NN 60/2019 (19.6.2019.), Pravilnik o pružanju i korištenju usluga povjerenja

MINISTARSTVO GOSPODARSTVA, PODUZETNIŠTVA I OBRTA

1150

Na temelju članka. 4., stavka 3. i članka 14. stavka 4. Zakona o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (»Narodne novine«, broj 62/17), ministar gospodarstva, poduzetništva i obrta donosi

PRAVILNIK

O PRUŽANJU I KORIŠTENJU USLUGA POVJERENJA

I. OPĆE ODREDBE

Članak 1.

Ovim Pravilnikom utvrđuju se mjere, postupci i oblici zaštite elektroničkih usluga povjerenja, druge metode identifikacije koje po pitanju pouzdanosti pružaju sigurnost jednaku fizičkoj prisutnosti, a kojima kvalificirani pružatelj usluga povjerenja provjerava identitet potpisnika, preduvjeti i pravila za automatizirano udaljeno elektroničko potpisivanje i pečatiranje, opći i posebni uvjeti poslovanja za pružatelje usluga povjerenja, pravila o privremenoj suspenziji certifikata za elektroničke potpise i certifikata za elektroničke pečate u slučajevima kada certifikat privremeno izgubi svoju valjanost, obvezno osiguranje pružatelja usluga povjerenja.

Članak 2.

(1) U smislu ovog Pravilnika pojmovi imaju sljedeća značenja:

1. *»udaljeni kvalificirani elektronički potpis«* znači kvalificirani elektronički potpis kod kojeg okruženjem za izradu elektroničkog potpisa u ime potpisnika upravlja kvalificirani pružatelj usluga povjerenja pri čemu jamči da se podatak za izradu elektroničkog potpisa, koristi pod isključivom kontrolom potpisnika

2. *»automatizirano kvalificirano udaljeno elektroničko potpisivanje«* znači automatizirani postupak izrade udaljenog kvalificiranog elektroničkog potpisa kojeg u ime potpisnika i uz njegovu prethodnu suglasnost izrađuje automatizirani računalni sustav, a nakon ispunjavanja dodatnih uvjeta određenih ovim Pravilnikom

3. *»udaljeni kvalificirani elektronički pečat«* znači kvalificirani elektronički pečat kod kojeg okruženjem za izradu elektroničkog pečata u ime autora pečata upravlja kvalificirani pružatelj usluga povjerenja pri čemu jamči da se podatak za izradu elektroničkog pečata, koristi pod kontrolom autora pečata

4. *»videoidentifikacija«* znači jednu od »drugih metoda identifikacije« iz članka 24., stavka 1. točke (d) Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (u daljnjem tekstu: Uredba eIDAS), koje po pitanju pouzdanosti pružaju sigurnost jednaku fizičkoj prisutnosti, a kojima kvalificirani pružatelj usluga povjerenja provjerava identitet i ako je to primjenjivo, posebna obilježja fizičke osobe kojoj se izdaje kvalificirani certifikat

5. *»pravna osoba«* znači sudionika obveznog pravnog odnosa koji ima pravnu sposobnost koja je prethodno utvrđena posebnim propisima

6. *»osoba ovlaštena za zastupanje pravne osobe«* znači osobu koja u ime i za račun pravne osobe ili organizacije poduzima i provodi pravne radnje te sklapa pravne poslove

7. *»udaljeno kvalificirano elektroničko potpisivanje«* znači izradu kvalificiranog elektroničkog potpisa podacima za izradu elektroničkog potpisa kojima u ime potpisnika upravlja kvalificirani pružatelj usluga povjerenja sukladno Prilogu II Uredbe eIDAS

8. *»certifikat za automatizirano udaljeno kvalificirano elektroničko potpisivanje«* znači kvalificirani certifikat koji se upotrebljava u automatiziranom udaljenom kvalificiranom elektroničkom potpisivanju

9. *»službenik za registraciju«* – znači osobu odgovornu za potvrđivanje podataka koji su potrebni za izdavanje certifikata te za odobravanje zahtjeva za izdavanje certifikata.

(2) U smislu ovoga Pravilnika ostali pojmovi imaju jednako značenje kao pojmovi korišteni u Uredbi eIDAS.

