Naslov dokumenta:	**Kvalifikovano elektronsko potpisivanje i vremensko žigosanje PDF dokumenata korišćenjem aplikacije Adobe Acrobat Reader DC**
Verzija:	1.21
Datum:	8.11.2021.
Autor:	Administratori Sertifikacionog tela Pošte

1. Preduslovi

Aplikacija **Adobe Acrobat Reader DC** (Document Cloud) može da se koristi za **kvalifikovano** elektronsko potpisivanje i vremensko žigosanje PDF i PDF/A dokumenata u skladu sa standardom ETSI EN 319 142-1, Electronic Signatures and Infrastructures (ESI); PAdES Digital Signatures; Part 1: Building blocks and PAdES baseline signatures. Aplikacija Adobe Acrobat Reader je besplatna, a može da se preuzme sa veb adrese: http://www.adobe.com.

Da bi moglo da se vrši **kvalifikovano** elektronsko potpisivanje i vremensko žigosanje PDF i PDF/A dokumenata korišćenjem aplikacije Adobe Acrobat Reader, u skladu sa standardom **ETSI EN 319 142-1 Part 1**, potrebno je da budu ispunjeni sledeći preduslovi:

1. Na računaru korisnika mora da bude instalisana aplikacija **Adobe Acrobat Reader DC** (ovaj dokument je napisan za aplikaciju Adobe Acrobat Reader DC 2021.005.20060 na Windows 10 računaru).

2. Na računaru korisnika mora da bude podešen **tačan datum, vreme i vremenska (časovna) zona (za korisnike u Srbiji: GMT+01:00)**.

3. Korisnik koji vrši potpisivanje mora da poseduje lični (personalni) **KVALIFIKOVANI elektronski sertifikat** i tajni (privatni) kriptografski ključ na smart kartici ili USB tokenu, a računar korisnika mora da bude podešen za korišćenje kvalifikovanog elektronskog sertifikata prema dokumentu **Instalisanje klijentskog softvera A.E.T. SafeSign i korišćenje smart kartica i USB tokena - sažeto uputstvo**.

4. Neophodno je da se na formi ***Creation and Appearance Preferences*** pored naziva polja *Default Signing Format* iz padajuće liste izabere ***CAdES-Equivalent*** i čekira opcija ***Include signature's revocation status***, kao što je prikazano na slici 1. Do te forme se dolazi na sledeći način: meni *Edit* → opcija *Preferences...* → kategorija *Signatures* → u sekciji *Creation & Appearance* pritisnuti dugme *More...*. Čekirana opcija ***Include signature's revocation status*** omogućava ugrađivanje OSCP (*Online Certificate Status Protocol*) odgovora i/ili registra opozvanih sertifikata (*Certificate Revocation List* - CRL) u potpisan PDF dokument, tako da je **neophodno imati pristup Internetu prilikom potpisivanja**.

5. Korisnik koji vrši potpisivanje i primalac potpisanog PDF dokumenta moraju da preuzmu i instališu sertifikate ROOT CA servera Sertifikacionog tela Pošte, da bi moglo da se izvrši uspešno verifikovanje potpisanog PDF dokumenta. Postupak preuzimanja i instalisanja sertifikata ROOT CA servera **Pošta Srbije CA Root** i **Posta CA Root** objašnjen je u

dokumentu **Preuzimanje i instalisanje sertifikata ROOT CA servera Sertifikacionog tela Pošte u Windows skladište sertifikata**. Osim toga, neophodno je da se na formi ***Signature Verification Preferences*** čekiraju **dve (2) opcije Windows integracije** i urade ostala podešavanja, kao što je prikazano na slici 2. Do te forme se dolazi na sledeći način: meni *Edit* → opcija *Preferences...* → kategorija *Signatures* → u sekciji *Verification* pritisnuti dugme *More...*.

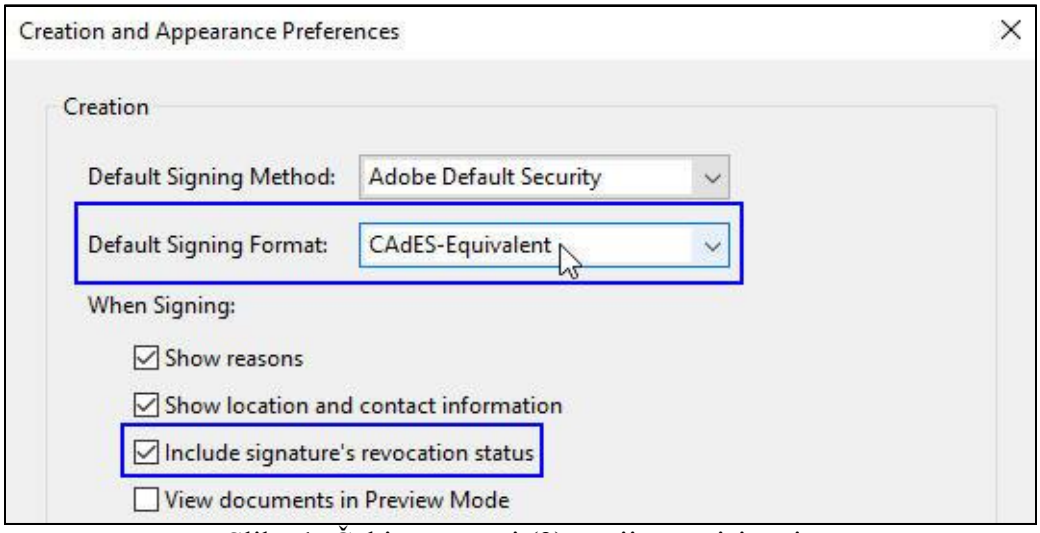
6. Poželjno/potrebno je da se pridruži vremenski žig. Pre vremenskog žigosanja neophodno je da se na formi ***New Time Stamp Server*** podese parametri pristupa Timestamp (TSA) serveru, kao što je prikazano na slici 4. Do te forme se dolazi na sledeći način: meni *Edit* → opcija *Preferences...* → kategorija *Signatures* → u sekciji *Document Timestamping* pritisnuti dugme More... → kategorija *Time Stamp Servers* → dugme za dodavanje novog Timestamp servera (slika 3.). Posle podešavanja Timestamp servera treba da se pritisne dugme *Set Default*. Prilikom vremenskog žigosanja **neophodan je pristup Internetu**.

