ELEKTRONSKO POTPISIVANJE DOKUMENATA KOJI SE PRIDRUŽUJU ELEKTRONSKIM FINANSIJSKIM IZVEŠTAJIMA

Dragan Spasić
Javno preduzeće "Pošta Srbije", dspasic@ptt.rs

Sadržaj: *Agencija za privredne registre je u skladu sa Zakonom o računovodstvu ("Službeni glasnik RS", br. 62/2013) početkom 2015. godine uspostavila Poseban informacioni sistem za sastavljanje i dostavljanje finansijskih izveštaja. Finansijski izveštaj je elektronski dokument potpisan kvalifikovanim elektronskim potpisom zakonskog zastupnika. Uz finansijski izveštaj se prilaže odgovarajuća dokumentacija koja je u formi PDF dokumenata koji moraju da budu kvalifikovano elektronski potpisani. Dostavljanje finansijskog izveštaja i dokumentacije Agenciji za privredne registre vrši se elektronski, preko Posebnog informacionog sistema. U radu će biti objašnjen način kvalifikovanog elektronskog potpisivanja PDF dokumenta koji treba pridružiti elektronskom finansijskom izveštaju pre dostavljanja Agenciji za privredne registre. Za objašnjenje elektronskog potpisivanja biće korišćena besplatna aplikacija Adobe Reader DC (Document Cloud), uz primenu elektronskih sertifikata i vremenskih žigova koje izdaje Sertifikaciono telo Pošte.*

Ključne reči: *PDF dokument, elektronski potpis, elektronski sertifikat, vremenski žig, Adobe Reader.*

1. Uvod

Zakonom o računovodstvu [1] je propisano da su pravna lica, odnosno preduzetnici dužni da redovne godišnje finansijske izveštaje za izveštajnu godinu dostave Agenciji za privredne registre (APR), radi javnog objavljivanja, najkasnije do 30. juna naredne godine. Finansijski izveštaji moraju da budu potpisani kvalifikovanim elektronskim potpisom [2] zakonskog zastupnika, a unose se u Poseban informacioni sistem Agencije i dostavljaju Agenciji u elektronskom obliku.

Agencija za privredne registre (APR) je od 2. marta 2015. godine omogućila pristup Posebnom informacionom sistemu Agencije za sastavljanje i dostavljanje finansijskih izveštaja za 2014. godinu [3]. Sastavljanje i dostavljanje finansijskih izveštaja vrši se u skladu sa Tehničkim uputstvom Agencije [4].

Dokumentacija koja se prilaže uz finansijske izveštaje mora da se pripremi i kvalifikovano elektronski potpiše nezavisno od Posebnog informacionog sistema Agencije. U Poseban informacioni sistem Agencije se pripremljeni PDF dokumenti samo prilažu preko odgovarajuće Web forme (slika 1.). Potpisnik zavisi od vrste dokumenta

koji se potpisuje: izveštaj revizora treba da kvalifikovano elektronski potpiše ključni revizorski partner, odluke potpisuje predsednik skupštine ili drugog nadležnog organa upravljanja, napomene uz finansijski izveštaj potpisuje zakonski zastupnik itd.

Slika 1. *Web forma za pridruživanje PDF dokumenta finansijskom izveštaju*

Za elektronsko potpisivanje i vremensko žigosanje PDF dokumenata mogu da se koriste komercijalne i besplatne aplikacije. Besplatne aplikacije koje mogu da se koriste za elektronsko potpisivanje i vremensko žigosanje PDF dokumenata su Adobe Reader 11.0.07 ili noviji [5, 6], JSignPdf [7], XolidoSign i druge. U nastavku rada je objašnjeno elektronsko potpisivanje i vremensko žigosanje PDF dokumenata korišćenjem besplatne aplikacije Adobe Reader DC (Document Cloud). Po Zakonu o računovodstvu [1] i Tehničkom uputstvu Agencije [4] vremensko žigosanje nije obavezno.

