REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

Tržaška cesta 21, 1000 Ljubljana

T: 01 478 83 30
F: 01 478 83 31
E: gp.mju@gov.si
www.mju.gov.si

Številka:007-722/2018-75
Ljubljana, 26. 3. 2021
EVA: 2016-3130-0039
GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE Gp.gs@gov.si

ZADEVA: **Zakon o elektronski identifikaciji in storitvah zaupanja – predlog za obravnavo**

1. Predlog sklepov vlade:

Na podlagi drugega odstavka 2. člena Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU – 1G, 65/14 in 55/17) je Vlada Republike Slovenije na ……. redni seji dne …… sprejela

SKLEP:

Vlada Republike Slovenije je določila besedilo predloga Zakona o elektronski identifikaciji in storitvah zaupanja (EVA: 2016-3130-0039) in ga pošlje v obravnavo Državnemu zboru Republike Slovenije.

mag. Janja Garvas Hočevar
v.d. generalnega sekretarja vlade

Sklep prejmejo:
– Ministrstvo za notranje zadeve,
– Ministrstvo za gospodarski razvoj in tehnologijo,
– Ministrstvo za izobraževanje, znanost in šport,
– Ministrstvo za pravosodje,
– Ministrstvo za delo, družino, socialne zadeve in enake možnosti,
– Ministrstvo za finance,
– Ministrstvo za kmetijstvo, gozdarstvo in prehrano,
– Ministrstvo za kulturo,
– Ministrstvo za obrambo,
– Ministrstvo za okolje in prostor,
– Ministrstvo za infrastrukturo,
– Ministrstvo za zdravje,
– Ministrstvo za zunanje zadeve,

– Služba Vlade Republike Slovenije za zakonodajo,
– Informacijski pooblaščenec

2. Predlog za obravnavo predloga zakona po nujnem ali skrajšanem postopku v državnem zboru z obrazložitvijo razlogov:

/

3.a Osebe, odgovorne za strokovno pripravo in usklajenost gradiva:

- Boštjan Koritnik, minister,
- mag. Peter Geršak, državni sekretar,
- Peter Jenko, v.d. generalnega direktorja Direktorata za informacijsko družbo,
- dr. Polonca Blaznik, sekretarka, Direktorat za informacijsko družbo

3.b Zunanji strokovnjaki, ki so sodelovali pri pripravi dela ali celotnega gradiva:

/

4. Predstavniki vlade, ki bodo sodelovali pri delu državnega zbora:

- Boštjan Koritnik, minister,
- mag. Peter Geršak, državni sekretar,
- Peter Jenko, v.d. generalnega direktorja Direktorata za informacijsko družbo,
- dr. Polonca Blaznik, sekretarka, Direktorat za informacijsko družbo

5. Kratek povzetek gradiva:

Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (v nadaljnjem besedilu: Uredba 910/2014/EU) je stopila v veljavo 17. septembra 2014, uporabljati pa se je začela 1. julija 2016. Predlog Zakona o elektronski identifikaciji in storitvah zaupanja v povezavi z Uredbo 910/2014/EU zagotavlja nacionalno pravno ureditev za področje storitev zaupanja, kjer ta uredba dopušča oziroma omogoča podrobnejšo opredelitev nacionalnih postopkov in ureditev, na področju elektronske identifikacije pa vključuje tudi ureditev izdajanja nacionalne elektronske identitete. Republika Slovenija bo s sprejemom predlaganega zakona tudi omogočila priglasitev svoje sheme elektronske identifikacije za čezmejno poslovanje in s tem svojim državljanom čezmejno elektronsko poslovanje.

Predlog zakona je vsebinsko povezan tudi s predvideno spremembo Zakona o osebni izkaznici, saj je Ministrstvo za notranje zadeve v skladu z Uredbo (EU) 2019/1157 Evropskega parlamenta in Sveta z dne 20. junija 2019 o okrepitvi varnosti osebnih izkaznic državljanov Unije in dokumentov za prebivanje, izdanih državljanom Unije in njihovim družinskim članom, ki uresničujejo svojo pravico do prostega gibanja (UL L št. 188 z dne 12. 7. 2019, str. 67), pripravilo pravne podlage za vključitev elektronske identitete na sredstvih elektronske identifikacije in digitalnega potrdila za elektronski podpis na novo biometrično osebno izkaznico. Za njeno izdajo mora veljati tudi predlagani Zakon o elektronski identifikaciji in storitvah zaupanja, saj šele ta opredeljuje izdajanje elektronske identitete s strani države na enem ali več sredstvih elektronske identifikacije.

6. Presoja posledic za:

a)	javnofinančna sredstva nad 40.000 EUR v tekočem in naslednjih treh letih	DA
b)	usklajenost slovenskega pravnega reda s pravnim redom Evropske unije	DA
c)	administrativne posledice	DA
č)	gospodarstvo, zlasti mala in srednja podjetja ter konkurenčnost podjetij	DA
d)	okolje, vključno s prostorskimi in varstvenimi vidiki	NE
e)	socialno področje	DA

f)	dokumente razvojnega načrtovanja: – nacionalne dokumente razvojnega načrtovanja – razvojne politike na ravni programov po strukturi razvojne klasifikacije programskega proračuna – razvojne dokumente Evropske unije in mednarodnih organizacij	NE

7.a Predstavitev ocene finančnih posledic nad 40.000 EUR:
Ocenjeni stroški Ministrstva za javno upravo so predstavljeni v nadaljevanju.

Stroški upravljanja sredstev elektronske identifikacije znašajo okoli 260.000 EUR za vzpostavitev in nato od 35.000 do 40.000 EUR letno:

i. stroški vzpostavitve infrastrukture za izdajanje sredstev elektronske identifikacije: 260.000 EUR
- stroški strojne opreme, okvirno 110.000 EUR;
- stroški vzpostavitve izdajateljev digitalnih potrdil za avtentikacijo, okvirno 80.000 EUR;
- stroški vzpostavitve evidence sredstev elektronske identifikacije ter razvoja aplikativne rešitve za upravljanje sredstev elektronske identifikacije, okvirno 70.000 EUR.

ii. stroški vzdrževanja:
- med 35.000 EUR in 40.000 EUR letno.

Zgoraj navedeni znesek predstavlja oceno stroškov vzpostavitve in delovanja infrastrukture za izdajanje sredstev elektronske identifikacije, ki temelji na odprtokodni rešitvi. Če bo sprejeta odločitev, da se uporabi licenčna programska oprema izdajateljev digitalnih potrdil za avtentikacijo, to pomeni dodatni strošek v višini približno 500.000 EUR za nakup licenčne programske opreme in dodatni strošek njenega vzdrževanja v višini 80.000 EUR letno.

Stroški upravljanja centralne storitve za spletno prijavo in elektronski podpis za potrebe zasebnega sektorja znašajo okoli 55.000 EUR za vzpostavitev in nato okrog 62.000 EUR letno:

i. stroški povečanja zmogljivosti infrastrukture centralne storitve:
- stroški strojne opreme, okvirno 45.000 EUR;
- stroški vzpostavitve dodatnih sistemov, okvirno 10.000 EUR.

ii. stroški vzdrževanja:
- okvirno 10.000 EUR letno.

iii. stroški dodatnih kadrov:
- strokovnjak za upravljanje centralne storitve, okvirno 30.000 EUR letno,
- izvajalec pomoči uporabnikom, okvirno 22.000 EUR letno.

Zgoraj navedeni znesek je potreben za vzpostavitev končnega stanja, ko se bo centralna storitev za spletno prijavo in elektronski podpis v zasebnem sektorju uporabljala v velikem obsegu, zato se lahko zmogljivosti dodajajo postopoma glede na izkazane potrebe. Ker bo za zasebni sektor uporaba storitve plačljiva, se bodo ti stroški prenesli na uporabnike storitve iz zasebnega sektorja.

I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu

	Tekoče leto (t)	t + 1	t + 2	t + 3

Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov državnega proračuna	/	/	/	/
Predvideno povečanje (+) ali zmanjšanje (**–**) prihodkov občinskih proračunov	/	/	/	/
Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov državnega proračuna	/	/	/	/
Predvideno povečanje (+) ali zmanjšanje (**–**) odhodkov občinskih proračunov	/	/	/	/
Predvideno povečanje (+) ali zmanjšanje (**–**) obveznosti za druga javnofinančna sredstva	/	/	/	/

II. Finančne posledice za državni proračun

II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:

Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1
Ministrstvo za javno upravo	3130-17-0004, Centralna informacijska infrastruktura PDC	153380 Razvoj ter vzdrževanje in upravljanje skupne informacijske infrastrukture (strežniške in licenčne)	260.000 500.000 (opcijsko)	40.000 80.000 (opcijsko)
SKUPAJ			260.000 oziroma 760.000	40.000 oziroma 120.000

II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:

Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1

SKUPAJ				

II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:		
Novi prihodki	Znesek za tekoče leto (t)	Znesek za t + 1
/	/	/
/	/	/
/	/	/
SKUPAJ	/	/

OBRAZLOŽITEV:

I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu

/

II. Finančne posledice za državni proračun

Odhodki državnega proračuna, ki so načrtovani na ukrepih oziroma projektih sprejetih proračunov, bodo predvidoma v letu 2021 znašali 260.000 EUR (z vključenim DDV) sredstev Ministrstva za javno upravo oziroma 760.000 EUR (z vključenim DDV) v primeru uporabe licenčne programske opreme izdajateljev digitalnih potrdil za avtentikacijo.

II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:

Ministrstvo za javno upravo bo stroške upravljanja sredstev elektronske identifikacije zagotovilo na proračunski podstavki 153380 Razvoj ter vzdrževanje in upravljanje skupne informacijske infrastrukture (strežniške in licenčne).

II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:

/

II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:

/

7.b Predstavitev ocene finančnih posledic pod 40.000 EUR:

/

8. Predstavitev sodelovanja z združenji občin:

Vsebina predloženega gradiva (predpisa) vpliva na:	DA/**NE**
- pristojnosti občin, - delovanje občin, - financiranje občin.	

Gradivo (predpis) je bilo poslano v mnenje:

- Skupnosti občin Slovenije SOS: DA/**NE**
- Združenju občin Slovenije ZOS: DA/**NE**
- Združenju mestnih občin Slovenije ZMOS: DA/**NE**

Predlogi in pripombe združenj so bili upoštevani:

- v celoti,
- večinoma,
- delno,
- niso bili upoštevani.

Bistveni predlogi in pripombe, ki niso bili upoštevani:/

9. Predstavitev sodelovanja javnosti:

Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja:	**DA**/NE

Predlog zakona je bil objavljen na portalu e-uprave, podportalu e-demokracija dne 26. 2. 2020. Na predlog zakona so se odzvali predstavniki zainteresirane javnosti.

Mnenja, predloge in pripombe so dali:
- Združenje za informatiko in telekomunikacije (v okviru Gospodarske zbornice Slovenije), Združenje bank Slovenije in Slovensko združenje za e-identifikacijo in e-storitve zaupanja
- podjetje EIUS d.o.o.,
- Notarska zbornica Slovenije

Upoštevani so bili:
- v celoti,
- večinoma,
- **delno,**
- niso bili upoštevani.

<u>- Združenje za informatiko in telekomunikacije (v okviru Gospodarske zbornice Slovenije), Združenje bank Slovenije in Slovensko združenje za e-identifikacijo in e-storitve zaupanja:</u>

Na pripombo, da ni jasno, ali velja zakon v delu izdaje in uporabe sredstev elektronske identifikacije le za javni ali tudi za zasebni sektor, odgovarjamo, da z vidika izdaje zakon regulira sredstva elektronske identifikacije, ki jih izdaja država oziroma pristojno ministrstvo. Z vidika uporabe pa sredstva elektronske identifikacije regulira že sama Uredba 910/2014/EU, ki zahteva od vseh organov javnega sektorja priznavanje priglašenih shem elektronske identifikacije in s tem v njih vključenih sredstev elektronske identifikacije. Zakon zato v tem okviru od organov javnega sektorja prav tako zahteva uporabo sredstev elektronske identifikacije, ki bodo izdana na podlagi tega zakona. Glede na predlagani 13. člen je vsem ponudnikom elektronskih storitev omogočena uporaba informacijske rešitve za uporabo teh sredstev elektronske identifikacije ter možnost preverjanja EŠEI. Zasebnega sektorja zakon ne regulira, enako, kot tudi Uredba 910/2014/EU, pa vsekakor spodbujamo zasebni sektor k uporabi informacijske rešitve za uporabo izdanih sredstev elektronske identifikacije, saj s tem razbremenimo zasebni sektor problematike elektronske identifikacije. Na ta način lahko tudi zasebni sektor uporabi elektronsko identiteto, ki jo po tem zakonu nudi in zanjo odgovarja država. Vsekakor pa zakon od zasebnega sektorja ne zahteva priznavanja sredstev elektronske identifikacije s strani zasebnega sektorja in ne omejuje možnosti, da bi slednji uporabljal oziroma priznaval tudi druge načine elektronske identifikacije.

Glede očitka o pomanjkanju obrazložitev ter predloga podzakonskega predpisa odgovarjamo, da zakon celovito opredeljuje regulirano materijo, podzakonski akti pa le specifično izvedbo, kar po našem mnenju omogoča dovolj dobro in jasno razumevanje materije zakona. Za medresorsko obravnavo zakona smo pripravili obrazložitve, predlog podzakonskega akta pa smo tudi priložili v fazi medresorskega usklajevanja.

Glede pripombe, da ni nikjer določeno, da predlog zakona ne velja za zaprte sisteme, odgovarjamo,

da je opredelitev in ureditev storitev zaupanja v zaprtih sistemih že vsebovana v 2. členu Uredbe 910/2014/EU, ki velja v našem pravnem redu neposredno, in se njene vsebine v nacionalnih predpisih ne sme podvojevati.

Pripomba, naj se ZEPEP v celoti razveljavi, ni bila upoštevana. V predlogu zakona se razveljavi zgolj tista določila ZEPEP, ki se nanašajo na področje storitev zaupanja (elektronski podpis in žig), so bila predmet prenosa prejšnje Direktive o elektronskem podpisu (Directiva 1999/93/EC) in ki so zaradi neposredne veljavnosti Uredbe 910/2014/EU postale obsoletne. Določbe glede elektronskega poslovanja pa ostajajo v veljavi, saj gre za splošna določila za elektronsko poslovanje in prenos dela Direktive 2000/31/ES, ki še vedno velja. Ker se na ravni EU obeta sprememba tudi na področju elektronskega poslovanja, bomo predvidoma po novi ureditvi spremenili ustrezno zakonodajo (vključno s preostalim delom ZEPEP) ter poenotili določbe glede elektronskega poslovanja.

Pobuda, da se izrazi "identiteta", "sredstvo e-identifikacije" zapišejo tako, kot je v Uredbi 910/2014/EU, ter da naj se izbriše izraz "elektronska identiteta", ni bila upoštevana iz razloga, ker izrazi, ki so vsebovani v navedeni uredbi veljajo neposredno in jih ni dopustno podvojevati ali spreminjati. Glede izraza "elektronska identiteta" pa pojasnjujemo, da gre za koncept, ki ga predlog zakona opredeljuje in iz njega izhaja, torej ga ni mogoče izbrisati. Gre za podoben koncept kot je pravna identiteta, ki jo posameznik ima, dokazuje jo pa na različne načine. Tako s predlogom zakona vzpostavljamo osebno elektronsko identiteto, ki smo jo definirali v 2. členu, ki se jo lahko dokazuje z več sredstvi elektronske identifikacije, kot to določa 5. člen (koncept ni v neskladju z Uredbo 910/2014/EU).

Glede pobude naj zakon celovito, tako za javni kot tudi za zasebni sektor, uredi izdajanje, uporabo in preklic sredstev elektronske identifikacije, pojasnjujemo, da zakon jasno določa takó izdajo, kot tudi uporabo sredstev elektronske identifikacije za javni sektor, z vidika izdaje in uporabe sredstev elektronske identifikacije v zasebnem sektorju pa predlog razumemo kot pobudo, da se v zakonu uredi tudi izdajanje sredstev elektronske identifikacije zasebnega sektorja ter se zasebnemu sektorju naloži obvezno uporabo sredstev elektronske identifikacije, ki jih zagotovi država. Glede tega odgovarjamo, da pobuda ni bila upoštevana, saj menimo, da bi v tem primeru šlo za prevelik in neupravičen poseg v zasebni sektor. Zakon izdajo sredstev elektronske identifikacije določa v kontekstu Uredbe 910/2014/EU, ki zavezuje le javni sektor. Vsekakor pa država spodbuja uporabo sredstev elektronske identifikacije v zasebnem sektorju, zakon pa to tudi omogoča. Zasebni sektor torej lahko v skladu s 13. členom predloga zakona uporablja informacijske rešitve za uporabo sredstev elektronske identifikacije, kar je jasna usmeritev tega zakona. S tem se zagotavlja tehnične pogoje za poenotene elektronske identifikacije v Sloveniji, istočasno pa se zagotavlja zasebnemu sektorju (npr. bančnemu) dovolj veliko fleksibilnost ureditve te problematike za lastne potrebe in hkrati zmanjšuje potrebo po visokih investicijah v različne lastne nepovezljive in ločene rešitve. Zasebni sektor ne sme biti zavezan k uporabi sredstev elektronske identifikacije izdane po tem zakonu, če tega ne želi, mu pa zakon to omogoča.

Glede pripombe, da mora biti izhodišče za pridobitev sredstva elektronske identifikacije (ne glede na to, kdo ga izda) zanesljiva ugotovitev istovetnosti in da mora v ta namen zakon določiti ustrezne pravne podlage za dostop do verodostojnih virov, odgovarjamo, da zakon to jasno določa v 11. členu v povezavi s 14. členom. To je povezano s pogoji za različne ravni zanesljivosti, ki jih določa Uredba 910/2014/EU sama in jih v tem smislu pravno ni mogoče spreminjati, zato zakon dejansko le operacionalizira vrsto dokumentov in potrebna preverjanja na nacionalni ravni, ki se izvedejo za predvidene različne ravni zanesljivosti.

Glede pripombe, naj se kot sistem za elektronsko identifikacijo določi delovanje nacionalnih shem,

odgovarjamo, da je okvir za sheme elektronske identifikacije že določen v Uredbi 910/2014/EU, na podlagi česar bo Slovenija pripravila tudi nacionalno shemo za elektronsko identifikacijo ter jo priglasila v skladu z Uredbo 910/2014/EU za čezmejno poslovanje.

Glede pripombe, da EŠEI nima dodane vrednosti in predloga za njeno ukinitev, pojasnjujemo, da je bilo glede na obstoječe stanje ocenjeno, da se potrebuje enotna pravna ureditev identifikacijske številke, ki bo uporabljena za identifikacijo v elektronskem poslovanju, kar trenutno ne obstaja. Uvedba EŠEI to sedaj sistemsko ureja tako za elektronsko identifikacijo, kot tudi za storitve zaupanja. Tvorjenje EŠEI temelji sicer na davčni številki, ki se danes že ponekod samostojno uporablja tudi pri elektronskem poslovanju, vendar je bila vzpostavljena za druge namene in je zato njena uporaba za prihodnost relativno omejena z resornim zakonom, s katerim je določena, kar lahko resno omeji fleksibilnost, ki jo v luči hitrega tehnološkega napredka potrebujemo na področju elektronskega poslovanja. EŠEI trenutno pove tudi osnovni tip subjekta, ki se mu dodeljuje elektronska identiteta (davčni številki se dodata preponi za fizično osebo ali za poslovni subjekt). S tem uvedba EŠEI omogoča ustrezno adaptacijo in prilagajanje zahtevam, ki bi lahko nastale na področju elektronskega poslovanja v prihodnosti, npr. zaradi razvoja novih okoliščin podeljevanja elektronske identitete (npr. imetnikov) ali tehnoloških sprememb (npr. uporaba različnih metod kriptiranja), s čimer bi morebitne spremembe omejili tako, da ne bi zahtevale sprememb npr. davčne številke. S predlogom zakona zato vzpostavljamo pravno podlago za uporabo EŠEI tako za ponudnike storitev zaupanja in izdajatelja sredstev elektronske identifikacije, kot tudi za njene uporabnike, t.j. ponudnike elektronskih storitev, s čimer sistemsko rešujemo trenutno stanje, ki do sedaj ni bilo jasno urejeno. S tem hkrati zmanjšujemo pravno negotovost za celoten ekosistem elektronskega poslovanja.