Način prijavljivanja (autentifikacije) korisnika na Timestamp (TSA) server Sertifikacionog tela Pošte (https://www.ca.posta.rs/vremenski_zigovi.htm) se vrši putem korisničkog imena i lozinke (slika 4. i 10.).

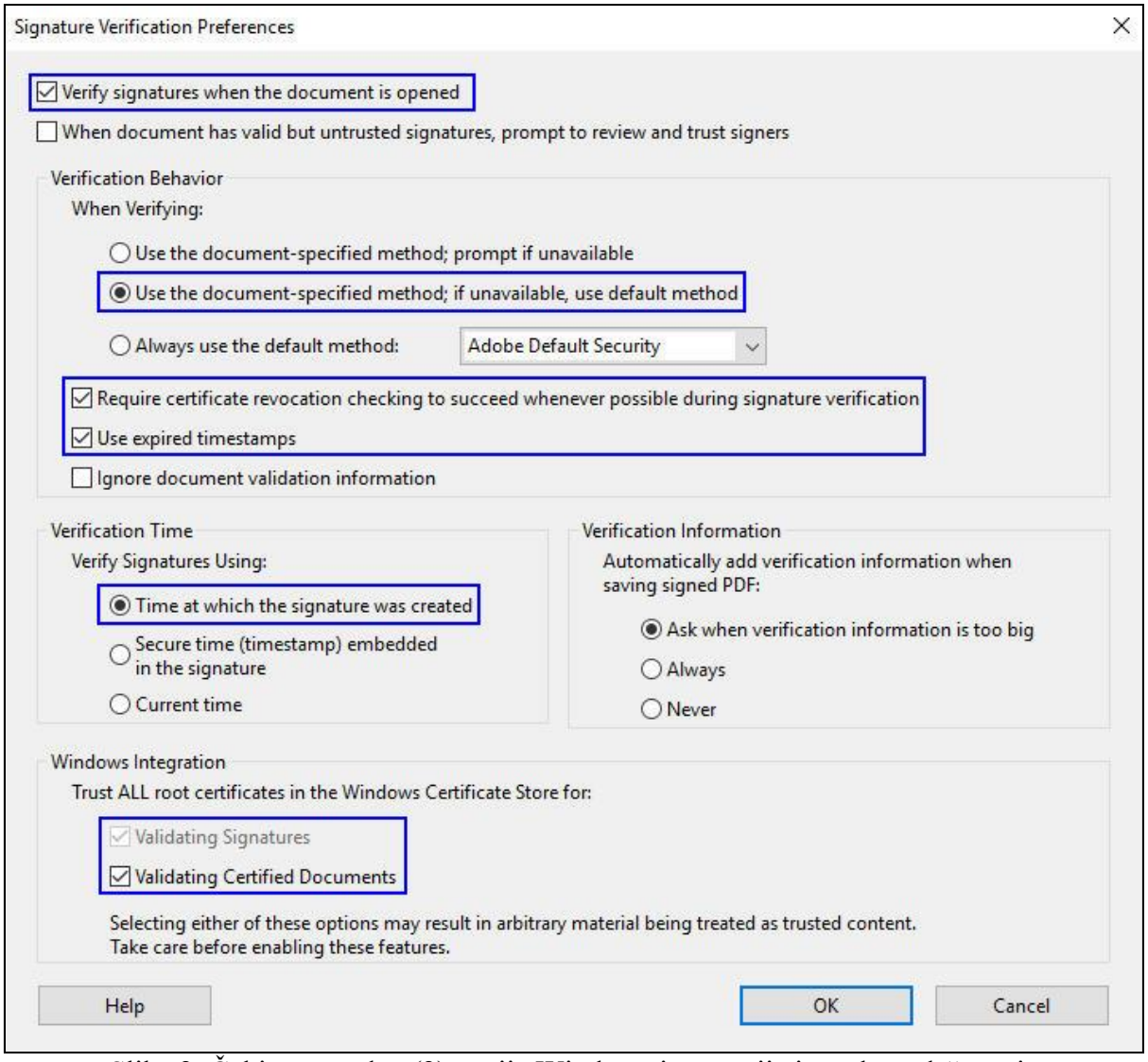
Anonimno prijavljivanje korisnika na Timestamp (TSA) server Pošte nije dozvoljeno.

Aplikacija **Adobe Acrobat Reader DC** omogućava:

- Elektronsko potpisivanje PDF dokumenta ( ). Jedan ili više korisnika mogu da elektronski potpišu isti PDF dokument (slika 17.).
- Elektronsko potpisivanje i vremensko žigosanje PDF dokumenta ( ).
- Vremensko žigosanje PDF dokumenta ( ).

