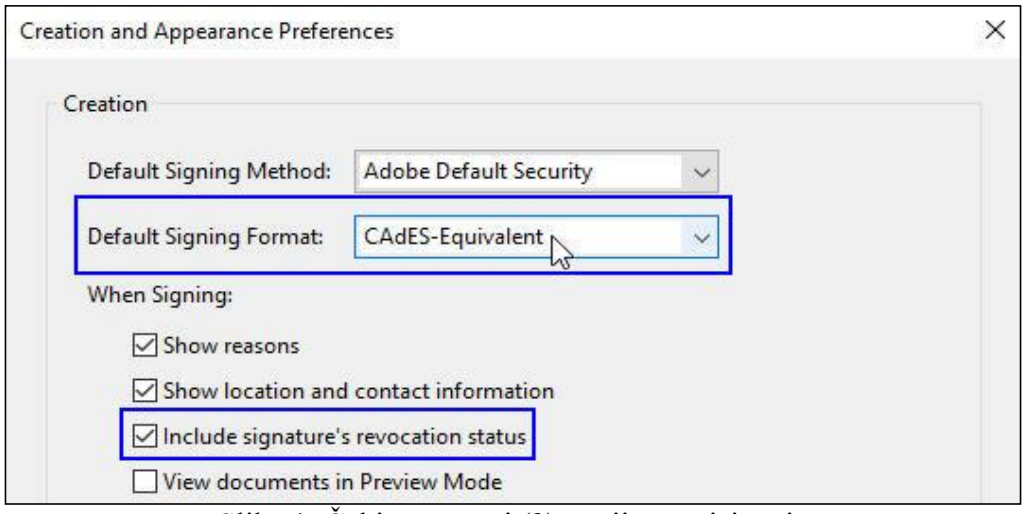
Naslov dokumenta:	**Kvalifikovano elektronsko potpisivanje i vremensko žigosanje PDF dokumenata korišćenjem aplikacije Adobe Acrobat Reader DC**
Verzija:	1.25
Datum:	7.10.2024.
Autor:	Administratori Sertifikacionog tela Pošte

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 2024.003.20112 na Windows 10 računaru).
2. Na računaru korisnika mora da bude podešen **tačan datum, vreme i vremenska (časovna) zona**.
3. Korisnik koji vrši potpisivanje mora da poseduje **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. 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** je objašnjen u dokumentu **Preuzimanje i instalisanje sertifikata ROOT CA servera Sertifikacionog tela Pošte u Windows skladište sertifikata**.
5. U aplikaciji Adobe Acrobat Reader je potrebno da se podesi format potpisivanja ***CadES-Equivalent.*** 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.

