MINISTARSTVO GOSPODARSTVA, PODUZETNIŠTVA I OBRTA

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.

(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, opće i posebne uvjete 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. „automatizirani kvalificirani udaljeni elektronički potpis“ znači postupak izrade udaljenog kvalificiranog elektroničkog potpisa standardizirane elektroničke dokumentacije kojeg u ime potpisnika automatski inicira računalni sustav nakon ispunjavanja unaprijed postavljenih preduvjeta i prema unaprijed utvrđenim pravilima

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. „video identifikacija“ 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 ELEKTRONIČKO POTPISIVANJE I ELEKTRONIČKO PEČATIRANJE

### *Članak 4.*

Automatizirano udaljeno kvalificirano elektroničko potpisivanje je udaljeno kvalificirano elektroničko potpisivanje koje se provodi automatiziranim postupkom, u kojem se potpis izrađuje autorizacijom potpisnika koji ima isključivu kontrolu nad korištenjem svojim podacima za izradu elektroničkog potpisa, bez svoje pravovremene i stalne prisutnosti.

## 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 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.

1a. Danom suglasnošću potpisnik prihvaća korištenje postupka automatiziranog udaljenog kvalificiranog elektroničkog potpisivanja u kojem se potpisniku ne moraju predočiti podaci prije njihovog potpisivanja.

1b. 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.

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

3. U certifikatu za automatizirano udaljeno kvalificirano elektroničko potpisivanje mora biti posebno naznačeno da se isti može koristiti i u postupcima automatiziranog udaljenog kvalificiranog elektroničkog potpisivanja.

3a. 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.

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

4a. 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.

4b. Pružatelj usluga povjerenja mora osigurati da se opozivanjem certifikata ujedno zaustavlja korištenje pripadajućih podatka za izradu elektroničkog potpisa u automatiziranom udaljenom kvalificiranom elektroničkom potpisivanju.

4c. Opozivom certifikata nepovratno se uništavaju i pripadajući podaci za izradu elektroničkog potpisa.

5. 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 visoko obrazovana 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

### Čanak 12.

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

## Identifikacija fizičkih osoba putem procedure video identifikacije

### Članak 13.

(1) U slučajevima video identifikacije, neovisno o fizičkoj razdvojenosti, fizičku osobu moguće je vizualno identificirati putem video dentifikacije, 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 video identifikacije nije moguća.

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

## Identifikacija od strane službenika za registraciju

### Članak 14.

(1) Video identifikaciju mogu provoditi samo za to posebno educirani službenici za registraciju koji su zaposlenici kvalificiranih pružatelja usluga povjerenja ili treća strana kojoj je kvalificirani pružatelj usluga povjerenja ugovorom povjerio poslove vezano uz video identifikaciju.

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

(3) Minimalni uvjet je da video identifikaciju provode službenici za registraciju koji razumiju tehničke zahtjeve i rad opreme kojom se obavlja video identifikacija, koji su upoznati sa sigurnosnim obilježjima isprava koji su dopuštene i mogu se vizualno provjeriti u proceduri video identifikacije (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 video identifikaciju, 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 video identifikacije je suglasnost fizičke osobe za obradu osobnih podataka (uključujući video i audio snimku, 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 video identifikacije 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 video zapisi dovoljne razlučivosti za neometano provođenje identifikacije.

Sigurnosni zahtjevi koje moraju ispunjavati sredstva za video identifikaciju:

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

• podacima koje aplikacija 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.

## Prihvaćene isprave za identifikaciju

### Članak 18.

Isprave prihvatljive za video identifikaciju 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 video identifikacijskog 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 video identifikacije 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.

(3) Kroz psihološko ispitivanje i opservacije tijekom identifikacijske procedure, službenik za registraciju koji provodi identifikaciju mora utvrditi vjerodostojnost informacija koje se nalaze na identifikacijskoj ispravi, informacija koje je pružila osoba koja se identificira, kao i s iskazanim namjerama osobe.

(4) Službenici za registraciju koji provode identifikaciju moraju biti educirani kako bi mogli bez sumnje utvrditi da osoba koja se identificira, kupuje proizvod vlastitom voljom (rizici uključuju phishing, socijalni inženjering, ponašanje pod pritiskom druge osobe i sl.).

(5) Gdje je primjenjivo, službenik za registraciju koji provodi identifikaciju mora utvrditi da podaci na identifikacijskoj ispravi osobe koja se identificira, odgovaraju podacima koji su već poznati kvalificiranom pružatelju usluga povjerenja ili trećoj strani kojoj su povjereni poslovi video identifikacije i dostupni su službeniku za registraciju koji provodi identifikaciju.