Glede pobude, da se omogoči videokonferenčna identifikacija pri elektronski identifikaciji, smo ocenili, da ta opcija za sredstvo elektronske identifikacije visoke ravni zanesljivosti, v skladu s prakso priznavanja te metode na ravni EU, ne pomeni preverjanja identitete posameznika enakovrednega fizični prisotnosti. V kontekstu trenutnega stanja tehnike slednje pomeni večje varnostno tveganje v luči vse bolj dostopne »deep fake« tehnologije zato video identifikacija na ravni EU ni podprta za visoko raven zanesljivosti. Glede na trenutno predvidena sredstva elektronske identifikacije, ki bodo uporabljena za izdajo elektronske identitete po tem zakonu, ki vključujejo izdajo na osebni izkaznici in v virtualnem okolju, in glede na zahteve Uredbe 910/2014/EU za postopke identifikacije imetnikov za visoko raven zanesljivosti, ta metoda trenutno ni primerna. V prihodnosti bi se lahko razmislilo o njeni uporabi za izdajo sredstev elektronske identifikacije srednje ali nizke ravni zanesljivosti, pod pogojem, da se bo to izkazalo za potrebno. Glede enakega predloga uporabe videokonferenčne identifikacije za izdajanje kvalificiranih potrdil za elektronski podpis odgovarjamo, da smo mnenja, da tudi v tem primeru v zakonu v povezavi s točko d prvega odstavka 24. člena Uredbe 910/2014/EU tega načina preverjanja istovetnosti fizične osebe ne moremo podpreti, saj so v trenutni zakonodaji kvalificirana potrdila za elektronski podpis uporabljena tudi za namene elektronske identifikacije in dostop do elektronskih storitev visoke ravni zanesljivosti, zato bi uporaba videokonferenčne identifikacije porušila sistemsko urejanje tega problema.

S predlogom za interoperabilnost sredstev elektronske identifikacije, predvsem pri čezmejnem poslovanju, se strinjamo, saj je interoperabilnost ena izmed ključnih ciljev Uredbe 910/2014/EU, ki že sama določa pogoje za interoperabilnost v svojih izvedbenih aktih. Ministrstvo za javno upravo ima večletno zgodovino sodelovanja pri vzpostavljanju čezmejne avtentikacijske infrastrukture in s tem nacionalnega vozlišča za namene Uredbe 910/2014/EU, ki je danes operativno, torej se zaveda pomembnosti izpolnjevanja zahtev za integracijo in interoperabilnost, ki jih določa Uredba 910/2014/EU. Glede na kompleksnost tovrstne infrastrukture je namen zakona, da slednjo ponudi vsem zainteresiranim deležnikom iz javnega, kot tudi zasebnega sektorja (pod ustreznimi pogoji) v Sloveniji.

Glede predloga urejanja določenih elementov delovanja ponudnikov nekvalificiranih storitev zaupanja zaradi zagotovitve pravne varnosti uporabnikov storitev odgovarjamo, da slednjega ne podpiramo, saj Uredba 910/2014/EU ločuje ponudnike nekvalificiranih in kvalificiranih storitev zaupanja, kjer posebej ureja pogoje delovanja predvsem ponudnikov kvalificiranih storitev zaupanja, posebno pa ne ureja ponudnikov nekvalificiranih storitev. Slednji morajo izvajati svoje storitve v skladu s splošnimi načeli in pogoji Uredbe 910/2014/EU, pri čemer je zanje še vedno na zahtevo oziroma na podlagi prijave nepravilnosti možen tudi nadzor (post festum), vendar Uredba 910/2014/EU zanje ne predvideva vnaprejšnjih pogojev in nadzora (ex-ante), kar jih ključno razlikuje od ponudnikov kvalificiranih storitev. V tem smislu v zakonu nismo predvideli posebne ureditve, saj menimo, da pravno podlago v zadostni meri nudi Uredba 910/2014/EU.

Glede predloga za opredelitev vsebine notranjih pravil za ponudnike storitve zaupanja odgovarjamo, da na tem področju neposredno veljajo določbe Uredbe 910/2014/EU in trenutno uveljavljen enoten sistem certificiranja ponudnikov storitev zaupanja, ki v standardih, ki so temelj certifikacije ponudnikov s strani organov za ugotavljanje skladnosti, že opredeljuje vsebino dokumentov, ki jih mora vsak ponudnik kvalificiranih storitev pripraviti, vzdrževati in jasno predočiti svojim uporabnikom za namene izvajanja kvalificiranih storitev zaupanja. Zaradi ustreznega poenotenja standardov v EU, ko se torej vsebina že sedaj skuša poenotiti na ravni EU, bi konkretne določbe v zakonu to poenotenje le otežile. Predlog zakona vsebuje zato le tiste dodatne vsebine, ki jih dopušča Uredba 910/2014/EU. Nekaj o notranjih pravilih sicer tudi v 33. členu predloga zakona.

Predlog natančnejše ureditve vpisa ponudnikov kvalificiranih storitev v nacionalni zanesljivi seznam ter postopkov preklica in začasne razveljavitve kvalificiranih potrdil v zakonu, deloma podpiramo, saj je slednje jasno določeno tako v Uredbi 910/2014/EU in samem zakonu, in ga bomo zagotovili tako, da bodo podrobnejši konkretni postopki opredeljeni v podzakonskem aktu.

Predloga, da se ponudnike storitev zaupanja uvrsti med ponudnike bistvenih storitev zaupanja (v skladu z Zakonom o informacijski varnosti), nismo upoštevali, ker glede na Zakon o informacijski varnosti, ki prenaša Direktivo 2016/1148/EU z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (konkretneje o sektorjih bistvenih storitev njena priloga II) (Direktiva NIS) v slovenski pravni red, področje zagotavljanja storitev zaupanja ne spada pod bistvene storitve. Zakon o informacijski varnosti tako poleg v Direktivi NIS opredeljenih 7 sektorjev kot nacionalno posebnost vključuje še področji preskrbe s hrano in varstva okolja zaradi poenotenja z Zakonom o kritični infrastrukturi. Samega področja zagotavljanja storitev zaupanja pa zaenkrat še nismo ocenili kot bistveno za nemoteno delovanje države v vseh varnostnih razmerah ter za ohranitev ključnih družbenih in gospodarskih dejavnosti v Republiki Sloveniji. Če bi se izkazalo, da se za vključitev izkaže potreba, predmet urejanja ne more biti predmetni zakon, temveč omenjeni Zakon o informacijski varnosti.

Predloga, da se ponudnike storitev zaupanja zaveže k imenovanju »Data protection officer« (pooblaščena oseba za varstvo osebnih podatkov), nismo upoštevali, saj bi s takšnim določilom posegali v vsebino drugih zakonov, saj obveznost imenovanja pooblaščene osebe urejajo predpisi s področja varstva osebnih podatkov.

Predlog, da bi centralna storitev za spletno prijavo in elektronski podpis morala biti na voljo tudi zasebnemu sektorju, smo upoštevali. Po premisleku in v okviru razpoložljivih virov je bilo odločeno, da se zasebnemu sektorju omogoči uporaba centralne storitve za spletno prijavo in elektronski podpis, pod različnimi pogoji (ang. SLA), ki jih bomo podrobneje določili v uredbi. Stroški upravljanja centralne

storitve za spletno prijavo in elektronski podpis za potrebe zasebnega sektorja bodo znašali okoli 55.000 EUR za vzpostavitev in nato okrog 62.000 EUR letno za delovanje, pri čemer se bodo ti stroški v določeni meri prenesli na uporabnike storitve SI-PASS iz zasebnega sektorja, ker bo za zasebni sektor uporaba storitve plačljiva, Za stroške storitve centralne storitve za spletno prijavo in elektronski podpis za e-pooblaščanja bo potrebno dodatnih 155.000 EUR za vzpostavitev in nato okrog 22.000 EUR letno za delovanje.

Predloga, da se normativno uredi možnost, da se centralna storitev za spletno prijavo in elektronski podpis, ki jo sedaj nudi Ministrstvo za javno upravo, lahko vzpostavi še pri kakšnem drugem ponudniku javnega ali zasebnega prava, se ne upošteva. Uredba 910/2014/EU namreč določa okvir za čezmejno priznavanje sredstev elektronske identifikacije in v tem okviru mora v skladu s 7. členom država zagotoviti infrastrukturo za spletno avtentikacijo za javni sektor, t.i. nacionalno avtentikacijsko vozlišče, ki se povezuje v mreži vseh vozlišč držav EU. Glede na odločitev, da se ta infrastruktura ponudi tudi zasebnemu sektorju, menimo, da ta predlog zato ni več relevanten.

Glede predloga za ureditev elementov različnih ravni priporočene dostave v javnem in zasebnem sektorju odgovarjamo, da so pravila glede priporočene dostave na ravni EU poenotena z Uredbo 910/2014/EU, česar z nacionalnimi predpisi ni mogoče spreminjati. Nacionalni predpisi lahko ureditev dopolnjujejo le na področju, kjer uredba to dopušča. Glede na to, da Uredba 910/2014/EU ureja le osnovne gradnike za elektronsko poslovanje, čemur je namenjen tudi ta zakon, slednji ni primeren za urejanje morebitnih različnih zahtev ali okoliščin za dejansko uporabo posameznih gradnikov (npr. okoliščin in pogojev za uporabo elektronske priporočene dostave). Za konkretne primere in zahteve je slednje smiselno urejati v specifičnih resornih zakonih, kjer so specifične potrebe tudi jasne. Zato predlog ni sprejet.

Na predlog, da bi morala biti s kvalificiranim potrdilom za elektronski podpis mogoča tudi elektronska identifikacija, odgovarjamo, da Uredba 910/2014/EU eksplicitno ureja izdajo in uporabo kvalificiranih potrdil za elektronski podpis kot storitev na trgu, ki je namenjena elektronskemu podpisovanju. Z vidika elektronske identifikacije je Slovenija sledila pravnemu sistemu, ki velja za identifikacijo v fizičnem svetu, v katerem veljavne osebne dokumente za identifikacijo oseb izdaja država, ki te dokumente tudi priznava pri izvajanju vseh javnih storitev. Prav tako so ti dokumenti uporabljeni za identifikacijo imetnikov v zasebnem sektorju, ki pri svojih storitvah celo temelji na nekaterih osebnih dokumentih (npr. osebni izkaznici). V tem smislu celoten sistem temelji na identiteti, ki jo državljanom podeli država, ki za to identiteto tudi jamči oziroma je zanjo v kontekstu Uredbe 910/2014/EU pri čezmejnem poslovanju tudi odgovorna. V tem smislu je bila sprejeta odločitev, da tudi v elektronskem svetu sledimo obstoječemu sistemu in podeljujemo elektronsko identiteto na podlagi že podeljene uradne pravne identitete, ki jo državljan/-ka pridobi ob rojstvu. Na ta način se lahko posameznik izkazuje v fizičnem svetu z veljavnimi osebnimi dokumenti, v elektronskem svetu pa z izdanimi sredstvi elektronske identifikacije. Bo pa v prehodni določbi predloga zakona vzpostavljeno prehodno obdobje 5 let po njegovi uveljavitvi, v katerem se za namene elektronske identifikacije še vedno omogoča uporaba kvalificiranih potrdil za elektronski podpis, ki so izdana tudi za namen avtentikacije. Na ta način bodo prebivalci lahko uporabljali obstoječa kvalificirana potrdila za elektronski podpis v celotnem obdobju njihove veljavnosti tudi za elektronsko identifikacijo, v tem prehodnem času pa bodo lahko pridobili elektronsko identiteto, ki bo izdana na podlagi tega zakona. Slednje zato praktično ne bo zahtevalo dodatnega napora ali stroškov za prilagoditev državljanov na novo elektronsko identifikacijo.

- podjetje EIUS d.o.o.

Na pripombo, naj zakon vsebuje le določila, ki se nanašajo na vse storitve zaupanja in pogoje za

njihovo izvajanje; izvajanje s strani države naj se uredi drugje; oziroma naj država zagotovi le podeljevanje elektronske identitete in storitve za preverjanje identitete, izvajanje kvalificiranih storitev pa naj se omogoča le za državne organe ali fizične osebe (sicer naj se storitev zaračunava oziroma naj jo plača tisti, ki jo uporablja), odgovarjamo, da pogoje za izvajanje storitev zaupanja opredeljuje že Uredba 910/2014/EU, zakon pa določa le tisti del, kjer je potrebno zahteve Uredbe 910/2014/EU konkretizirati glede na nacionalno ureditev. Zaradi konsistentnosti zakon vključuje tudi določila namenjena reguliranju ponudnika storitev zaupanja v državni upravi, kar glede na vsebino zakon smiselno dopolnjuje splošne zahteve za vse ponudnike storitev zaupanja. Iz istega razloga zakon vključuje tudi regulacijo izdajanja sredstev elektronske identifikacije s strani države, kar je v skladu z Uredbo 910/2014/EU prepuščeno nacionalni ureditvi. Glede predloga, da naj se izvajanje kvalificiranih storitev omeji na državne organe in fizične osebe oziroma naj se v nasprotnem storitve zaračunavajo, odgovarjamo, da je že sedaj vzpostavljena praksa, da se storitve zaračunavajo za pravne osebe, za fizične osebe pa z vidika zagotavljanja možnosti digitalnega poslovanja z državo ne.

Predloga, naj se kot sredstvo elektronske identifikacije uporabljajo tudi kvalificirana potrdila za elektronski podpis, v smislu trenutnega stanja, naj se le določi katere podatke mora v ta namen vsebovati, ne podpiramo. Pojasnilo smo podali že pri obravnavi zadnjega predloga prejšnjega pripombodajalca. Področje uporabe digitalnih potrdil za namene elektronske identifikacije pred Uredbo 910/2014/EU ni bilo regulirano, Uredba 910/2014/EU pa slednje na novo regulira za javni sektor (razen same izdaje, ki je prepuščena nacionalnim ureditvam) poleg storitev zaupanja, ki jih regulira splošno kot storitve. Način in obseg regulacije obeh področij je v Uredbi 910/2014/EU različen, zato smo v izogib pravni nejasnosti pri regulaciji področja elektronske identifikacije sledili obstoječi nacionalni pravni ureditvi in praksi na področju identifikacije državljanov v fizičnem svetu. Zaradi zatečenega stanja pa zakon za uporabo kvalificiranih potrdil za elektronski podpis predvideva prehodno obdobje, ki omogoča, da slednje imetniki lahko uporabijo tudi za elektronsko identifikacijo do poteka veljavnosti potrdil.

Pripombe, da naj bi se zahtevana raven zanesljivosti določila glede na posamezno storitev zaupanja, ne glede na to, kdo je njen ponudnik, se z vidika Uredbe 910/2014/EU ne da upoštevati, saj ta v točki b) prvega odstavka 6. člena zahteva, da raven zanesljivosti za dostop do storitve določi organ javnega sektorja.

Na pripombo, da "javni sektor" ni določen pojem in odpira mnoga vprašanja, odgovarjamo, da je v predlaganem 2. členu, v 3. točki, vsebovana opredelitev pojma »organ javnega sektorja«, ki je po predlogu zakona državni organ, organ samoupravne lokalne skupnosti, javna agencija, javni sklad, javni zavod ali druga oseba javnega prava, nosilec javnega pooblastila ali izvajalec javne službe.

Glede očitka o nesorazmernosti opredelitve stopnje izobrazbe (3 osebe z 8. ravnijo izobrazbe), odgovarjamo, da smiselno enako določilo vsebovala že na podlagi ZEPEP sprejeta Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje, po kateri smo se zgledovali pri konkretizaciji člena o ustreznosti izobrazbe Uredbe 910/2014/EU, in kar po našem vedenju ni predstavljalo problemov v zadnjih 20 letih. Zaradi povečanja tehnične in pravne kompleksnosti področja z uvedbo Uredbe 910/2014/EU, ne želimo tega pogoja zmanjševati. Predlagani 37. člen tudi ne določa, da mora ponudnik kvalificiranih storitev zaupanja imeti sklenjeno ustrezno samo svetovalno pogodbo z osebo s pravno izobrazbo z najmanj 8. ravnjo izobrazbe, ki ima najmanj dve leti delovnih izkušenj iz določenega področja, ampak dopušča tudi, da se tako osebo zaposli. Smo pa po premisleku pogoj pravniškega državnega izpita (to je bil namreč pogoj v 22. členu Uredbe o pogojih za elektronsko poslovanje in elektronsko podpisovanje) nadomestili z 2 leti delovnih izkušenj s področja storitev zaupanja ali elektronskega poslovanja. Prav tako smo spremenili področje na katerem mora imeti zaposleni delovne izkušnje, in sicer smo področje »storitev zaupanja ali sorodno področje« zamenjali s »s področja storitev zaupanja ali elektronskega poslovanja«. S to razširitvijo smo omogočili, da se sprejeme tudi strokovnjaka, ki ni uspel pridobivati izkušenj iz storitev zaupanja ali sorodnih področij, ki je relativno mlada panoga, ampak štejejo tudi izkušnje iz elektronskega poslovanja. V interesu čimbolj kvalitetnega

in zanesljivega izvajanja navedenih storitev pa smo dodali nov odstavek, ki določa, da morajo določene osebe imeti posebna strokovna znanja glede upravljanja in poznavanja tehnologije, varnostnih postopkov in pravnih zahtev s področja storitev zaupanja ali elektronskega poslovanja in delovanja ponudnikov kvalificiranih storitev zaupanja, pridobljena na strokovnih usposabljanjih

Glede pripombe, da naj bi država uvajala monopol in dodatne pogoje za kvalificirane ponudnike zaupanja, pojasnjujemo, da država s 40. členom predloga zakona ureja le način poslovanja državnih organov in ne uvaja dodatnih pogojev za ponudnike storitev zaupanja.

Pripombodajalec je posredoval tudi predlagane spremembe členov ZEPEP v verziji »sledi spremembam«. Glede na to, da ZEPEP ni predmet trenutne obravnave, pripravlja se popolnoma nov zakon, ki bo urejal elektronsko identifikacijo in storitve zaupanja, pripomb ni mogoče upoštevati.

- Notarska zbornica:

Predlog, naslovljen najprej na novelo Zakona o osebni izkaznici in kasneje še na predlog tega zakona, da bi tudi notarji lahko uporabljali podobo obraza imetnika osebne izkaznice in prstne odtise, shranjene kot biometrične podatke na pomnilniškem mediju, za preverjanje verodostojnosti osebne izkaznice in istovetnosti imetnika osebne izkaznice pri opravljanju elektronskih notarskih storitev (avtentikacija na daljavo oz. preveritev verodostojnosti osebnih dokumentov in ugotavljanje istovetnosti preko varne videokonferenčne povezave), ni bil upoštevan. Uredba (EU) 2019/1157 v 6. odstavku 11. člena omogoča, da se biometrični podatki, shranjeni na pomnilniškem mediju osebnih izkaznic uporabljajo za preverjanje pristnosti osebne izkaznice in identitete imetnika s pomočjo neposredno dostopnih primerljivih značilnosti, kadar zakon zahteva predložitev osebne izkaznice, če je to skladno tudi z nacionalnim pravom države izdajateljice osebne izkaznice. Zakon o varstvu osebnih podatkov v 79. členu izrecno določa, da se biometrijske ukrepe v javnem sektorju lahko določi le z zakonom, če je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi. Izjemoma pa tudi, če gre za izpolnjevanje obveznosti iz obvezujoče mednarodne pogodbe ali za identifikacijo posameznikov pri prehajanju državnih meja. Avtentikacija na daljavo oz. preveritev verodostojnosti osebnih dokumentov in ugotavljanje istovetnosti preko varne videokonferenčne povezave, pa nista takšne narave, da bi lahko opravičila nujno uporabo zaradi varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ne bi bilo možno doseči z milejšimi sredstvi.

10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:	**DA**/NE
11. Gradivo je uvrščeno v delovni program vlade:	DA/**NE**

Boštjan Koritnik
minister

Priloga:
– predlog zakona

PRILOGA:

PREDLOG

(EVA: 2016-3130-0039)

ZAKON O ELEKTRONSKI IDENTIFIKACIJI IN STORITVAH ZAUPANJA

I. UVOD

1.1 OCENA STANJA IN RAZLOGI ZA SPREJEM PREDLOGA ZAKONA

Predlog zakona je pripravljen kot podlaga na državni ravni za elektronsko poslovanje v povezavi z evropsko Uredbo (EU) št. 910/2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (v nadaljnjem besedilu: Uredba 910/2014/EU).