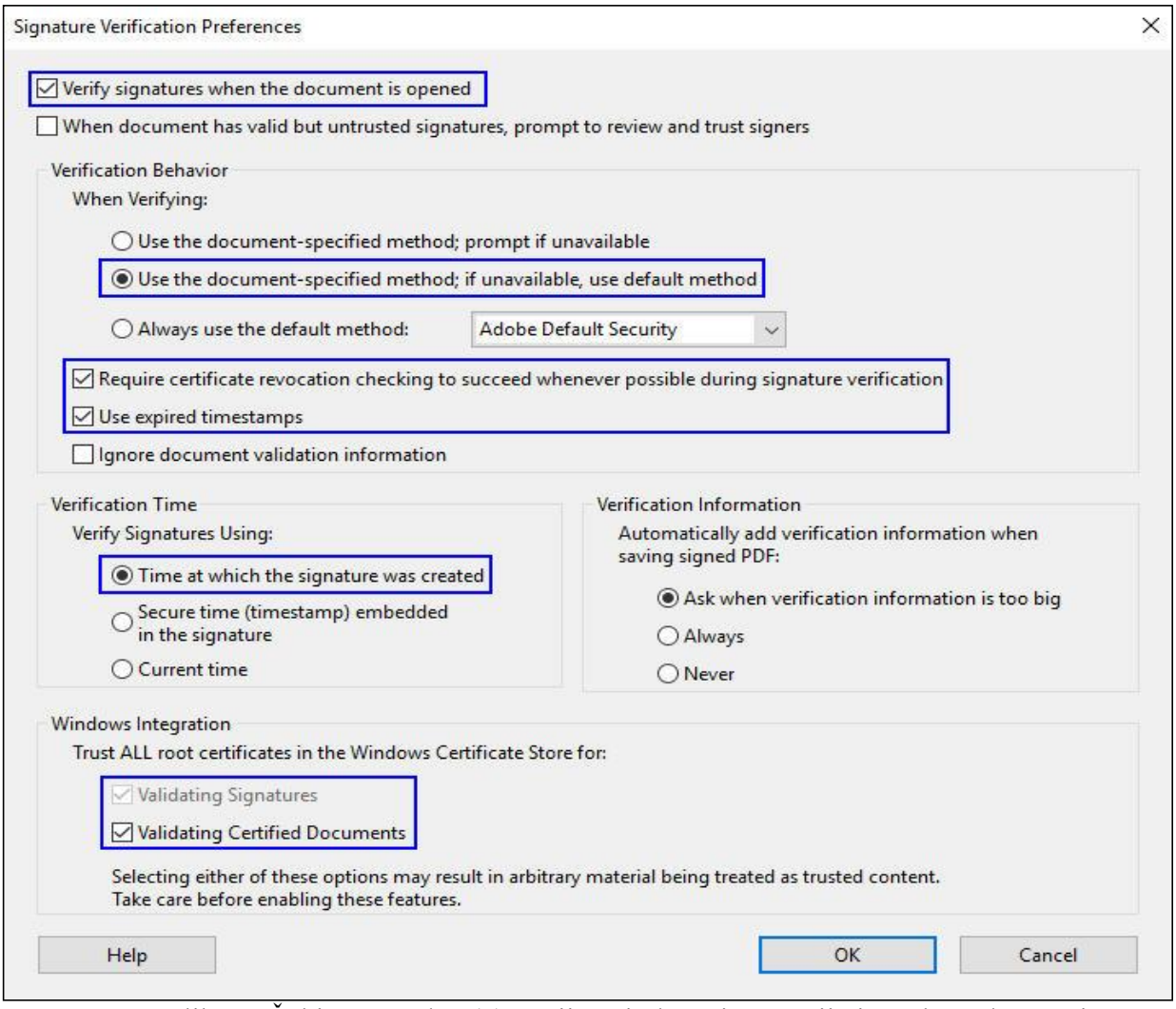


Slika 1. Čekirane su tri (3) opcije potpisivanja

Do forme prikazane na slici 1 se dolazi na sledeći način: meni *Edit* → opcija *Preferences...* → kategorija *Signatures* → u sekciji *Creation & Appearance* pritisnuti dugme *More...*. Čekira se opcija ***Include signature's revocation status*** koja 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**.

6. 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 forme ***Signature Verification Preferences*** se dolazi na sledeći način: meni *Edit* → opcija *Preferences...* → kategorija *Signatures* → u sekciji *Verification* pritisnuti dugme *More...*.

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.



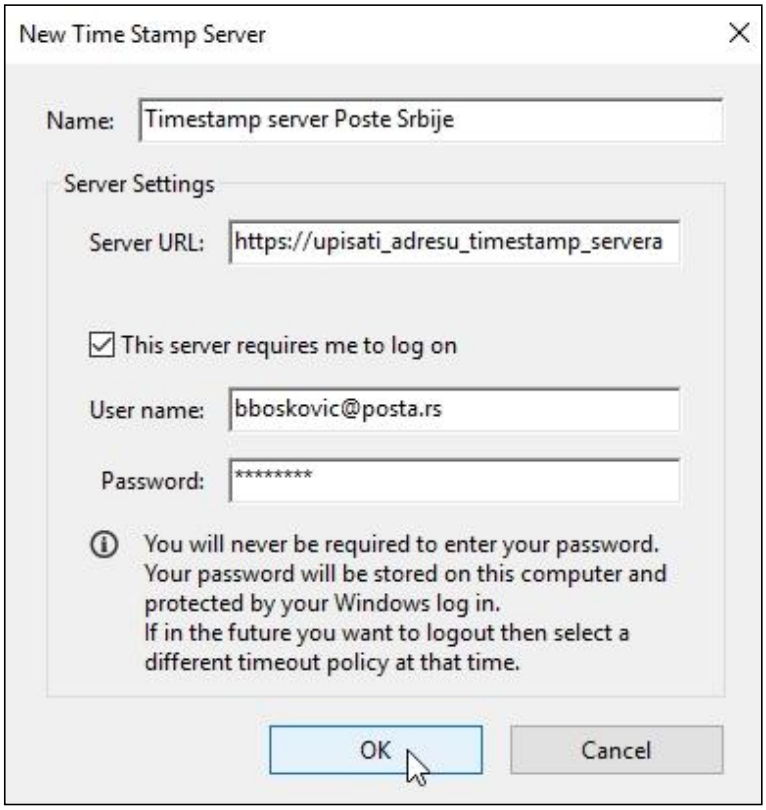
Slika 2. Čekirane su dve (2) opcije Windows integracije i ostala podešavanja

VAŽNO: Ukoliko niste korisnik usluge izdavanja kvalifikovanih elektronskih vremenskih žigova preskočite korak 7. Ukoliko želite da postanete korisnik, odnosno da biste kupili ovu uslugu za više informacija posetite: https://www.ca.posta.rs/vremenski_zigovi.htm

7. Poželjno/potrebno je da se pridruži vremenski žig. Vremenski žig je posebna usluga Sertifikacionog tela Pošte koja se dodatno naplaćuje. 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. korak 1). Posle podešavanja Timestamp servera (slika 4.) treba da se obeleži server mišem (slika 3. korak 2) i pritisne dugme *Set Default* (slika 3. korak 3). Prilikom vremenskog žigosanja **neophodan je pristup internetu**.

