



Governance Accountability Project
Projekat upravne odgovornosti

PRILOG 1

Procedura kreiranja, potpisivanja, slanja, prijema i provjere digitalnih dokumenata



Kingdom of the Netherlands

PRILOG 1

Procedura kreiranja, potpisivanja, slanja, prijema i provjere digitalnih dokumenata

Mišljenja koja su izražena u ovoj publikaciji predstavljaju isključivo mišljenje autora, i ne moraju nužno odražavati stavove Američke agencije za međunarodni razvoj, Vlade Sjedinjenih Američkih Država, Švedske agencije za međunarodni razvoj i saradnju, Vlade Švedske ili Vlade Kraljevine Holandije.

Procedura kreiranja, potpisivanja, slanja, prijema i provjere digitalnih dokumenata

Izrada dokumenta podrazumijeva direktno kreiranje digitalnog dokumenta u odgovarajućem računarskom programu ili obrada papirne kopije i njenu transformaciju u digitalni oblik (npr. skeniranje).

(član 14.)

1. Izrada dokumenta

1. Izradu dokumenta može vršiti bilo koje lice u organizaciji te ga prosljediti nadležnom licu koje posjeduje certifikat za digitalni potpis na potpisivanje.

Izrada elektronskog dokumenta se vrši standardnim softverskim alatima (npr. MS Word, MS Excel, Adobe Acrobat, AutoCAD, CorelDraw, (...)) ili iz pojedinačnih softverskih aplikacija.

2. Izrađeni elektronski dokument se internom poštom ili na drugi prikladan način u poslovnom sistemu (npr. korištenjem ftp servera) šalje ovlaštenoj osobi da izvrši njegovo digitalno potpisivanje. Ukoliko osoba sa ovlaštenjem elektronskog potpisivanja sama izrađuje elektronski dokument, ovaj korak je suvišan.

(član 14.)

3. Elektronski potpis

Elektronsko potpisivanje elektronskog dokumenta može izvršiti isključivo ovlaštena osoba u poslovnom sistemu (ili više njih) koja posjeduje ranije izdat certifikat za digitalni potpis, izdat od strane nadležne akreditovane institucije ili privatne kompanije (CA). U procesu izdavanja certifikata za digitalni potpis, korisnik dobija javni ključ koji CA distribuiraju svim korisnicima putem interneta, a korisnik dobija i tajni ključ koji je samo njemu dostupan. Tajni ključ se može koristiti u obliku softverske zaštite (lozinke) ili što trenutno predstavlja najveći tehnički nivo zaštite – upotrebom hardverskih dodataka u vidu pametnih (SMART) kartica i čitača, USB tokena ili vremenskih token uređaja.

Proces digitalnog potpisivanja zahtjeva od potpisnika da koristi proceduru koja se razlikuje između različitih vrsta i verzija programa, ali koja je u osnovi slična i bazira se na sljedećem principu:

- na korisničkom računaru se nalazi instaliran digitalni certifikat;
- prolaskom kroz softversku proceduru, korisnik aktivira svoj hardverski uređaj (npr. SMART karticu u čitač) te nakon dodatne identifikacije korištenjem PIN-a i/ili korisničke lozinke, vrši digitalno potpisivanje.

Nakon digitalnog potpisivanja elektronskog dokumenta, nemoguća je izmjena njegovog sadržaja. U slučaju potrebe, prije slanja primaocu, moguće je isključiti već načinjeni potpis, napraviti potrebne izmjene u sadržaju dokumenta, te ga treba ponovo digitalno potpisati (prethodni digitalni potpis je poništen). Novi elektronski potpis u sebi sadrži novi datum potpisivanja.

Elektronski potpis ima ograničeni rok trajanja - najčešće jednu godinu i potrebno ga je produživati.

(član 15.)