Ključni pogoji za izkoriščanje razvojnih možnosti elektronskega poslovanja za nadaljnje razvijanje digitalnega gospodarstva in družbe v okvirih notranjega trga EU so omogočanje čezmejnega elektronskega poslovanja, obstoj čezmejne elektronske identifikacije in zagotavljanje učinkovitega elektronskega poslovanja slovenskih državljanov, javne uprave in poslovnih subjektov. Analize so razkrile ključne težave pri vzpostavljanju učinkovitega okolja za elektronsko poslovanje, kar vključuje odsotnost pravne varnosti zaradi različnih nacionalnih določb, ki izhajajo iz različnih razlag prejšnjih direktiv, pomanjkanje interoperabilnosti sistemov, neenotno uporabo tehničnih standardov ter odsotnost pravnega in tehnološkega okvira za vzajemno priznavanje elektronskih identifikacij. Vse skupaj krni zaupanje, ki je prepotrebno za elektronsko poslovanje, posebno čezmejno.

Ključna rešitev na tem področju mora okrepiti zaupanje v elektronske transakcije med državljani, podjetji in javnimi organi na državnem kakor tudi na celotnem notranjem trgu EU, čemur v osnovi sledi izvajanje Uredbe 910/2014/EU.

Ministrstvo za javno upravo je kot ministrstvo, pristojno za informacijsko družbo, odgovorno za pripravo zakonodajnega okvira in izvajanje Uredbe 910/2014/EU. Ta je eden ključnih ukrepov za vzpostavitev enotnega digitalnega trga EU. Namenjena je povečanju zaupanja v spletno okolje in pospešitvi čezmejnega elektronskega poslovanja na notranjem trgu tako, da se zagotovijo varne in zanesljive elektronske transakcije med podjetji, državljani in javnimi organi.

Uredba 910/2014/EU po eni strani razširja področje dosedanje evropske zakonodaje o elektronskih podpisih na devet storitev zaupanja. Storitev zaupanja je storitev na notranjem trgu in pomeni elektronsko storitev, ki se praviloma opravlja za plačilo. Ta storitev vključuje:

- ustvarjanje, preverjanje in potrjevanje veljavnosti elektronskih podpisov, elektronskih žigov ali elektronskih časovnih žigov, storitev elektronske priporočene dostave in potrdil, povezanih s temi storitvami; ali
- ustvarjanje, preverjanje in potrjevanje veljavnosti potrdil za avtentikacijo spletišč ali
- hrambo elektronskih podpisov, žigov ali potrdil, povezanih s temi storitvami.

Uredba 910/2014/EU postavlja enotne zahteve za najvišjo raven izvajanja teh storitev, to je kvalificiranih storitev zaupanja, ki vključujejo tako zahteve in pogoje za ponudnike kvalificiranih storitev zaupanja kakor tudi zahteve in pogoje za kvalificirane storitve zaupanja, ki jih nudijo. Hkrati Uredba 910/2014/EU postavlja enotni okvir EU za izvajanje storitev zaupanja kakor tudi nadzor nad njimi. Po drugi strani pa Uredba 910/2014/EU ureja tudi področje elektronske identifikacije, kjer določa okvir za vzajemno priznavanje elektronskih identifikacijskih sredstev za čezmejno poslovanje. Pri tem prepušča samo izdajanje sredstev elektronske identifikacije državam in njihovim ureditvam. Novi evropski zakonski okvir je obvezen za elektronske storitve javnega sektorja, usmeritev in želja pa sta, da so rešitve na voljo tudi zasebnemu sektorju.

Uredba 910/2014/EU je začela veljati 17. septembra 2014, uporabljati pa se je začela 1. julija 2016. Republika Slovenija je Uredbo 910/2014/EU uvedla v svoj pravni red junija leta 2016 z Uredbo o izvajanju Uredbe (EU) o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (Uradni list RS, št. 46/16; v nadaljnjem besedilu: Uredba o izvajanju Uredbe 910/2014/EU). Ob tem je velik del obstoječe zakonodaje na področju elektronskega poslovanja postal obsoleten, kar je bilo poleg dejstva, da Republika Slovenija želi urediti tudi izdajanje sredstev elektronske identifikacije, razlog, da potrebujemo nov zakon o elektronski identifikaciji in storitvah zaupanja, ki bo vseboval posebno nacionalno pravno ureditev za storitve zaupanja, kjer Uredba 910/2014/EU seveda to dopušča, načrtno uredil področje elektronske identifikacije, razveljavil zastarele vsebine predpisov in hkrati ustrezne prilagodil evropskim predpisom in obstoječemu stanju na trgu. Predlog zakona bo torej nadomestil del Zakona o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14; v nadaljnjem besedilu: ZEPEP), ki je do sprejetja Uredbe 910/2014/EU na podlagi evropske Direktive za elektronski podpis 1999/93/ES med drugim urejal področje elektronskega podpisa, ter Uredbo o izvajanju Uredbe 910/2014/EU, s katero je bila Uredba 910/2014/EU vključena v slovenski pravni red.

Predvsem je treba poudariti pomemben cilj zakona, da bo Republika Slovenija, v kateri že od leta 2007 potekajo dejavnosti za ureditev elektronske identitete, z njegovim sprejemom nazadnje omogočila priglasitev svoje sheme elektronske identifikacije za čezmejno poslovanje in bo tako svojim državljanom omogočila čezmejno elektronsko poslovanje.

Na ravni EU so nekatere države že priglasile svoje sheme elektronske identifikacije za čezmejno poslovanje. Nemčija, Italija, Španija, Luksemburg, Hrvaška, Estonija, Portugalska, Belgija, Češka, Slovaška, Latvija in Litva so za čezmejno priznavanje v okviru svojih shem elektronske identifikacije kot sredstva elektronske identifikacije priglasile svoje elektronske osebne izkaznice. Italija, Združeno kraljestvo, Nizozemska in Latvija so priglasile tudi sheme, ki vključujejo sredstva, katerih izdajatelj je zasebni sektor. Estonija, Belgija, Portugalska, Danska in Latvija so priglasile sheme, ki vključujejo sredstva, izdana tudi na drugih tehnoloških podlagah (na primer mobilnih). Pregled trenutnega stanja priglasitev je na voljo na spletni strani Evropske komisije[1].

Pri tem je treba poudariti, da bo pravno podlago za izdajo elektronske identitete na biometrični osebni izkaznici, ki bo ena izmed možnih nosilk sredstva elektronske identifikacije, pripravilo

[1] https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

že Ministrstvo za notranje zadeve Republike Slovenije v spremembi Zakona o osebni izkaznici, ki se sprejema zaradi nove Uredbe (EU) 2019/1157 Evropskega parlamenta in Sveta z dne 20. junija 2019 o okrepitvi varnosti osebnih izkaznic državljanov Unije in dokumentov za prebivanje, izdanih državljanom Unije in njihovim družinskim članom, ki uresničujejo svojo pravico do prostega gibanja (UL L št. 188 z dne 12. 7. 2019, str. 67). Za njeno izdajo mora veljati tudi predlagani zakon, saj šele ta opredeljuje, kako država izdaja elektronsko identiteto na enem ali več sredstvih elektronske identifikacije.

Trenutno so operativno predvidena tri sredstva elektronske identifikacije:

- eID na biometrični osebni izkaznici – visoke in nizke ravni zanesljivosti,
- virtualni eID (to je na podlagi rešitve smsPASS).

V prihodnje pa bo elektronska identiteta lahko izdana na katerem koli dodatnem nosilcu (na primer na mobilnem telefonu, USB-pametnem ključku, platformi veriženja blokov in tako dalje), tehnologiji ali navsezadnje tudi na že obstoječih elektronskih dokumentih (na primer na kartici ZZZS, dovoljenju za bivanje in podobno), če se za to ugotovi potreba in zagotovijo zmožnosti glede na prihodnji razvoj na tem področju.

Biometrična osebna izkaznica je zaradi svoje pravne veljave, tehnološke zasnove in varnostnih mehanizmov pri različnih postopkih, na primer vložitvi vloge, izdelavi, podeljevanju in uporabi osebne izkaznice, primerna za izdajo sredstva elektronske identifikacije na najvišji ravni zanesljivosti, to je visoki ravni, kot to določa Uredba 910/2014/EU, kar bo omogočilo njenim imetnikom dostop do tako rekoč vseh elektronskih storitev javnega sektorja na celotnem notranjem trgu EU, spodbuja pa se uporaba informacijske rešitve za uporabo elektronske identifikacije tudi v zasebnem sektorju. Zaradi navedenih razlogov bo Republika Slovenija novo biometrično osebno izkaznico v skladu z Uredbo 910/2014/EU prijavila za čezmejno elektronsko poslovanje in tako bo sledila vrsti držav, ki so v ta namen prav tako prijavile svoje sheme elektronske identifikacije na podlagi nacionalnih osebnih izkaznic.

Nova biometrična osebna izkaznica bo tudi nosilka sredstva elektronske identifikacije nizke ravni zanesljivosti, saj takšno sredstvo omogoča razmah elektronskega poslovanja tudi za storitve, za katere enolična identifikacija posameznika, ki storitev uporabi, ni tako zelo pomembna, kot so druge prvine z vidika zagotavljanja določene storitve (na primer prijetna uporabniška izkušnja).

Nova biometrična osebna izkaznica bo vključevala tudi kvalificirano potrdilo za elektronski podpis izdajatelja na Ministrstvu za javno upravo. Na Ministrstvu za javno upravo namreč deluje Državni center za storitve zaupanja, ki je v skladu z zahtevami Uredbe 910/2014/EU ponudnik kvalificiranih storitev zaupanja in zagotavlja več kvalificiranih storitev zaupanja. Ena izmed njegovih osnovnih storitev zaupanja je izdajanje kvalificiranih potrdil za elektronski podpis, ki fizičnim osebam omogočajo elektronsko podpisovanje dokumentov.

Zaradi velike razširjenosti osebnih izkaznic (trenutno jih je približno 1,8 milijona) bomo z vključitvijo elektronske identitete in kvalificiranih potrdil za elektronski podpis širokemu krogu državljanov omogočili elektronsko identifikacijo in ustvarjanje elektronskih podpisov, ki so enakovredni lastnoročnim podpisom, in tako pospešili uporabo elektronskih storitev tako v javnem kot tudi v zasebnem sektorju.

1.2 Odprava določb Zakona o elektronskem poslovanju in elektronskem podpisu (ZEPEP)

Predlagani zakon bo torej nadomestil del ZEPEP, ki je do sprejetja Uredbe 910/2014/EU na podlagi Direktive Evropskega parlamenta in Sveta 1999/93/ES z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis med drugim urejal področje elektronskega podpisa in elektronskega časovnega žiga, ter Uredbo o izvajanju Uredbe 910/2014/EU, s katero je bila Uredba 910/2014/EU vključena v slovenski pravni red.

2. CILJI, NAČELA IN POGLAVITNE REŠITVE PREDLOGA ZAKONA

2.1 Cilji

Predlog zakona bo zagotovil nacionalno pravno ureditev za področje storitev zaupanja, kjer Uredba 910/2014/EU to dopušča oziroma omogoča nacionalne postopke in ureditev. Na področju elektronske identifikacije pa predlog zakona vključuje tudi ureditev izdajanja nacionalne elektronske identitete, česar sicer Uredba 910/2014/EU ne ureja in slednje prepušča samim državam. Republika Slovenija bo s sprejemom predlaganega zakona tako omogočila pripravo in priglasitev svoje sheme elektronske identifikacije za čezmejno poslovanje in tako bo svojim državljanom omogočila elektronsko identifikacijo pri dostopu do vseh storitev javnega sektorja na notranjem trgu EU, torej tako elektronsko poslovanje na nacionalni ravni kakor tudi čezmejno poslovanje.

2.2 Načela

Zakonski predlog vsebinsko uresničuje načela, ki sicer izhajajo že iz Uredbe 910/2014/EU, in sicer načela objektivnosti, nediskriminacije, preglednosti in sorazmernosti. Hkrati predlog stremi k zmanjševanju upravnih ovir v kar največji možni meri, saj širi možnost uporabe elektronskih storitev javne uprave. Predlog zakona sledi tudi načelom pravne varnosti ob identifikaciji v interesu preprečevanja zlorabe identitet z zagotavljanjem jasnosti in predvidljivosti ureditve ob zagotovitvi spoštovanja varstva osebnih podatkov.

2.3 Poglavitne rešitve

Poglavitne rešitve so:

- rešitev enotne elektronske identitete, ki jo izda država slovenskim državljanom in državljankam ter pod določenimi pogoji tudi tujcem na enem ali več sredstvih elektronske identifikacije;
- zagotovitev nacionalne pravne ureditve za področje storitev zaupanja, kjer Uredba 910/2014/EU dopušča oziroma omogoča nacionalne postopke in ureditev;
- vpeljava enoličnega identifikatorja fizične osebe ali poslovnega subjekta pri elektronskem poslovanju (tako imenovani EŠEI);
- zagotavljanje ponudnikom elektronskih storitev, registriranim v Republiki Sloveniji, možnost uporabe informacijske rešitve za uporabo sredstev elektronske identifikacije, izdanih s strani izdajatelja sredstva elektronske identifikacije, ter možnost preverjanja EŠEI na podlagi identifikacijske oznake sredstva elektronske identifikacije;

- omogočanje brezplačnega preverjanja podatkov v verodostojnem viru za identifikacijo ob kvalificiranih potrdilih, ki jih izdajo ponudniki kvalificiranih storitev zaupanja;
- možnost uporabe centralne storitve za spletno prijavo in elektronski podpis organov javnega sektorja ter ponudnikov elektronskih storitev.

3. OCENA FINANČNIH POSLEDIC PREDLOGA ZAKONA ZA DRŽAVNI PRORAČUN IN DRUGA JAVNA FINANČNA SREDSTVA

Ministrstvo za javno upravo bo bremenil strošek vzpostavitve in upravljanja sistema za izdajanje elektronskih istovetnosti, vzpostavitev in upravljanje evidence izdanih elektronskih istovetnosti in njene ustrezne povezave z evidenco izdanih osebnih izkaznic ter povezav s centralnim registrom prebivalstva, davčnim registrom, poslovnim registrom in javnimi evidencami za potrebe preverjanja pristnosti in veljavnosti javne listine.

Ministrstvo za javno upravo bosta bremenila tudi strošek razvoja in vzdrževanja rešitev za uporabo elektronskih istovetnosti ter strošek upravljanja centralne storitve za spletno prijavo in elektronski podpis za potrebe zasebnega sektorja.

Konkretni ocenjeni stroški Ministrstva za javno upravo so predstavljeni v nadaljevanju.

Stroški upravljanja sredstev elektronske identifikacije znašajo okoli 260.000 EUR za vzpostavitev in nato od 35.000 do 40.000 EUR letno:

Navedeni znesek predstavlja oceno stroškov vzpostavitve in delovanja infrastrukture za izdajanje sredstev elektronske identifikacije, ki temelji na odprtokodni rešitvi. Če bo sprejeta odločitev, da se uporabi licenčna programska oprema izdajateljev digitalnih potrdil za avtentikacijo, to pomeni dodatni strošek v višini približno 500.000 EUR za nakup licenčne programske opreme in dodatni strošek njenega vzdrževanja v višini 80.000 EUR letno.

Stroški upravljanja centralne storitve za spletno prijavo in elektronski podpis za potrebe zasebnega sektorja znašajo okoli 55.000 EUR za vzpostavitev in nato okrog 62.000 EUR letno.

Navedeni znesek je potreben za vzpostavitev končnega stanja, ko se bo centralna storitev za spletno prijavo in elektronski podpis v zasebnem sektorju uporabljala v velikem obsegu, zato se lahko zmogljivosti dodajajo postopoma glede na izkazane potrebe. Ker bo za zasebni sektor uporaba storitve plačljiva, se bodo ti stroški v določeni meri prenesli na uporabnike storitve iz zasebnega sektorja.

Navedena sredstva bodo bremenila proračun MJU. Predlog zakona nima neposrednih finančnih posledic za druga javna finančna sredstva (proračune lokalne samouprave, pokojninska in zdravstvena blagajna)

4. NAVEDBA, DA SO SREDSTVA ZA IZVAJANJE ZAKONA V DRŽAVNEM PRORAČUNU ZAGOTOVLJENA, ČE PREDLOG ZAKONA PREDVIDEVA PORABO PRORAČUNSKIH SREDSTEV V OBDOBJU, ZA KATERO JE BIL DRŽAVNI PRORAČUN ŽE SPREJET

Finančna sredstva za izvajanje zakona so zagotovljena v sprejetem državnem proračunu.

Finančna sredstva za upravljanje sredstev elektronske identifikacije so zagotovljena:

- v okviru projekta: 3130-17-0004, Centralna informacijska infrastruktura PDC,
- na šifri proračunske postavke: 153380 Razvoj ter vzdrževanje in upravljanje skupne informacijske infrastrukture (strežniške in licenčne),
- v višini skupaj: 260.000 oziroma 760.000 (za tekoče leto) in 40.000 oziroma 120.000 (za vsako naslednje leto).

Finančna sredstva za upravljanje centralne storitve za spletno prijavo in elektronski podpis za potrebe zasebnega sektorja

- znašajo okoli 55.000 EUR za vzpostavitev in nato okrog 62.000 EUR letno;

- so potrebna za vzpostavitev končnega stanja, ko se bo centralna storitev za spletno prijavo in elektronski podpis v zasebnem sektorju uporabljala v velikem obsegu, zato se lahko zmogljivosti dodajajo postopoma glede na izkazane potrebe. Ker bo za zasebni sektor uporaba storitve plačljiva, se bodo ti stroški prenesli na uporabnike storitve iz zasebnega sektorja in jih posledično ne bo treba zagotavljati iz javnih sredstev.

5. PRIKAZ UREDITVE V DRUGIH PRAVNIH SISTEMIH IN PRILAGOJENOSTI PREDLAGANE UREDITVE PRAVU EVROPSKE UNIJE

Predlog zakona je predmet usklajevanja s pravnim redom EU, in sicer z Uredbo 910/2014/EU.

V nadaljevanju je podan pregled po nekaterih državah, ki so v skladu z Uredbo 910/2014/EU že uspešno priglasile svoje sheme elektronske identifikacije za čezmejno poslovanje.

5.1 Belgija

Belgija je uspešno priglasila dve svoji rešitvi, in sicer svojo elektronsko osebno izkaznico (eOI) in mobilno rešitev "Itsme®".

5.1.1 Elektronska osebna izkaznica (eOI)

Belgijska elektronska osebna izkaznica (eOI) je pametna kartica, skladna z ISO 7816, ki vsebuje vse informacije, vključene v tradicionalno osebno izkaznico, in služi kot identifikacijski dokument za fizične in elektronske namene. eOI je izdana fizičnim osebam na podlagi državne registrske številke (abr. RRN). Kartica je za belgijske državljane obvezna od 12. leta. Običajna veljavnost eOI je deset let. EOI je pametna kartica z čipom, ki vsebuje dve digitalni potrdili. Prvo potrdilo je namenjeno za elektronsko identifikacijo, drugo potrdilo pa za generiranje elektronskega podpisa. Tako e-identifikacija kot e-podpis se izvedeta z dvofaktorsko overovitvijo, to je z vstavitvijo eOI v bralnik pametnih kartic in vnosom štirimestne kode PIN. Potrdilo za e-podpis se aktivira samo za odrasle (nad 18 let).

Za upravljanje in registracijo identifikacijskih podatkov oseb so odgovorni Nacionalni register fizičnih oseb ter občine in konzulati. Izdajo eOI izvajajo občine, za državljane, ki živijo v tujini, pa konzulati. EOI izdeluje in personalizira na podlagi pogodbe zunanje podjetje, ki ga imenuje svet ministrov (ang. Council of Ministers). Občine so odgovorne za začetek postopka izdelave eOI in dostavo ustrezne dokumentacije prosilcem, prav tako so odgovorne za dostavo eOI. Vlagatelj mora eOI prevzeti osebno na občini, kamor eOI dostavi zunanje podjetje. Vlagatelj lahko eOI prevzame od javnega uslužbenca občine, potem ko ta izvede identifikacijo in preverjanje vlagatelja in po aktiviranju eOI s PUK-kodo, ki jo je vlagatelj prejel po pošti, vse s ciljem, da bi se zmanjšalo tveganje izgubljenih, ukradenih, preklicanih ali pretečenih dokumentov (osebno preverjanje). Vlagatelj pri tem predloži fotografijo in se mora podpisati, njegov podpis pa bo zapisan na eOI. Javni uslužbenec občine preveri pristnost in veljavnost fotografije, ki jo je prinesel vlagatelj, ter jo primerja z videzom vlagatelja, ki mora biti zato fizično prisoten. Javni uslužbenec občine za preverjanje identifikacijskih podatkov osebe uporablja eOI v kombinaciji s podatki iz Nacionalnega registra fizičnih oseb. Če vlagatelj ne predloži eOI (v primeru izgube ali tatvine), lahko javni uslužbenec uporabi posebno aplikacijo za primerjavo med fotografijo, ki je že shranjena v sistemu (če obstaja), in fotografijo vlagatelja, ki jo je vlagatelj prinesel s seboj.