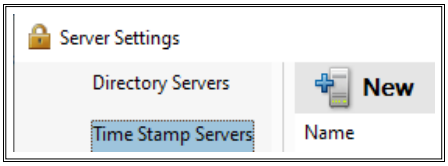


Slika 1. Čekirane su tri (3) opcije potpisivanja

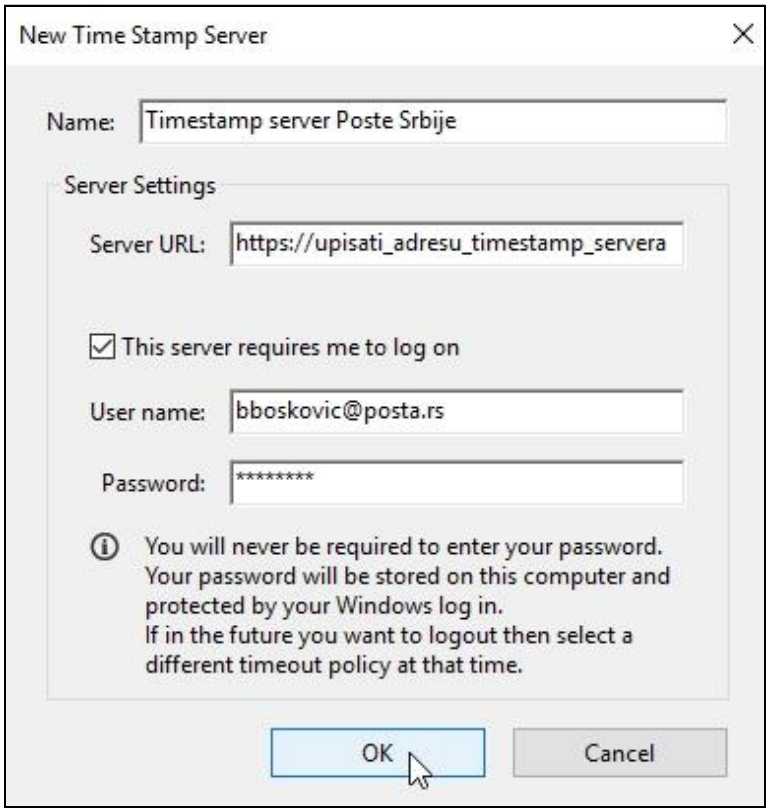


Slika 2. Čekirane su dve (2) opcije Windows integracije i ostala podešavanja

Čekirane dve (2) opcije Windows integracije sa slike 2. omogućavaju aplikaciji Adobe Reader da veruje ROOT sertifikatima koji se nalaze u Windows skladištu ROOT sertifikata.



Slika 3. Dodavanje novog Timestamp servera



Slika 4. Podaci o Timestamp serveru

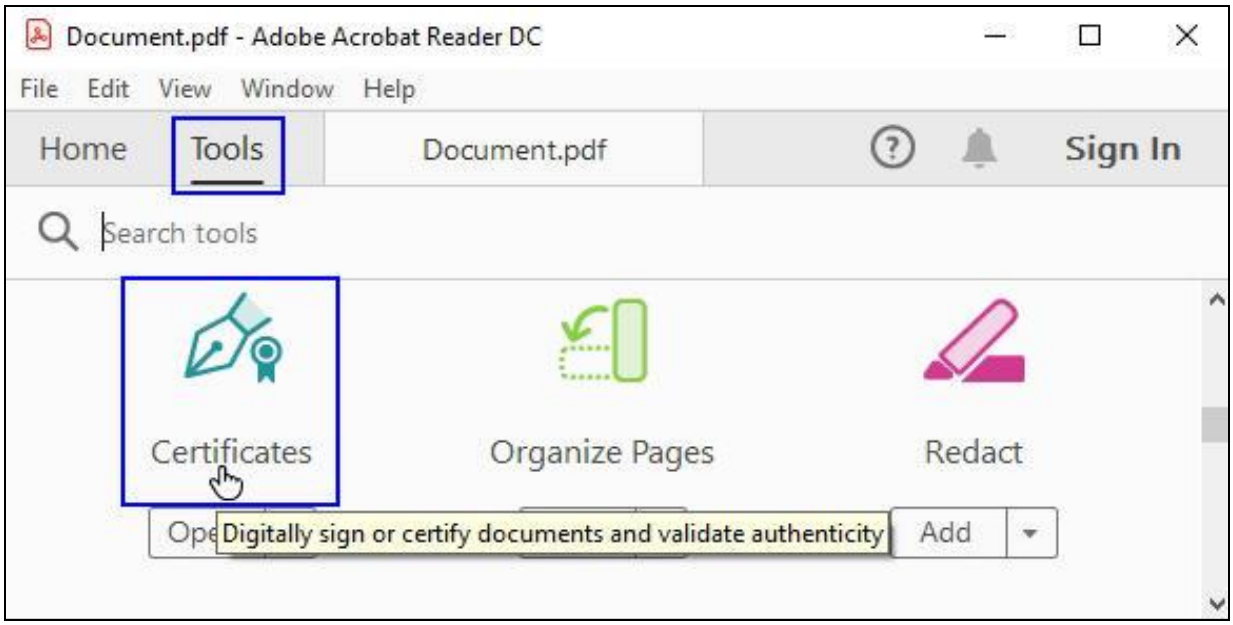
2. Elektronsko potpisivanje i vremensko žigosanje PDF dokumenta

Elektronsko potpisivanje i vremensko žigosanje PDF dokumenta izvršava se na sledeći način:

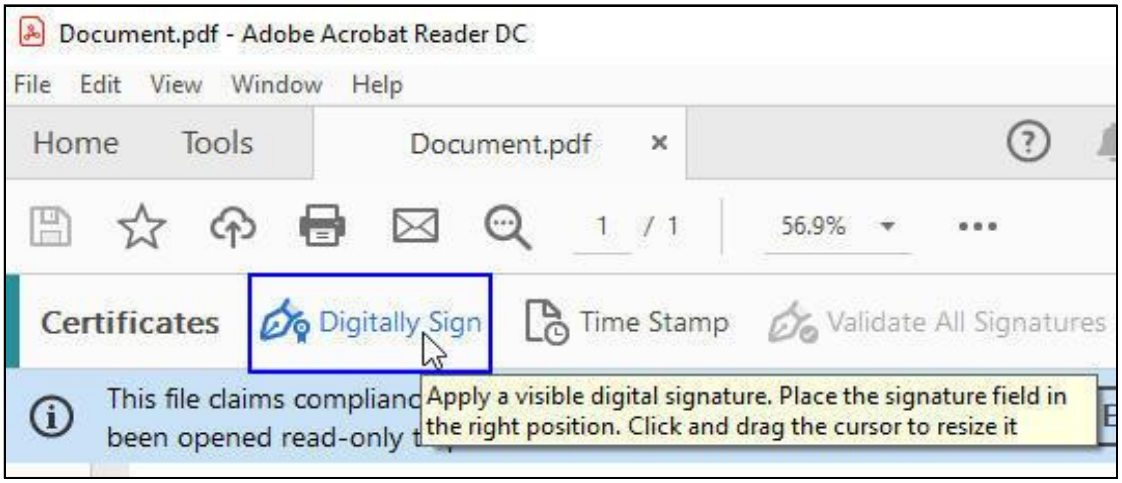
- Startuje se aplikacija Adobe Reader i otvori PDF dokument koji treba da se potpiše.
- Pritisne se dugme *Tools*, pa se izabere opcija *Certificates* (slika 5.).
- Na panelu za rad sa sertifikatima se pritisne dugme *Digitally Sign* (slika 6.).
- Na formi *Acrobat Reader* se pritisne dugme *OK*.
- Na željenom mestu u PDF dokumentu se kreira pravougaoni okvir u kome će biti prikazani podaci o potpisniku. Okvir se kreira korišćenjem miša. Ako korisnik ne želi vizuelni prikaz elektronskog potpisa u PDF dokumentu, umesto pravougaonog okvira treba da se kreira linija.
- Na formi *Sign with a Digital ID* se izabere sertifikat za potpisivanje i pritisne dugme *Continue* (slika 7.).
- Na formi *Sign Document* se izabere sertifikat za potpisivanje i pritisne dugme *Sign* (slika 8.).
- Na formi *Save As* se izabere lokacija na hard disku računara na kojoj će biti snimljen potpisani PDF dokument i pritisne dugme *Save*.
- Unese se lozinka smart kartice/USB tokena i pritisne dugme *OK* (slika 9.).
- Prijavljivanje na Timestamp (TSA) server unosom korisničkog imena i lozinke (slika 10.).

Na ovaj način je završen postupak elektronskog potpisivanja i vremenskog žigosanja PDF dokumenta. U potpisanom PDF dokumentu postoji vizuelni prikaz elektronskog potpisa sa podacima o korisniku koji je izvršio potpisivanje i datum i vreme potpisivanja (slika 11.).

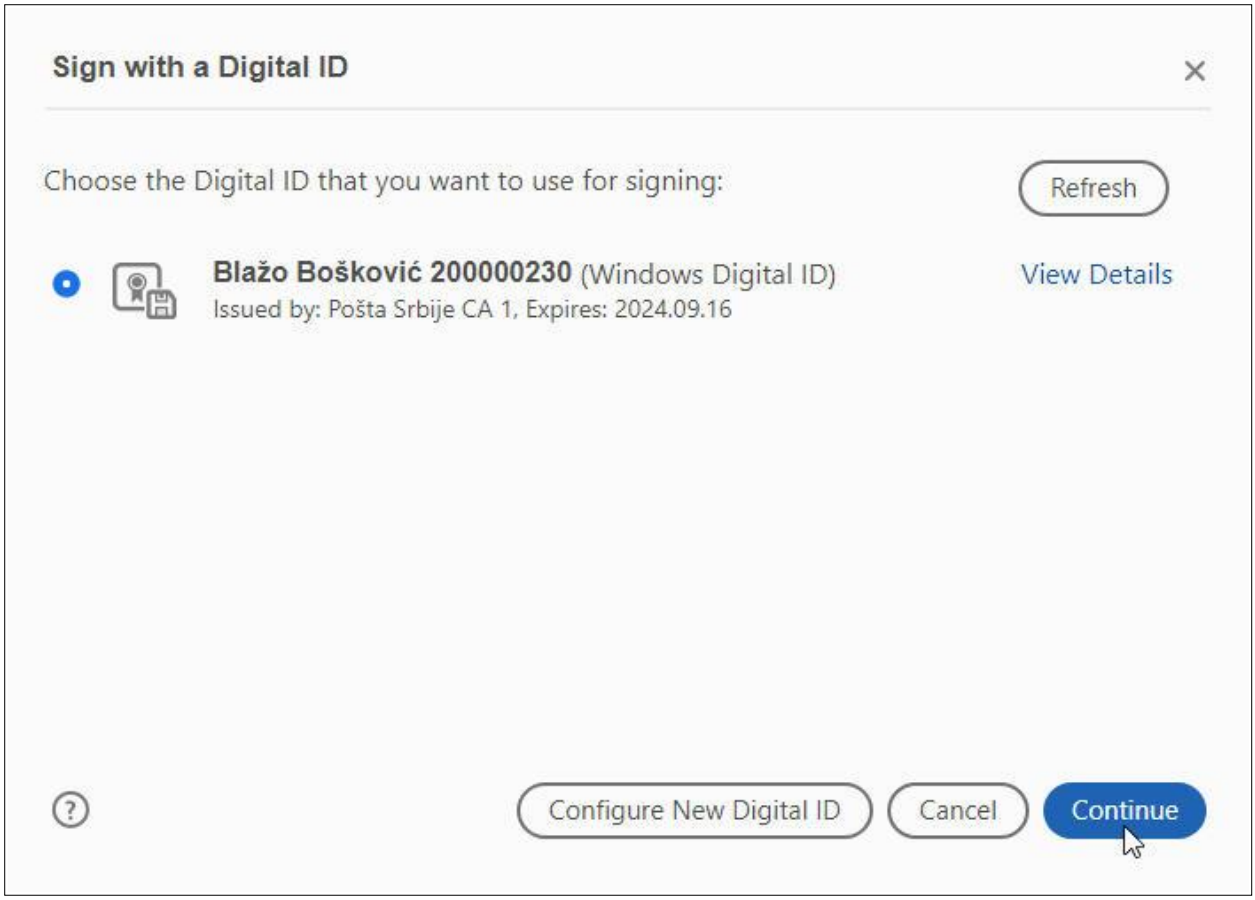
Posle zatvaranja i otvaranja potpisanog PDF dokumenta, osnovni podaci o elektronskom potpisu PDF dokumenta postoje na formi *Signatures* koja se otvara pritiskom na ikonicu plave olovke u *Navigation Panel*-u (slika 11.). Standard potpisa može da se vidi na formi *Advanced Signature Properties* kao što je prikazano na slici 12. Do te forme se dolazi na sledeći način: *Signatures* (u *Navigation Panel*-u) → Desni taster miša na elektronski potpis korisnika → *Show Signature Properties...* → *Advanced Properties...*