Članak 3.

(1) Pružatelj usluga povjerenja koji izdaje certifikate ili kvalificirane certifikate primjenjivat će informacijsku tehnologiju i tehnička i programska sredstva čije je djelovanje u skladu s važećim međunarodnim normama, a koje se odnose na:

– opća pravila pružanja usluga certificiranja,

– obrazac (profil) certifikata,

– sigurnost sredstava za izradu elektroničkog potpisa,

– sigurnost sustava certificiranja.

(2) Pružatelj usluga povjerenja koji izdaje elektroničke vremenske žigove ili kvalificirane elektroničke vremenske žigove primjenjivat će informacijsku tehnologiju i tehnička i programska sredstva čije je djelovanje u skladu s važećim međunarodnim normama, a koje se odnose na:

– opća pravila pružanja usluga izdavanja vremenskog žiga,

– obrazac (profil) certifikata za izradu vremenskog žiga,

– sigurnost sustava za izdavanje vremenskog žiga.

II. AUTOMATIZIRANO UDALJENO KVALIFICIRANO ELEKTRONIČKO POTPISIVANJE I ELEKTRONIČKO PEČATIRANJE

Članak 4.

»Automatizirano kvalificirano udaljeno elektroničko potpisivanje« znači automatizirani postupak izrade udaljenog kvalificiranog elektroničkog potpisa kojeg u ime potpisnika i uz njegovu prethodnu suglasnost izrađuje automatizirani računalni sustav, a nakon ispunjavanja dodatnih uvjeta određenih ovim Pravilnikom.

Uvjeti za izdavanje, upravljanje i korištenje kvalificiranih certifikata za izradu udaljenog kvalificiranog automatiziranog elektroničkog potpisa

Članak 5.

Za izdavanje, upravljanje i korištenje kvalificiranog certifikata za automatizirano udaljeno kvalificirano elektroničko potpisivanje moraju biti ispunjeni sljedeći uvjeti:

1. Prije davanja suglasnosti za izdavanje, upravljanje i korištenje kvalificiranog certifikata za automatizirano udaljeno kvalificirano elektroničko potpisivanje, potpisnik mora biti upoznat sa svim uvjetima izdavanja, upravljanja i korištenja istog certifikata.

2. Prije izdavanja certifikata za automatizirano udaljeno kvalificirano elektroničko potpisivanje potpisnik pružatelju usluga povjerenja daje suglasnost za korištenje certifikata i pripadajućih podataka za izradu elektroničkog potpisa u automatiziranom udaljenom kvalificiranom elektroničkom potpisivanju.

2a. Danom suglasnošću potpisnik prihvaća korištenje postupka automatiziranog udaljenog kvalificiranog elektroničkog potpisivanja u kojem se potpisniku ne moraju predočiti podaci prije njihovog potpisivanja.

2b. Potpisnik se ne može pozivati na nemogućnost uvida u podatke prije potpisivanja. Pružatelj usluga povjerenja u svojem pravilniku o postupcima izdavanja certifikata mora jasno navesti obavezu i elemente ove suglasnosti potpisnika.

3. Ako potpisnik izrađuje potpis automatiziranim udaljenim kvalificiranim elektroničkim potpisivanjem, potpisnik može upotrebljavati zasebne podatke za izradu elektroničkog potpisa, koji su različiti od drugih podatka za izradu elektroničkog potpisa koje potpisnik posjeduje.

4. U certifikatu za automatizirano udaljeno kvalificirano elektroničko potpisivanje mora biti posebno naznačeno da se isti koristi samo u postupcima automatiziranog udaljenog kvalificiranog elektroničkog potpisivanja.

4a. Ova se naznaka u certifikatu ostvaruje navođenjem identifikatora pravila certificiranja (Certificate Policy Identifier) kojeg je kvalificirani pružatelj usluga povjerenja dodijelio pravilima certificiranja za certifikat za automatizirano udaljeno kvalificirano elektroničko potpisivanje. Povezanost ovog identifikatora pravila certificiranja i definiranih pravila certificiranja pružatelj usluga povjerenja dokumentira u dokumentu opća pravila pružanja usluga certificiranja odnosno pravilniku o postupcima izdavanja certifikata.