Nacionalni register fizičnih oseb ima ključno vlogo pri razvoju in nadzoru sistema eOI. Razvija in vodi ga Zvezna služba za notranje zadeve / Generalni direktorat za institucije in prebivalstvo (ang. Federal Public Service Home Affairs/ Directorate General Institutions and Population). Operativna struktura Nacionalnega registra in informacijske infrastrukture občin sta prilagojena tako, da omogočata izdajo eOI v varnem okolju. V zvezi z eOI opravlja nadzor nad občinami Zvezna služba za notranje zadeve, nad konzulati pa Zvezna služba za zunanje zadeve.

5.1.2 Mobilna rešitev "Itsme®"

Itsme® je belgijska rešitev mobilne ID, ki jo upravlja konzorcij štirih vodilnih bank (Belfius, BNP Paribas Fortis, ING, KBC) in treh operaterjev mobilnih omrežij (Orange Belgium, Proximus, Telenet) v Belgiji. Skupaj so želeli ljudem olajšati varno in hitro identifikacijo na daljavo.

Itsme® je zelo varna aplikacija za mobilni telefon, ki omogoča varno digitalno prijavo in digitalno izmenjavo osebnih podatkov v transakcijah. Zagotavlja edinstveno digitalno identiteto vsakemu prebivalcu, starejšemu od 18 let v Belgiji, ki ima mobilni telefon in belgijsko eOI oziroma belgijsko kartico za tujce.

Itsme® je dobrodošla priročna alternativa čitalnikov kartic, gesel in različnih kod PIN. Itsme® zagotavlja enostavno uporabo in varno mobilno identifikacijo. Na voljo je na mobilnih telefonih, ki temeljijo na Androidu ali iOS.

Ko je aplikacija nameščena, lahko uporabnik svojo petmestno kodo ali prstni odtis uporabi za:
- prijavo na spletnih mestih in aplikacijah,
- potrditev (bančne) transakcije in druge interakcije (ni del uporabe v okviru priglasitve),
- digitalni podpis dokumentov (od leta 2019).

5.2 Češka

Češka republika (Češka) je priglasila za čezmejno e-poslovanje svojo elektronsko osebno izkaznico visoke ravni zanesljivosti.

Češka elektronska osebna izkaznica (eOI) je kartica s čipom, izdana češkim državljanom, ki služi kot osnovni upravni dokaz identitete (z najvišjo stopnjo zanesljivosti) in državljanstva imetnika ter vsebuje vse informacije, vključene v tradicionalno osebno izkaznico. eOI vključuje potrdilo za elektronsko identifikacijo, prav tako pa ima dodaten prostor na čipu (16 vsebnikov), ki ga imetnik lahko uporabi za hrambo drugih potrdil, predvsem kvalificiranih potrdil za elektronski podpis. Češki državljani imajo z eOI možnost pridobitve svojih podatkov iz baze podatkov rezidentov, davčnega portala in drugih uradnih sistemov Češke. eOI je obvezna za vsakega državljana Češke, starega 15 let ali več, aktiviranje funkcije elektronske identifikacije pa je izbirno. Državljan, čigar pravna sposobnost je omejena, lahko prav tako ima osebno izkaznico (ali njeno predhodnico brez čipa). eOI se lahko izda tudi državljanu, mlajšemu od 15 let, ali državljanu, ki nima prebivališča na ozemlju države članice Češka. V primeru državljana, mlajšega od 15 let, za izdajo eOI zaprosi njegov zakoniti zastopnik. Del za elektronsko identifikacijo OI lahko aktivira samo imetnik, ki je starejši od 15 let in čigar pravna sposobnost ni bila omejena.

eOI se izdajo državljanom, mlajšim od 15 let, za čas veljavnosti pet let, za državljane, starejše od 15 let, za čas veljavnosti 10 let, in za državljane, starejše od 70 let, za čas veljavnosti 35 let. Dostavo eOI imetniku lahko opravi samo uradna oseba, ki mora obvezno preveriti fizično identiteto imetnika.

Postopek registracije edinstvenih identifikacijskih podatkov osebe upravljata občinski organ z razširjeno pristojnostjo in Ministrstvo za notranje zadeve. Taisti organi tudi izdajo osebi OI, in sicer navedeni občinski organi za rezidente, ministrstvo pa v primeru izdaje OI za krajše obdobje. OI izdeluje državno podjetje STC, ki izvaja dejavnost personalizacije. Avtentikacijski proces opravi Organ za državne registre (SZR), ki je upravni organ v pristojnosti ministrstva za notranje zadeve. ID številka OI omogoča nedvoumno identifikacijo imetnika kartice. Za elektronsko identifikacijo se uporablja dvofaktorska avtentikacija. Za navedeno sta potrebni fizična posest OI ter poznavanje dostopne kode IOK za uporabo identifikacijskega potrdila (od štiri do 10 mest).

Prepoznavanje prek OI se lahko opravi z osebnim računalnikom, mobilnim telefonom, tabličnim računalnikom ali z osebnim stikom s ponudnikom storitve. Uporabnik dokazuje identiteto s svojo OI prek programske opreme „eObčanka“ pri nacionalnem vozlišču za identifikacijo in overjanje (NIA), ki ga upravlja država. Nato NIA prenese informacije o uporabniku do ponudnika spletne storitve (SeP). SeP ima zaupanje v prejete osebne podatke, ki jih je zagotovila shema CZ eID. SeP je lahko kateri koli organ javnega sektorja, ki ponuja spletno storitev, ki zahteva preverjanje identitete. SeP je lahko tudi zasebna oseba, ki je dolžna potrditi identiteto osebe na spletu storitev.

Nadzorni organ nad izdajo je ministrstvo za notranje zadeve.

5.3 Danska

Danska je za elektronsko identifikacijo za čezmejno e-poslovanje priglasila svojo storitev NemID, z različnimi sredstvi srednje ravni zanesljivosti.

Danska ima dolgo zgodovino uporabe elektronskega podpisa v naših digitalnih storitvah – zlasti v javnem sektorju že od leta 2003. Trenutna rešitev NemID je že od leta 2010. Uporablja se tako v javnem kot v zasebnem sektorju, zlasti za poslovanje z bankami in zavarovalnicami. NemID predstavlja nacionalni eID, omogoča e-podpis in se lahko uporablja za državljane, zaposlene in podjetja.

Danska ima od leta 2012 obvezne digitalne storitve, kar je povzročilo veliko povečanje uporabe NemID. Danski eID ima tako 5,16 milijona državljanov, NemID pa je imel v letu 2019 v povprečju več kot 60 milijonov transakcij mesečno.

NemID se izdaja na različnih sredstvih, da omogoča različne potrebe državljanov. Sredstvo NemID zagotavlja varnost, v kateri se mora uporabnik overiti z uporabo dvofaktorskega mehanizma za preverjanje pristnosti. Ta je sestavljen iz "nečesa, kar veš" – osebnega uporabniškega imena in izbranega gesla – in "nečesa, kar imaš" – na primer ključne kartice ali katerega koli drugega spodaj navedenega sredstva. Vsa sredstva NemID so osebna in jih je mogoče povezati samo z eno identiteto. NemID uporablja naslednja sredstva za preverjanje pristnosti:

- ključno kartico (OTP)/ Key card (OTP),
- mobilno aplikacijo,
- ključni žeton (OTP)/Key token (OTP),
- strojno opremo NemID.

Obstaja tudi podpora za slabovidne uporabnike, ki imajo na voljo dve možnosti za preverjanje pristnosti:

- interaktivni glas/odziv (OTP),
- tipkovnico Magna (OTP).

NemID deluje v okviru Agencije za digitalizacijo pri ministrstvo za finance, dobavitelj pa je zasebno podjetje Nets DanID A / S. Nets DanID A / S je lastnik rešitve NemID in je odgovoren ne samo za razvoj, temveč tudi avtentikacijo, vzdrževanje, vpis in zaustavitev elektronske identitete. NemID temelji na danskem standardu Javna potrdila o elektronski storitvi (OCES), ki določa zahteve in obveznosti za različne organe, vključene v shemo eID. Ta standard je bil razvit leta 2003, pred uredbo 910/2014/EU.

5.4 Estonija

Estonija je za čezmejno e-poslovanje priglasila šest različnih rešitev, vse z visoko ravnjo zanesljivosti. Tri rešitve združujejo fizični identifikacijski dokumenti in digitalni osebni dokumenti (osebna izkaznica, dovoljenje za bivanje – kartica RP) – in diplomatska osebna izkaznica). Drugi trije (Digi-ID, Digi-ID za e-prebivališče in Mobiil-ID) so samo digitalni osebni dokumenti.

Tehnično so vsi estonski eID-ji rešitve, ki temeljijo na infrastrukturi javnih ključev (PKI), kjer je zasebni ključ na varnem modulu čipa. Pri Mobiil-ID je eID čip z varnim modulom vgrajen na kartico SIM. Čipi so SSCD/QSCD-naprave. To so pametne kartice, ki ščitijo zasebni ključ pred nepooblaščenim dostopom, kopiranjem ali nedovoljenim posegom. Podatki o identiteti - ime, priimek in edinstvena identifikacijska številka osebe (osebna identifikacijska koda) – so

shranjeni v potrdilu javnega ključa. Ta potrdila so prosto dostopna na pametni kartici ali v javnem katalogu LDAP.

Prvi pogoj za Mobiil-ID je osebna ali RP-kartica. Mobiil-ID se lahko pridobi pri estonskih mobilnih operaterjih. Mobiile-ID uporabnik aktivira s svojo osebno izkaznico ali kartico RP ali na ustreznem mestu organa, ki izdaja dovoljenje. Pri upravljanju sheme eID sodelujejo naslednje strani:

- estonski Policijski in carinski urad (PBGB) in ministrstvo za zunanje zadeve (za izdajo diplomatske osebne izkaznice, uradna tuja predstavništva Republike Estonije);
- organ za informacijski sistem (EISA) je državna institucija, ki je odgovorna predvsem za upravljanje IT v javnem sektorju. Poleg tega gosti nacionalni CERT-EE in opravlja vlogo nadzornega organa za izvajalce CIIP in zaupnih storitev (več informacij na https://www.ria.ee/en/). EISA je odgovorna za zahteve po strojni in programski opremi eID. Na splošno EISA ohranja vrsto zahtev za eID, sodeluje pri naročilih in potrjuje rezultate kot partnerska organizacija PBGB. Poleg tega razvija in vzdržuje programsko opremo in programsko opremo za končne uporabnike za vzdrževanje eID kartic (koda PIN in uradno upravljanje e-poštnih naslovov), tudi programsko opremo za e-podpise;
- PBGB ima izvajalca za izdelavo in personalizacijo osebnih dokumentov, Gemalto AG. Prilagoditev opravi hčerinsko podjetje Gemalto AG Trüb Baltic AS s sedežem v Estoniji;
- certifikacijski organ (ponudnik certifikacijskih storitev) je kvalificirani ponudnik zaupnih storitev (v skladu z uredbo 910/2014/EU): SK ID Solutions AS. Je pogodbena stranka za dobavo storitve Mobiil-ID (kartice SIM in kvalificirane storitve zaupanja) in podizvajalec za kvalificirane storitve zaupanja za osebne dokumente PBGB. Njegova odgovornost je vzdrževanje življenjskega cikla certifikata: ustvarjanje, aktiviranje, zaustavitev in preklic;
- mobilni operaterji (Telia Eesti AS, Elisa EestiAS, Tele2 Eesti AS) so podizvajalci podjetja SK ID Solutions AS. Uporabnikom Mobiil-ID dostavijo kartice SIM, ki so nosilci državnega eID-ja s funkcionalnostjo elektronske overitve in kvalificiranega digitalnega podpisa;
- ustvarjanje in aktiviranje potrdila Mobiil-ID se opravi v imenu PBGB po potrditvi identitete uporabnika, kar opravi PBGB.

Estonski eID se uporabljajo samo za identifikacijo fizičnih oseb.

5.5 Hrvaška

Hrvaška je priglasila osebno izkaznico za čezmejno e-poslovanje z visoko ravnjo zanesljivosti.

Osebna izkaznica je elektronski javni dokument, s katerim državljan izkazuje identiteto, državljanstvo, spol, datum rojstva in prebivališče v Republiki Hrvaški. Osebna izkaznica je obvezna za državljane, ki so dopolnili 18 let starosti in imajo prijavljeno prebivališče v Republiki Hrvaški, pridobijo pa jo lahko tudi hrvaški državljani, ki ne živijo na Hrvaškem.

Osebna izkaznica vsebuje elektronski nosilec podatkov – čip, na katerega se poleg podatkov o identiteti, ki so vidni na izkaznici, shranita tudi eno ali dve digitalni potrdili, eno za elektronsko

identifikacijo, drugo za kvalificirani elektronski podpis oziroma elektronski podpis, ki je pravno enakovreden lastnoročnemu podpisu.

Veljavnost osebne izkaznice in pripadajočih potrdil na čipu je pet let in je ni mogoče podaljševati. Po preteku veljavnosti je treba osebno izkaznico zamenjati (ni post-personalizacije za elektronski del). Za osebe nad 65 let zamenjava osebne izkaznice ni potrebna in je veljavna za nedoločen čas. Če je izdana s potrdilom, lahko oseba po poteku potrdila še naprej uporablja osebno izkaznico, vendar ne more uporabljati potrdil. Osebna izkaznica, izdana za otroke do petih let starosti, ne vsebuje potrdila za elektronsko identifikacijo niti kvalificiranega potrdila za kvalificirani elektronski podpis. Osebna izkaznica, izdana za osebo od petega do 18. leta starosti, vsebuje potrdilo za elektronsko identifikacijo, za osebe, starejše od 18 let, pa vsebuje poleg potrdila za elektronsko identifikacijo tudi potrdilo za kvalificirani elektronski podpis. Osebe, starejše od 65 let, lahko na zahtevo dobijo osebno izkaznico s potrdilom ali brez njega.

Osebne izkaznice v Republiki Hrvaški izdaja policijska uprava oziroma policijske postaje pod okriljem ministrstva za notranje zadeve, izdela pa jih Agencija za komercijalnu djelatnost d. o. o. (AKD), ki je podjetje v državni lasti in ga je Vlada HR na podlagi Zakona o osebni izkaznici pooblastila za izdajanje osebnih izkaznic in ustreznih kvalificiranih potrdil. AKD sicer izdeluje različne vrste osebnih dokumentov in kartic ter vzdržuje celoten elektronski identifikacijski ekosistem z izdelavo osebnih izkaznic, vgradnjo čipov, vzdrževanjem portala in podobno, prav tako pa izvaja tudi kvalificirane storitve zaupanja po Uredbi 910/2014/EU. Slednje izvaja pod nadzorom ministrstva, odgovornega za gospodarstvo.

Oseba vlogo za pridobitev osebne izkaznice poda osebno na policijski upravi oziroma policijski postaji, kjer ima prijavljeno stalno prebivališče. Če nima prijavljenega stalnega prebivališča v Republiki Hrvaški, lahko poda vlogo osebno na kateri koli policijski upravi oziroma policijski postaji. Za nedvoumno identifikacijo vlagatelja se uporablja posebna osebna številka občana (osobni identifikacijski broj). Vlagatelj pri tem predloži ustrezno fotografijo v zahtevani velikosti ter poda prstna odtisa kazalcev leve in desne roke. Osebno izkaznico ter podatke za aktivacijo elektronskega dela osebne izkaznice in podatke za registracijo na portalu elektronske osebne izkaznice vlagatelj prevzame na policijski upravi oziroma policijski postaji, na kateri je bila podana zahteva za izdajo.

Elektronska identifikacija in preverjanje elektronske identitete potekata centralno preko NIAS (ang. National Identification and Authentication System), ki je edina integracijska točka za vse ponudnike e-storitev. NIAS (in v okviru tega 910/2014/EU avtentikacijsko vozlišče za čezmejne transakcije) nudi in upravlja Agencija za finance (hr. Financijska agencija – izhaja iz nekdanjega SDK, podobno kot pri nas Urad za javna plačila). Za izvajanje dejavnosti v okviru sistema NIAS so ministrstvo za notranje zadeve, ministrstvo za javno upravo in Agencija za finance podpisali posebno pogodbo. Ministrstvo za javno upravo je kot ministrstvo, odgovorno za področje e-Hrvaške odgovorno za izvajanje Uredbe 910/2014/EU v delu, ki se nanaša na elektronsko identifikacijo.

Cene elektronske osebne izkaznice:

- osebna izkaznica za otroka do petega leta starosti, ki ne vsebuje certifikatov, je 60 HRK (8,01 EUR;
- osebna izkaznica za otroka od dopolnjenega petega leta starosti in za polnoletne osebe, ki vsebuje enega ali oba certifikata, je 79,50 HRK (10,61 EUR);
- osebna izkaznica za osebe, ki so dopolnile 65 let starosti in ne vsebuje certifikatov, je 49,50 HRK (6,61 EUR).

5.6 Italija

Italija je priglasila svoj sistem digitalnih identitet SPIS, ki omogoča vključitev javnih in zasebnih ponudnikov sredstev elektronske identifikacije. Italija je v tem okviru priglasila različne ponudnike različnih ravni zaupanja, med drugim tudi elektronsko osebno izkaznico.

Ponudniki sredstev elektronske identifikacije so lahko iz javnega ali zasebnega sektorja, ki jih uspešno akreditira Agencija za digitalno Italijo (AgID) v skladu s Kodeksom za digitalno upravo (ali "CAD", italijanska zakonska uredba št. 82 z dne 7. marca 2003).

Državljani lahko pridobijo različne "SPID identitete", ki jih lahko izdajajo javne ali zasebne institucije. Okvir SPID določa zahteve za izdajanje "SPID identitet". Italija je uspešno priglasila različne rešitve, ki izpolnjujejo zahteve od nizke pa do visoke ravni zanesljivosti. Država je poskušala notificirati v okviru SPID tudi videoidentifikacijo, vendar ta postopek v času priprave zakona še ni končan.

5.6.1 Italijanska osebna izkaznica

Italija je kot sredstvo visoke ravni zanesljivosti uspešno priglasila tudi svojo elektronsko osebno izkaznico, ki je osebni dokument. Narejena je iz plastike v velikosti kreditne kartice in je opremljena s prefinjenimi zaščitnimi lastnostmi ter radijskim frekvenčnim (RF) mikročipom, ki hrani podatke imetnika.

Po pooblastilu ministrstva za notranje zadeve jih izdajajo občine, in to vsem državljanom, ki prebivajo v Italiji (ali priseljencem z dovoljenjem za prebivanje), in konzulati vsem državljanom iz tujine na zahtevo. Izkaznica je narejena v skladu z zahtevami za potovalni dokument.

Trajanje dokumenta se razlikuje glede na starost imetnika:
- tri leta za imetnike, mlajše od treh let;
- pet let za imetnike, stare od tri do 18 let;
- deset let za lastnike, starejše od 18 let.

Osebna izkaznica kot sredstvo elektronske identifikacije vsebuje digitalno potrdilo za avtentikacijo in zasebni ključ. Dostop do njega ima samo imetnik kartice, če vnese posebno osemmestno geslo (PIN). Uporaba kartice poteka s pomočjo strojne naprave (RF-čitalnik ali NFC-bralnik) in programske opreme, ki jo poganja. RF-čitalniki so na trgu prosto dostopni po nizki ceni ali prek mobilnih telefonov, ki imajo vgrajen čitalnik NFC.

5.7 Nemčija

Nemčija je na svojo osebno izkaznico vključila tudi elektronsko identiteto, ki jo je v skladu z Uredbo 910/2014/EU priglasila za čezmejno e-poslovanje.

Nemčija osebne izkaznice z eID funkcijo in čipom izdaja že 10 let. Posledica sprejema Uredbe bo zgolj sprememba, da bo odvzem prstnih odtisov po novem obvezen (do zdaj je bil namreč neobvezen). Prav tako so predvidene spremembe v oblikovni rešitvi osebne izkaznice zaradi logotipa EU in drugih oznak, ki jih predvideva uredba.

Osebna izkaznica je v prvi vrsti dokument za izkazovanje istovetnosti in državljanstva ter potovalni dokument. Dodatno ima eID funkcijo za spletno izkazovanje identitete.