Način prijavljivanja (autentifikacije) korisnika na Timestamp (TSA) server Sertifikacionog tela Pošte moguć je korisničkim imenom i lozinkom, ili sertifikatom koji je izdalo Sertifikaciono telo Pošte. Primer formi za unos podataka kada se autentifikacija vrši putem korisničkog imena i lozinke prikazan je na slikama 4. i 10. Anonimno prijavljivanje korisnika na Timestamp (TSA) server Pošte nije dozvoljeno. Ukoliko ne unesete korisničko ime i lozinku kao što je prikazano na slici 4. prilikom svakog dodeljivanja vremenskog žiga pojavljivaće se forma kao na slici 10.

Slika 3. Dodavanje novog Timestamp servera



Slika 4. Podaci o Timestamp serveru

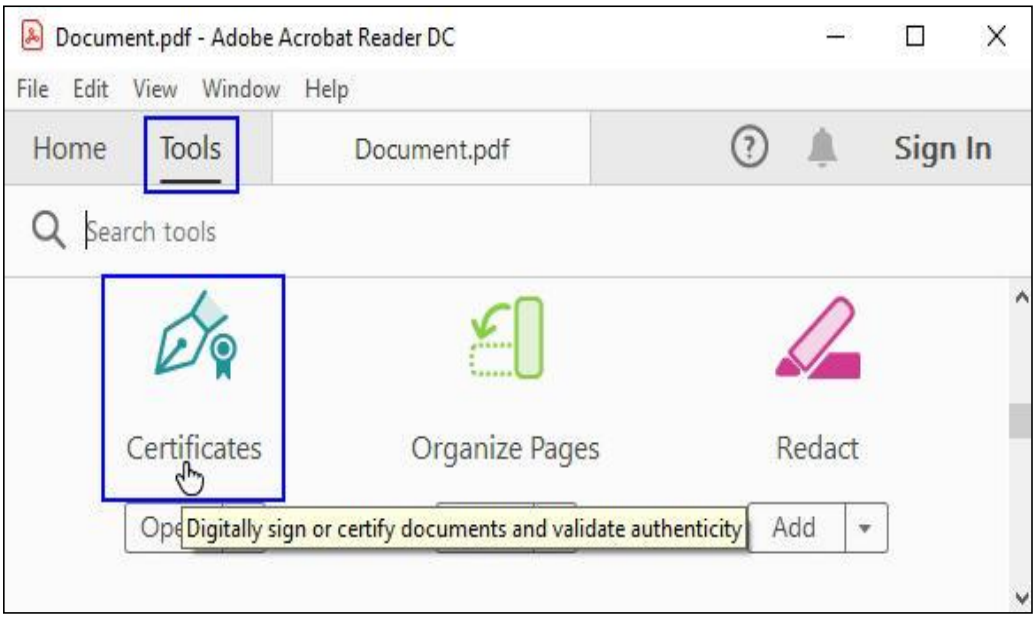
Aplikacija **Adobe Acrobat Reader DC** omogućava:

- Elektronsko potpisivanje PDF dokumenta ( ). Jedan ili više korisnika mogu da elektronski potpišu isti PDF dokument (slika 19).
- Elektronsko potpisivanje i vremensko žigosanje PDF dokumenta ( ).
- Vremensko žigosanje PDF dokumenta ( ).

2. Elektronsko potpisivanje i vremensko žigosanje PDF dokumenta

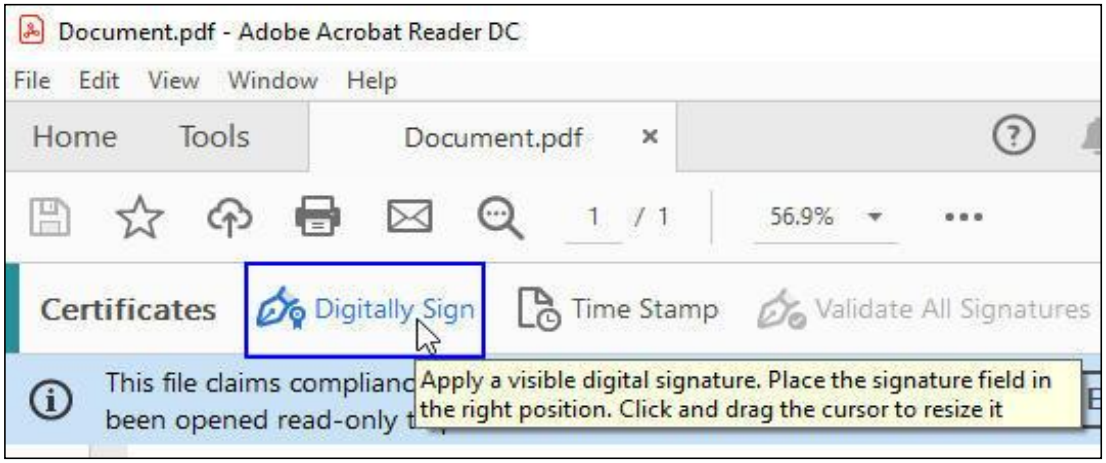
Elektronsko potpisivanje i vremensko žigosanje PDF dokumenta može da se uradi na sledeći način:

- 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).



