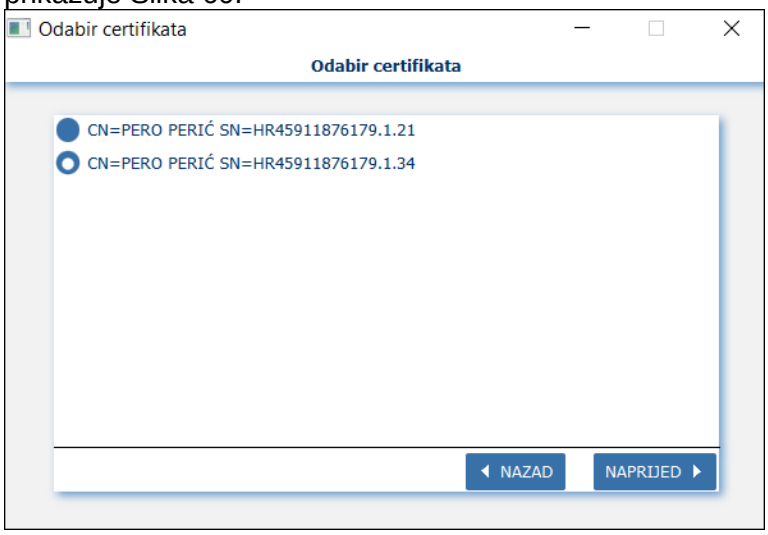
Kako bi potpisivanje bilo moguće korisnik prvo mora lokalno instalirati 32-bitni i/ili 64-bitni PKI modul, ovisno o njegovom operacijskom sustavu.

Prilikom pokretanja PKI modula prvo se otvara komponenta za odabir datoteke koju se želi potpisati (Slika 59). Tu postoji i kućica sa oznakom da li se radi o prvom potpisu.
Prvi potpisnik dokumenta označava opciju „Prvi potpis“. Kod svakog sljedećeg potpisa istog dokumenta navedena opcija treba biti isključena te je na tom mjestu potrebno pronaći datoteku koja već sadrži potpise. Nakon odabira potrebno je kliknuti gumb za nastavak.



Slika 59. PKI modul - odabir datoteke za potpis

U slučaju da postoji više certifikata za odabir pojavit će se ekran za njihov odabir kao što prikazuje Slika 60.

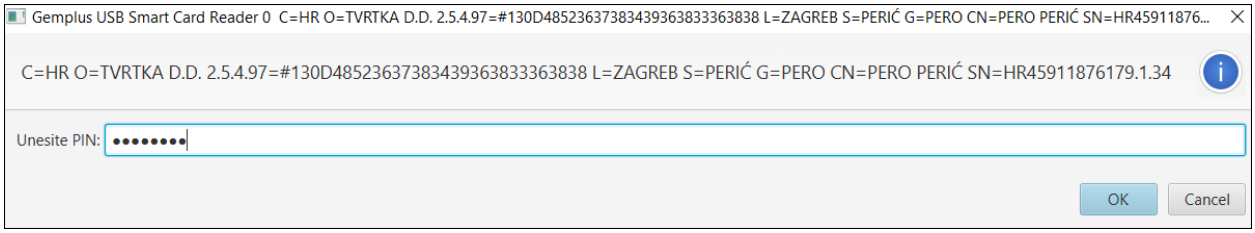


Slika 60. PKI modul – ekran odabira certifikata

Nakon izvršenog odabira pojavljuje se gumb *Potpiši* kojeg je potrebno kliknuti za završetak procesa potpisivanja (Slika 61).