Nemčija je tako v shemi eID prijavila osebno izkaznico (German identity cards – Personalausweis), ki se izda nemškim državljanom, ki živijo v Nemčiji ali tujini, in dovoljenje za prebivanje (German resident permits – Aufenthaltstitel), ki se izda ljudem, ki živijo v Nemčiji, a niso državljani Evropske unije (če identitete tujca ni mogoče potrditi, se v takem primeru izda dovoljenje za prebivanje brez elektronske identifikacijske funkcije). Nemški državljan ima lahko naenkrat aktivno le eno kartico eID.

Nemško shemo eID neposredno upravlja nemška vlada, zvezno ministrstvo za notranje zadeve je odgovorno za shemo in IT-varnost. Nemška eID temelji na karticah s čipom, ki jih izdaja država (kartice eID), in s certifikati za identifikacijo in kvalificirani elektronski podpis. Na čipu so shranjene vse informacije osebe, vključene v tradicionalno osebno izkaznico, in ključi, ki omogočajo avtentikacijo. Za uporabo eID kartice sta potrebna dvofaktorska avtentikacija, posest kartice in znanje šestmestne kode PIN.

Vloga za pridobitev kartice se poda osebno, če je treba, preko zakonitega zastopnika, in poteka v prostorih lokalnih vladnih služb. Nacionalna osebna izkaznica se pridobi pri organu oziroma uradu za osebno izkaznico oziroma za registracijo rezidentov, kjer ima prosilec prebivališče. Id-sistem upravlja Zvezna republika Nemčija, ki zagotavlja vmesno programsko opremo drugim državam članicam. Nadzorni organ pa je zvezno ministrstvo za notranje zadeve.

Organ, ki izdaja kartico (javni organ) preveri identiteto prosilca in izda nemški eID. Preverjanje istovetnosti se opravi z uradnim dokumentom s fotografijo. Poleg tega lahko organi pri izdaji uporabijo podatke iz svojih registrov za preverjanje istovetnosti. Nemški eID se izda le, če je identiteta prosilca nedvoumno preverjena. Organ, ki kartico izda, potrebne osebne podatke vlagatelja pošlje proizvajalcu kartice eID. Kot del proizvodnje je izdelana tudi številka PIN. Imetnik nemške eID prejme od proizvajalca kartice pismo (številko PIN), ki ga pošilja po pošti na naslov osebe, ki ji pripada eID. Odgovorni organ za izdajo eID pa kartico osebno izda vlagatelju oziroma osebi, ki jo je prosilec odobril za prevzem kartice. Proizvajalec kartic Bundesdruckerei je zasebno podjetje, ki je v celoti v lasti Zvezne republike Nemčije. Bundesdruckerei upravlja certificirani sistem upravljanja informacijske varnosti v skladu z [ISO / IEC 27001].

Uporaba funkcije za elektronsko identifikacijo osebne izkaznice je zakonsko urejena na dveh področjih, in sicer v bančništvu pri odpiranju bančnega računa in na področju telekomunikacij (to je nakup kartice SIM za telefon), oboje zaradi preprečevanja pranja denarja.

Sicer pa se ponudniki različnih storitev sami odločajo, kako preverjajo identiteto svojih strank pri spletnih storitvah. Če se odločijo za preverjanje s pomočjo eID funkcije osebne izkaznice, zato potrebujejo dovoljenje zveznega ministrstva za notranje zadeve. Ob tem so določeni časovna veljavnost podeljenega certifikata in podatki, do katerih ponudnik lahko dostopa.

Aktivacija eID funkcije je sicer mogoča šele z dopolnjenim 16. letom imetnika osebne izkaznice.

V Nemčiji je obvezno imeti vsaj en osebni dokument, bodisi potni list bodisi osebno izkaznico. V praksi je sicer osebna izkaznica zaradi praktičnosti veliko bolj razširjena in verjetnost, da ima nekdo samo potni list, je majhna. Izjema so otroci (do 16. leta), ki sicer lahko imajo osebno izkaznico, vendar večinoma posedujejo tako imenovani otroški potni list.

Obveznosti lastništva osebnega dokumenta (potnega lista ali osebne izkaznice) so lahko oproščene osebe, ki bivajo v domovih za ostarele in ne morejo več skrbeti zase, ali zaporniki; torej osebe, za katere ni predvideno, da bodo spremenile svoj kraj bivanja.

Osebne izkaznice se izdajajo z veljavnostjo 10 let za osebe od dopolnjenega 24. leta starosti in 6 let za osebe, mlajše od 24 let.

Pri (javnem) dostopu do podatkov o veljavnosti osebnih izkaznic je treba ločiti obe funkciji osebne izkaznice. Osebna izkaznica namreč ne izgubi veljavnosti, če je njena funkcija eID neveljavna (na primer če je funkcija eID preklicana ali sploh ni bila aktivirana). Seznam neveljavnih (oziroma blokiranih) identifikacij eID je javno dostopen vsem ponudnikom. Seznam neveljavnih oziroma izgubljenih osebnih izkaznic (kot dokumenta, ki izkazuje državljanstvo, oziroma potovalnega dokumenta) je viden samo preko Interpolove baze; tam lahko za podatke na primer zaprosijo ponudniki letalskih storitev.

Cena osebnih izkaznic je:
– osebna izkaznica z 10-letno veljavnostjo: 28,80 EUR
– osebna izkaznica s šestletno veljavnostjo: 22,80 EUR

Če je vloga vložena zunaj kraja stalnega prebivališča prosilca (bodisi na upravni enoti v drugem kraju v Nemčiji bodisi v tujini), je treba doplačati 13 EUR. 30 EUR pa je treba doplačati tudi za vlogo, vloženo na območju Nemčije, če ima oseba stalno prebivališče v tujini.

Aktivacija funkcije eID osebne izkaznice je ob vlogi oziroma dopolnitvi 16. leta starosti brezplačna. Za poznejšo aktivacijo ali spremembo PIN (v primeru, da ga imetnik pozabi) se plača taksa šest EUR, prav tako za ponovno aktivacijo sicer predhodno preklicane funkcije.

Nemčija bo zaradi spremembe oblikovanja osebnih izkaznic (vezano na sprejem uredbe) z Zvezno tiskarno začela nove pogovore glede nabavne cene osebnih izkaznic, vendar spremembe cen za državljane zaradi tega za zdaj niso predvidene.

Sicer je nabavna cena osebne izkaznice do nedavnega znašala 22,70 EUR, po novem pa znaša 21,70 EUR. Zvezno ministrstvo za notranje zadeve pri Zvezni tiskarni redno preverja, ali cena nabave še ustreza dejanskim stroškom izdelave in dogovorjenemu dobičku tiskarne, zato se nabavna cena lahko spreminja. Pri osebnih izkaznicah s šestletno veljavnostjo je sicer razlika med nabavno ceno in ceno, ki jo plača državljan, tako rekoč neopazna.

V Nemčiji v povprečju na leto izdajo od 7,5 do 8,8 milijona osebnih izkaznic. V obtoku je sicer od 60 do 70 milijonov veljavnih nemških osebnih izkaznic.

Funkcija eID za državljane, ki nimajo stalnega prebivališča v Nemčiji: osebne izkaznice se nemškim državljanom, ki živijo v tujini, izdajajo brez navedbe naslov oziroma z zaznambo na osebni izkaznici "brez stalnega prebivališča v Nemčiji". Večina ponudnikov eID sicer storitve pogojuje s preverjanjem naslova, kar tistim, ki živijo v tujini, preprečujejo uporabo funkcije eID osebne izkaznice. V prihodnje bo sicer mogoče na osebno izkaznico vpisati tudi naslov v tujini.

Funkcija eID za državljane tretjih držav: lahko se aktivira z izdanim dovoljenjem za prebivanje v Nemčiji.

Funkcija za državljane držav članic EU: uporaba storitev je državljanom EU za zdaj onemogočena (na primer slovenski državljan, ki živi in dela v Nemčiji, ne more z uporabo funkcije eID oddati davčne napovedi). V pripravi je možnost, da bi se državljanom DČ EU na zaprosilo izdala "bianko" izkaznica s to funkcijo, vendar se s tem čaka, da bodo vse DČ EU implementirale uredbo 910/2014/EU. Te bianko izkaznice bodo predvidoma na voljo od jeseni 2020.

Funkcija eID osebne izkaznice ne omogoča samodejnega elektronskega podpisovanja dokumenta (na primer pri elektronskem vročanju): da bi bila ta funkcija omogočena, je treba pridobiti dodatni certifikat, ki se naloži na osebno izkaznico.

5.8 Nizozemska

Nizozemska je priglasila svoj sistem "Trust Framework for Electronic Identification", ki zajema rešitve za srednjo in visoko raven zanesljivosti.

Nizozemski skrbniški okvir za elektronsko identifikacijo je enoten sveženj standardov, sporazumov in določb za dovoljeni dostop do digitalnih storitev. Področje poslovanja nizozemskega eID, znanega kot eHerkenning, je prva priglašena shema za pravne osebe v okviru 910/2014/EU. Predstavniki poslovnih ali javnih služb, ki so prejeli posebno pooblastilo, ga uporabljajo za dostop do spletnih storitev v imenu svoje organizacije in za popolnoma varno upravljanje svojih transakcij z vlado. Uporabijo lahko prijavni žeton, predhodno pridobljen od številnih pooblaščenih ponudnikov storitev. Žetoni so lahko v obliki imena/gesla, pošiljanja sporočil SMS, telefona, enkratnega gesla (OPT) ali potrdila javnega ključa.

Shema predstavlja javno-zasebno partnerstvo med ministrstvom za notranje zadeve in kraljevske odnose ter različnimi akreditiranimi zasebnimi "ponudniki identitet". V okviru sistema "Trust Framework for Electronic Identification" različni akreditirani zasebni ponudniki ponujajo storitve kot del omrežja z uporabo blagovne znamke imena eHerkenning (ali "eRecognition") za podjetja in Idensys za državljane. Sistem omogoča uporabnikom, da potrdijo svojo identiteto in pooblastilo. To uporabnikom omogoča samostojno opravljanje transakcij v imenu ali v imenu

organizacije, medtem ko je vlada lahko prepričana, da je uporabnik tisti, za katerega trdi, da je, in da je ta oseba pooblaščena za opravljanje storitev.

5.9 Slovaška

Slovaška je priglasila svojo e-osebno izkaznico visoke ravni zanesljivosti.

Slovaška republika izdaja dve vrsti kartic eID:

- kartica eID – elektronska izkaznica za državljane, izdana slovaškim državljanom pri starosti 15 let in več,
- kartica ePR – elektronska prebivališča, izdana tujim državljanom s prebivališčem v Slovaški republiki.

Slovaške eID izda Ministrstvo za notranje zadeve Slovaške republike s pomočjo naslednjih organizacijskih enot Policijske vojske Slovaške republike:

- Oddelek za dokumente in evidence predsedstva policijskih sil izdaja kartice eID na okrožnih direktoratih Policijskih sil Slovaške republike,
- obmejni in tujci na predsedstvu policijskih sil izdajajo kartice eRP v oddelkih za tujce Policije Policijske vojske,
- obe vrsti eID uporabljata enak mehanizem EAC v.1, ki je implementiran na isti strojni platformi, certificiran kontaktni čip Infineon SLE78CFX3000P, vgrajen v polikarbonatno kartico formata ID-1, in uporabljata identični certificirani matični operacijski sistem čipa ATOS CardOS v. 5.0.

6. PRESOJA POSLEDIC, KI JIH BO IMEL SPREJEM ZAKONA

6.1 Presoja administrativnih posledic

a) v postopkih oziroma poslovanju javne uprave ali pravosodnih organov:

Predlog zakona določa, da z osebno elektronsko identiteto fizična oseba izkazuje svojo istovetnost pri elektronskem poslovanju, osebno elektronsko identiteto pa pridobi oseba s pridobitvijo prvega sredstva elektronske identifikacije. Nova osebna biometrična izkaznica bo ena izmed nosilk sredstev elektronske identifikacije ter bo, kadar bo vlogo vložil državljan po dopolnjenem 12. letu starosti, vsebovala tudi kvalificirano potrdilo za elektronski podpis, zato je glede na število imetnikov osebnih izkaznic pričakovati dolgoročno izredno dobro pokritost državljanov z nacionalnim nosilcem elektronske identitete. Poleg tega bo elektronsko identiteto lahko pridobil tudi tujec, ki ima v Republiki Sloveniji prijavljeno stalno ali začasno prebivališče. Vse skupaj pa bo vplivalo tudi na povečano uporabo storitev javne uprave, ki temelji na elektronski identifikaciji in uporabi vseh novih, temu prilagojenih storitev. Spodbuja pa se tudi uporaba informacijske rešitve za uporabo elektronske identifikacije s strani ponudnikov elektronskih storitev.

b) pri obveznostih strank do javne uprave ali pravosodnih organov:

Predlog zakona ne bo imel posledic na tem področju.

6.2 Presoja posledic za okolje, vključno s prostorskimi in varstvenimi vidiki:

Predlog zakona ne bo imel posledic za okolje.

6.3 Presoja posledic za gospodarstvo:

Centralna storitev za spletno prijavo in elektronski podpis bo na voljo tudi zasebnemu sektorju (storitev, ki omogoča, da informacijski sistemi gospodarskih subjektov uporabijo centralno storitev pri preverjanju veljavnosti posameznega elektronskega identifikacijskega sredstva posameznika). S tem se zagotovi široka uporaba izdanih sredstev elektronske identifikacije tako v javnem kakor tudi zasebnem sektorju, zaradi poenotenja poslovanja ponudnikov e-storitev s svojimi uporabniki/komitenti pa se povečuje možnost digitalizacije vseh postopkov poslovanja s posamezniki v Republiki Sloveniji. Zaradi uporabe enotne platforme gospodarskim subjektom ne bo več treba vlagati v ločene specifične rešitve za identifikacijo in avtentikacijo svojih uporabnikov oziroma strank pri e-poslovanju, s čimer se razbremenijo tako tehnološko kakor tudi finančno. Zasebni sektor bo tako lahko prostovoljno uporabljal informacijske rešitve za uporabo sredstva elektronske identifikacije za identifikacijo uporabnikov pri vseh e-storitvah, kadar je to potrebno za izvedbo storitve ali elektronske transakcije. Možnost uporabe takšnih sredstev elektronske identifikacije s strani zasebnega sektorja bo zasebnemu sektorju omogočila uporabo elektronske identifikacije in avtentikacije, ki se v številnih državah članicah že uporabljata vsaj za javne storitve; podjetja in državljani pa bi tako imeli lažji dostop do čezmejnih spletnih storitev. S tem bo zasebni sektor močno razbremenjen postopkov fizične identifikacije strank oziroma uporabnikov njihovih storitev ter s tem povezanih finančno-kadrovskih bremen, saj bo preverjanje pristnosti identitete posameznika pri vseh poslih lahko potekalo elektronsko z uporabo sredstva elektronske identifikacije. Hkrati bosta zato zasebnemu sektorju omogočena razvoj novih in nadgradnja obstoječih inovativnih elektronskih storitev v primerih, ko so ta še bila vezane na potrebo po fizični prisotnosti uporabnika za preverjanje njegove identifikacije.

Dodana vrednost predloga zakona za ponudnike kvalificiranih storitev zaupanja pa je možnost brezplačne pridobitve ali preverjanja podatkov v verodostojnem viru za identifikacijo ob izdaji kvalificiranih potrdil.

6.4 Presoja posledic za socialno področje:

Predlog zakona odpira široke možnosti za nadaljnji razvoj elektronskega poslovanja, ki ga v zadnjem času povezujemo predvsem z izrazoma privzeto digitalno poslovanje in digitalna transformacija poslovnih, upravnih procesov oziroma postopkov. Z zagotovitvijo skupnega temelja za varne elektronske interakcije med državljani, podjetji in javnimi organi se bo posledično povečala učinkovitost javnih in zasebnih spletnih storitev, elektronskega poslovanja ter elektronskega trgovanja v Republiki Sloveniji. Zagotovil se bo tudi temelj za široko uporabo elektronske identitete (možnost elektronske identitete na več sredstvih elektronske identifikacije, ena izmed nosilk bo tudi nova biometrična osebna izkaznica, ki je dokument, ki

ga ima 1,8 milijona državljanov), zaradi poenotenja poslovanja posameznikov pa se bo dvignila stopnja digitalizacije v Republiki Sloveniji.

Vzajemno priznana sredstva elektronske identifikacije bodo tako poenostavila čezmejno zagotavljanje številnih storitev na notranjem trgu in podjetjem omogočila čezmejno poslovanje z velikim zmanjšanjem ovir pri interakciji z javnimi organi, hkrati pa bodo storitve za avtentikacijo spletišč obiskovalcu spletišča dala zagotovilo, da za tem spletiščem stoji pristen in legitimen subjekt. Z določanjem minimalne obveznosti glede varnosti in odgovornosti za ponudnike in njihove storitve pa se bodo krepili zaupanje in zagotavljanje boljše izkušnje uporabnikov ter spodbujanje rasti na notranjem trgu.

6.5 Presoja posledic za dokumente razvojnega načrtovanja:

Predlog zakona ne bo imel posledic za dokumente razvojnega načrtovanja.

6.6 Presoja posledic za druga področja:

Predlog zakona ne bo imel posledic za druga področja.

6.7 Izvajanje sprejetega predpisa:

Ministrstvo za javno upravo bo spremljalo izvajanje sprejetega predpisa s pomočjo odzivov izvajalcev zakona, uporabnikov sredstev elektronske identifikacije (npr. osebnih izkaznic, SMS-PASS) ter uporabnikov storitev zaupanja.

Predlog zakona na področju elektronske identifikacije pa bo posredno v okviru novele Zakona o osebni izkaznici predstavljen tudi ciljnim skupinam, to je uradnim osebam, pristojnim za izdajo osebnih izkaznic na upravnih enotah in diplomatskih predstavništvih in konzulatih Republike Slovenije v tujini, v obliki usmeritev in navodil. Ministrstvu za javno upravo bo kot ministrstvu, pristojnemu za centralno storitev za spletno prijavo in elektronski podpis, z novelo Zakona o osebni izkaznici dana pristojnost, da ima v okviru nadzora pravico vpogleda v dokumentacijo, ki se nanaša na postopke izdelave, personalizacije in skladiščenja obrazcev osebnih izkaznic, njihovega prenosa, prostore, v katerih potekajo njihova izdelava, personalizacija in skladiščenje, ter preverja, ali osebe, ki opravljajo te naloge, izpolnjujejo pogoje, kakršne določajo predpisi, ki urejajo elektronsko identifikacijo in elektronski predpis.

6.8 Druge pomembne okoliščine v zvezi z vprašanji, ki jih ureja predlog zakona:

/

7. PRIKAZ SODELOVANJA JAVNOSTI PRI PRIPRAVI PREDLOGA ZAKONA:

Predlog zakona je bil objavljen na državnem portalu eUprava, podportalu e-demokracija, 26. februarja 2020. Na predlog zakona se je odzivala zainteresirana javnost. Mnenja, predlogi in pripombe, ki so jih podali Združenje za informatiko in telekomunikacije (v okviru Gospodarske zbornice Slovenije), Združenje bank Slovenije in Slovensko združenje za e-identifikacijo in e-

storitve zaupanja, podjetje EIUS, d. o. o., ter Notarska zbornica Slovenije, so bili delno upoštevani.

8. PODATEK O ZUNANJEM STROKOVNJAKU OZIROMA PRAVNI OSEBI, KI JE SODELOVALA PRI PRIPRAVI PREDLOGA ZAKONA, IN ZNESKU PLAČILA ZA TA NAMEN:

Pri pripravi predloga zakona niso sodelovali zunanji strokovnjaki ali pravne osebe, ki bi za svoje sodelovanje prejeli plačilo.

9. NAVEDBA, KATERI PREDSTAVNIKI PREDLAGATELJA BODO SODELOVALI PRI DELU DRŽAVNEGA ZBORA IN DELOVNIH TELES

- Boštjan Koritnik, minister;
- mag. Peter Geršak, državni sekretar;
- Peter Jenko, sekretar, v.d. generalnega direktorja Direktorata za informacijsko družbo,
- dr. Polonca Blaznik, sekretarka, Direktorat za informacijsko družbo.