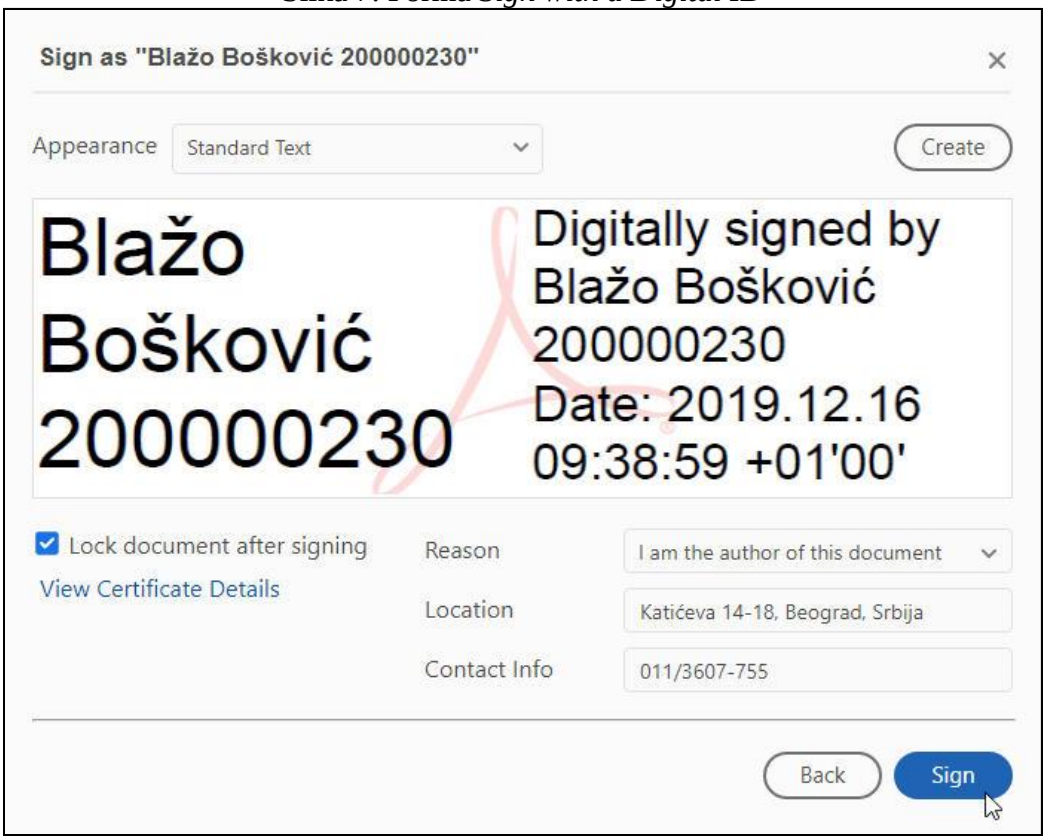
Slika 5. Izbor panela za rad sa elektronskim sertifikatima