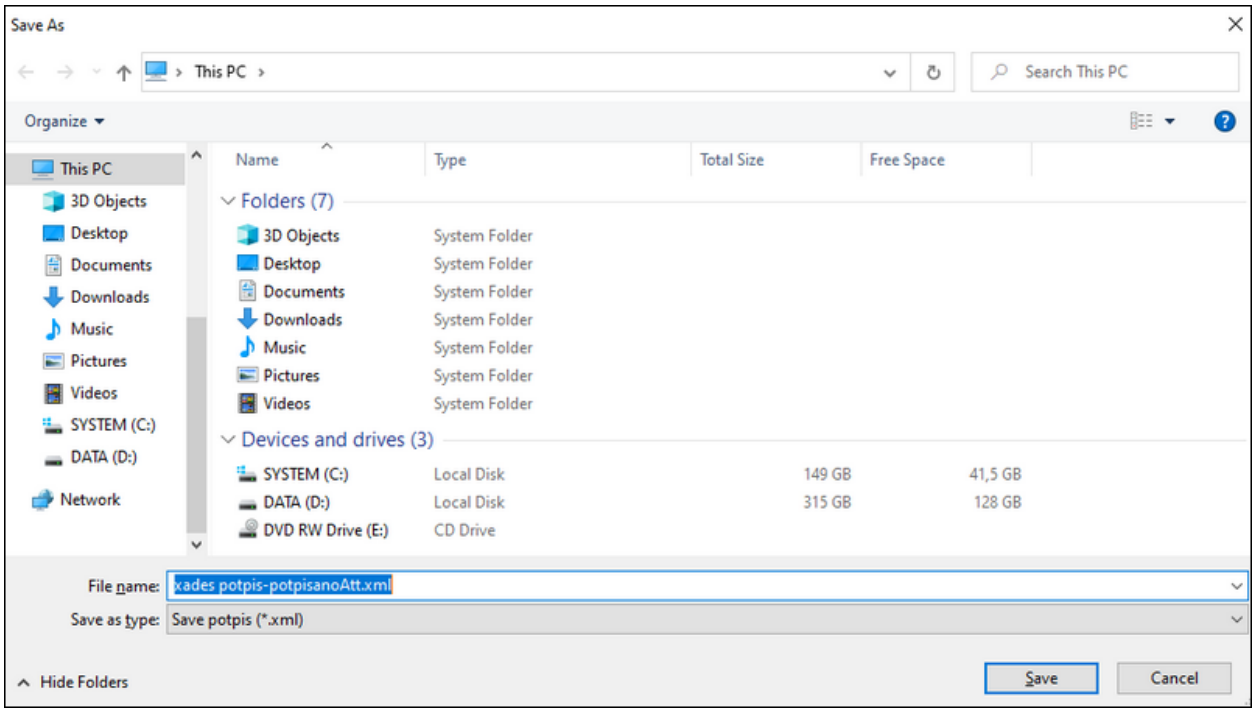
Slika 61. PKI modul – potpisivanje

Nakon klika na gumb *Potpiši* pojavljuje se polje za unos PIN-a (Slika 62).



Slika 62. PKI modul - unos PIN-a za potpisivanje dokumenta

Unosom PIN-a izvršava se potpisivanje te u slučaju uspjeha aplikacija traži korisnika da definira lokaciju na koju će pohraniti potpisanu datoteku (Slika 63).



Slika 63. Spremanje datoteke kod XAdES potpisa

5.7. Validacija potpisa

5.7.1. PAdES

Jednom potpisane datoteke moguće je validirati kroz aplikaciju odabirom stavke menija *Potpisivanje PAdES → Validacija.*

Odabirom stavke menija otvara se ekran za validaciju gdje za početak validacije korisnik mora odabrati gumb *Pripremi* (Slika 64).

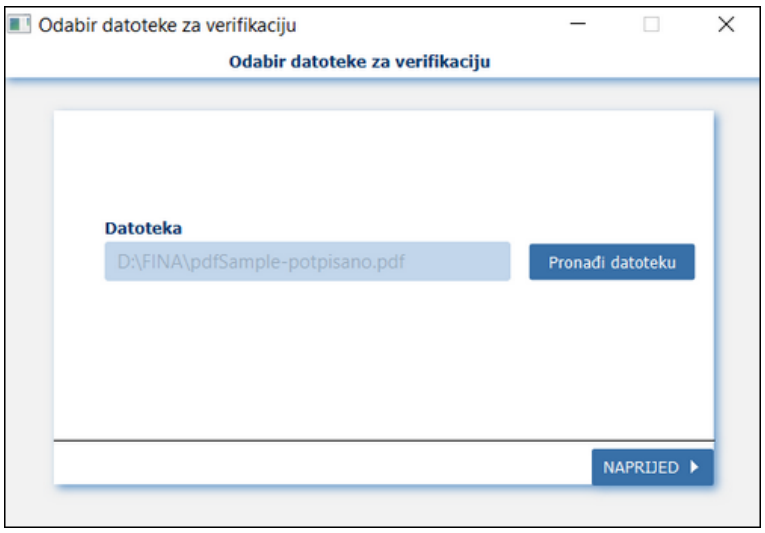
Slika 64. Ekran za validaciju potpisa

Klikom na gumb „*Pripremi*“ pojavljuju se opcije za pokretanje PKI modula kojima se vrši validacija (Slika 65). U slučaju korištenja 32-bitnog operacijskog sustava odabire se opcija