## Prekid procedure video identifikacije

### Članak 21.

(1) Ukoliko proceduru video identifikacije nije moguće provesti u skladu s uvjetima navedenim u ovom Pravilniku – npr. zbog loše rasvjete, loše kvalitete slika ili prijenosa – i/ili nije moguća govorna komunikacija s osobom koja se identificira, procedura se mora prekinuti.

(2) Isto je primjenjivo i u drugim slučajevima odstupanja ili nesigurnosti.

(3) U takvim slučajevima identifikacija se može obaviti drugim metodama iz članka 24. Uredbe eIDAS

## Prikupljanje i čuvanje dokaza

### Članak 22.

(1) Procedura video identifikacije mora biti u cijelosti snimljena i pohranjena od strane kvalificiranog pružatelja usluga povjerenja ili treće strane kojoj su povjereni poslovi video identifikacije, u obliku koji omogućuje provjeru snimke od strane internih auditora ili tijela za ocjenjivanje sukladnosti. Prikupljeni dokumenti i dokazi (logovi sustava, fotografije, slike sadržaja ekrana, video i audio snimke) moraju pokazati sukladnost s Uredbom eIDAS te da su ispunjeni svi zahtjevi za video identifikaciju iz ovog Pravilnika.

(2) Prikupljeni dokumenti i dokazi se moraju čuvati najmanje deset (10) godina.

## Mobilne aplikacije

### Članak 23.

(1) Udaljena identifikacija fizičkih osoba putem mobilnih aplikacija temeljena na prepoznavanju lica i ispravnosti identifikacijskih dokumenata je moguća.

(2) Udaljena identifikacija pravnih osoba putem mobilnih aplikacija temeljena na prepoznavanju lica i ispravnosti identifikacijskih dokumenata nije moguća. Procedura se međutim može primijeniti prilikom identifikacije fizičke osobe koja je ovlaštena za zastupanje pravne osobe, ili predstavnika pravne osobe.

## Suglasnost

### Članak 24.

(1) Preduvjet za nastavak procesa udaljene identifikacije je privola fizičke osobe za obradu osobnih podataka (uključujući video zapis i fotografije).

(2) Privola 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).

## Sigurnosni zahtjevi za mobilne aplikacije

### Članak 25.

(1) Sigurnosni zahtjevi za mobilne aplikacije:

• integritet i povjerljivost podataka 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 aplikacije mora biti zaštićen od neželjenog pristupa i izmjena, primjeri odgovarajućih mjera zaštite su: enkripcija i obfuskacija,

• podaci koje aplikacija sprema lokalno moraju biti zaštićeni enkripcijom,

• ne smiju se spremati PIN-ovi i ostale sigurnosne značajke, koje predstavljaju nešto što samo korisnik zna, uz to treba poduzeti mjere zaštite kod unosa PIN-a u aplikaciju npr. dinamička tipkovnica.

(2) 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.

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

## Prihvaćene isprave za identifikaciju

### Članak 26.

Prihvaćene isprave za identifikaciju su navedene u članku 25. ovoga Pravilnika.

## Verifikacija isprave za identifikaciju

### Članak 27.

(1) Verifikacija isprave za identifikaciju temelji se na provjeri vizualnih sigurnosnih obilježja identifikacijske isprave navedenim u članku 26. ovoga Pravilnika.

(2) Utvrđivanje valjanosti i vjerodostojnosti podataka koji se nalaze na identifikacijskoj ispravi mora se provesti kao dio identifikacijskog 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 ortografije znamenki, autorizacijskog koda i tipografije, ukoliko je primjenjivo.

(3) Automatsko računanje kontrolnih znamenki u strojno čitljivoj zoni te uspoređivanje dobivenih rezultata s podacima koji se nalaza na ispravi je neophodan dio procesa identifikacije.

## Verifikacija osobe koja se identificira

### Članak 28.

(1) Verifikacija osobe koja se identificira se temelji na metodi računalnog prepoznavanja lica uz usporedbu s fotografijom iz identifikacijske isprave.

(2) Tijekom provođenja računalnog prepoznavanja lica, od korisnika se zahtjeva da napravi snimke lica kamerom potrebne za usporedbu, te napravi pokrete lica (npr. zatvori oči, nasmiješi se – pokaže zube), kako bi se utvrdilo da je ispred kamere živa osoba.

(3) Prije i tijekom procesa računalnog prepoznavanja lica, korisniku se daju detaljne upute kako provesti proces, s ciljem postizanja kvalitetnije usporedbe i smanjenja rizika od prijevara.

(4) Metoda računalnog prepoznavanja lica mora biti napredna biometrijska tehnologija, koja osigurava dvije ključne funkcionalnosti:

• opis lica i

• usporedbu lica.