Slika 6. Početak potpisivanja PDF dokumenta

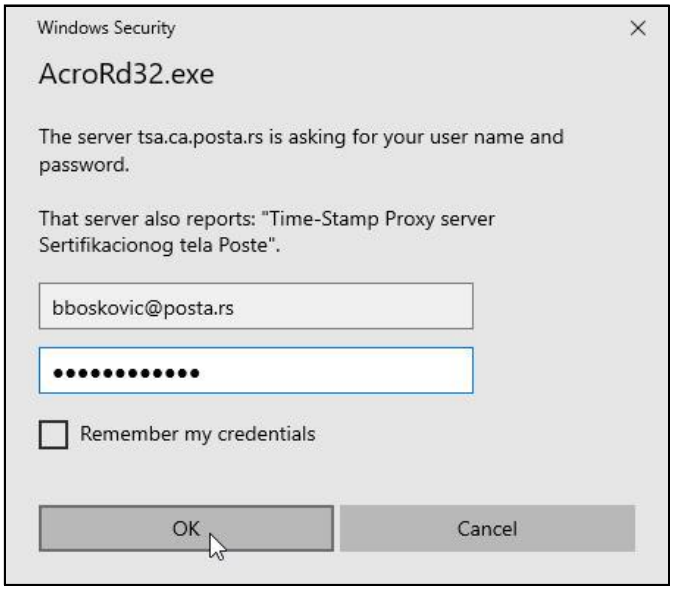


Slika 7. Forma *Sign with a Digital ID*

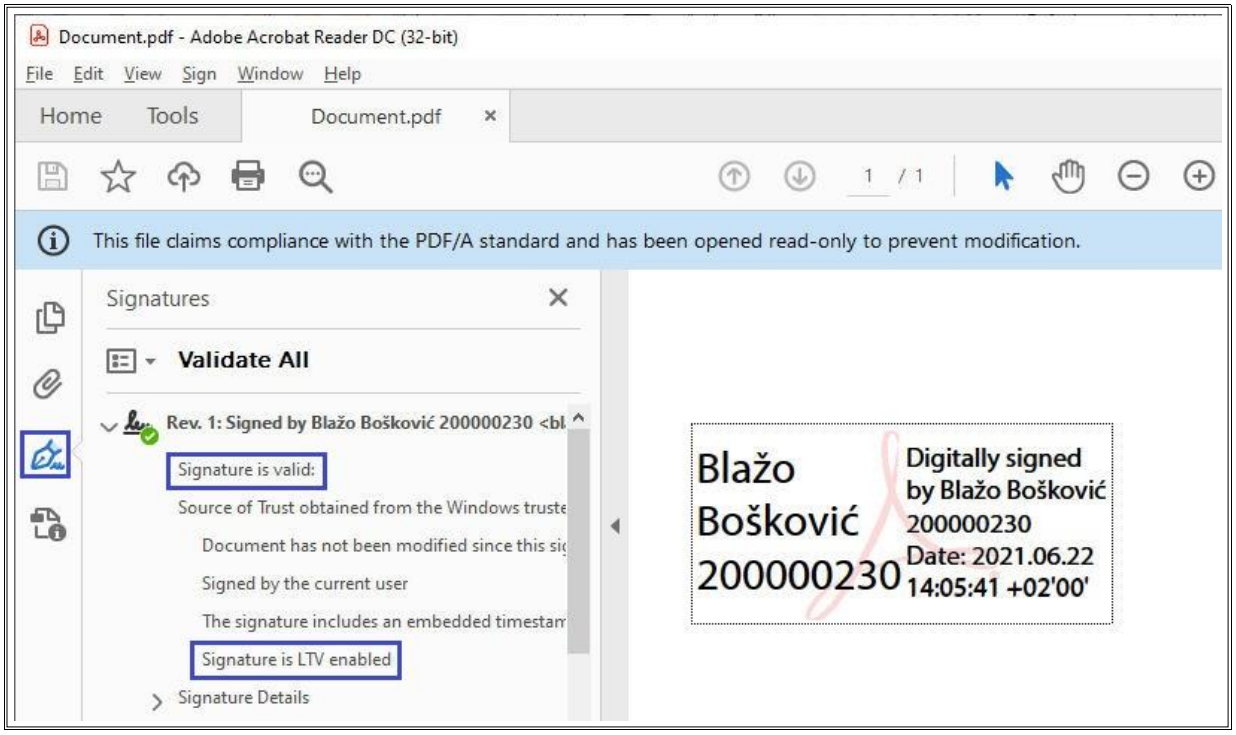


Slika 8. Forma *Sign Document* sa izabranim sertifikatom za potpisivanje

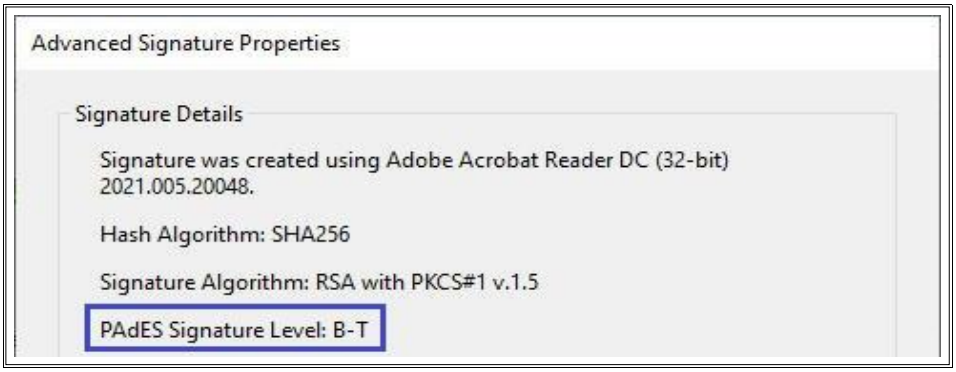
Slika 9. Unos lozinke smart kartice/USB tokena



Slika 10. Unos korisničkog imena i lozinke za pristup Timestamp (TSA) serveru



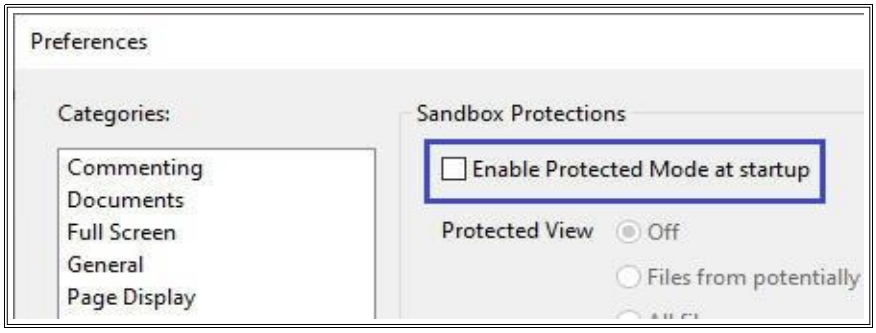
Slika 11. Potpisan PDF dokument i forma *Signatures* sa podacima o elektronskom potpisu



Slika 12. Standard potpisa PAdES baseline signatures

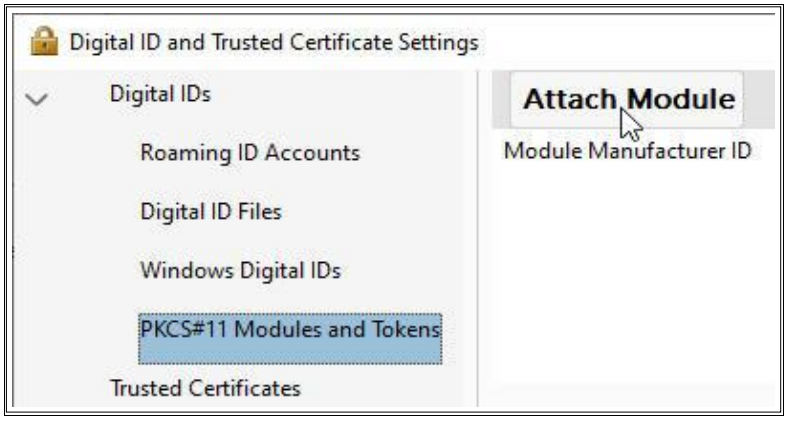
3. Podešavanje Adobe Acrobat Reader DC za potpisivanje dokumenata korišćenjem PKCS#11 interfejsa

U nekim slučajevima, moguće je da se prilikom pokušaja potpisivanja dokumenata, iako je Adobe Acrobat Reader DC podešen prema ovom uputstvu, javlja greška i potpisivanje bude neuspešno. To je posledica promena koje nekada donesu nove verzije Adobe Reader-a. U tom slučaju je moguć drugačiji način korišćenja sertifikata sa smart kartice/USB tokena.
Potrebno je da se sledeći putanju: meni *Edit* → opcija *Preferences...* → kategorija *Security (Enhanced)* dečekira opcija *Enable Protected Mode at startup* kao na slici 13. i restartuje Adobe Acrobat Reader DC.