„*VALIDIRAJ (32-BITNI PKI MODUL)*“, dok se u slučaju 64-bitnog operacijskog sustava odabire opcija „*VALIDIRAJ (64-BITNI PKI MODUL)*“ kojom se pokreće 64-bitna verzija PKI modula. Korisnici 64-bitnog operacijskog sustava mogu validirati datoteke i putem gumba „VALIDIRAJ *(32-BITNI PKI MODUL)*“, ali prije toga moraju izvršiti instalaciju 32-bitnog PKI modula.

Slika 65. Validacija potpisa – odabir 32-bit ili 64-bit verzije modula

Prilikom pokretanja PKI modula prvo se otvara komponenta za odabir datoteke koju se želi validirati (Slika 66). Nakon odabira potrebno je kliknuti gumb za nastavak.

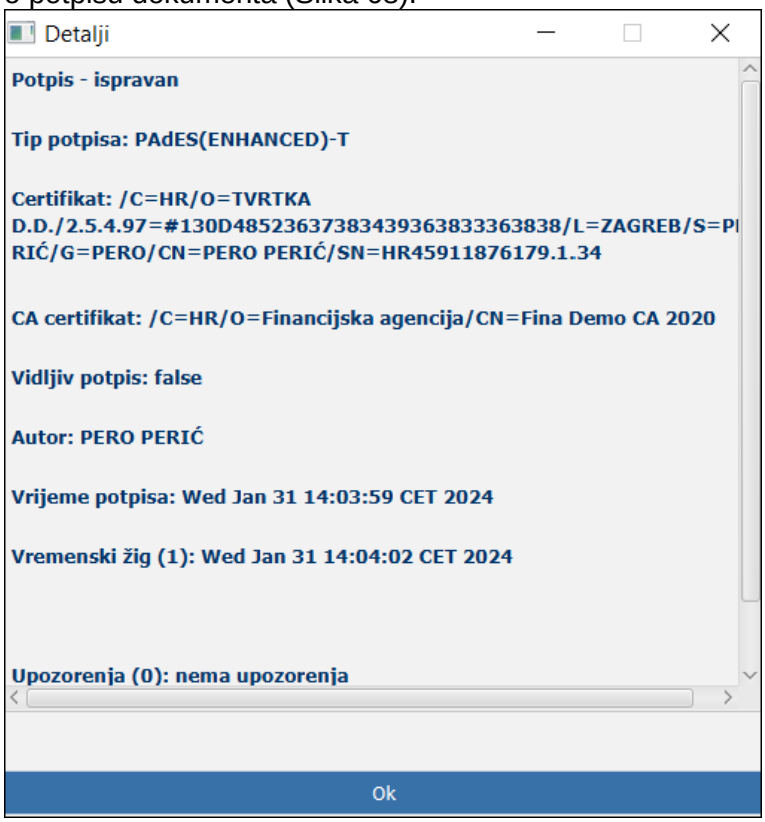


Slika 66. PKI modul – odabir datoteke za validaciju

PKI modul će pokrenuti validaciju te na kraju ispisati rezultat sa informacijom da li je potpis validan ili nije kao što prikazuje Slika 67.

Slika 67. PKI modul – rezultat validacije

Odabirom ikone kružića kod potpisa te klikom na strelicu za dalje moguće je doći do više detalja o potpisu dokumenta (Slika 68).



Slika 68. PKI modul – Detalji potpisa

5.7.2. CAdES

Jednom potpisane datoteke moguće je validirati kroz aplikaciju odabirom stavke menija *Potpisivanje CAdES → Validacija.*