(5) Opis lica se provodi kroz prikupljanje:

• podataka o geometriji lica uzimajući u obzir ključne dijelove lica oči, nos i usta, i

• dodatnih atributa lica, npr. starost, spol, 3D poza glave, dlake na licu, intenzitet smijeha – prihvatljiva metoda računalnog prepoznavanja lica koristi barem 3 (tri) dodatna atributa lica.

(6) Rezultat opisa lica je identifikator lica, koji mora biti baziran na gore prikupljenim podacima i pridijeljen osobi.

(7) Usporedba lica je usporedba identifikatora lica. Mobilna aplikacija za identifikaciju temeljenu na prepoznavanju lica mora osigurati da se identifikatori lica za usporedbu dobivaju iz različitih izvora, a najmanje iz:

• fotografije iz isprave za identifikaciju i

• snimke lica kamerom.

(8) Metoda računalnog prepoznavanja lica mora biti pouzdana s prihvatljivim postotkom pozitivnih i negativnih pogrešaka u iznosu od najviše 1% od ukupnog broja obavljenih računalnih poznavanja lica.

(9) Ukoliko rezultat računalnog prepoznavanja lica nije uspješan proces se obustavlja.

## Nadzor korištenja i dodatne pozadinske provjere za smanjenje rizika od prijevara

### Članak 29.

(1) Pozadinske provjere vezane uz identifikaciju provode službenici za registraciju koji provode identifikaciju, u najkraćem roku, najkasnije do kraja idućeg radnog dana nakon provedenih procesa identifikacije.

(2) Pozadinske provjere mogu uključivati:

• ako je primjenjivo, usporedbu podataka dobivenih u procesu identifikacije, s podacima koji postoje u sustavu,

• provjeru podataka vezanih uz osobni identifikator (OIB) uvidom u javni registar,

• provjeru identifikacijske isprave kod izdavatelja,

• provjeru adrese prebivališta u RH.

(3) U slučaju sumnji u autentičnost tijekom procesa identifikacije nakon pozadinskih provjera, potvrda identiteta se može obaviti fizičkom prisutnošću fizičke osobe.

(4) Nakon procesa identifikacije i ugovaranja usluga i/ili proizvoda, provodi se aktivni nadzor poslovnog odnosa s potpisnikom s naglaskom na mjere zaštite od prijevara.

## Prekid udaljene identifikacije putem mobilnih aplikacija

### Članak 30.

(1) U slučaju bilo kojeg odstupanja od zahtjeva ovog Pravilnika na identifikaciju putem mobilnih aplikacija ili sumnje na autentičnost kod verifikacije identifikacijske isprave ili osobe, proces se prekida. Proces se prekida i ako osoba ne da privolu za obradu osobnih podataka.

(2) U takvim slučajevima identifikacija se može obaviti i drugim dopuštenim procedurama, sukladno članku 24. Uredbe eIDAS.

## Dokumentacija

### Članak 31.

(1) Tijekom procesa identifikacije i prije ugovaranja usluga i/ili proizvoda, korisniku se prezentiraju sljedeći dokumenti i informacije:

• upute za proces identifikacije,

• opći uvjeti poslovanja,

• informacije o uslugama i/ili proizvodima,

• informacije o uvjetima uporabe i sigurnosnim mjerama,

• ugovori za usluge i/ili proizvode.

(2) Svi dokumenti u elektroničkom obliku šalju se korisniku odmah po završetku procesa identifikacije na adresu elektroničke pošte, koju je korisnik predao u procesu.

## Prikupljanje i čuvanje dokaza

### Članak 32.

(1) Proces udaljene identifikacije putem mobilnih aplikacija mora biti u cijelosti biti dokumentiran, na način koji omogućava internu ili vanjsku reviziju obavljene identifikacije za svakog korisnika.

(2) Prikupljeni dokumenti i dokazi (logovi sustava, fotografije, video zapisi) moraju pokazati da su ispunjeni svi zahtjevi za identifikaciju iz ovog Pravilnika, te sukladnost s ostalom zakonskom regulativom vezanom uz identifikaciju klijenata.

(3) Prikupljeni dokumenti i dokazi se moraju čuvati najmanje deset (10) godina.

## Registar certifikata

### Članak 33.

(1) Podaci iz urednih zahtjeva za izdavanje certifikata upisuju se i arhiviraju se u informacijskom sustavu pružatelja usluga povjerenja.

(2) Sadržaj certifikata upisuje se u Registar (izdanih i opozvanih) certifikata pružatelja usluga povjerenja.

## Postupci opoziva certifikata

### Članak 34.

(1) Opoziv je trajan prestanak važenja certifikata prije isteka roka valjanosti naznačenog u certifikatu.