4. Slanje ili štampanje elektronski potpisanog dokumenta

Nakon digitalnog potpisivanja, potpisnik prosljeđuje elektronski dokument primaoca, različitim sredstvima elektronske komunikacije, najčešće elektronskom poštom (za pojedinačne dokumente) ili korištenjem zajedničkih IS (korištenjem zajedničkih aplikacija i baza podataka, kao što su, npr. bankarski sistem, sistem javnih nabavki, porezne prijave, ...).

Dokument se smatra poslanim kada napusti (izađe) IS pošiljaoca, što znači da je (u slučaju elektronske pošte) e-mail poruku preuzeo ISP. U slučaju korištenja zajedničkih IS, dokument se smatra poslanim kada se pojavi u IS-u primaoca.

Pošiljalac potvrdu o slanju elektronskog dokumenta (izlaz iz svog IS-a) čuva kao dokaz slanja elektronskog dokumenta.

Slanje digitalno potpisanog digitalnog dokumenta se vrši e-mailom, slanjem na FTP server, prenosom putem CD/DVD, flash memorije, hard diska ili na drugi način, te korištenjem zajedničkog IS.

Digitalno potpisani elektronski dokument je moguće i prenijeti na papir (štampanje) pri čemu on ima odgovarajuću oznaku na osnovu koje je kasnije moguće izvršiti njegovu provjeru.

(član 16.)

5. Prijem elektronskog dokumenta

Primalac elektronskog dokumenta vrši njegov prijem sredstvima elektronske komunikacije. Elektronski dokument se smatra primljenim kada uđe u IS primaoca, što u slučaju prijema e-maila znači da je od strane ISP-a primaoca isporučen na

njegovu e-mail adresu, a u slučaju korištenja zajedničkog IS-a, da se elektronski dokument pojavio u njegovom sistemu (aplikacija i baza podataka).

(član 16.)

Potvrda prijema elektronskog dokumenta

U određenim slučajevima moguće je dogovoriti međusobnu obaveznu potvrdu prijema elektronskog dokumenta koja se vrši istim elektronskim sredstvima komunikacije kao i njegovo slanje. U slučaju da primalac ne potvrdi prijem elektronskog dokumenta, pošiljalac obavještava primaoca da nije dobio potvrdu prijema. Ukoliko potvrda prijema i nakon ovog upozorenja izostane, smatra se da elektronski dokument nije ni poslan.

U slučaju korištenja elektronske pošte, potrebno je aktivirati opciju automatskog izvještavanja o isporuci e-maila; U slučaju korištenja zajedničkog IS-a, potrebno je izvršiti preuzimanje (download) podataka iz sistema primaoca nakon njegove obrade (npr. potvrda o uplati, potvrda o kreiranju javne nabavke, ...).

Potvrda o prijemu elektronskog dokumenta može da služi kao dostavnica – dokaznica o njegovom prijemu u upravnom postupku.

(član 19.)

Arhiva

Nakon slanja elektronskog dokumenta primaocu, pošiljac zadržava njegovu kopiju u digitalnoj arhivi IS-a svog poslovnog sistema. U digitalnoj arhivi se čuvaju i potvrde o slanju elektronskog dokumenta, te potvrde o njegovom prijemu od strane primaoca elektronskog dokumenta.

Arhiva elektronskih dokumenata se može vršiti:

- na pojedinačnim računarima na kojima se vrši izrada, digitalno potpisivanje, slanje elektronskog dokumenta ili prijem elektronskog dokumenta, ili
- centralizirano na FTP servere ili drugi oblik koji zavisi od informacionog sistema

Način arhiviranja digitalnih dokumenata treba internim pravilnikom propisati svaki poslovni sistem.

6. Provjera elektronskog potpisa

Međusobnom razmjenom javnih ključeva digitalnog potpisa koju objavljuju CA, svaki korisnik, nakon njihove instalacije na svoj računar, može da izvrši provjeru ispravnosti elektronskog potpisa na primljenom elektronskom dokumentu.

DIJAGRAM TOKA KORIŠTENJA ELEKTRONSKOG DOKUMENTA