Slika 5. Izbor panela za rad sa elektronskim sertifikatima

- Na panelu za rad sa sertifikatima se pritisne dugme *Digitally Sign* (slika 6).

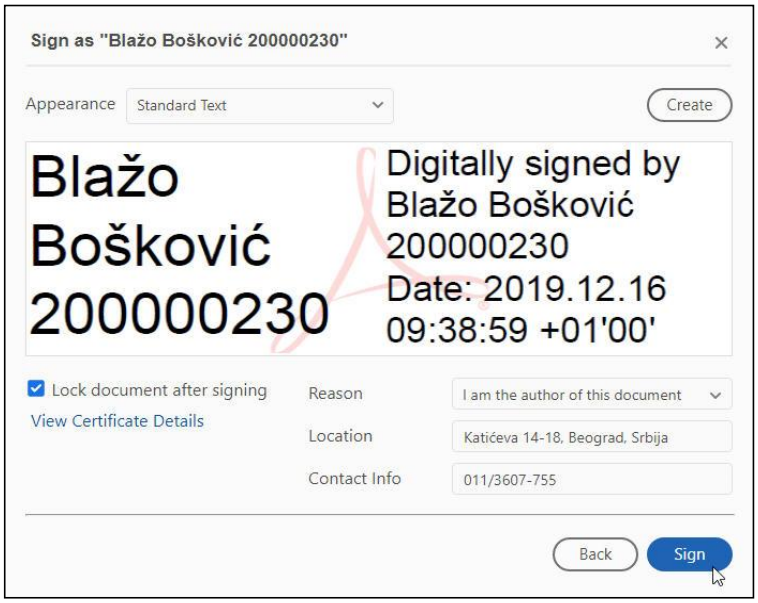


Slika 6. Početak potpisivanja PDF dokumenta

- Na formi *Adobe Acrobat* na kojoj se prikazuje objašnjenje postupka se pritisne dugme *OK*.
- Na željenom mestu u PDF dokumentu se označi 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 može da nacrta liniju.
- Na formi *Sign with a Digital ID* se izabere sertifikat za potpisivanje i pritisne dugme *Continue* (slika 7).

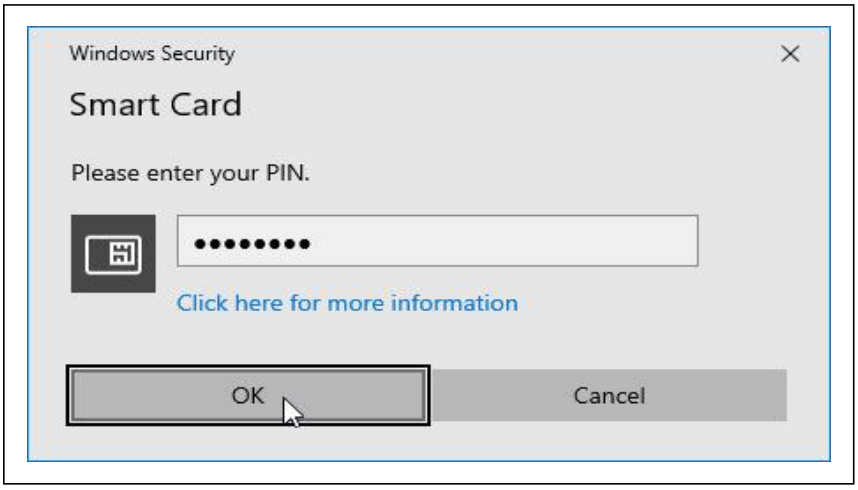
Slika 7. Forma *Sign with a Digital ID*

- Na formi *Sign Document* se izabere sertifikat za potpisivanje i pritisne dugme *Sign* (slika 8).



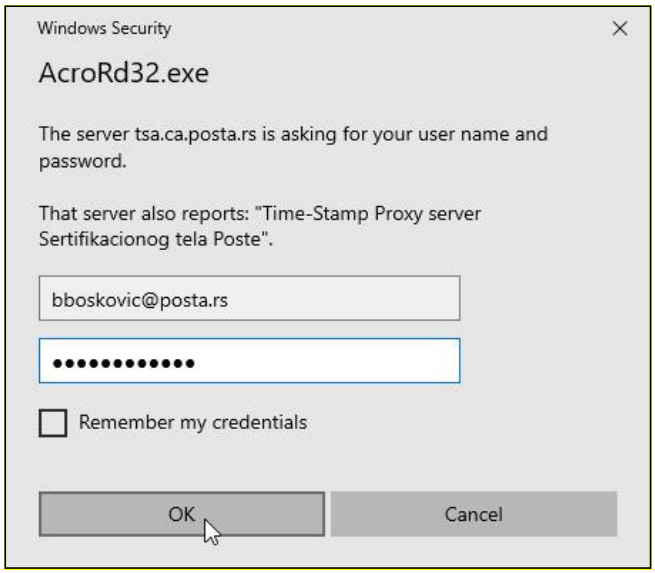
Slika 8. Forma *Sign Document* sa izabranim sertifikatom za potpisivanje

- 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).