### Članak 35.

(1) Suspenzija je privremeni prestanak važenja certifikata.

(2) Povlačenje suspenzije je vraćanje suspendiranog certifikata u status važećeg certifikata, a prije njegovog isteka važenja.

(3) Kvalificirani pružatelj usluga povjerenja može provoditi suspenziju kvalificiranih certifikata.

(4) Kvalificirani pružatelj usluga povjerenja koji provodi suspenziju kvalificiranih certifikata može provoditi povlačenje suspenzije certifikata.

(5) Ukoliko kvalificirani pružatelj usluga povjerenja provodi suspenziju kvalificiranih certifikata, pravila i provođenje suspenzije i povlačenje suspenzije certifikata jasno opisuje u svojim dokumentima opća pravila pružanja usluga certificiranja i pravilnik o postupcima izdavanja certifikata.

(6) Kvalificirani pružatelj usluga povjerenja u dokumentima iz stavka 4. ovog članka jasno naznačuje maksimalni vremenski period u trajanja suspenzije kvalificiranog certifikata.

### Članak 36.

(1) Kvalificirani certifikat se suspendira na zahtjev:

– potpisnika, odnosno autora pečata,

– osobe ovlaštene za zastupanje pravne osobe ili organizacije s kojom je potpisnik povezan,

– izdavatelja certifikata.

(2) Kvalificirani certifikat se može suspendirati zbog sumnji do potvrde razloga navedenih za opoziv certifikata. Kvalificirani pružatelj usluga povjerenja razloge za suspendiranje certifikata jasno opisuje u svojim dokumentima opća pravila pružanja usluga certificiranja i pravilnik o postupcima izdavanja certifikata

(3) Nakon zaprimanja valjanog zahtjeva za suspenziju certifikata Kvalificirani pružatelj usluga povjerenja u najkraćem razumnom roku, a najkasnije u roku od 24 sata od primitka valjanog zahtjeva za suspenziju certifikata suspendira certifikat.

(4) Ako je kvalificirani certifikat suspendiran, taj certifikat gubi valjanost tijekom razdoblja suspenzije.

(5) Kvalificirani pružatelj usluga povjerenja jasno naznačuje razdoblje suspenzije u internoj bazi podataka certifikata sukladno članku 24. stavak 2. točke (k) Uredbe eIDAS, te osigurava da je status suspenzije tijekom razdoblja suspenzije vidljiv iz usluge u okviru koje pružaju informacije o statusu certifikata.

### Članak 37.

(1) Zahtjev za povlačenje suspenzije kvalificiranog certifikata može podnijeti potpisnik, odnosno autor pečata, nakon čega kvalificirani pružatelj usluga povjerenja provjeru identiteta podnositelja obavlja razinom koja je jednaka ili viša od razine koju osigurava dvofaktorska autentikacija.

(2) Nakon zaprimanja valjanog zahtjeva za povlačenje suspenzije certifikata kvalificirani pružatelj usluga povjerenja povlači suspenziju certifikata, te uklanja status suspenzije.

(3) Nakon provedenog povlačenja suspenzije kvalificiranog certifikata smatra se da je certifikat bio valjan tijekom razdoblja suspenzije koje je završilo povlačenjem suspenzije certifikata.

### Članak 38.

(1) Nakon isteka maksimalnog vremenskog perioda trajanja suspenzije iz članka 35. stavak 6. ovog Pravilnika, kvalificirani pružatelj usluga opoziva suspendirani kvalificirani certifikat.

(2) Vremenski trenutak opoziva suspendiranog certifikata jednak je trenutku kojem je certifikat suspendiran (trenutak u kojem je započelo razdoblje suspenzije).

# V. PRIJELAZNE I ZAVRŠNE ODREDBE

### Članak 39.

(1) Podaci u postojećim Registrima izdanih certifikata smatraju se podacima upisanim u sukladnosti s ovim Pravilnikom.

(2) Stupanjem na snagu ovoga Pravilnika prestaje važiti Pravilnik o izradi elektroničkog potpisa, uporabi sredstva za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (Narodne novine, broj 107/10 i 89/13).

(3) Postojeći pružatelji usluga povjerenja u Republici Hrvatskoj uskladiti će svoje poslovanje sukladno odredbama ovoga Pravilnika u roku od dvanaest mjeseci od dana stupanja na snagu ovoga Pravilnika.

### Članak 40.

Ovaj Pravilnik stupa na snagu danom donošenja.

Klasa:

Urbroj:

Zagreb, \_\_\_\_\_\_\_\_\_\_\_ 2019.

MINISTAR

Darko Horvat