



Naslov dokumenta:	Kvalifikovano elektronsko potpisivanje i vremensko žigosanje PDF dokumenata korišćenjem aplikacije Adobe Reader 11.0.10
Verzija:	1.0
Datum:	9.4.2015.
Autor:	Administratori Sertifikacionog tela Pošte

1. Preduslovi

Aplikacija **Adobe Reader 11.0.07 ili novija** može da se koristi za **kvalifikovano** elektronsko potpisivanje i vremensko žigosanje PDF i PDF/A dokumenata u skladu sa tehničkom specifikacijom **ETSI TS 102 778** (PAdES - PDF Advanced Electronic Signatures) **Part 2** (PAdES Basic - Profile based on ISO 32000-1). Aplikacija Adobe Reader je besplatna, a može da se preuzme sa adrese: <u>http://www.adobe.com</u>.

Da bi moglo da se vrši **kvalifikovano** elektronsko potpisivanje i vremensko žigosanje PDF i PDF/A dokumenata korišćenjem aplikacije Adobe Reader, u skladu sa tehničkom specifikacijom **ETSI TS 102 778 Part 2**, potrebno je da budu ispunjeni sledeći preduslovi:

- 1. Na računaru korisnika mora da bude instalisana aplikacija Adobe Reader 11.0.07 ili novija. Ovaj dokument je napisan za aplikaciju Adobe Reader 11.0.10 na Windows 7 računaru.
- 2. Na računaru korisnika mora da bude podešen **tačan datum, vreme i vremenska (časovna) zona (GMT+01:00)**.
- 3. Korisnik koji vrši potpisivanje mora da poseduje lični (personalni) **KVALIFIKOVANI** elektronski sertifikat i tajni (privatni) kriptografski ključ.
- 4. Neophodno je na formi Creation and Appearance Preferences čekirati opciju 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 → pritisnuti dugme More... u sekciji Creation & Appearance. 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 sertifikat 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 "Posta CA Root" objašnjen je u dokumentu "Preuzimanje i instalisanje sertifikata ROOT CA servera Sertifikacionog tela Pošte u Microsoft Internet Explorer". Osim toga, neophodno je na formi Signature Verification Preferences čekirati dve (2) opcije Windows integracije i uraditi ostala podešavanja, kao što je prikazano na slici 2. Do te forme se dolazi na sledeći način: meni Edit → opcija Preferences... → kategorija Signatures → pritisnuti dugme More... u sekciji Verification.



6. Poželjno/potrebno je, a prema Uputstvu o elektronskom kancelarijskom poslovanju ("Službeni glasnik Republike Srbije", br. 102/2010) neophodno je elektronskom potpisu pridružiti vremenski žig. Pre vremenskog žigosanja neophodno je na formi *New Time Stamp Server* podesiti parametre pristupa Timestamp (TSA) serveru, kao što je prikazano na slici 3. Do te forme se dolazi na sledeći način: meni *Edit* → opcija *Preferences...* → kategorija *Signatures* → pritisnuti dugme *More...* u sekciji *Document Timestamping* → izabrati kategoriju *Time Stamp Servers* → pritisnuti dugme *New*. Posle podešavanja Timestamp servera treba pritisnuti dugme *Set Default*. Osim toga, neophodno je u Windows registru dodati DWORD vrednost "iSize = 0x00002800(10240)", na sledećoj lokaciji: HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\11.0\Security\cASPKI\ cAdobe_TSPProvider (slika 4.). Ako se ne uradi navedeno podešavanje, nije moguće vremenski žigosanja neophodno je imati pristup Internetu.

Postoje dva (2) načina prijavljivanja (autentifikacije) korisnika na Timestamp (TSA) server Sertifikacionog tela Pošte (<u>http://www.ca.posta.rs/vremenski_zigovi.htm</u>):

- Korisničko ime i lozinka (slika 3. i 8.).
- Elektronski sertifikat (slika 3. bez čekirane opcije za podešavanje korisničkog imena i lozinke i slika 9.).

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

Aplikacija Adobe Reader 11.0.07 ili novija omogućava:

- Elektronsko potpisivanje PDF dokumenta (🖾).
- Elektronsko potpisivanje i vremensko žigosanje PDF dokumenta (🗇).
- Vremensko žigosanje PDF dokumenta (🇳).

Jedan ili više korisnika mogu da elektronski potpišu isti PDF dokument (slika 11.).