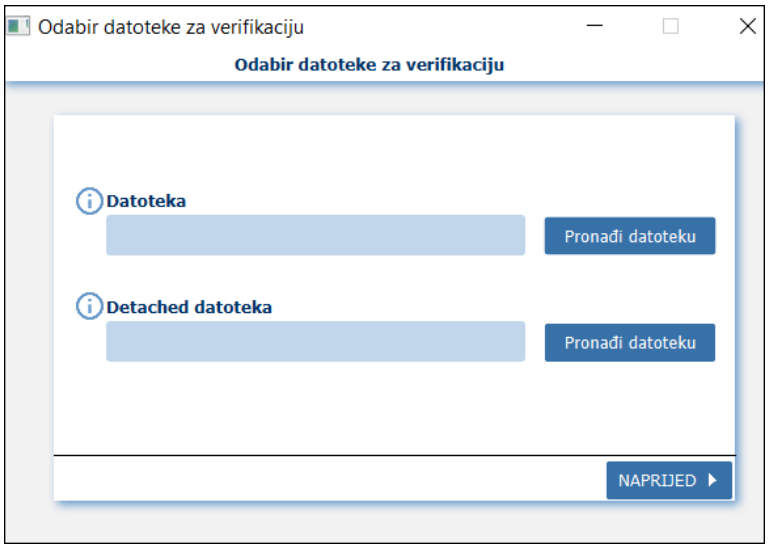
Odabirom stavke menija otvara se ekran za validaciju gdje za početak validacije korisnik mora odabrati gumb *Pripremi* (Slika 69).

Slika 69. Ekran za validaciju potpisa

Klikom na gumb „*Pripremi*“ pojavljuju se opcije za pokretanje PKI modula kojima se vrši validacija (Slika 70). U slučaju korištenja 32-bitnog operacijskog sustava odabire se opcija „*VALIDIRAJ (32-BITNI PKI MODUL)*“, dok se u slučaju 64-bitnog operacijskog sustava odabire opcija „*VALIDIRAJ (64-BITNI PKI MODUL)*“ kojom se pokreće 64-bitna verzija PKI modula. Korisnici 64-bitnog operacijskog sustava mogu validirati datoteke i putem gumba „*VALIDIRAJ (32-BITNI PKI MODUL)*“, ali prije toga moraju izvršiti instalaciju 32-bitnog PKI modula.

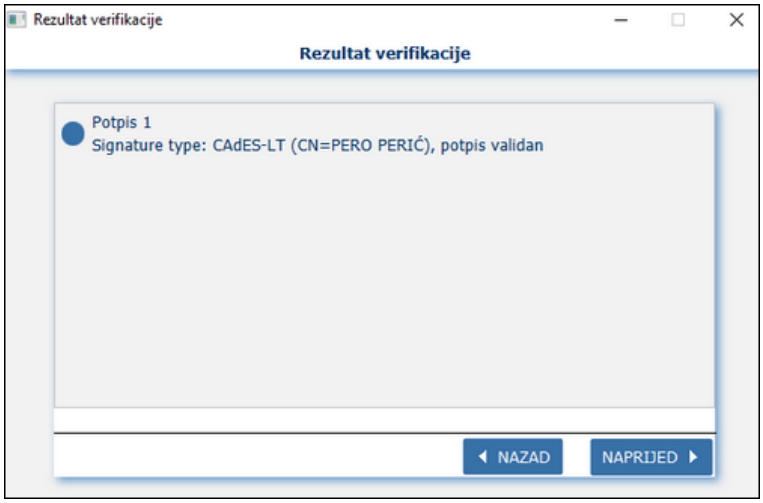
Slika 70. Validacija potpisa – odabir 32-bit ili 64-bit verzije modula

Prilikom pokretanja PKI modula prvo se otvara komponenta za odabir datoteke koju se želi validirati (Slika 71). U slučaju da je potpis u izdvojenoj datoteci, potrebno je odabrati originalnu datoteku i izdvojenu (detached) datoteku. Nakon odabira potrebno je kliknuti gumb za nastavak.