Slika 9. Unos lozinke smart kartice/USB tokena

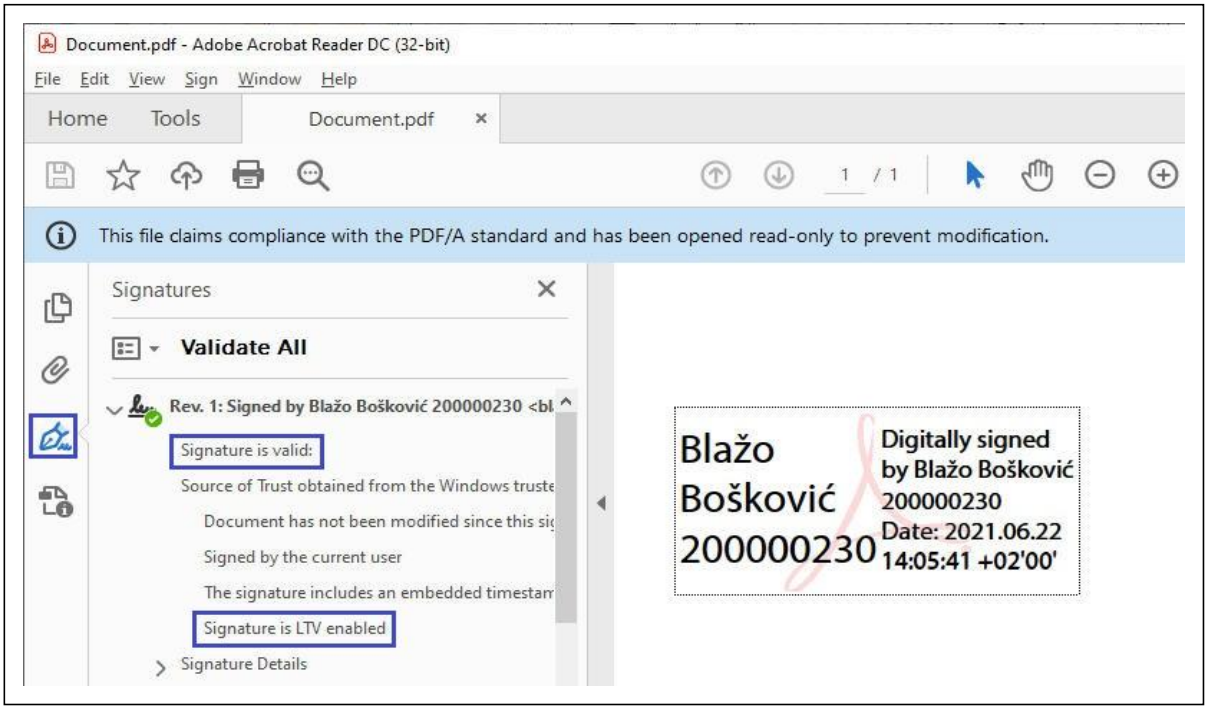
- Prijavljivanje na Timestamp (TSA) server unosom korisničkog imena i lozinke (slika 10). Ova forma će da se pojavi u slučaju da niste uneli korisničko ime i lozinku prilikom podešavanja Timestamp servera.



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

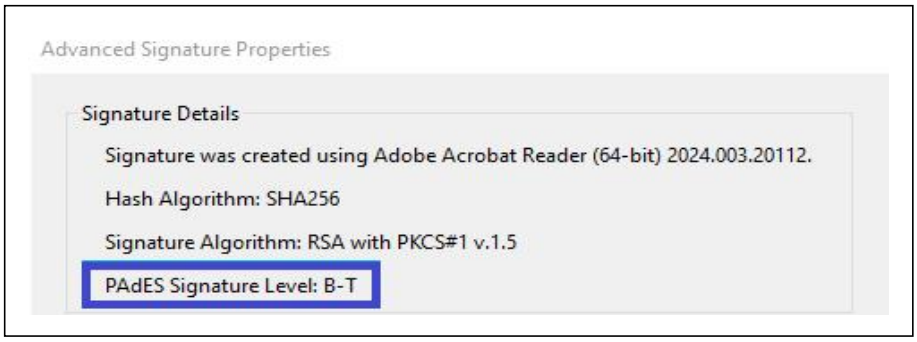
Na ovaj način je završen postupak elektronskog potpisivanja i vremenskog žigosanja PDF dokumenta. U potpisanom PDF dokumentu postoji vizuelni prikaz elektronskog potpisa sa podacima o korisniku koji je izvršio potpisivanje, kao i datum i vreme potpisivanja (slika 11).