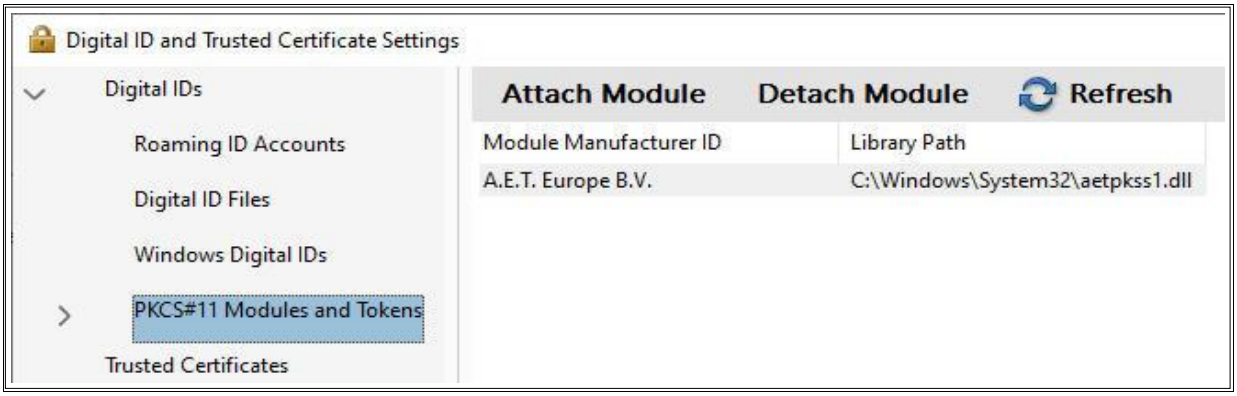
Slika 13. Opcija *Enable Protected Mode at startup*

Zatim je potrebno da se podesi PKCS#11 modul na sledeći način: meni *Edit* → opcija *Preferences...* → kategorija *Signatures* → dugme *More...* u sekciji *Identities & Trusted Certificates*. Na formi *Digital ID and Trusted Certificate Settings* treba da se klikne na opciju *PKCS#11 Modules and Tokens*, a zatim na dugme *Attach Module* (slika 14.).



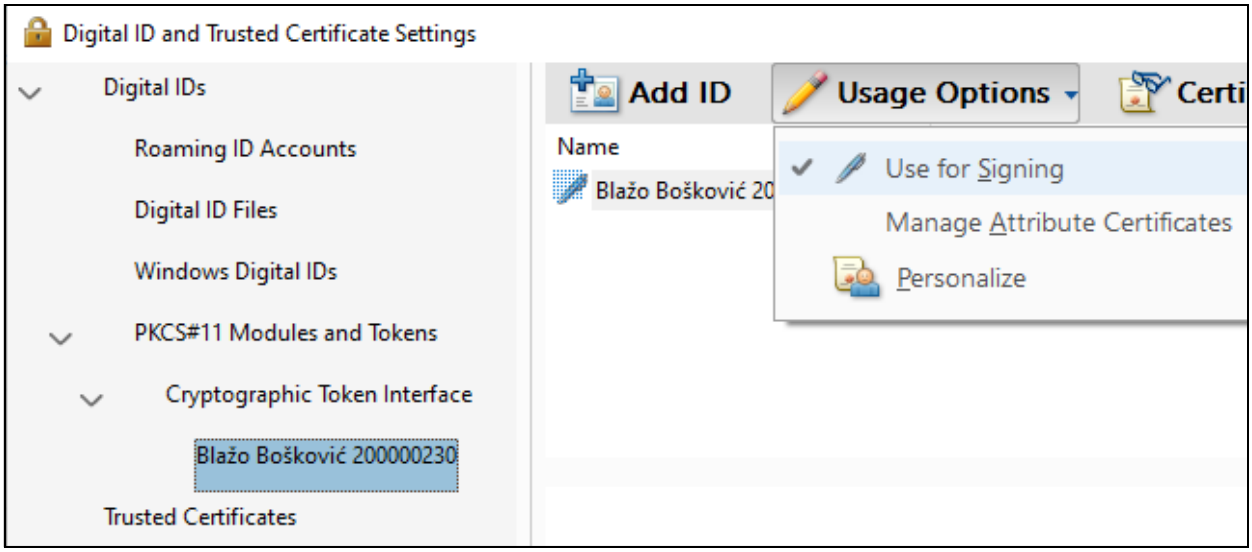
Slika 14. Forma *Digital ID and Trusted Certificate Settings*

Potrebno je da se unese putanja PKCS#11 modula, koja je u ovom slučaju C:\Windows\System32\aetpkss1.dll i pritisne dugme *Open*. U spisku PKCS#11 modula će da se pojavi modul kao na slici 15.