Aplikacija Adobe Reader ne omogućava sertifikovanje PDF dokumenta (🟦).

reation and Appearance Pre	ferences	
Creation		
Default Signing Method:	Adobe Default Security	Ē
Default Signing Format:	PKCS#7 - Detached	•
When Signing:		
Show reasons		
Show location and	d contact information	
Include signature	s revocation status	
View documents	n Preview Mode	

Slika 1. Čekirane su tri (3) opcije potpisivanja





nati	ure Verification Preferences
⊽ v	erify signatures when the document is opened
T N	When document has valid but untrusted signatures, prompt to review and trust signers
Ver	rification Behavior
W	/hen Verifying:
	C Use the document specified method prompt if up wildble
	Use the document specified method, if unavailable use default method
	se ose the document-specified method; il unavaliable, use deladit method
	C Always use the default method: Adobe Default Security
V	Require certificate revocation checking to succeed whenever possible during signature verification
Г	Ignore document validation information
	 Time at which the signature was created Secure time (timestamp) embedded in the signature Current time Use expired timestamps
Ver	rification Information
A	utomatically add verification information when saving signed PDF:
	Ask when verification information is too big
	C Always
	C Never
_	
-Win	ndows Integration
11	rust ALL root certificates in the Windows Certificate Store for:
	Validating Signatures
	Validating Certified Documents

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 Microsoft Internet Explorer tj. u Windows skladištu ROOT sertifikata.



Slika 3. Podaci o Timestamp serveru

Edit View Favorites Help			
Security	Name	Туре	Data
🗄 🍌 cASPKI	ab (Default)	REG_SZ	(value not set)
CAdobe_LTVProvider	BauthRegd	REG_DWORD	0x00000001 (1)
cAdobe_OCSPRevChecker	L BB bUseExpiredTimestamps	REG_DWORD	0x00000001 (1)
cAdobe_P11CredentialProvider	iSize	REG_DWORD	0x00002800 (10240)
CAdobe_TSPProvider	38 sLockboxId	REG_BINARY	6e 79 54 46 76 71 79 7
CASPKI CMSCAPI_DirectoryProvider	- BURL	REG_BINARY	68 74 74 70 73 3a 2f 2
IN IN			1

Slika 4. U Windows registru je dodata DWORD vrednost "iSize = 0x00002800(10240)"

2. Elektronsko potpisivanje i vremensko žigosanje PDF dokumenta

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

- Startovati aplikaciju Adobe Reader i otvoriti PDF dokument koji treba potpisati.
- Pritisnuti dugme *Fill & Sign*, izabrati opciju *Work with Certificates* i podopciju *Sign with Certificate* (slika 5.).
- Na formi Adobe Reader pritisnuti dugme Drag New Signature Rectangle ...
- Na željenom mestu u PDF dokumentu kreirati pravougaoni okvir u kome će biti prikazani podaci o potpisniku. Okvir se kreira korišćenjem miša. Ako se ne želi vizuelan prikaz elektronskog potpisa u PDF dokumentu, umesto pravougaonog okvira kreirati liniju.
- Na formi Sign Document izabrati sertifikat za potpisivanje i pritisnuti dugme Sign (slika 6.).





- Na formi *Save As* izabrati lokaciju na hard disku računara na kojoj će biti snimljen potpisani PDF dokument i pritisnuti dugme *Save*.
- Uneti lozinku smart kartice/USB tokena i pritisnuti dugme OK (slika 7.).
- U zavisnosti od podešenog načina prijavljivanja na Timestamp (TSA) server, uneti korisničko ime i lozinku (slika 8.) ili izabrati elektronski sertifikat (slika 9.).

Time je elektronsko potpisivanje i vremensko žigosanje PDF dokumenta završeno. U potpisanom PDF dokumentu postoji vizuelni prikaz elektronskog potpisa sa podacima o korisniku koji je izvršio potpisivanje, razlog potpisivanja dokumenta od strane korisnika, lokacija i datum i vreme potpisivanja (slika 10.).

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 10.).



Slika 5. Početak potpisivanja PDF dokumenta

Aplikacija **Adobe Reader ne** omogućava sertifikovanje PDF dokumenta (\Re), s obzirom na to da ocije *Certify (Visible)* i *Certify (Not Visible)* nisu dostupne (slika 5.). Sertifikovanje može da se uradi korišćenjem aplikacije **Adobe Acrobat**.