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).



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

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…*

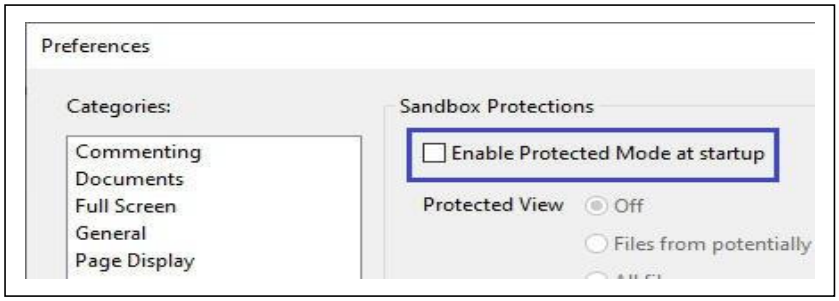


Slika 12. Standard potpisa PAdES baseline signatures

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

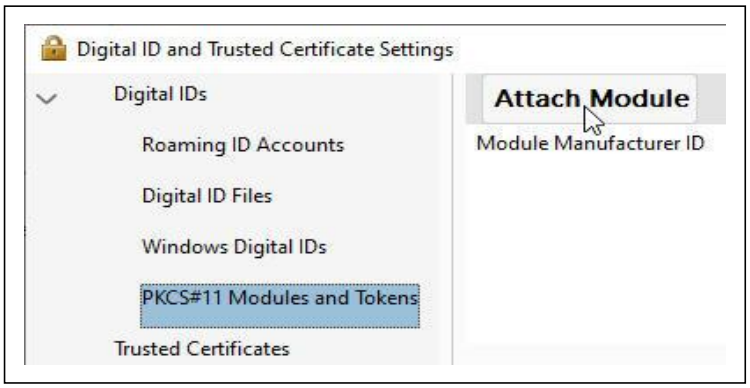
U nekim slučajevima, moguće je da se prilikom pokušaja da se dokument potpiše, iako je Adobe Acrobat Reader DC podešen prema ovom uputstvu, pojavi greška i potpisivanje bude neuspešno. To je posledica promena koje nekada sa ažuriranjem donesu nove verzije Adobe Reader-a. U tom slučaju je moguć drugačiji način korišćenja sertifikata sa smart kartice/USB tokena.

Kako biste podesili Adobe Acrobat Reader DC za potpisivanje dokumenata korišćenjem PKCS#11 interfejsa, 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.



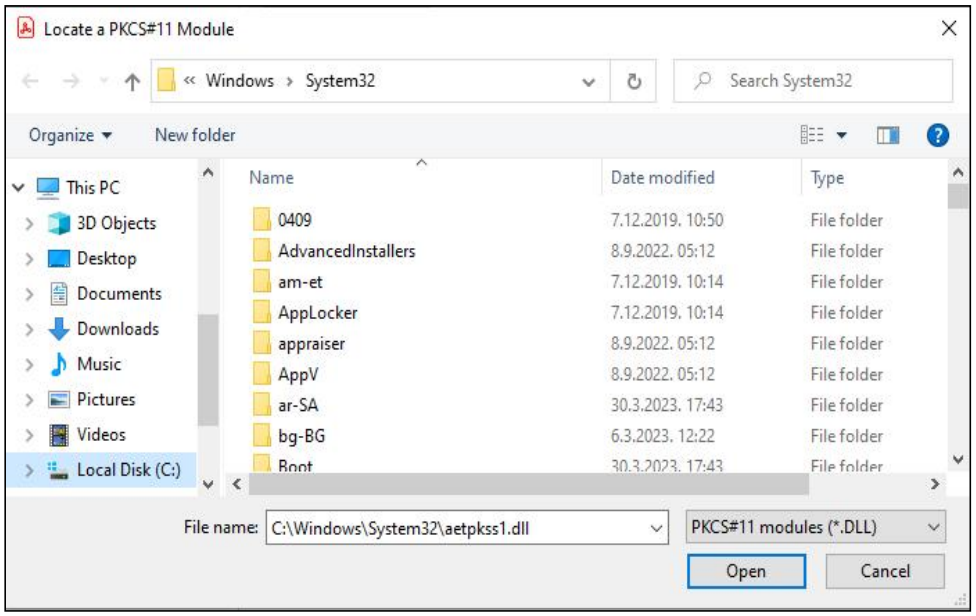
Slika 13. Opcija *Enable Protected Mode at startup*

Zatim je potrebno da se podesi PKCS#11 modul na sledeći način: meni *Edit* → opcija *Preferences...* → kategorija *Signatures* → u sekciji *Identities & Trusted Certificates* pritisnuti dugme *More...*. 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).