5. Pružatelj usluga povjerenja mora u svakom trenutku omogućiti potpisniku izravnu udaljenu dostavu zahtjeva za opoziv certifikata za automatizirano udaljeno kvalificirano elektroničko potpisivanje.

5a. Dostava zahtjeva za opoziv obavlja se na način kojeg je odredio pružatelj usluga povjerenja, a koji mora biti opisan u pravilniku o postupcima izdavanja certifikata.

5b. Pružatelj usluga povjerenja mora osigurati da se opozivanjem certifikata ujedno zaustavlja korištenje pripadajućih podatka za izradu elektroničkog potpisa u automatiziranom udaljenom kvalificiranom elektroničkom potpisivanju.

5c. Opozivom certifikata nepovratno se uništavaju i pripadajući podaci za izradu elektroničkog potpisa.

6. Pružatelj usluga povjerenja potpisniku kojem je izdan certifikat za automatizirano udaljeno kvalificirano elektroničko potpisivanje mora osigurati uvid u dnevnu evidenciju potpisa izrađenih automatiziranim udaljenim kvalificiranim elektroničkim potpisivanjem.

III. OPĆI UVJETI POSLOVANJA ZA PRUŽATELJE USLUGA POVJERENJA

Opći uvjeti

Članak 6.

Pružatelj usluga povjerenja koji izdaje certifikate ili kvalificirane certifikate može obavljati i usluge izdavanja elektroničkog vremenskog žiga ili elektroničkog kvalificiranog vremenskog žiga ukoliko ispunjava uvjete iz Uredbe eIDAS.

Članak 7.

(1) Pružatelj usluga povjerenja koji izdaje kvalificirane certifikate i pružatelj usluga povjerenja koji izdaje kvalificirani elektronički vremenski žig dužan je osigurati rizik od odgovornosti za štete koje nastanu obavljanjem usluga.

(2) Osiguranje sadržano u stavku 1. ovoga članka predstavlja obvezno osiguranje.

(3) Najniži iznos na koji pružatelj usluga povjerenja iz stavka 1. ovoga članka mora osigurati odgovornost za štete iznosi 2.000.000,00 kuna.

Osoblje

Članak 8.

Zaposlenici zaposleni kod jednog pružatelja usluga povjerenja ne smiju biti u radnom, odnosno poslovnom odnosu s drugim pružateljima usluga povjerenja.

Članak 9.

Kvalificirani pružatelj usluga povjerenja mora imati stalno zaposleno:

– najmanje dva stručnjaka s visokom stručnom spremom tehničkog, prirodoslovno-matematičkog ili informatičkog usmjerenja, specijaliziranih za rad s kriptografskim tehnologijama;

– najmanje tri visokoobrazovana stručnjaka tehničkog usmjerenja za zaštitu računalnih sustava i informacijskih baza te s iskustvom u radu sa sustavima izdavanja, opoziva i održavanja certifikata;

– najmanje jednog visokoobrazovanog pravnika s poznavanjem sustava zaštite osobnih podataka, uporabe i pravne sukladnosti elektroničkog potpisa.

IV. POSEBNI UVJETI POSLOVANJA ZA PRUŽATELJE USLUGA POVJERENJA

Članak 10.

(1) Pružatelj usluga povjerenja koji izdaje certifikate ili kvalificirane certifikate mora prije početka obavljanja usluga utvrditi opća pravila pružanja usluga certificiranja koja potpisnicima i pouzdajućim stranama pružaju dovoljno informacija na temelju kojih mogu odlučiti o prihvaćanju usluga i u kojem opsegu.

(2) Opća pravila iz stavka 1. ovoga članka pružatelj usluga povjerenja ugrađuje u dokument opća pravila pružanja usluga certificiranja.

(3) Pružatelj usluga povjerenja koji izdaje kvalificirane certifikate mora izraditi i pravilnik o postupcima izdavanja certifikata.

Infrastruktura

Članak 11.

(1) Pružatelj usluga povjerenja koji izdaje kvalificirane certifikate mora za obavljanje usluga certificiranja imati poslovni prostor, sukladno relevantnoj važećoj ETSI normizacijskoj dokumentaciji

(2) Pristup prostoru u kojem se provode radnje iz stavka 1. ovoga članka, mogu imati samo ovlaštene osobe i o svakom pristupu prostoru mora se voditi evidencija.