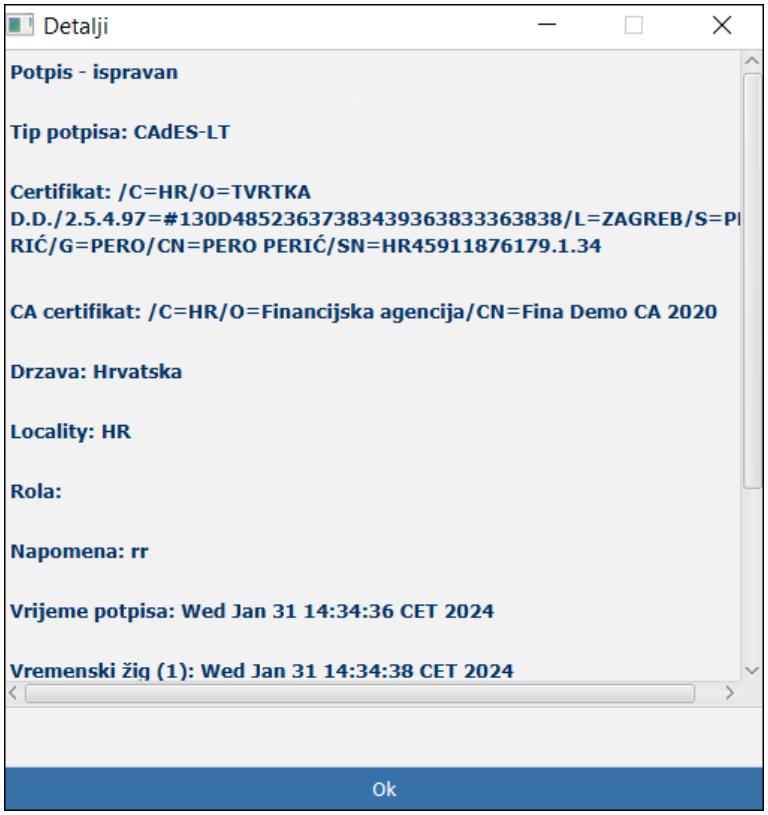
Slika 71. PKI modul – odabir datoteke za validaciju

PKI modul će pokrenuti validaciju te na kraju ispisati rezultat sa informacijom da li je potpis validan ili nije kao što prikazuje Slika 72.



Slika 72. PKI modul – rezultat validacije

Odabirom ikone kružića kod potpisa te klikom na strelicu za dalje moguće je doći do više detalja o potpisu dokumenta (Slika 73).



Slika 73. PKI modul – Detalji potpisa

5.7.3. XAdES

Jednom potpisane datoteke moguće je validirati kroz aplikaciju odabirom stavke menija *Potpisivanje XAdES → Validacija.*

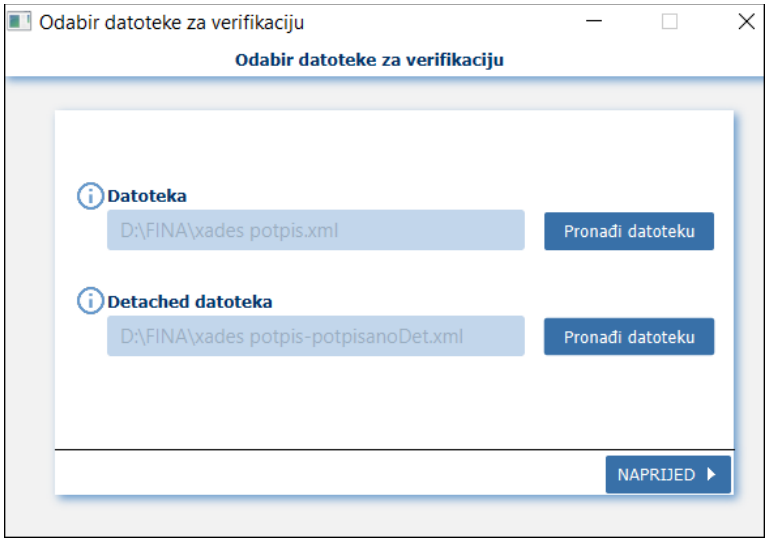
Odabirom stavke menija otvara se ekran za validaciju gdje za početak validacije korisnik mora odabrati gumb *Pripremi* (Slika 74).

Slika 74. Ekran za validaciju potpisa

Klikom na gumb „*Pripremi*“ pojavljuju se opcije za pokretanje PKI modula kojima se vrši validacija (Slika 75). U slučaju korištenja 32-bitnog operacijskog sustava odabire se opcija „*VALIDIRAJ (32-BITNI PKI MODUL)*“, dok se u slučaju 64-bitnog operacijskog sustava odabire opcija „*VALIDIRAJ (64-BITNI PKI MODUL)*“ kojom se pokreće 64-bitna verzija PKI modula. Korisnici 64-bitnog operacijskog sustava mogu validirati datoteke i putem gumba „*VALIDIRAJ (32-BITNI PKI MODUL)*“, ali prije toga moraju izvršiti instalaciju 32-bitnog PKI modula.