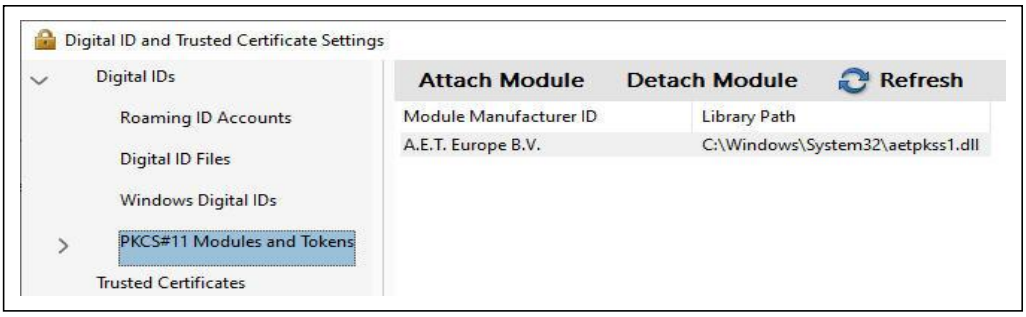


Slika 14. Forma *Digital ID and Trusted Certificate Settings*

Potrebno je da se u polje filename unese putanja PKCS#11 modula, koja je u ovom slučaju **C:\Windows\System32\aetpkss1.dll** kao na slici 15. i pritisne dugme *Open*. U spisku PKCS#11 modula će da se pojavi modul kao na slici 16.

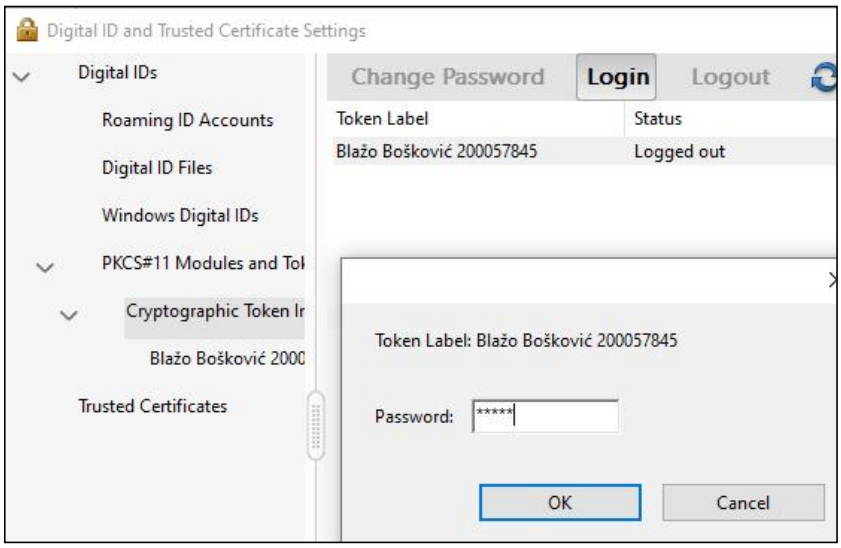


Slika 15. Lokacija PKCS#11 bibiloteke C:\Windows\System32\aetpkss1.dll



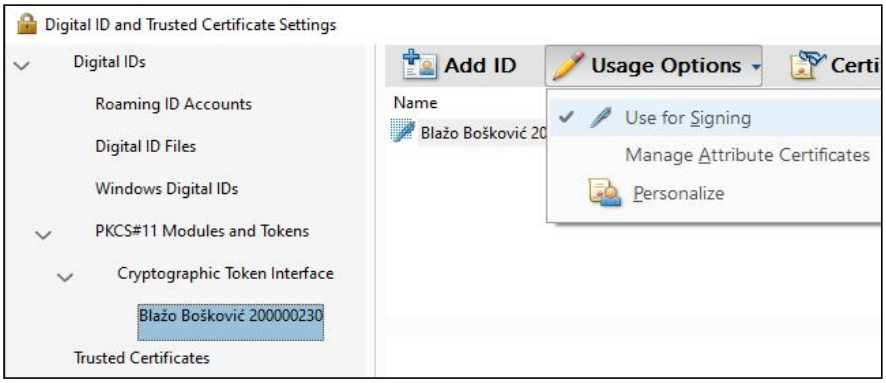
Slika 16. Prikaz dodatog PKCS#11 modula

Potom treba da se otvori meni *Cryptographic Token Interface*, pritisne *Login*, a potom unese lozinka (PIN) kartice/tokena i potvrdi na dugme OK, kao što je prikazano na slici 17.



Slika 17. Prikaz logovanja putem PKCS#11 interfejsa

Kao poslednji korak potrebno je da se izabere 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 18.