igan Spasić 10 er: Configurat)0034159 (Con tion, Services,	figuration, Services	i, Public Key Servi	ces, AIA, Posta 💽 🧝
er: Configurat	tion, Services,	Dublis Marchael		
		PUDIIC Key Services	, AIA, Posta CA 1	Info
ļ	Appearance:	Standard Text	•	
1	Digitally signed 100034159 DN: dc=rs, dc=p Nce, ou=Javno 07461429; cn=1 Reason; 1 am th Location: Katici	i by Dragan Spasić posta, dc=ca, ou=Pravno preduzeče Posta Srbije Dragan Spasić 100034159 e author of this document eva 14-18, Beograd, Srbija		
ment After Sig	Ining			
nature Inform	ation			<u>a</u>
n the author o	of this docume	ent		
itićeva 14-18,	Beograd, Srbi	ja		
011/3607-7	55			
	A A A A A A A A A A A A A A A A A A A	Appearance: Digitally signed 100034159 DN: dc=rs, dc=p Nce, ou=Javno 07461429, cm=1 Reason: 1 am th Location: Katice Date: 2015.03.1 ment After Signing nature Information n the author of this docume atićeva 14-18, Beograd, Srbi 011/3607-755	Appearance: Standard Text Digitally signed by Dragan Spasic 100034159 DN: dc=rs, dc=posta, dc=ca, ou=Pravno Ice, ou=Javno preduzece Posta Srbije DV: dc=rs, dc=pragan Spasic 4159 Presson: Fam the author of this document Location: Katteva 14-18, Beograd, Srbija ment After Signing In the author of this document nature Information In the author of this document aticeva 14-18, Beograd, Srbija In the author of this document Inthe author of this document In the author of this document Inthe author of this document In the author of this document Inthe author of this document In the author of this document Inthe author of this document In the author of this document Inticeva 14-18, Beograd, Srbija Inticeva 14-18, Beograd, Srbija Inthe author of this document Inticeva 14-18, Beograd, Srbija Inthe author of this document Inticeva 14-18, Beograd, Srbija Inthe author of this document Inticeva 14-18, Beograd, Srbija Inthe author of this document Inticeva 14-18, Beograd, Srbija Inticeva 14-18, Beograd, Srbija Inticeva 14-18, Beograd, Srbija Inticeva 14-18, Beograd, Srbija Inticeva 14-18, Beograd, Srbija Inticeva 14-18, Beograd, Sr	Appearance: Standard Text Image: Digitally signed by Dragan Spask 100034159 Image: Digitally signed by Dragan Spask 100034159 Image: Divide rs, dc=posta, dc=ca, ou=Pravno Rce, ou=Javno preduzece Posta Srbije 07461429; cn=Dragan Spask 100034159 Image: Divide rs, dc=posta, dc=ca, ou=Pravno Rce, ou=Javno preduzece Posta Srbije 07461429; cn=Dragan Spask 100034159 4159 Divide rs, dc=posta, dc=ca, ou=Pravno Rce, ou=Javno preduzece Posta Srbije 07461429; cn=Dragan Spask 100034159 ment After Signing Image: Divide rs, dc=ca, ou=Pravno This document Location: Katiceva 14-18, Beograd, Srbija Date: 2015.03.11 10:29:56 +01'00 nature Information Image: Divide rs, dc=ca, ou=Pravno This document After Signing nature Information Image: Divide rs, dc=ca, ou=Pravno This document Divide rs, dc=ca, ou=Pravno This dc=ca, o

Slika 6. Forma Sign Document sa izabranim sertifikatom za potpisivanje

o log in to "Dragan S	Spasić"
inter PIN: ******	**
🗸 Minimum PIN leng	th 4 bytes
🖌 Maximum PIN len	gth 15 bytes
OK	Cancel

Slika 7. Unos lozinke smart kartice/USB tokena

Strana 6 od 8



JP "Pošta Srbije" Sertifikaciono telo Pošte





Slika 8. Unos korisničkog imena i lozinke za pristup Timestamp (TSA) serveru

aberite elektr	onski sertifikat za pristup TSA serveru.
	Dragan Spasić 100038133 Issuer: Posta CA 1 Valid From: 04/03/2015 to 04/03/2020
	Dragan Spasić 100034159' Issuer: Posta CA 1 Valid From: 12/08/2014 to 12/08/2019 <u>Click here to view certificate properties</u>

Slika 9. Izbor elektronskog sertifikata za pristup Timestamp (TSA) serveru



Slika 10. Potpisan PDF dokument i forma Signatures sa podacima o elektronskom potpisu



3. Razlozi zbog kojih elektronski potpis PDF dokumenta nije ispravan

Ako je elektronski potpis PDF dokumenta **neispravan** (INVALID) ili je status potpisa **nepoznat** (UNKNOWN), Adobe Reader će na formi *Signatures* takvom potpisu dodeliti ikonicu crvenog krsta (***), odnosno, ikonicu žutog trougla (****), kao što je prikazano na slici 11. Forma sa slike 11. je dobijena kao rezultat verifikovanja tri (3) potpisa korišćenjem aplikacije Adobe Reader 11.0.10.



Slika 11. Statusi elektronskih potpisa tri potpisnika (INVALID, VALID i UNKNOWN)

Razlozi zbog kojih je elektronski potpis PDF dokumenta neispravan (🐄) su:

- 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 (🖾) su:

- Ne može da se proveri identitet sertifikata kojim je izvršeno elektronsko potpisivanje. Predlog za rešenje problema: Instalisati sertifikat "**Posta CA Root**" u skladište sertifikata Microsoft Internet Explorer-a i čekirati **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 omogućiti pristup ka OCSP i CRL serverima Sertifikacionog tela Pošte. Referentni dokumenti: "Proveravanje opozvanosti elektronskih sertifikata korišćenjem OCSP servisa Sertifikacionog tela Pošte" i "Omogućavanje pristupa CRL serverima Sertifikacionog tela Pošte iz računarske mreže korisnika sertifikata".
- 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 proveriti da li je podešen **tačan datum, vreme i vremenska (časovna) zona (GMT+01:00)**.

Strana 8 od 8