2. Preduslovi za Adobe Reader elektronsko potpisivanje i vremensko žigosanje

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 tehničkom specifikacijom ETSI TS 102 778 Part 2 - PAdES [8]. Aplikacija Adobe Reader DC je besplatna, a može da se preuzme sa 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 Reader DC, 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 DC. Ovaj rad je napisan za aplikaciju Adobe Reader DC 2015.007.20033 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 na smart kartici ili USB tokenu i na računaru korisnika mora da bude podešeno korišćenje kvalifikovanog elektronskog sertifikata prema dokumentu "Instalisanje klijentskog softvera A.E.T. SafeSign i korišćenje smart kartica i USB tokena - sažeto uputstvo" [9].
4. Neophodno je u aplikaciji Adobe Reader DC podesiti ugrađivanje OSCP (Online Certificate Status Protocol) odgovora i/ili registra opozvanih sertifikata (Certificate Revocation List - CRL) u potpisan PDF dokument (slika 2.), 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" [10]. Osim toga, neophodno je podesiti Windows integraciju ROOT CA sertifikata u aplikaciji Adobe Reader DC (slika 3.).
6. Iako se po Zakonu o računovodstvu [1] vremensko žigosanje ne zahteva, poželjno je elektronskom potpisu pridružiti vremenski žig. Pre vremenskog žigosanja neophodno je u aplikaciji Adobe Reader DC podesiti parametre pristupa Timestamp (TSA) serveru (slika 4.). Osim toga, neophodno je u Windows registru dodati DWORD vrednost "iSize = 0x00002800(10240)", na sledećoj lokaciji: HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\Security\cASPKI\cAdobe_TSPProvider (slika 5.). Ako se ne uradi navedeno podešavanje, nije moguće vremenski žigosati PDF dokument (poruka o grešci: SigValue is X bytes larger then expected). Prilikom vremenskog žigosanja neophodno je imati pristup Internetu.

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

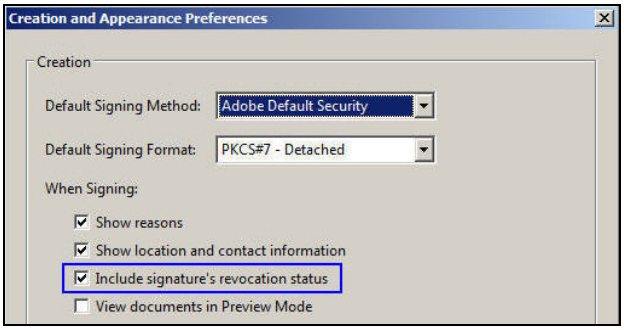
- Korisničko ime i lozinka.
- Elektronski sertifikat.

Anonimno prijavljivanje korisnika na Timestamp (TSA) server Pošte nije dozvoljeno. Pošta pruža mogućnost korisnicima da za potrebe testiranja vremenskog žigosanja koriste testni TSA server Pošte (http://test-tsa.ca.posta.rs).

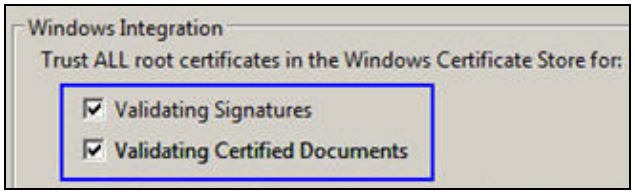
Aplikacija Adobe Reader DC omogućava:

- Elektronsko potpisivanje PDF dokumenta.
- Elektronsko potpisivanje i vremensko žigosanje PDF dokumenta.
- Vremensko žigosanje PDF dokumenta.