Slika 15. Prikaz dodatog PKCS#11 modula

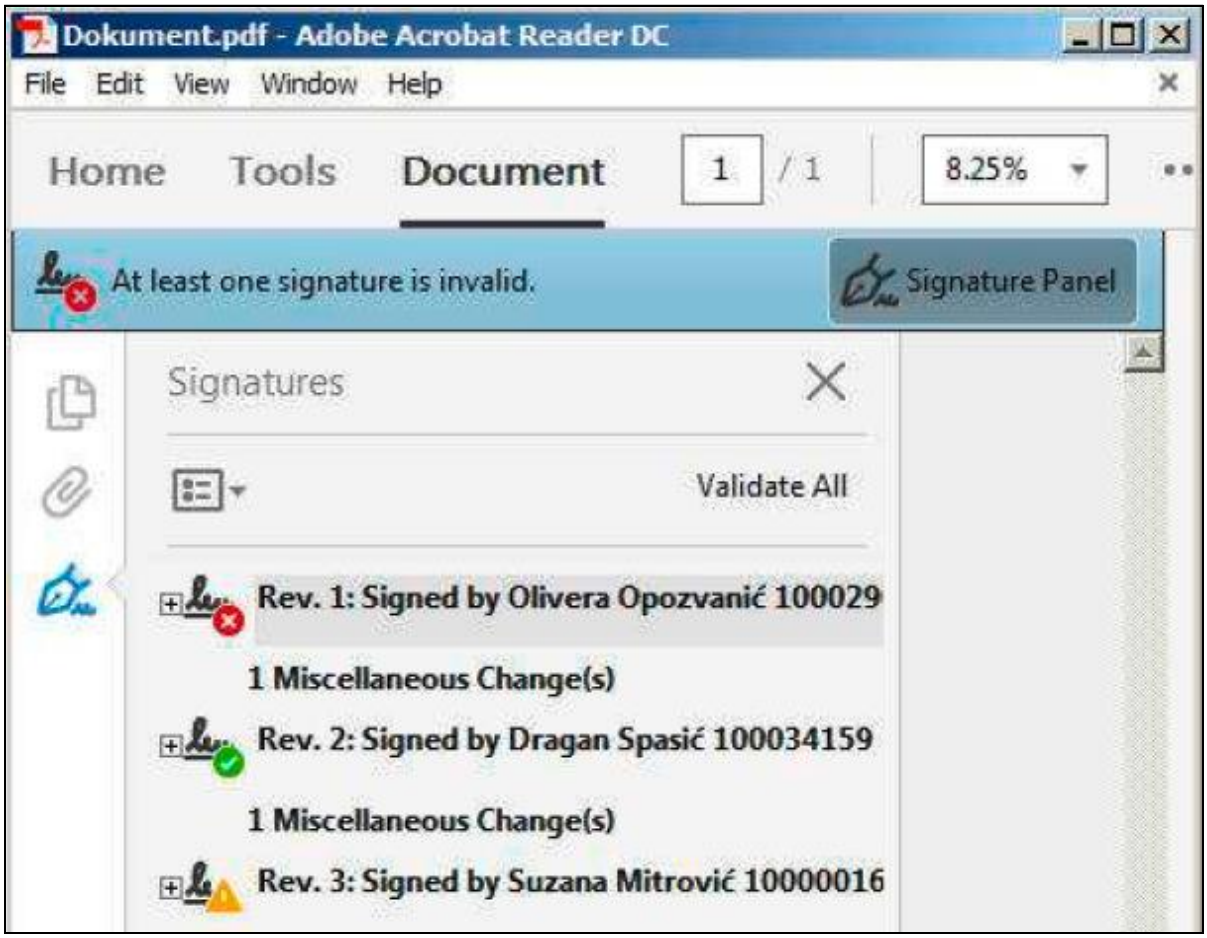
Potom treba da se otvori meni *Cryptographic Token Interface*, kao i da se izabere klikom miša sertifikat klikom na ime i prezime korisnika, a zatim klikne na dugme sa ikonicom olovke i iz menija koji se otvori treba da se izabere opcija *Use for Signing*, kao što je prikazano na slici 16.



Slika 16. Podešavanje sertifikata za potpisivanje

4. Razlozi zbog kojih elektronski potpis PDF dokumenta nije ispravan

Ako je elektronski potpis PDF dokumenta **neispravan** (INVALID), ili je status potpisa **nepoznat** (UNKNOWN), aplikacija Adobe Reader će na formi *Signatures* takvom potpisu da dodeli ikonicu crvenog kruga sa belim krstom (), odnosno, ikonicu žutog trougla (), kao što je prikazano na slici 13. Forma sa slike 13. je dobijena kao rezultat verifikovanja tri (3) potpisa korišćenjem aplikacije Adobe Acrobat Reader DC.



Slika 17. Statusi elektronskih potpisa tri potpisnika (INVALID, VALID i UNKNOWN)

Razlozi zbog kojih je elektronski potpis PDF dokumenta **neispravan** ( ) mogu da budu:

- Sadržaj PDF dokumenta je izmenjen posle potpisivanja (narušen je integritet dokumenta).
- Sertifikat kojim je izvršeno elektronsko potpisivanje je opozvan ili je suspendovan.
- Format elektronskog potpisa je defektan (primer: Error encountered while BER decoding).

Razlozi zbog kojih je status elektronskog potpisa PDF dokumenta **nepoznat** ( ) mogu da budu:

- Ne može da se proveri identitet sertifikata kojim je izvršeno elektronsko potpisivanje. Predlog za rešenje problema: instalisanje sertifikata **Posta Srbije CA Root** i **Posta CA Root** u Windows skladište sertifikata i čekiranje **dve (2) opcije Windows integracije** (slika 2.).
- Ne može da se proveri opozvanost sertifikata kojim je izvršeno elektronsko potpisivanje. Predlog za rešenje problema: od računara na kome se radi verifikovanje potpisanog PDF dokumenta treba da se omogući pristup ka OCSP i CRL serverima Sertifikacionog tela Pošte.
- Sertifikatu kojim je izvršeno elektronsko potpisivanje je istekao rok važnosti ili još nije počela njegova važnost. Predlog za rešenje problema: na računaru na kome se radi verifikovanje potpisanog PDF dokumenta treba da se proveri da li je podešen **tačan datum, vreme i vremenska (časovna) zona (za korisnike u Srbiji: GMT+01:00)**.