Druge metode identifikacije

Članak 12.

Druge metode identifikacije koje ovaj Pravilnik propisuje provode se temeljem odgovarajućih odredbi Uredbe eIDAS.

Identifikacija fizičkih osoba putem procedure videoidentifikacije

Članak 13.

(1) U slučajevima videoidentifikacije, fizičku osobu moguće je vizualno identificirati putem videoidentifikacije, neovisno o fizičkoj razdvojenosti, budući da osoba koju se identificira i službenik za registraciju mogu ostvariti vizualni kontakt i komuniciraju jedno s drugim putem video prijenosa.

(2) Identifikacija pravnih osoba putem videoidentifikacije nije moguća.

(3) Procedura videoidentifikacije se može primijeniti za identifikaciju fizičke osobe koja je ovlaštena za zastupanje pravne osobe ili predstavnika pravne osobe.

Identifikacija posredstvom službenika za registraciju

Članak 14.

(1) Videoidentifikaciju mogu provoditi samo za to posebno educirani službenici za registraciju koji su ili zaposlenici kvalificiranog pružatelja usluga povjerenja ili treće strane kojoj je kvalificirani pružatelj usluga povjerenja ugovorom povjerio poslove vezano uz videoidentifikaciju.

(2) Daljnje podugovaranje koje bi provela treća strana nije dopušteno.

(3) Minimalni uvjet je da videoidentifikaciju provode službenici za registraciju koji razumiju tehničke zahtjeve i rad opreme kojom se obavlja videoidentifikacija, koji su upoznati sa sigurnosnim obilježjima isprava koji su dopuštene i mogu se vizualno provjeriti u proceduri videoidentifikacije (uključujući i primjenjive metode provjere) zajedno s najčešćim oblicima krivotvorenja te s relevantnim zakonskim i podzakonskim propisima.

(4) Kvalificirani pružatelj usluge povjerenja ili treća strana kojoj je kvalificirani pružatelj usluga povjerenja povjerio poslove vezano uz videoidentifikaciju, koja provodi identifikaciju mora donijeti interne akte, kojima se uređuje i definira provođenje mjera za smanjenje rizika od prijevara i eventualnoga sukoba interesa.

(5) Službenici za registraciju koji provode identifikaciju, se redovito educiraju najmanje jedanput godišnje o:

– mjerama zaštite od prijevara, uključujući učenje na slučajevima ili pokušajima prijevara,

– prihvatljivim ispravama i njihovim sigurnosnim obilježjima i

– eventualnim promjenama u zakonskoj regulativi.

Prostorije

Članak 15.

Tijekom provođenja procedure identifikacije, službenici za registraciju moraju biti u odvojenom prostoru s kontrolom pristupa, a kojem mogu pristupiti samo ovlaštene osobe.

Suglasnost

Članak 16.

(1) Preduvjet za pokretanje procesa videoidentifikacije je suglasnost fizičke osobe za obradu osobnih podataka (uključujući video i audiosnimku, slike sadržaja ekrana i fotografije).

(2) Suglasnost mora biti sukladna zahtjevima regulative vezane uz zaštitu podataka – Uredba EU/2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i Zakon o provedbi Opće uredbe o zaštiti podataka (»Narodne novine«, broj 42/2018).

Tehnički, sigurnosni i organizacijski uvjeti

Članak 17.

(1) Prilikom dodjeljivanja predmeta službenicima za registraciju koje provode identifikaciju, moraju postojati mehanizmi koji će osigurati nasumično dodjeljivanje predmeta, kako bi se izbjegla mogućnost manipulacije.

(2) Tijekom videoidentifikacije ostvaruje se video i zvučni prijenos u realnom vremenu i bez prekida. Video i zvučni prijenos moraju biti zadovoljavajuće kvalitete da osiguraju:

• nesmetanu identifikaciju,

• provjeru sigurnosnih obilježja isprave za identifikaciju i

• da su fotografije i videozapisi dovoljne razlučivosti za neometano provođenje identifikacije.