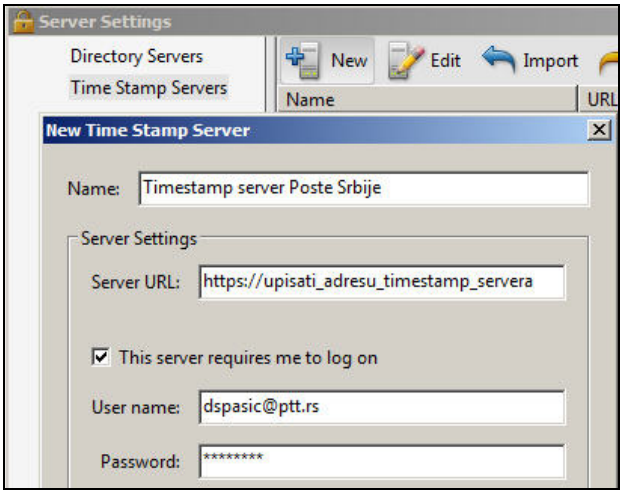
Jedan ili više korisnika mogu da elektronski potpišu isti PDF dokument (slika 8.). Aplikacija Adobe Reader DC ne omogućava sertifikovanje PDF dokumenta.



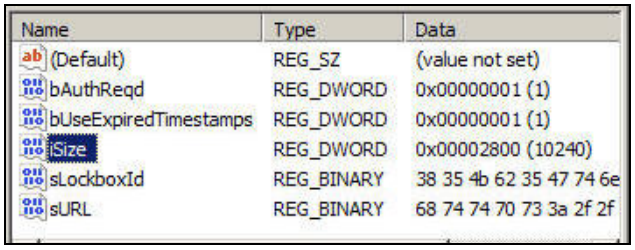
Slika 2. *Podešeno je ugrađivanje OCSP/CRL*



Slika 3. *Podešena je Windows integracija ROOT CA sertifikata*



Slika 4. *Podešeni su podaci o Timestamp serveru*



Slika 5. *Dodata je vrednost "iSize = 0x00002800(10240)" u Windows registru*

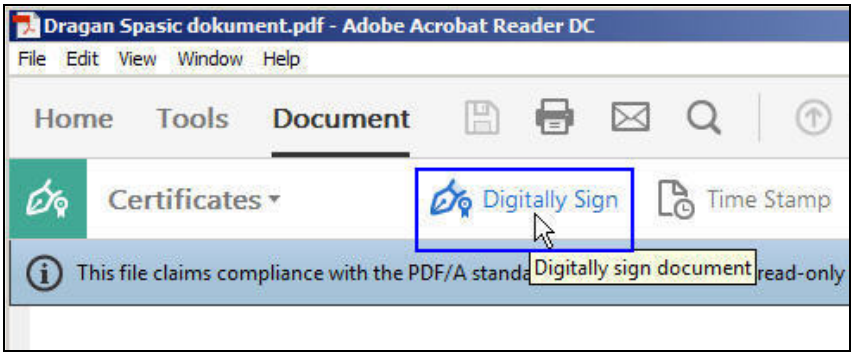
3. Adobe Reader elektronsko potpisivanje i vremensko žigosanje

Elektronsko potpisivanje i vremensko žigosanje PDF dokumenta korišćenjem aplikacije Adobe Reader DC izvršava se na sledeći način [6]:

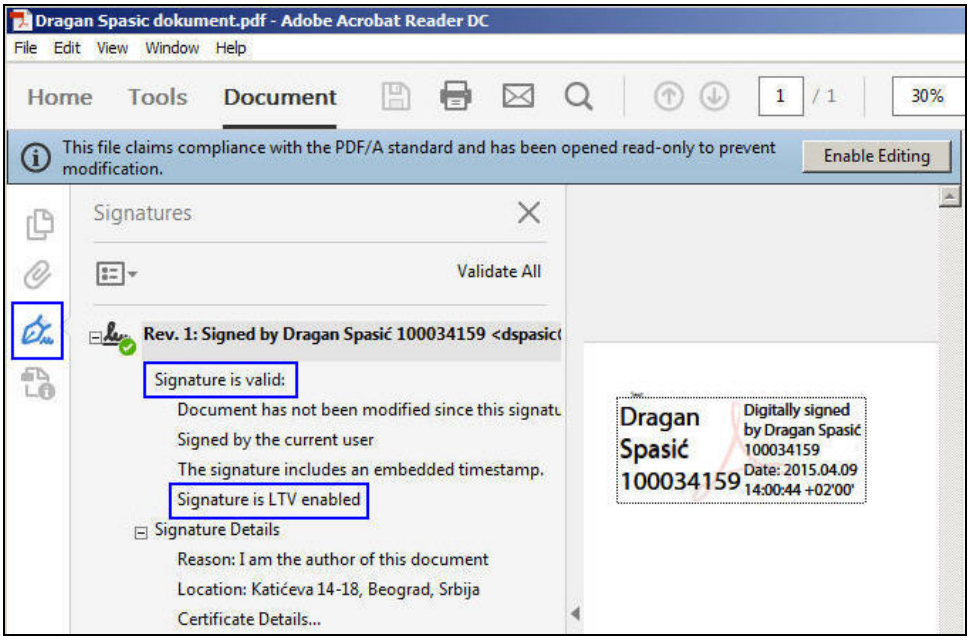
- Startovati aplikaciju Adobe Reader DC i otvoriti PDF dokument koji treba potpisati.
- Pritisnuti dugme *Tools*, pa izabrati opciju *Certificates*.
- Na panelu za rad sa sertifikatima pritisnuti dugme *Digitally Sign* (slika 6.).
- Na formi *Acrobat Reader* pritisnuti dugme *OK*.
- Na željenom mestu 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*.
- 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*.
- U zavisnosti od podešenog načina prijavljivanja na Timestamp (TSA) server, uneti korisničko ime i lozinku ili izabrati elektronski sertifikat.

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 i datum i vreme potpisivanja (slika 7.).

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 7.)



Slika 6. *Početak potpisivanja PDF dokumenta*



Slika 7. *Potpisan PDF dokument i forma Signatures sa podacima o elektronskom potpisu*

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 DC će na formi *Signatures* takvom potpisu dodeliti ikonicu crvenog kruga sa belim krstom, odnosno, ikonicu žutog trougla, kao što je prikazano na slici 8. Forma sa slike 8. je dobijena kao rezultat verifikovanja tri (3) potpisa korišćenjem aplikacije Adobe Reader DC.

Razlozi zbog kojih je elektronski potpis PDF dokumenta neispravan su:

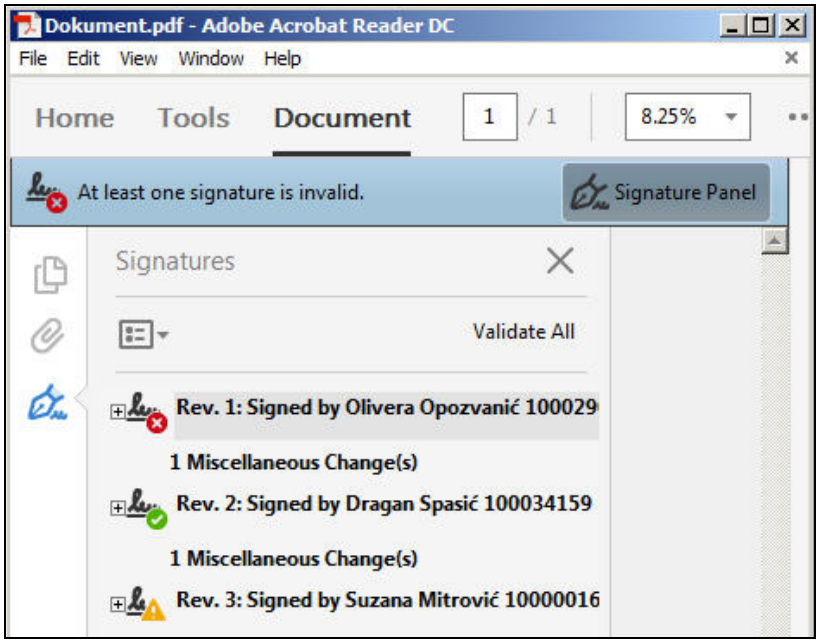
- Sadržaj PDF dokumenta je izmenjen posle potpisivanja (narušen je integritet dokumenta).
- Sertifikat kojim je izvršeno elektronsko potpisivanje je opozvan ili je suspendovan.
- Format elektronskog potpisa je defektan (primer: Error encountered while BER decoding).