II. BESEDILO ČLENOV

1. SPLOŠNE DOLOČBE

1. člen
(vsebina in namen zakona)

(1) Ta zakon ureja osebno elektronsko identiteto, ki jo dodeli Republika Slovenija, in sredstva elektronske identifikacije, s katerimi se dokazuje ta elektronska identiteta, ter na tej elektronski identiteti temelječo shemo elektronske identifikacije v skladu z zahtevami iz Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (UL L št. 257 z dne 28. 8. 2014, str. 73, v nadaljnjem besedilu: Uredba 910/2014/EU) za priglasitev shem elektronske identifikacije.

(2) Ta zakon ureja storitve zaupanja v delu, kjer Uredba 910/2014/EU to omogoča.

2. člen
(pomen izrazov)

Izrazi, uporabljeni v tem zakonu, pomenijo:

1. podatki v elektronski obliki so podatki, ki so elektronsko oblikovani, shranjeni, poslani, prejeti ali izmenljivi;
2. informacijski sistem je programska, strojna, komunikacijska oziroma druga oprema, ki deluje samostojno ali v omrežju in je namenjena zbiranju, procesiranju, distribuciji, uporabi in drugi obdelavi podatkov v elektronski obliki;
3. organ javnega sektorja po tem zakonu je državni organ, organ samoupravne lokalne skupnosti, javna agencija, javni sklad, javni zavod ali druga oseba javnega prava, nosilec javnega pooblastila ali izvajalec javne službe;
4. osebna elektronska identiteta je niz identifikacijskih podatkov fizične osebe, ki jih država dodeli za uporabo pri elektronskem poslovanju;
5. kvalificirano potrdilo je kvalificirano potrdilo za elektronski podpis, kvalificirano potrdilo za elektronski žig ali kvalificirano potrdilo za avtentikacijo spletišč;
6. nacionalni zanesljivi seznam je zanesljivi seznam ponudnikov kvalificiranih storitev zaupanja v Republiki Sloveniji v skladu z 22. členom Uredbe 910/2014/EU;
7. ponudnik kvalificiranih storitev zaupanja, registriran v Republiki Sloveniji, je ponudnik kvalificiranih storitev zaupanja, ki je vpisan v nacionalni zanesljivi seznam ponudnikov kvalificiranih storitev zaupanja v Republiki Sloveniji;
8. nosilec sredstva elektronske identifikacije je strojna oziroma programska oprema, ki imetniku omogoča hrambo in uporabo sredstva elektronske identifikacije za namene elektronske identifikacije.

3. člen
(enotna številka elektronske identifikacije)

(1) Enotna številka elektronske identifikacije (v nadaljnjem besedilu: EŠEI) je enolični identifikator fizične osebe, fizične osebe z dejavnostjo ali pravne osebe pri elektronskem poslovanju.

(2) EŠEI se lahko določi imetnikom iz prejšnjega odstavka, ki so vpisani v davčni register.

(3) EŠEI je sestavljen:
– za fizično osebo iz številke 11 in davčne številke fizične osebe,
– za poslovni subjekt iz številke 21 in davčne številke poslovnega subjekta.

(4) Za zagotavljanje čezmejnega elektronskega poslovanja v skladu z Uredbo 910/2014/EU se uporablja enolični identifikator, ki se preračuna iz EŠEI. Vlada z uredbo določi obliko preračunane številke in način preračunavanja.

4. člen
(skrbnost ravnanja imetnika)

(1) Imetnik sredstva elektronske identifikacije mora sredstvo uporabljati osebno in s skrbnostjo dobrega gospodarja.

(2) Imetnik kvalificiranega potrdila mora podatke, ki so potrebni za njegovo uporabo, hraniti s skrbnostjo dobrega gospodarja ali gospodarstvenika in storitve zaupanja uporabljati v skladu z veljavnimi predpisi.

2. OSEBNA ELEKTRONSKA IDENTITETA IN SREDSTVA ELEKTRONSKE IDENTIFIKACIJE

5. člen
(osebna elektronska identiteta)

(1) Z osebno elektronsko identiteto fizična oseba izkazuje svojo istovetnost pri elektronskem poslovanju.

(2) Osebno elektronsko identiteto pridobi oseba s pridobitvijo prvega sredstva elektronske identifikacije.

(3) Oseba ima eno osebno elektronsko identiteto, ki jo lahko dokazuje z več sredstvi elektronske identifikacije.

(4) Osebno elektronsko identiteto lahko pridobi oseba, ki dopolni šest let, in preneha ob smrti osebe ali izgubi statusa osebe, ki je podlaga za pridobitev osebne elektronske identitete.

(5) Osebno elektronsko identiteto lahko pridobi državljan Republike Slovenije (v nadaljnjem besedilu: državljan).

(6) Osebno elektronsko identiteto lahko pridobi tujec, ki ima v Republiki Sloveniji prijavljeno stalno ali začasno prebivališče.

6. člen
(sredstva elektronske identifikacije za osebno elektronsko identiteto)

(1) Vlada z uredbo glede na nosilec sredstva elektronske identifikacije in predpise, ki slednjega določajo, predpiše sredstva elektronske identifikacije, ki so izdana z namenom dokazovanja osebne elektronske identitete iz prejšnjega člena, njihovo obliko, raven zanesljivosti, obdobje veljavnosti, najnižjo starost, pri kateri oseba lahko pridobi sredstvo elektronske identifikacije, organe, pristojne za sprejem vlog in preverjanje istovetnosti, način izdaje, preklica in začasne razveljavitve ter tehnične specifikacije posameznega sredstva elektronske identifikacije.

(2) Vlada z uredbo določi tudi morebitni namen čezmejne uporabe posameznega sredstva elektronske identifikacije.

7. člen
(ravni zanesljivosti sredstev elektronske identifikacije)

Ravni zanesljivosti in zahteve za določanje ravni zanesljivosti, kot so določene v Uredbi 910/2014/EU in njenih izvedbenih aktih za sredstva elektronske identifikacije, se uporabljajo tudi za določanje ravni zanesljivosti sredstev elektronske identifikacije na državni ravni.

8. člen
(obdobje veljavnosti sredstva elektronske identifikacije)

Sredstvo elektronske identifikacije velja največ deset let od dneva njegove izdaje.

9. člen
(izdajatelj sredstva elektronske identifikacije)

(1) Izdajatelj sredstva elektronske identifikacije je ministrstvo, pristojno za centralno storitev za spletno prijavo in elektronski podpis.

(2) Izdajatelj sredstva elektronske identifikacije ima pravico vpogleda v dokumentacijo, ki jo za potrebe izdaje, preklica in začasne razveljavitve sredstva elektronske identifikacije hranijo organi, pristojni za sprejem vlog in preverjanje istovetnosti.

10. člen
(identifikacija fizične osebe ob izdaji sredstva elektronske identifikacije)

(1) Za izdajo sredstva elektronske identifikacije:

a) nizke ravni zanesljivosti izdajatelj sredstva elektronske identifikacije izvede:
– preverjanje istovetnosti fizične osebe na podlagi veljavne javne listine ter s fizično prisotnostjo fizične osebe, ki se identificira,
– preverjanje istovetnosti fizične osebe na podlagi podatkov, ki jih ima izdajatelj na voljo in ki s precej veliko verjetnostjo potrjujejo istovetnost fizične osebe,
– preverjanje istovetnosti fizične osebe na podlagi veljavne javne listine ter s potrditvijo istovetnosti fizične osebe, ki se identificira, z uporabo informacijskih tehnologij ali
– avtentikacijo fizične osebe na podlagi sredstva elektronske identifikacije najmanj nizke ravni zanesljivosti;
b) srednje ravni zanesljivosti izdajatelj sredstva elektronske identifikacije izvede:
– preverjanje istovetnosti fizične osebe na podlagi veljavne javne listine, ki je opremljena s fotografijo, ter s fizično prisotnostjo fizične osebe, ki se identificira, ali
– avtentikacijo fizične osebe na podlagi sredstva elektronske identifikacije najmanj srednje ravni zanesljivosti;
c) visoke ravni zanesljivosti izdajatelj sredstva elektronske identifikacije izvede:
– preverjanje istovetnosti fizične osebe na podlagi veljavne javne listine, ki je opremljena s fotografijo, in preverjanja pristnosti in veljavnosti javne listine v javnih evidencah ter s fizično prisotnostjo fizične osebe, ki se identificira, ali
– avtentikacijo fizične osebe na podlagi sredstva elektronske identifikacije visoke ravni zanesljivosti.

(2) Če fizična oseba nima veljavne javne listine, ki bi ji omogočala identifikacijo za pridobitev sredstva elektronske identifikacije v skladu s prejšnjim odstavkom, je njeno istovetnost mogoče preveriti tako, kot to omogoča kateri od predpisov, na podlagi katerih fizična oseba v Republiki Sloveniji lahko pridobi javno listino, ki jo je mogoče uporabiti za prehod državne meje.

11. člen
(evidenca imetnikov sredstev elektronske identifikacije)

(1) Izdajatelj sredstva elektronske identifikacije vodi evidenco imetnikov sredstev elektronske identifikacije za vsako sredstvo elektronske identifikacije posebej.

(2) Evidenca imetnikov sredstev elektronske identifikacije vsebuje podatke:
1. identifikacijsko oznako sredstva elektronske identifikacije;
2. identifikacijsko oznako nosilca sredstva elektronske identifikacije;
3. osebno ime imetnika;
4. vrsto in številko veljavne javne listine imetnika, opremljene s fotografijo, ki jo je izdal državni organ, oziroma navedbo postopka, s katerim je bila opravljena identifikacija imetnika;
5. EŠEI imetnika;
6. davčno številko imetnika;
7. EMŠO imetnika;
8. stalno prebivališče ali stalni naslov v tujini, začasno prebivališče ali začasni naslov v tujini in naslov za vročanje, če je to potrebno za pridobitev sredstva elektronske identifikacije;

9. telefonsko številko imetnika, če jo imetnik posreduje ali če je to potrebno za pridobitev ali uporabo sredstva elektronske identifikacije;
10. naslov elektronske pošte imetnika, če ga imetnik posreduje ali če je to potrebno za pridobitev ali uporabo sredstva elektronske identifikacije;
11. status sredstva elektronske identifikacije;
12. obdobje veljavnosti sredstva elektronske identifikacije;
13. obdobje začasne razveljavitve sredstva elektronske identifikacije;
14. datum preklica sredstva elektronske identifikacije.

(3) Če je tehnično mogoče izdati in uporabljati sredstvo elektronske identifikacije tako, da se za to ne potrebuje določenih podatkov iz prejšnjega odstavka, vlada z uredbo določi manjši nabor podatkov posamezne evidence imetnikov sredstev elektronske identifikacije.

(4) Evidenca imetnikov sredstev elektronske identifikacije se na podlagi EMŠO ali davčne številke povezuje s centralnim registrom prebivalstva. Iz centralnega registra prebivalstva se v evidenco sredstev elektronske identifikacije pošljejo podatki o davčni številki ali EMŠO, osebnem imenu, stalnem prebivališču ali stalnem naslovu v tujini, začasnem prebivališču ali začasnem naslovu v tujini in naslovu za vročanje, državljanstvu in datumu smrti posameznika.

(5) Podatki iz prejšnjega odstavka se iz centralnega registra prebivalstva v evidenco sredstev elektronske identifikacije pošljejo ob sprejemu vloge in ob vsaki spremembi navedenih podatkov v centralnem registru prebivalstva.

(6) Podatki se hranijo deset let po koncu veljavnosti sredstva elektronske identifikacije.

(7) EMŠO imetnika se po izvedeni povezavi iz četrtega odstavka tega člena in po izračunu starosti imetnika, na podlagi katere se ugotovi upravičenost do sredstva elektronske identifikacije, izbriše iz evidence.

(8) Če se izda sredstvo elektronske identifikacije v skladu s prvo alinejo točke c prvega odstavka 10. člena tega zakona, se evidenca imetnikov sredstev elektronske identifikacije povezuje z uradnimi evidencami iz prve alineje točke c prvega odstavka 10. člena tega zakona tako, da se na podlagi vrste in številke javne listine v evidenco imetnikov sredstev elektronske identifikacije na posamezno zahtevo organa za sprejem vloge prenesejo podatki o tem, ali je javna listina veljavna.

12. člen
(podatki na sredstvu elektronske identifikacije)

(1) Sredstvo elektronske identifikacije vsebuje naslednje podatke:
1. podatke, ki nedvoumno predstavljajo izdajatelja sredstva elektronske identifikacije;
2. osebno ime imetnika,
3. identifikacijsko oznako sredstva elektronske identifikacije.

(2) Sredstvo elektronske identifikacije vsebuje tudi podatke o času veljavnosti sredstva elektronske identifikacije in podatke, s katerimi je mogoče preveriti veljavnost tega sredstva, če je to tehnično potrebno za uporabo sredstva elektronske identifikacije.

(3) Če je tehnično mogoče izdati sredstvo elektronske identifikacije tako, da za to niso potrebni določeni podatki iz prvega odstavka tega člena, vlada z uredbo določi, da posamezno sredstvo elektronske identifikacije nekaterih podatkov ne vsebuje.

13. člen
(uporaba sredstva elektronske identifikacije)

(1) Informacijska rešitev za uporabo sredstev elektronske identifikacije je informacijska rešitev, ki omogoča avtentikacijo uporabnika in preverjanje veljavnosti sredstva elektronske identifikacije.

(2) Izdajatelj sredstva elektronske identifikacije zagotavlja ponudnikom elektronskih storitev, registriranim v Republiki Sloveniji, možnost uporabe informacijske rešitve za uporabo sredstev elektronske identifikacije iz 6. člena tega zakona ter možnost preverjanja EŠEI na podlagi identifikacijske oznake sredstva elektronske identifikacije.

(3) Izdajatelj sredstva elektronske identifikacije zagotavlja ponudnikom elektronskih storitev v organih javnega sektorja tudi možnost pridobivanja EŠEI na podlagi identifikacijske oznake sredstva elektronske identifikacije.

14. člen
(sredstvo elektronske identifikacije za dostop do elektronskih storitev v javnem sektorju)

(1) Organ javnega sektorja, ki za dostop do svoje elektronske storitve in njeno uporabo zahteva uporabo sredstev elektronske identifikacije srednje ali visoke ravni zanesljivosti, v ta namen prizna sredstva elektronske identifikacije ravni zanesljivosti, ki je enaka ali višja od zahtevane ravni zanesljivosti.

(2) Pred uporabo sredstva elektronske identifikacije srednje ali visoke ravni zanesljivosti mora vsak organ javnega sektorja v sistemu za samodejno strojno preverjanje veljavnosti sredstva elektronske identifikacije preveriti veljavnost sredstva elektronske identifikacije ali drugače zagotoviti, da se uporablja veljavno sredstvo elektronske identifikacije.

15. člen
(zahtevana raven zanesljivosti sredstva elektronske identifikacije za dostop do elektronskih storitev v javnem sektorju)

(1) Organ javnega sektorja za dostop in uporabo posamezne elektronske storitve iz prejšnjega člena določi raven zanesljivosti v skladu s 7. členom tega zakona.

(2) Raven zanesljivosti iz prejšnjega odstavka se določi na podlagi ocene tveganja, da identiteta uporabnika, ki dostopa do elektronske storitve in jo uporablja, ni enaka identiteti, ki se izkazuje pri dostopu do storitve. Slednje temelji na:
– oceni verjetnosti pojavitve neželenih varnostnih dogodkov, povezanih z uporabo sredstva elektronske identifikacije;
– oceni vrste in obsega povzročene škode in drugih morebitnih nezaželenih posledic in

– oceni obsega dejavnosti in stroškov, potrebnih za odpravo nezaželenih posledic.

(3) Ocena tveganja se ocenjuje na podlagi naslednjih meril:
1. pravne posledice nepravilnosti in zlorabe,
2. pravne zahteve za raven zanesljivosti e-storitve,
3. vrst obdelave osebnih podatkov,
4. vrsta obdelave podatkov iz registrov identifikacijskih podatkov,
5. gospodarska škoda,
6. vpliv na javni interes in
7. vpliv na osebno varnost.

(4) Podrobnejšo specifikacijo uporabe meril in načina določanja ravni zanesljivosti določi vlada z uredbo.

16. člen
(obdelava in varstvo podatkov pri elektronskih storitvah v javnem sektorju)

(1) Organ javnega sektorja lahko za namene elektronske identifikacije, avtentikacije ali preverjanja identifikacijskih podatkov fizične osebe hrani in obdeluje identifikacijsko oznako sredstva elektronske identifikacije.

(2) Organ javnega sektorja, ki ima za zagotavljanje elektronskih storitev pravico hraniti in obdelovati osebno ime fizične osebe, lahko za namen elektronske identifikacije, avtentikacije ali preverjanja identifikacijskih podatkov fizične osebe hrani in obdeluje tudi EŠEI fizične osebe.

(3) Če fizična oseba nima EŠEI, lahko organ uporabi za namene iz prejšnjega odstavka najmanjši nabor drugih identifikacijskih podatkov iz minimalnega nabora podatkov za fizično osebo, kot jih določa Izvedbena uredba Komisije (EU) 2015/1501 z dne 8. septembra 2015 o interoperabilnostnem okviru v skladu s členom 12(8) Uredbe 910/2014/EU, ki še vedno omogočajo doseganje istega namena.

17. člen
(preklic sredstva elektronske identifikacije)

(1) Izdajatelj sredstva elektronske identifikacije prekliče sredstvo elektronske identifikacije takoj oziroma v najpozneje v 24 urah:
1. po prejemu zahtevka, če preklic sredstva elektronske identifikacije zahteva imetnik sredstva elektronske identifikacije pri izdajatelju;
2. ko izdajatelj izve, da je imetnik sredstva elektronske identifikacije umrl;
3. ko izdajatelj izve, da so se spremenile okoliščine, ki so bistvene za veljavnost sredstva elektronske identifikacije;
4. ko izdajatelj izve, da je podatek v sredstvu elektronske identifikacije ali evidenci sredstev elektronske identifikacije, ki vpliva na veljavnost oziroma raven zanesljivosti sredstva elektronske identifikacije, spremenjen ali napačen ali je bilo sredstvo elektronske identifikacije izdano na podlagi napačnih podatkov;

5. ko izdajatelj izve, da so bili podatki, nosilec sredstva elektronske identifikacije, naprave ali informacijski sistem izdajatelja sredstva elektronske identifikacije tako ogroženi, da to vpliva na raven zanesljivosti sredstva elektronske identifikacije;
6. ko izdajatelj izve, da so bili podatki, nosilec sredstva elektronske identifikacije, naprave ali informacijski sistem imetnika sredstva elektronske identifikacije tako ogroženi, da to vpliva na raven zanesljivosti sredstva elektronske identifikacije, in je izdajatelj sredstva elektronske identifikacije s tem seznanjen:
7. ko izdajatelj izve, da je preklic odredilo pristojno sodišče, sodnik za prekrške, upravni organ ali nadzorni organ za elektronsko identifikacijo; ali
8. ko izdajatelj izve, da je nosilec sredstva elektronske identifikacije neveljaven, izgubljen, odtujen ali ogrožen tako, da vpliva na veljavnost oziroma raven zanesljivosti sredstva elektronske identifikacije.

(2) Po preklicu izdajatelj sredstva elektronske identifikacije onemogoči nadaljnjo uporabo tega sredstva oziroma zagotovi informacijo o preklicu v svojem sistemu za samodejno strojno preverjanje veljavnosti sredstva elektronske identifikacije.

(3) Izdajatelj sredstva elektronske identifikacije mora najpozneje v 24 urah obvestiti imetnika preklicanega sredstva elektronske identifikacije, razen v primeru iz druge točke prvega odstavka tega člena. Podatke o preklicu posreduje tretji osebi, ki jih zahteva, ali jih javno objavi.

18. člen
(dolžnosti imetnikov glede preklica sredstev elektronske identifikacije)

Imetnik sredstva elektronske identifikacije zahteva preklic svojega sredstva elektronske identifikacije, če:
– so bili podatki, nosilec sredstva elektronske identifikacije, naprave ali informacijski sistem imetnika sredstva elektronske identifikacije spremenjeni, izgubljeni, odtujeni ali ogroženi tako, da to vpliva na veljavnost oziroma raven zanesljivosti sredstva elektronske identifikacije, ali če obstaja nevarnost zlorabe, ali če
– so se spremenili podatki, ki so navedeni v sredstvu elektronske identifikacije ali v evidenci sredstev elektronske identifikacije, ki vplivajo na veljavnost oziroma raven zanesljivosti sredstva elektronske identifikacije.

19. člen
(učinek preklica sredstva elektronske identifikacije)

(1) Preklic sredstva elektronske identifikacije učinkuje med imetnikom sredstva elektronske identifikacije in izdajateljem sredstva elektronske identifikacije od trenutka preklica dalje.