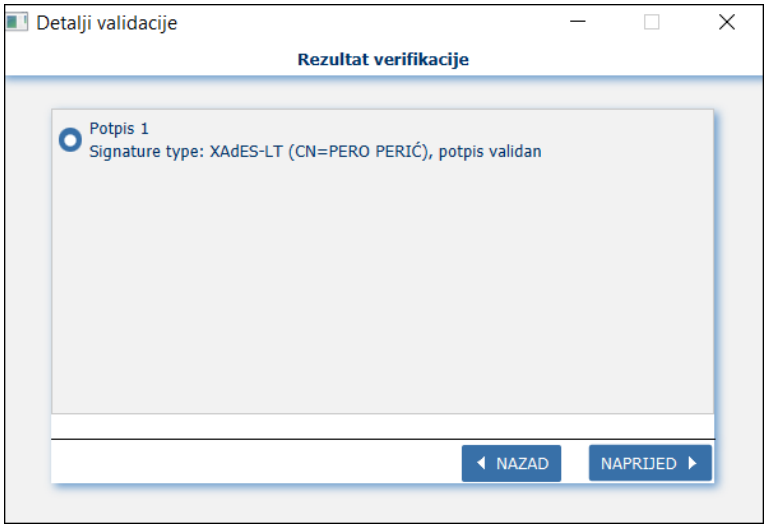
Slika 75. Validacija potpisa – odabir 32-bit ili 64-bit verzije modula

Prilikom pokretanja PKI modula prvo se otvara komponenta za odabir datoteke koju se želi validirati (Slika 76). U slučaju da je potpis u izdvojenoj datoteci, potrebno je odabrati originalnu datoteku i izdvojenu (detached) datoteku. Nakon odabira potrebno je kliknuti gumb za nastavak.



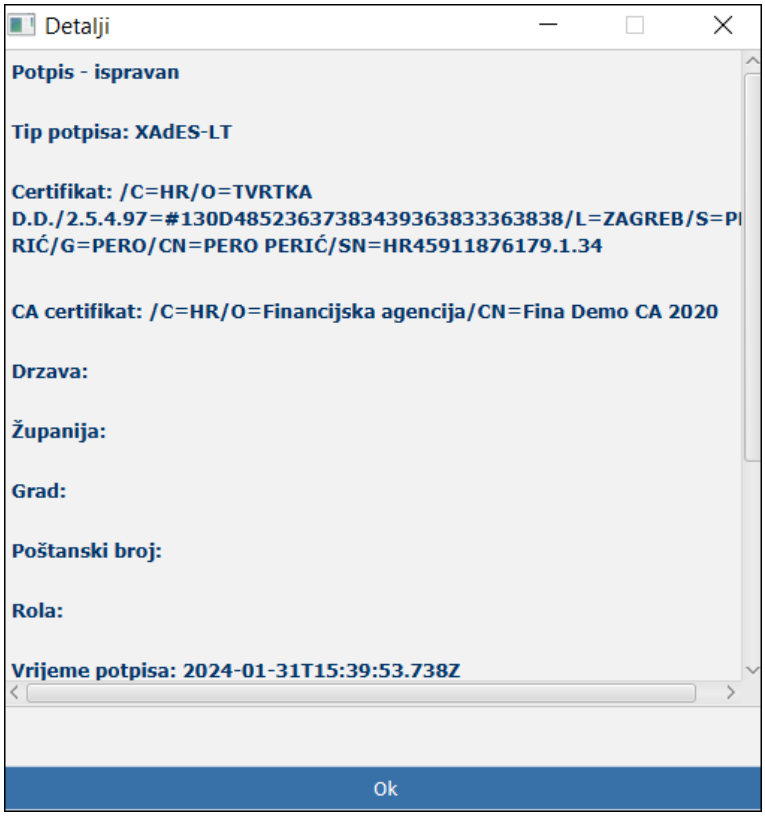
Slika 76. PKI modul – odabir datoteke za validaciju

PKI modul će pokrenuti validaciju te na kraju ispisati rezultat sa informacijom da li je potpis validan ili nije kao što prikazuje Slika 77.



Slika 77. PKI modul – rezultat validacije

Odabirom ikone kružića kod potpisa te klikom na strelicu za dalje moguće je doći do više detalja o potpisu dokumenta (Slika 78).



Slika 78. PKI modul – Detalji potpisa