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 opcije Windows integracije (slika 3.).
- 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 su: "Proveravanje opozvanosti elektronskih sertifikata korišćenjem OCSP servisa Sertifikacionog tela

Pošte" [11] i "Omogućavanje pristupa CRL serverima Sertifikacionog tela Pošte iz računarske mreže korisnika sertifikata" [12].

- 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).



Slika 8. *Statusi elektronskih potpisa tri potpisnika (invalid, valid i unknown)*

5. Proveravanje opozvanosti elektronskih sertifikata

Sertifikaciono telo Pošte pruža korisnicima informacije o opozvanosti elektronskih sertifikata preko:

- OCSP servisa (Online Certificate Status Protocol) [11]. OCSP servis je aktivan od 1.1.2014. i radi u skladu sa standardima RFC 2560 i RFC 5019.
- Registra opozvanih sertifikata (Certificate Revocation List - CRL) [12].

Proveravanje opozvanosti elektronskih sertifikata korišćenjem OCSP servisa je naprednije u odnosu na konsultovanje registra opozvanih sertifikata (CRL), zato što se veličina CRL-a povećava sa povećanjem broja opozvanih sertifikata, dok je veličina OCSP odgovora fiksne veličine i iznos 3 KB [13, 14].

Da bi klijentska aplikacija mogla da izvrši proveru opozvanosti elektronskog sertifikata preko OCSP protokola, ona mora da zna adresu OCSP servera, koju može da očita na jedan od dva (2) načina:

- Očitavanjem adrese iz polja "Authority Information Access" elektronskog sertifikata čija se opozvanost proverava. Sertifikati koje izdaje Pošta, a koji su izdati posle 1.1.2014. sadrže polje AIA sa adresom OCSP servera.
- Očitavanjem adrese iz polja aplikacije u kome je korisnik aplikacije upisao adresu OCSP servera.

Ako u elektronskom sertifikatu čija se opozvanost proverava postoji polje "Authority Information Access" sa adresom OCSP servera i polje "CRL Distribution Points" sa adresom CRL-a, klijentska aplikacija uvek prvo treba da pokuša da proveri opozvanost sertifikata konsultovanjem OCSP servera, u skladu sa standardom RFC 5019. Ako klijentska aplikacija ne može da proveri opozvanost sertifikata preko OCSP protokola, posle nekoliko neuspešnih pokušaja i/ili posle isteka određenog vremenskog perioda (timeout), klijentska aplikacija treba da pokuša da proveri opozvanost sertifikata konsultovanjem CRL-a.

Aplikacija Adobe Reader DC omogućava da se prilikom elektronskog potpisivanja PDF dokumenta izvrši ugrađivanje OCSP odgovora u elektronski potpis za sertifikat potpisnika. Ugrađivanje OCSP odgovora se vrši bez dodatnih podešavanja ako sertifikat potpisnika sadrži polje "Authority Information Access" u kome je navedena adresa OCSP servera.

Prilikom elektronskog potpisivanja PDF dokumenata korišćenjem aplikacije Adobe Reader DC, primećeno je da se ne vrši ugrađivanje OCSP odgovora u elektronski potpis za sertifikat potpisnika i kada sertifikat potpisnika sadrži polje AIA sa adresom OCSP servera, već se vrši ugrađivanje CRL-a, ako u Adobe CRL kešu na lokalnom računaru postoji CRL koji odgovara sertifikatu potpisnika. Taj problem može da se reši brisanjem sadržaja Adobe CRL keša pre elektronskog potpisivanja. Adobe CRL keš se na Windows 7 računaru nalazi na sledećoj lokaciji: C:\Users\<user>\AppData\Roaming\Adobe\Acrobat\DC\Security\CRLCache.