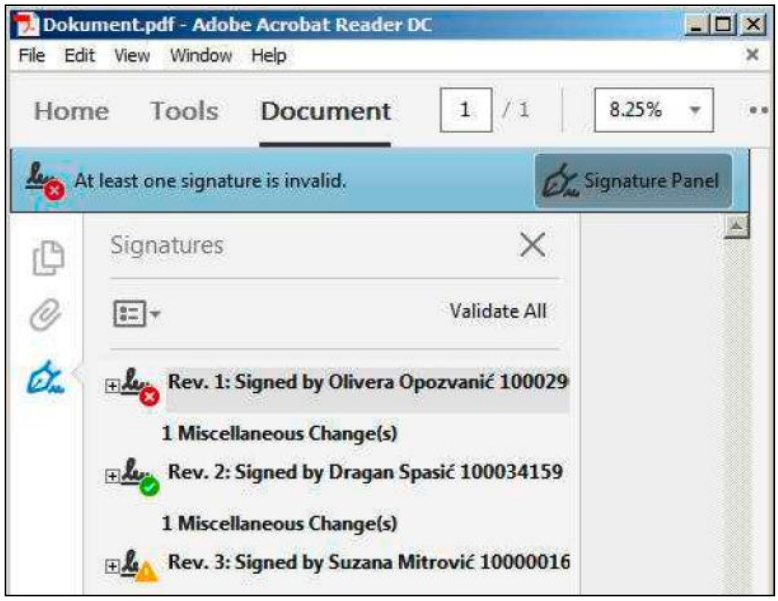
Slika 18. Podešavanje sertifikata za potpisivanje

Na ovaj način je Adobe Reader DC podešen za potpisivanje putem PKCS#11 interfejsa. Razlike kada se potpisivanje obavlja putem PKCS#11 interfejsa u odnosu na korišćenje sertifikata iz Windows skladišta (MSCAPI) su:

1. prilikom izbora sertifikata za potpisivanje u nastavku se prikazuje (PKCS#11 device),
2. PIN kartice/tokena unosi se u Adobe formi 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 19. Forma sa slike 19. je dobijena kao rezultat verifikovanja tri (3) potpisa korišćenjem aplikacije Adobe Acrobat Reader DC.



Slika 19. 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 **Pošta Srbije 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**.

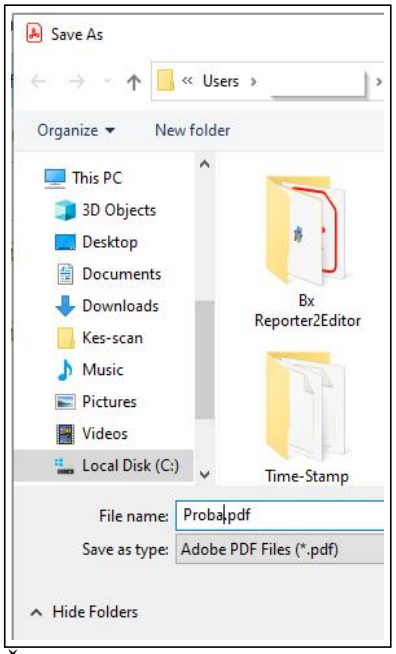
5. Vremensko žigosanje PDF dokumenta

PDF dokumentu je moguće da se, ukoliko postoji potreba, pridruži samo vremenski žig bez obzira na to da li dokument sadrži prethodne potpise i/ili vremenske žigove ili ih ne sadrži. Da biste mogli da dokumentu pridružite vremenski žig, neophodno je da ste prethodno podesili Adobe Reader DC u skladu sa postupkom koji je opisan u poglavlju 1. ovog dokumenta. Prilikom vremenskog žigosanja **neophodan je pristup internetu**. Po završenom podešavanju Adobe Reader DC vremensko žigosanje PDF dokumenta možete da uradite na sledeći način:

- Izabrati *Tools* → *Certificates*. Otvoriće se forma kao na slici 20.

Slika 20. Vremensko žigosanje dokumenta

Posle klika na opciju *Time Stamp* otvoriće se Windows forma *Save As* kao na slici 21. u kojoj je potrebno da izaberete lokaciju na kojoj želite da dokument bude sačuvan, a po potrebi možete i da preimenujete naziv dokumenta.



Slika 21. Čuvanje dokumenta koji će biti žigosan

U zavisnosti od toga kako ste podesili autentifikaciju na Timestamp server može da se pojavi forma za unos korisničkog imena i lozinke ili forma za izbor sertifikata i unos lozinke (PIN). Ukoliko ste korisničko ime i lozinku uneli i sačuvali prilikom podešavanja kao što je prikazano na slici 4. forma za unos ovih podataka se neće pojaviti. U suprotnom pojaviće se forma kao na slici 10. i biće potrebno da unesete korisničko ime i lozinku. Kada je dokument uspešno sačuvan završili ste vremensko žigosanje dokumenta. Da biste proverili da li je dokumentu uspešno pridružen vremenski žig zatvorite i otvorite PDF dokument. Klikom na dugme sa simbolom

olovke, kao na slici 22. pojaviće se prikaz sa detaljima vremenskog žiga. Na slici 23. je prikazan primer neuspešnog vremenskog žiga.

Slika 22. Prikaz uspešnog vremenskog žiga u PDF dokumentu

Slika 23. Prikaz neuspešnog vremenskog žiga u PDF dokumentu