(2) Preklic sredstva elektronske identifikacije učinkuje med tretjimi osebami in izdajateljem sredstva elektronske identifikacije od trenutka objave, ali če preklic še ni javno objavljen, od trenutka, ko tretje osebe izvedo zanj.

(3) Čas preklica se evidentira v evidenci sredstev elektronske identifikacije.

20. člen
(začasna razveljavitev sredstva elektronske identifikacije)

(1) Začasna razveljavitev sredstva elektronske identifikacije pomeni neveljavnost tega sredstva v obdobju njegove razveljavitve.

(2) Začasna razveljavitev se izvede le na podlagi izrecne zahteve imetnika sredstva elektronske identifikacije.

(3) Začasna razveljavitev lahko traja največ 48 ur. Če imetnik v tem roku ne zahteva vzpostavitve veljavnosti sredstva elektronske identifikacije, izdajatelj prekliče to sredstvo.

(4) Izdajatelj sredstva elektronske identifikacije posreduje podatke o začasni razveljavitvi tretji osebi, ki jih zahteva, ali jih javno objavi. Pri tem mora biti jasno razvidno, da gre za začasno razveljavitev.

(5) Izdajatelj sredstva elektronske identifikacije pri ureditvi začasne razveljavitve smiselno upošteva določila tega zakona, ki se nanašajo na preklic sredstva elektronske identifikacije.

21. člen
(priglasitev sheme elektronske identifikacije)

Organ, pristojen za priglasitev shem elektronske identifikacije, kot sheme elektronske identifikacije priglasi tista sredstva elektronske identifikacije, za katera je določen namen čezmejne uporabe.

3. STORITVE ZAUPANJA

22. člen
(začetek zagotavljanja nekvalificirane storitve zaupanja)

(1) Ponudniki kvalificiranih storitev zaupanja pred začetkom zagotavljanja nekvalificirane storitve zaupanja obvestijo nadzorni organ za storitve zaupanja, in sicer najmanj osem dni pred začetkom izvajanja te storitve.

(2) Nadzorni organ uvrsti storitev zaupanja na seznam nekvalificiranih storitev zaupanja.

23. člen
(oprema za zagotavljanje nekvalificirane storitve zaupanja)

Če ponudnik storitev zaupanja za izvajanje nekvalificiranih storitev zaupanja uporablja strojno oziroma programsko opremo, ki se uporablja tudi za izvajanje kvalificiranih storitev zaupanja, mora ponudnik na tej strojni oziroma programski opremi izvajati postopke v skladu z zahtevami za kvalificirano storitev zaupanja.

24. člen
(uporaba EŠEI pri kvalificiranih potrdilih)

(1) Če je fizični osebi mogoče določiti EŠEI, kvalificirano potrdilo za elektronski podpis poleg podatkov iz Priloge I Uredbe 910/2014/EU vsebuje tudi:
– EŠEI imetnika,
– podatke za dostop do storitve za pridobivanje EŠEI imetnika na podlagi identifikacijskih podatkov kvalificiranega potrdila za elektronski podpis ali
– podatke za dostop do storitve za preverjanje EŠEI imetnika na podlagi identifikacijskih podatkov kvalificiranega potrdila za elektronski podpis.

(2) Če je poslovnemu subjektu mogoče določiti EŠEI, kvalificirano potrdilo za elektronski podpis, ki se izdaja za fizično osebo pri poslovnem subjektu, poleg podatkov iz prvega odstavka tega člena vsebuje tudi:
– EŠEI poslovnega subjekta,
– podatke za dostop do storitve za pridobivanje EŠEI poslovnega subjekta na podlagi identifikacijskih podatkov kvalificiranega potrdila za elektronski podpis ali
– podatke za dostop do storitve za preverjanje EŠEI poslovnega subjekta na podlagi identifikacijskih podatkov kvalificiranega potrdila za elektronski podpis.

(3) Če je poslovnemu subjektu mogoče določiti EŠEI, kvalificirano potrdilo za elektronski žig poleg podatkov iz Priloge III Uredbe 910/2014/EU vsebuje tudi:
– EŠEI poslovnega subjekta,
– podatke za dostop do storitve za pridobivanje EŠEI poslovnega subjekta na podlagi identifikacijskih podatkov kvalificiranega potrdila za elektronski žig ali
– podatke za dostop do storitve za preverjanje EŠEI poslovnega subjekta na podlagi identifikacijskih podatkov kvalificiranega potrdila za elektronski žig.

(4) Če je fizični osebi ali poslovnemu subjektu mogoče določiti EŠEI, kvalificirano potrdilo za avtentikacijo spletišč poleg podatkov iz Priloge IV, Uredbe 910/2014/EU vsebuje tudi:
- EŠEI imetnika,
- podatke za dostop do storitve za pridobivanje EŠEI imetnika na podlagi identifikacijskih podatkov kvalificiranega potrdila za avtentikacijo spletišč ali
- podatke za dostop do storitve za preverjanje EŠEI imetnika na podlagi identifikacijskih podatkov kvalificiranega potrdila za avtentikacijo spletišč.

(5) Vlada z uredbo določi tehnične specifikacije za zapis EŠEI v kvalificirano potrdilo ter za dostop do storitve za pridobivanje oziroma preverjanje EŠEI na podlagi identifikacijskih podatkov kvalificiranega potrdila iz tega člena.

25. člen
(evidenca imetnikov kvalificiranih potrdil za elektronski podpis)

(1) Ponudnik kvalificiranih storitev zaupanja, registriran v Republiki Sloveniji, za identifikacijo in preverjanje identifikacijskih podatkov fizične osebe, za katero se izdaja kvalificirano potrdilo za

elektronski podpis, ter za izdajo kvalificiranega potrdila za elektronski podpis in zagotavljanja njegove uporabe vodi evidenco imetnikov kvalificiranih potrdil za elektronski podpis.

(2) Evidenca imetnikov kvalificiranih potrdil za elektronski podpis vsebuje naslednje podatke:
1. identifikacijske podatke kvalificiranega potrdila za elektronski podpis;
2. identifikacijske podatke naprave za ustvarjanje kvalificiranega elektronskega podpisa;
3. osebno ime imetnika;
4. vrsto in številko veljavne javne listine imetnika, opremljene s fotografijo, ki jo je izdal državni organ, oziroma navedbo postopka, na podlagi katerega je bila opravljena identifikacija imetnika;
5. EŠEI imetnika;
6. davčno številko imetnika;
7. rojstni datum imetnika;
8. stalno prebivališče ali stalni naslov v tujini, začasno prebivališče ali začasni naslov v tujini in naslov za vročanje, če je to potrebno za pridobitev kvalificiranega potrdila za elektronski podpis;
9. telefonsko številko imetnika, če jo imetnik posreduje ali če je to potrebno za pridobitev kvalificiranega potrdila za elektronski podpis;
10. naslov elektronske pošte imetnika, če ga imetnik posreduje ali če je to potrebno za pridobitev kvalificiranega potrdila za elektronski podpis;
11. status kvalificiranega potrdila za elektronski podpis;
12. obdobje veljavnosti kvalificiranega potrdila za elektronski podpis;
13. obdobje začasne razveljavitve kvalificiranega potrdila za elektronski podpis;
14. datum preklica kvalificiranega potrdila za elektronski podpis.

(3) Če se izdaja kvalificirano potrdilo za elektronski podpis fizične osebe pri poslovnem subjektu, evidenca imetnikov kvalificiranih potrdil poleg podatkov iz prejšnjega odstavka vsebuje tudi podatke poslovnega subjekta iz 2., 3., 4., 5. in 7. točke drugega odstavka 26. člena tega zakona.

(4) Določila tega člena, ki veljajo za kvalificirana potrdila za elektronski podpis, smiselno veljajo tudi v primeru izdaje kvalificiranega potrdila za avtentikacijo spletišč, če je imetnik fizična oseba.

26. člen
(evidenca imetnikov kvalificiranih potrdil za elektronski žig)

(1) Ponudnik kvalificiranih storitev zaupanja, registriran v Republiki Sloveniji, lahko za identifikacijo in preverjanje identifikacijskih podatkov poslovnega subjekta in pooblaščenega predstavnika poslovnega subjekta, za katerega se izdaja kvalificirano potrdilo za elektronski žig, ter za izdajo kvalificiranega potrdila za elektronski žig in zagotavljanja njegove uporabe vodi evidenco imetnikov kvalificiranih potrdil za elektronski žig, ki so poslovni subjekti.

(2) Evidenca imetnikov kvalificiranih potrdil za elektronski žig vsebuje podatke:
1. identifikacijske podatke kvalificiranega potrdila za elektronski žig;
2. firmo poslovnega subjekta;
3. davčno in matično številko poslovnega subjekta;
4. sedež in naslov poslovnega subjekta;

5. podatke o njegovih zastopnikih, ki obsegajo osebno ime in elektronski naslov;
6. podatke o pooblaščenem predstavniku poslovnega subjekta, ki obsegajo: osebno ime, vrsto in številko veljavne javne listine pooblaščenega predstavnika oziroma navedbo postopka, na podlagi katerega je bila opravljena identifikacija pooblaščenega predstavnika, in elektronski naslov;
7. EŠEI poslovnega subjekta;
8. status kvalificiranega potrdila za elektronski žig;
9. obdobje veljavnosti kvalificiranega potrdila za elektronski žig;
10. obdobje začasne razveljavitve kvalificiranega potrdila za elektronski žig;
11. datum preklica kvalificiranega potrdila za elektronski žig.

(3) Določila tega člena, ki veljajo za kvalificirana potrdila za elektronski žig, smiselno veljajo tudi v primeru izdaje kvalificiranega potrdila za avtentikacijo spletišč, če je imetnik poslovni subjekt.

27. člen
(hramba podatkov o imetniku kvalificiranega potrdila)

Podatke glede kvalificiranega potrdila ponudnik kvalificiranih storitev zaupanja hrani deset let po prenehanju veljavnosti izdanega kvalificiranega potrdila ali deset let po koncu postopka, če se postopek ni končal z izdajo kvalificiranega potrdila.

28. člen
(hramba podatkov za potrjevanje veljavnosti elektronskega podpisa, elektronskega žiga in elektronskega časovnega žiga)

(1) Če predpis določa, da se elektronski dokument, zapis ali podatek, ki je elektronsko podpisan, elektronsko žigosan ali elektronsko časovno žigosan, hrani, mora tisti, ki mora dokument, zapis ali podatek hraniti, hraniti tudi podatke za potrjevanje veljavnosti elektronskega podpisa, elektronskega žiga ali elektronskega časovnega žiga.

(2) Podatki za potrjevanje veljavnosti se hranijo enako dolgo kakor elektronski dokumenti, zapisi ali podatki iz prejšnjega odstavka.

29. člen
(identifikacija ob izdaji kvalificiranih potrdil)

(1) Za izdajo kvalificiranega potrdila za elektronski podpis ali overovitev spletišč fizični osebi v skladu s točko a prvega odstavka 24. člena Uredbe 910/2014/EU ponudnik kvalificirane storitve zaupanja izvede identifikacijo fizične osebe v skladu s prvo alinejo točke b prvega odstavka 10. člena tega zakona.

(2) Za izdajo kvalificiranega potrdila za elektronski podpis fizične osebe pri poslovnem subjektu v skladu s točko a prvega odstavka 24. člena Uredbe 910/2014/EU ponudnik kvalificirane storitve zaupanja izvede:

– identifikacijo fizične osebe, za katero se izdaja kvalificirano potrdilo, na smiselno enak način, kot je naveden v prejšnjem odstavku;
– preverjanje poslovnega subjekta, za potrebe katerega se izdaja kvalificirano potrdilo, na podlagi podatkov poslovnega subjekta iz verodostojnega vira države, v kateri je poslovni subjekt registriran.

(3) Za izdajo kvalificiranega potrdila za elektronski žig ali avtentikacijo spletišč poslovnemu subjektu v skladu s točko a prvega odstavka 24. člena Uredbe 910/2014/EU ponudnik kvalificirane storitve zaupanja izvede:
– identifikacijo pooblaščenega predstavnika poslovnega subjekta, za potrebe katerega se izdaja kvalificirano potrdilo, na smiselno enak način, kot je naveden v prvem odstavku tega člena;
– preverjanje poslovnega subjekta, za potrebe katerega se izdaja kvalificirano potrdilo, na podlagi podatkov poslovnega subjekta iz verodostojnega vira države, v kateri je poslovni subjekt registriran.

(4) Sprejem zahtevkov za izdajo, preklic in začasno razveljavitev kvalificiranega potrdila ter identifikacijo iz tega člena lahko izvede prijavna služba.

30. člen
(preverjanje podatkov v verodostojnih virih v Republiki Sloveniji)

Ponudniki kvalificiranih storitev zaupanja imajo za namene prejšnjega člena pravico brezplačno pridobiti ali preveriti podatke v verodostojnem viru.

31. člen
(verodostojni vir v Republiki Sloveniji)

(1) Verodostojni vir podatkov o državljanih Republike Slovenije je centralni register prebivalstva, in sicer za podatke iz 3., 6., 7. in 8. točke drugega odstavka 25. člena tega zakona.

(2) Verodostojna vira podatkov o tujcih v Republiki Sloveniji sta centralni register prebivalstva in davčni register, in sicer za podatke iz 3., 6., 7. in 8. točke drugega odstavka 25. člena tega zakona.

(3) Verodostojni vir podatkov o poslovnih subjektih, registriranih v Republiki Sloveniji, je poslovni register Slovenije, in sicer za podatke iz 2., 3. in 4. točke drugega odstavka 26. člena tega zakona ter osebno ime zastopnika poslovnega subjekta.

32. člen
(povezovanje evidenc imetnikov kvalificiranih potrdil)

(1) Evidenca imetnikov kvalificiranih potrdil se povezuje:
– s centralnim registrom prebivalstva tako, da se na podlagi davčne številke v evidenco imetnikov kvalificiranih potrdil na posamezno zahtevo ponudnika kvalificiranih storitev zaupanja ali njegove prijavne službe pridobijo podatki o davčni številki, osebnem imenu, rojstnem datumu in stalnem prebivališču ali stalnem naslovu v tujini, začasnem prebivališču ali začasnem naslovu v tujini in naslovu za vročanje;

– z davčnim registrom tako, da se na podlagi davčne številke v evidenco imetnikov kvalificiranih potrdil na posamezno zahtevo ponudnika kvalificiranih storitev zaupanja ali prijavne službe pridobijo podatki o osebnem imenu, rojstnem datumu in o stalnem prebivališču ali stalnem naslovu v tujini, začasnem prebivališču ali začasnem naslovu v tujini in naslovu za vročanje,
– s poslovnim registrom tako, da se na podlagi davčne številke v evidenco imetnikov kvalificiranih potrdil na posamezno zahtevo ponudnika kvalificiranih storitev zaupanja ali prijavne službe pridobijo drugi podatki iz tretjega odstavka prejšnjega člena.

(2) Če prijavna služba v okviru izvajanja drugega zakona pridobi EMŠO imetnika, se izvajanje prve alineje prejšnjega odstavka zagotovi s posredovanjem EMŠO namesto s posredovanjem davčne številke. Po pridobitvi podatkov iz prejšnjega odstavka se EMŠO izbriše.

33. člen
(notranja pravila)

(1) Ponudnik kvalificiranih storitev zaupanja posluje v skladu s svojimi notranjimi pravili, ki jih opredeli v skladu z zahtevami Uredbe 910/2014/EU za ponudnike kvalificiranih storitev zaupanja in standardov, na podlagi katerih je bila skladnost njegovega poslovanja certificirana s strani organa za ugotavljanje skladnosti.

(2) Notranja pravila morajo vsebovati javni in zaupni del.

(3) Vse bistvene določbe notranjih pravil, ki vplivajo na odnos med ponudnikom in imetniki od njega izdanih kvalificiranih potrdil ter tretjimi osebami, ki se zanašajo na ta potrdila, morajo biti vsebovane v javnem delu notranjih pravil.

34. člen
(preklic kvalificiranih potrdil)

(1) Ponudnik kvalificiranih storitev zaupanja prekliče kvalificirano potrdilo za elektronski podpis, elektronski žig ali avtentikacijo spletišč v času njegove veljavnosti v skladu s svojimi notranjimi pravili, ki urejajo preklice potrdil, vendar takoj oziroma v skladu s tretjim odstavkom 24. člena Uredbe 910/2014/EU:
1. po prejemu zahtevka, če preklic kvalificiranega potrdila zahteva imetnik kvalificiranega potrdila;
2. po prejemu zahtevka, če preklic kvalificiranega potrdila za elektronski podpis, izdanega fizični osebi pri poslovnem subjektu, zahteva zastopnik poslovnega subjekta;
3. ko izve, da je imetniku kvalificiranega potrdila – fizični osebi – imenovan skrbnik, da je imetnik umrl ali da so se spremenile okoliščine, ki bistveno vplivajo na veljavnost kvalificiranega potrdila;
4. ko izve, da je poslovni subjekt, za potrebe katerega je bilo izdano kvalificirano potrdilo, prenehal obstajati ali da so se spremenile okoliščine, ki bistveno vplivajo na veljavnost kvalificiranega potrdila;
5. ko izve, da je poslovni subjekt, kjer je zaposlena fizična oseba, ki ji je bilo izdano kvalificirano potrdilo za elektronski podpis za fizično osebo pri poslovnem subjektu, prenehal obstajati ali da so

se spremenile okoliščine, ki bistveno vplivajo na veljavnost kvalificiranega potrdila fizične osebe, ki je pridobila kvalificirano potrdilo za potrebe poslovnega subjekta;
6. če je podatek v kvalificiranem potrdilu napačen ali je bilo kvalificirano potrdilo izdano na podlagi napačnih podatkov;
7. če so bili podatki ali naprave za ustvarjanje elektronskega podpisa ali informacijski sistem ponudnika kvalificiranih storitev zaupanja ogroženi na način, ki vpliva na zanesljivost kvalificiranega potrdila;
8. če so bili podatki ali naprave za ustvarjanje elektronskega podpisa ali informacijski sistem imetnika kvalificiranega potrdila ogroženi na način, ki vpliva na zanesljivost kvalificiranega potrdila, in je ponudnik kvalificiranih storitev zaupanja s tem seznanjen;
9. če ponudnik kvalificiranih storitev zaupanja preneha delovati ali mu je delovanje prepovedano in njegove dejavnosti ni prevzel drug ponudnik kvalificiranih storitev zaupanja ali
10. če ponudnik izve, da je preklic odredilo pristojno sodišče, sodnik za prekrške, upravni organ ali nadzorni organ za storitve zaupanja.

(2) Imetnik kvalificiranega potrdila mora zahtevati preklic svojega kvalificiranega potrdila, če:
– so bili podatki za elektronsko podpisovanje, žigosanje ali avtentikacijo spletišč izgubljeni ali odtujeni, ali
– so bili podatki ali informacijski sistem imetnika kvalificiranega potrdila spremenjeni, odtujeni ali ogroženi tako, da to vpliva na zanesljivost oblikovanja elektronskega podpisa, žigosanje ali avtentikacijo spletišč, ali
– obstaja nevarnost zlorabe, ali
– so se spremenili podatki, ki so navedeni v kvalificiranem potrdilu ali evidenci kvalificiranih potrdil, ki vplivajo na veljavnost kvalificiranega potrdila.

(3) Ponudnik kvalificiranih storitev zaupanja mora v svojih notranjih pravilih določiti, kdaj in kako se obvešča o izdaji oziroma preklicu kvalificiranega potrdila.

35. člen
(učinek preklica kvalificiranih potrdil)

(1) Preklic kvalificiranega potrdila učinkuje med imetnikom kvalificiranega potrdila in ponudnikom kvalificiranih storitev zaupanja od trenutka preklica.

(2) Preklic potrdila učinkuje med tretjimi osebami in ponudnikom kvalificiranih storitev zaupanja od trenutka objave, če pa preklic še ni javno objavljen, od trenutka, ko zanj izvedo tretje osebe.

(3) Čas preklica se evidentira v evidenci kvalificiranih potrdil.

36. člen
(začasna razveljavitev kvalificiranih potrdil za elektronski podpis in elektronski žig)

(1) Začasna razveljavitev kvalificiranega potrdila za elektronski podpis in elektronski žig pomeni neveljavnost kvalificiranega potrdila v času njegove razveljavitve.

(2) Če ponudnik kvalificiranih storitev zaupanja omogoča začasno razveljavitev kvalificiranega potrdila, pogoje in postopke v zvezi z začasno razveljavitvijo uredi v svojih notranjih pravilih.