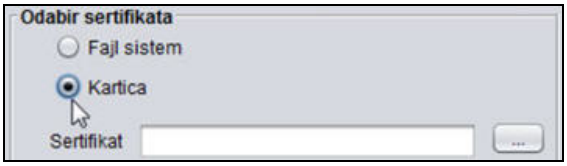
6. Stečena iskustva prilikom rada na Posebnom informacionom sistemu Agencije

Stečena iskustva prilikom rada na Posebnom informacionom sistemu Agencije za privredne registre (APR) sa aspekta korišćenja elektronskih sertifikata su:

- U Tehničkom uputstvu Agencije [4] se navodi: "Ne postoje ograničenja u pogledu operativnog sistema koji koristite na svom računaru.". Prilikom rada, zaključeno je da samo zakonski zastupnici koji su Windows korisnici mogu da elektronski potpišu finansijske izveštaje, dok Linux i MAC OS X korisnici ne mogu.
- Dokumenti koji se prilažu uz finansijske izveštaje (slika 1.) moraju da budu PDF dokumenti i kvalifikovano elektronski potpisani. Pojedini korisnici prave grešku pokušavajući da prilože Word dokumente ili pokušavajući da prilože PDF dokumente koji nisu elektronski potpisani. Ime PDF dokumenta ne treba da bude dugačko.
- U Posebnom informacionom sistemu Agencije, posle pritiska dugmeta "Potpiši dokument" pojavljuje se forma "Digitalno potpisivanje dokumenta", na kojoj treba izabrati opciju "Kartica" (slika 9.), bez obzira da li se sertifikat korisnika nalazi na smart kartici ili USB tokenu. Opciju "Fajl sistem" ne treba izabrati, jer kvalifikovani elektronski sertifikat za kvalifikovani elektronski potpis nikada nije u formi fajla tj. u

formi .PFX datoteke. Korisnici koji imaju sertifikat na USB tokenu, često greše izborom opcije "Fajl sistem".

- Ako se korisniku ne pojavljuje dugme "Potpiši dokument", potrebno je u Web pretraživaču dozvoliti Javu (allow), pod uslovom da je izvršeno Java podešavanje prema Tehničkom uputstvu Agencije [4].
- Da bi elektronski sertifikat sa smart kartice ili USB tokena mogao da se koristi za elektronsko potpisivanje, on mora da se iskopira u skladište sertifikata Microsoft Internet Explorer-a. Ako se to ne dogodi, predloge za rešenje problema pročitati u korisničkom uputstvu "Razlozi zbog kojih se sertifikat korisnika ne kopira sa smart kartice ili USB tokena u skladište sertifikata Microsoft Internet Explorer-a i predlozi za rešenje problema" [15].
- Elektronsko potpisivanje finansijskog izveštaja nije moguće uraditi opozvanim ili suspendovanim elektronskim sertifikatom, što je očekivano. Zapaženo je da neki korisnici pokušavaju elektronsko potpisivanje opozvanim ili suspendovanim elektronskim sertifikatima.
- Ako korisnik ne može da elektronski potpiše finansijski izveštaj, a može sa istog računara da potpiše PDF dokument korišćenjem aplikacije Adobe Reader, pri čemu računar korisnika izlazi na Internet preko proxy servera, treba pokušati potpisivanje finansijskog izveštaja sa računara koji direktno pristupa Internetu.
- Posle elektronskog potpisivanja finansijskog izveštaja, potpisnik tj. zakonski zastupnik ne može da proveri (verifikuje) svoj elektronski potpis, i ne može da pogleda kojim elektronskim sertifikatom je potpisao finansijski izveštaj.