Sigurnosni zahtjevi koje moraju ispunjavati sredstva za videoidentifikaciju:

• integritet i povjerljivost podataka u prijenosu se osigurava enkripcijom cijelim putem komunikacije (eng. end-to-end),

• Kriptografski protokoli, kriptografski algoritmi i duljine pripadajućih ključeva moraju biti odabrani u skladu s aktualnim stanjem tehnologije i aktualnim preporukama za ostvarivanje sigurne komunikacije u području pružanja kvalificiranih usluga povjerenja

• softverski kod računalnog softvera mora biti zaštićen od neželjenog pristupa i izmjena, primjeri odgovarajućih mjera zaštite su: kontrola pristupa, digitalni potpis, enkripcija i obfuskacija,

• podacima koje računalni softver sprema lokalno mora biti zaštićen integritet te pristup istim mora biti omogućen samo ovlaštenim osobama.

(3) Provedbu sigurnosnih mjera treba periodično testirati i vrednovati (testovi ranjivosti, penetracijski testovi), uz dokumentiranje svih pronađenih ranjivosti i prijetnji, te osigurati provedbu sigurnosnih mjera za njihovo uklanjanje.

(4) Kod implementacije mjera sigurnosti posebno treba uzeti u obzir dostupne tehnologije i razvoj informacijske tehnologije.

Prihvatljive isprave za identifikaciju

Članak 18.

Isprave prihvatljive za videoidentifikaciju moraju sadržavati sigurnosne značajke koje na dostatan način štite od krivotvorenja, te se mogu vizualno identificirati koristeći dostupnu tehnologiju za vizualni prijenos, a ujedno moraju sadržavati i strojno čitljive podatke.

Verifikacija isprave za identifikaciju

Članak 19.

(1) Kako bi se utvrdio identitet osobe koja se identificira na osnovu prihvatljive isprave za identifikaciju, službenik za registraciju koji provodi identifikaciju prvo mora utvrditi da isprava za identifikaciju sadrži potrebna sigurnosna obilježja.

(2) Službenik za registraciju koji provodi identifikaciju:

• mora provjeriti vizualno provjerljiva sigurnosna obilježja isprave za identifikaciju,

• mora provjeriti da isprava za identifikaciju nije oštećena ili krivotvorena, posebno da nije mijenjana fotografija,

• mora provjeriti serijski broj identifikacijske isprave,

• mora tražiti od osobe koja se identificira da nagne svoju ispravu vodoravno ili okomito ispred kamere i tražiti dodatne adekvatne pokrete osobe, te korištenjem snimaka navedenih pokreta, koji se zatim izrežu i uvećaju, mora utvrditi da identifikacijska isprava sadržava sva sigurnosna obilježja i da ne postoje indikacije koje bi ukazivale na manipulaciju,

• može tražiti od osobe koja se identificira da prijeđe prstom preko sigurnosnih elemenata na ispravi ili da prijeđe jednom rukom preko vlastitog lica s ciljem smanjenja rizika od prijevara krivotvorenjem isprave.

(3) Utvrđivanje valjanosti i vjerodostojnosti podataka koji se nalaze na identifikacijskoj ispravi mora se provesti kao dio videoidentifikacijskog procesa i to uključuje provjeru:

• datuma izdavanja i datuma isteka valjanosti isprave, posebno se treba obratiti pozornost da kao datum izdavanja nije upisan neki budući datum,

• razdoblja valjanosti isprave, koji ne smije biti suprotan standardu za takav tip isprave,

• valjanosti pravopisa znamenki, i tipografije.

(4) Neophodan dio procesa videoidentifikacije je i automatsko računanje i provjera kontrolnih znamenki u strojno čitljivoj zoni isprave za identifikaciju te uspoređivanje dobivenih rezultata s podacima koji su vidljivi na ispravi.

Verifikacija osobe koja se identificira

Članak 20.

(1) Struktura procedure identifikacije mora biti nasumično odabrana, osobito redoslijed i tip pitanja koje postavlja službenik za registraciju koji provodi identifikaciju.

(2) Službenik za registraciju koji provodi identifikaciju mora utvrditi da fotografija i osobni opis na identifikacijskoj ispravi koja se koristi odgovaraju osobi koja se identificira.

Fotografija, datum izdavanja i datum rođenja također moraju biti usklađeni.