Slika 9. *Izabrana opcija "Kartica" na formi "Digitalno potpisivanje dokumenta"*

Literatura

[1] Zakon o računovodstvu ("Službeni glasnik Republike Srbije", br. 62/2013).
[2] Zakon o elektronskom potpisu ("Službeni glasnik Republike Srbije", br. 135/2004).
[3] Poseban informacioni sistem Agencije za sastavljanje i dostavljanje finansijskih izveštaja: https://aplikacije3.apr.gov.rs/fiexternal.
[4] "Tehničko uputstvo: Aplikacija za sastavljanje i dostavljanje finansijskih izveštaja", Agencija za privredne registre, Beograd, 2015.
[5] D. Spasić, "Kvalifikovano elektronsko potpisivanje i vremensko žigosanje PDF dokumenata korišćenjem aplikacije Adobe Reader 11.0.10", Sertifikaciono telo Pošte, 9.4.2015.
[6] D. Spasić, "Kvalifikovano elektronsko potpisivanje i vremensko žigosanje PDF dokumenata korišćenjem aplikacije Adobe Reader DC", Sertifikaciono telo Pošte, 17.4.2015.

[7] D. Spasić, "Kvalifikovano elektronsko potpisivanje i sertifikovanje PDF dokumenata korišćenjem aplikacije JSignPdf", Sertifikaciono telo Pošte, 25.9.2012.
[8] ETSI TS 102 778-2, V1.2.1 (2009-07), "PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1".
[9] D. Spasić, "Instalisanje klijentskog softvera A.E.T. SafeSign i korišćenje smart kartica i USB tokena - sažeto uputstvo", Sertifikaciono telo Pošte, 12.8.2013.
[10] D. Spasić, "Preuzimanje i instalisanje sertifikata ROOT CA servera Sertifikacionog tela Pošte u Microsoft Internet Explorer", Sertifikaciono telo Pošte, 12.8.2010.
[11] D. Spasić, "Proveravanje opozvanosti elektronskih sertifikata korišćenjem OCSP servisa Sertifikacionog tela Pošte", Sertifikaciono telo Pošte, 15.4.2015.
[12] D. Spasić, "Omogućavanje pristupa CRL serverima Sertifikacionog tela Pošte iz računarske mreže korisnika sertifikata", Sertifikaciono telo Pošte, 23.4.2012.
[13] D. Spasić, "Proveravanje opozvanosti elektronskih sertifikata korišćenjem OCSP servisa", V konferencija o bezbednosti informacija "BISEC 2013", Zbornik radova, str. 70-75, Univerzitet Metropolitan, Beograd, jun 2013.
[14] D. Spasić, "Karakteristike nekih klijentskih aplikacija koje podržavaju proveru opozvanosti sertifikata preko OCSP protokola", XXVIII naučno-stručni skup "Infotech 2013", Zbornik radova (medijum je CD-ROM), JURIT - Asocijacija za računarstvo, informatiku, telekomunikacije, automatizaciju i menadžment Srbije, Aranđelovac, jun 2013.
[15] D. Spasić, "Razlozi zbog kojih se sertifikat korisnika ne kopira sa smart kartice ili USB tokena u skladište sertifikata Microsoft Internet Explorer-a i predlozi za rešenje problema", Sertifikaciono telo Pošte, 17.3.2015.

Abstract: *Serbian Business Registers Agency in accordance with Accounting act ("Official Journal of the Republic of Serbia", no. 62/2013) established a special information system for preparation and submission of financial reports at the beginning of 2015. Financial report is an electronic document signed by legal representative using qualified electronic certificate. Financial report is accompanied by appropriate documentation in PDF format which also has to be signed with qualified electronic certificate. Submission of financial report and documentation to the Business Registers Agency is carried out electronically, through a special information system. This paper will explain the method of qualified electronic signature creation on PDF documents that are accompanying financial report before the submission to the Business Registers Agency. For the explanation of the electronic signature creation free application Adobe Reader DC (Document Cloud) will be used. For the purpose of signature creation, electronic certificates and time-stamps issued by Serbian Post Certification Authority will be used.*

Keywords: *PDF document, electronic signature, electronic certificate, time-stamp, Adobe Reader.*

ELECTRONIC SIGNING OF DOCUMENTS WHICH ARE JOINED TO ELECTRONIC FINANCIAL REPORTS

Dragan Spasić