(3) Začasna razveljavitev se izvede le na podlagi izrecne zahteve imetnika kvalificiranega potrdila.

(4) Začasna razveljavitev lahko traja največ 48 ur. Če imetnik v tem roku ne zahteva vzpostavitve veljavnosti kvalificiranega potrdila, ponudnik kvalificirane storitve prekliče kvalificirano potrdilo.

(5) Ponudnik kvalificiranih storitev zaupanja pri ureditvi začasne razveljavitve smiselno upošteva določila tega zakona in Uredbe 910/2014/EU, ki se nanašajo na preklic kvalificiranih potrdil.

37. člen
(zaposleni pri ponudniku kvalificiranih storitev zaupanja)

(1) Ponudnik kvalificiranih storitev zaupanja mora zaposlovati najmanj tri osebe z najmanj osmo ravnjo izobrazbe v skladu z zakonom, ki določa slovensko ogrodje kvalifikacij. Od tega morata najmanj dve osebi imeti izobrazbo tehnične oziroma naravoslovne smeri, najmanj dve osebi pa morata imeti tudi najmanj dve leti delovnih izkušenj s področja storitev zaupanja ali elektronskega poslovanja.

(2) Ponudnik kvalificiranih storitev zaupanja mora zaposlovati ali imeti sklenjeno ustrezno svetovalno pogodbo z osebo s pravno izobrazbo z najmanj osmo ravnjo izobrazbe po zakonu, ki določa slovensko ogrodje kvalifikacij, in ima najmanj dve leti delovnih izkušenj s področja storitev zaupanja ali elektronskega poslovanja.

(3) Vse osebe iz prejšnjih dveh odstavkov morajo imeti posebna strokovna znanja o upravljanju in poznavanju tehnologije, varnostnih postopkih, pravnih zahtevah s področja storitev zaupanja ali elektronskega poslovanja ter delovanja ponudnikov kvalificiranih storitev zaupanja, pridobljena na strokovnih usposabljanjih.

(4) Naloge zaposlenih pri ponudniku kvalificiranih storitev zaupanja morajo biti porazdeljene med več oseb tako, da se prepreči možnost zlorab, ki bi jih storili zaposleni. Naloge zaposlenih morajo biti določene tako, da so med seboj jasno ločeni upravljanje kvalificirane storitve zaupanja, upravljanje informacijskega sistema ponudnika ter področje varovanja in kontrole.

(5) Zaposleni v prijavni službi ponudnika kvalificiranih storitev zaupanja morajo biti usposobljeni za zanesljivo preverjanje istovetnosti oseb.

38. člen
(uporaba podatkov za ustvarjanje kvalificiranega elektronskega podpisa)

(1) Vsaka uporaba podatkov za ustvarjanje kvalificiranega elektronskega podpisa mora od podpisnika zahtevati prostovoljno, specifično, ozaveščeno, razumljivo, nedvoumno in zanesljivo dejanje za predstavitev napravi za ustvarjanje kvalificiranega elektronskega podpisa (na primer vnos gesla, prstni odtis).

(2) Če dejanje za predstavitev iz prejšnjega odstavka vključuje tudi voljo podpisnika za več podpisov, se podatki za ustvarjanje kvalificiranega elektronskega podpisa uporabijo za te konkretne podpise.

39. člen
(časovna veljavnost kvalificiranega potrdila)

Časovna veljavnost kvalificiranega potrdila je največ deset let od dneva njegove izdaje.

40. člen
(ponudnik kvalificiranih storitev zaupanja v državnih organih)

(1) Ponudnik kvalificiranih storitev zaupanja Republika Slovenija izvaja kvalificirane storitve zaupanja za potrebe državnih organov.

(2) Informacijske rešitve za elektronsko poslovanje v podporo poslovanju organov iz prejšnjega odstavka, ki vključujejo tudi uporabo kvalificiranih storitev zaupanja, uporabljajo kvalificirane storitve zaupanja ponudnika kvalificiranih storitev zaupanja Republika Slovenija in njemu podrejenih ali od njega potrjenih drugih ponudnikov kvalificiranih storitev zaupanja.

(3) Ponudnik kvalificiranih storitev zaupanja Republika Slovenija deluje v okviru ministrstva, pristojnega za centralno storitev za spletno prijavo in elektronski podpis.

41. člen
(prijavna služba ponudnika kvalificiranih storitev zaupanja Republika Slovenija)

(1) Naloge v zvezi s prijavo in preverjanjem istovetnosti imetnikov v postopkih izdaje in upravljanja kvalificiranih potrdil ponudnika kvalificiranih storitev zaupanja Republika Slovenija lahko opravljajo državni organi.

(2) Ponudnik kvalificiranih storitev zaupanja Republika Slovenija v svojih notranjih pravilih določi pogoje in način izvajanja nalog prijavne službe.

(3) Ponudnik kvalificiranih storitev zaupanja Republika Slovenija ima pravico vpogleda v dokumentacijo, ki jo v postopkih izdaje in upravljanja kvalificiranih potrdil hranijo prijavne službe.

42. člen
(preverjanje interesa za certificiranje kvalificiranih naprav za ustvarjanje kvalificiranega elektronskega podpisa)

Ministrstvo, pristojno za informacijsko družbo, z javnim pozivom vsaj vsaki dve leti pozove javnost k priglasitvi interesa za certificiranje kvalificiranih naprav za ustvarjanje kvalificiranega elektronskega podpisa.

43. člen
(vpis v nacionalni zanesljivi seznam)

(1) Pristojni organ ponudnika storitev zaupanja in kvalificirane storitve zaupanja, ki jih želi zagotavljati, vpiše v nacionalni zanesljivi seznam, če so za to izpolnjeni vsi pogoji iz tega zakona in Uredbe 910/2014/EU.

(2) Pristojni organ ponudniku kvalificiranih storitev zaupanja posreduje o izvedenem vpisu iz prejšnjega odstavka potrdilo.

(3) Če pristojni organ ugotovi, da ponudnik storitev zaupanja ali kvalificirane storitve zaupanja, ki jih želi zagotavljati, ne izpolnjuje vseh pogojev, o tem izda upravno odločbo.

(4) Zoper odločbo iz prejšnjega odstavka ni pritožbe, zagotovljeno pa je sodno varstvo v upravnem sporu.

44. člen
(sprememba ali odvzem kvalificiranega statusa v nacionalnem zanesljivem seznamu)

(1) O spremembi ali odvzemu kvalificiranega statusa ponudnika kvalificiranih storitev zaupanja ali kvalificiranih storitev zaupanja, ki jih ta zagotavlja, iz nacionalnega zanesljivega seznama pristojni organ odloči z upravno odločbo.

(2) Zoper odločbo iz prejšnjega odstavka ni pritožbe, zagotovljeno pa je sodno varstvo v upravnem sporu.

4. CENTRALNA STORITEV ZA SPLETNO PRIJAVO IN ELEKTRONSKI PODPIS

45. člen
(centralna storitev za spletno prijavo in elektronski podpis)

(1) Centralna storitev za spletno prijavo in elektronski podpis je informacijska rešitev:
– preko katere se posameznik identificira in avtenticira z uporabo sredstev elektronske identifikacije;
– preko katere posameznik lahko elektronsko podpiše dokument z uporabo potrdila za elektronski podpis;
– ki zagotavlja funkcionalnosti čezmejne avtentikacije v skladu s 6. členom Uredbe 910/2014/EU;
– ki zagotavlja ustvarjanje pooblastil v elektronski obliki za identifikacijo in avtentikacijo pooblaščenca in njihovo uporabo v pravnem prometu.

(2) Centralno storitev za spletno prijavo in elektronski podpis iz prejšnjega odstavka lahko za svoje poslovanje uporabljajo organi javnega sektorja, ki ponujajo elektronske storitve. Za te organe je storitev brezplačna.

(3) Centralno storitev za spletno prijavo in elektronski podpis iz prvega odstavka tega člena lahko za svoje poslovanje uporabljajo ponudniki elektronskih storitev, registrirani v Republiki Sloveniji.

(4) Storitev iz tretje alineje prvega odstavka tega člena lahko za svoje poslovanje uporabljajo vsi ponudniki elektronskih storitev.

(5) Vlada z uredbo določi pogoje in tehnične specifikacije za izvajanje prejšnjih treh odstavkov tega člena. Vlada z uredbo določi tudi cenik storitev za ponudnike elektronskih storitev.

(6) Pooblastilo v elektronski obliki se pripravi preko centralne storitve za spletno prijavo in elektronski podpis s podatki o pooblastitelju in pooblaščencu, obsegu in času pooblastila. Pooblastilo podpiše pooblastitelj s kvalificiranim elektronskim podpisom.

(7) Pooblastilo v fizični obliki s podatki o pooblastitelju in pooblaščencu, obsegu in času pooblastila pred uradno osebo na upravni enoti pooblastitelj lastnoročno podpiše ali prizna podpis, ki je že na listini, za svoj podpis. Istovetnost predlagatelja listine ugotovi uradna oseba na podlagi veljavne javne listine, opremljene s fotografijo, ki jo je izdal državni organ, razen v primerih, ko je predlagatelj uradni osebi osebno znan. Nato pooblastilo uradna oseba skenira in ga s podatki vnese v centralno storitev za spletno prijavo in elektronski podpis.

46. člen
(obdelava osebnih podatkov in povezovanje centralne storitve za spletno prijavo in elektronski podpis)

(1) V okviru centralne storitve za spletno prijavo in elektronski podpis se za njeno uporabo iz prvih treh alinej prvega odstavka prejšnjega člena hranijo naslednji podatki:
– identifikator sredstva elektronske identifikacije;
– elektronski naslov posameznika, ki je storitev uporabil;
– EŠEI;
– davčna številka;
– identifikator uporabniškega računa posameznika, ki je storitev uporabil.

(2) Podatke iz prejšnjega odstavka se hrani še pet let po izvedeni zahtevi za izbris podatkov s strani posameznika, ki je storitev iz prejšnjega odstavka uporabil, ali po zadnji uporabi te storitve s strani posameznika.

(3) V okviru centralne storitve za spletno prijavo in elektronski podpis se za njeno uporabo iz četrte alineje prvega odstavka prejšnjega člena hrani pooblastilo in za potrebe preverjanja pooblaščanja obdelujejo naslednji podatki:
– osebno ime fizične osebe ali firme poslovnega subjekta pooblaščenca in pooblastitelja,
– EŠEI pooblaščenca in pooblastitelja,
– elektronski naslov pooblaščenca in pooblastitelja,
– čas veljavnosti pooblastila,
– identifikator pooblastila,
– obseg pooblastila,
– podpis pooblastila,
– datum smrti pooblastitelja.

(4) Centralna storitev za spletno prijavo in elektronski podpis v delu, ki omogoča ustvarjanje in hrambo pooblastil, ni uradna evidenca, v kateri organi preverjajo obstoj ali obseg pooblastila. Pooblastitelj ali pooblaščenec je dolžan zagotoviti, da organ, pred katerim se izvaja zastopanje, dobi pooblastilo iz centralne storitve za spletno prijavo in elektronski podpis in ne more zahtevati, da ga pridobi organ po uradni dolžnosti. Organ, ki vodi postopek, nima dostopa do podatkov iz prejšnjega člena.

(5) Pooblastilo in podatki iz tretjega odstavka se hranijo šest mesecev po posredovanju zahteve za preklic ali odpoved elektronskega pooblastila s strani pooblaščenca ali pooblastitelja in največ pet let po zadnji uporabi te storitve s strani pooblaščenca.

(6) Centralna storitev za spletno prijavo in elektronski podpis pri zagotavljanju storitev iz prvih treh alinej prvega odstavka prejšnjega člena obdeluje tudi druge podatke, kot so navedeni v prvem odstavku tega člena, in sicer za njihovo posredovanje ponudnikom elektronskih storitev, vendar izključno na zahtevo posameznika, ki storitev uporablja. Ti podatki se po njihovem posredovanju ponudnikom elektronskih storitev izbrišejo. Za te namene se centralna storitev za spletno prijavo in elektronski podpis povezuje:
– s centralnim registrom prebivalstva tako, da se na zahtevo posameznika, imetnika sredstva elektronske identifikacije, na podlagi davčne številke iz centralnega registra prebivalstva pridobijo podatki o osebnem imenu, EMŠO, rojstnem datumu, rojstnem kraju, državi rojstva, spolu, državljanstvu in stalnem prebivališču ali stalnem naslovu v tujini, začasnem prebivališču ali začasnem naslovu v tujini in naslovu za vročanje ter datumu smrti;
– s centralnim registrom prebivalstva tako, da se na zahtevo posameznika, ki prijavo izvaja na podlagi čezmejne avtentikacije prek spleta v skladu z Uredbo 910/2014/EU, na podlagi EMŠO iz centralnega registra prebivalstva pridobijo podatki o osebnem imenu in rojstnem datumu;
– z davčnim registrom tako, da se na zahtevo posameznika, ki prijavo izvaja na podlagi čezmejne avtentikacije prek spleta v skladu z Uredbo 910/2014/EU, na podlagi davčne številke, osebnega imena in rojstnega datuma iz davčnega registra pridobi podatek o ujemanju posredovanih podatkov z zapisom v davčnem registru;
– s poslovnim registrom tako, da se na zahtevo posameznika, imetnika sredstva elektronske identifikacije, na podlagi davčne številke iz poslovnega registra pridobi podatek o poslovnih subjektih, pri katerih nastopa v vlogi zakonitega zastopnika.

(7) Centralna storitev za spletno prijavo in elektronski podpis se pri zagotavljanju storitev iz četrte alineje prvega odstavka prejšnjega člena ob ustvarjanju pooblastila v elektronski obliki za preverjanje ustreznosti vnesenih podatkov na zahtevo pooblastitelja ali pooblaščenca povezuje s centralnim registrom prebivalstva oziroma s poslovnim registrom, in sicer tako, da centralna storitev za spletno prijavo in elektronski podpis:
– centralnemu registru prebivalstva posreduje osebno ime in davčno številko pooblaščenca ali pooblastitelja, ki je fizična oseba, centralni register prebivalstva pa posreduje podatek o ujemanju prejetih podatkov ter v primeru ujemanja podatkov tudi podatek o morebitnem datumu smrti pooblastitelja;
– poslovnemu registru posreduje firmo in davčno številko pooblaščenca ali pooblastitelja, ki je poslovni subjekt, poslovni register pa posreduje podatek o ujemanju prejetih podatkov.

5. PRISTOJNOSTI ORGANOV

47. člen
(pristojni organi za elektronsko identifikacijo)

(1) Za priglasitev shem elektronske identifikacije v skladu s prvim odstavkom 9. člena in 12. členom Uredbe 910/2014/EU je pristojno ministrstvo, pristojno za informacijsko družbo.

(2) Za varnostno sodelovanje v skladu z 10. členom Uredbe 910/2014/EU je pristojen organ, pristojen za informacijsko varnost.

(3) Za shemo elektronske identifikacije iz prejšnjega člena tega zakona v skladu s točko c prvega odstavka 9. člena Uredbe 910/2014/EU je odgovorno ministrstvo, pristojno za centralno storitev za spletno prijavo in elektronski podpis.

(4) Za zagotovitev informacijskega sistema za vzajemno priznavanje sredstev elektronske identifikacije, izdanih v drugi državi članici v skladu s 6. členom Uredbe 910/2014/EU, je pristojno ministrstvo, pristojno za centralno storitev za spletno prijavo in elektronski podpis.

(5) Za zagotovitev čezmejne avtentikacije prek spleta v skladu s točko f 7. člena Uredbe 910/2014/EU je pristojno ministrstvo, pristojno za centralno storitev za spletno prijavo in elektronski podpis.

(6) Nadzorni organ za elektronsko identifikacijo je organ, pristojen za informacijsko varnost.

(7) Za vzpostavitev in vzdrževanje interoperabilnostnega okvirja v skladu z 12. členom Uredbe 910/2014/EU je pristojno ministrstvo, pristojno za centralno storitev za spletno prijavo in elektronski podpis.

48. člen
(pristojnosti nadzornega organa za elektronsko identifikacijo)

Nadzorni organ za elektronsko identifikacijo:
– preverja skladnost delovanja izdajatelja sredstev elektronske identifikacije s predpisi;
– v okviru inšpekcijskega nadzorstva inšpektor preverja, ali organi javnega sektorja, ki so ponudniki elektronskih storitev v skladu s 6. členom Uredbe 910/2014/EU, ves čas izvajanja dejavnosti izpolnjujejo zahteve Uredbe 910/2014/EU, tega zakona in na njegovi podlagi izdanih podzakonskih predpisov.

49. člen
(pristojni organi za storitve zaupanja)

(1) Nadzorni organ za storitve zaupanja je organ, pristojen za informacijsko varnost.

(2) Za vodenje nacionalnega zanesljivega seznama v skladu z 22. členom Uredbe 910/2014/EU in seznama nekvalificiranih storitev zaupanja je pristojen organ, pristojen za informacijsko varnost.

(3) Za akreditacijo organov za ugotavljanje skladnosti je pristojna Slovenska akreditacija.

50. člen
(pristojnosti nadzornega organa za storitve zaupanja)

Nadzorni organ za storitve zaupanja:
– preverja zagotavljanje storitev zaupanja po tem zakonu,
– je pristojen za izvajanje nadzornih nalog v skladu s 17. členom Uredbe 910/2014/EU.

51. člen
(ukrepi nadzornih organov in pravna sredstva)

(1) V postopku nadzora po tem zakonu se uporabljajo določbe zakona, ki ureja inšpekcijski nadzor.

(2) Inšpektor po tem zakonu lahko z odločbo odredi ukrepe za odpravo ugotovljenih nepravilnosti in določi rok za njihovo odpravo.

(3) Inšpektor lahko po tem zakonu ob uporabi določb zakona, ki ureja inšpekcijski nadzor, glede prepovedi opravljanja dejavnosti s posebnim ukrepom tudi prepove delovanje ponudnika kvalificiranih storitev zaupanja.

(4) Prepoved delovanja iz prejšnjega odstavka ne vpliva na obveznosti ponudnika kvalificiranih storitev zaupanja do pred tem izdanih kvalificiranih potrdil in že izvedenih kvalificiranih storitev zaupanja.

(5) Zoper odločbo inšpektorja ni pritožbe, zagotovljeno pa je sodno varstvo v upravnem sporu.

6. KAZENSKE DOLOČBE

52. člen
(prekrški ponudnika storitev zaupanja)

(1) Z globo od 5.000 do 30.000 eurov se za prekršek kaznuje pravna oseba če:
1. ne izvaja ustreznih tehničnih in organizacijskih ukrepov za obvladovanje nevarnosti, povezanih z varnostjo storitev zaupanja, oziroma ti ukrepi ob upoštevanju najnovejših tehnoloških dosežkov ne zagotavljajo, da je raven varnosti sorazmerna s stopnjo nevarnosti (prvi odstavek 19. člena Uredbe 910/2014/EU);
2. ob vsaki kršitvi varnosti ali izgubi celovitosti, ki znatno vpliva na zagotovljeno storitev zaupanja ali osebne podatke, vsebovane v njej, v 24 urah po njeni ugotovitvi uradno ne obvesti

nadzornega organa in po potrebi drugih pristojnih organov, fizičnih ter pravnih oseb (drugi odstavek 19. člena Uredbe 910/2014/EU);
3. začne zagotavljati kvalificirane storitve zaupanja, ne da bi bil njegov kvalificirani status naveden na zanesljivem seznamu (tretji odstavek 21. člena Uredbe 910/2014/EU);
4. uporablja znak zaupanja EU za kvalificirane storitve zaupanja v nasprotju s prvim odstavkom 23. člena Uredbe 910/2014/EU.

(2) Z globo od 3.000 do 30.000 eurov se za prekršek iz prejšnjega odstavka kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost.

(3) Z globo od 3.000 do 15.000 eurov se za prekršek kaznuje pravna oseba, če kot ponudnik kvalificiranih storitev zaupanja:
1. ne zagotovi, da je na njegovem spletišču navedena povezava do ustreznega zanesljivega seznama (drugi odstavek 23. člena Uredbe 910/2014/EU);
2. ne preveri identitete in drugih posebnih lastnosti osebe, za katero izdaja kvalificirano potrdilo (prvi odstavek 24. člena Uredbe 910/2014/EU);
3. pri zagotavljanju kvalificiranih storitev zaupanja ne izpolnjuje zahtev iz drugega odstavka 24. člena Uredbe 910/2014/EU;
4. sklene, da potrdilo prekliče, preklica pa ne zabeleži v svoji podatkovni zbirki potrdil ali ga ne objavi pravočasno (tretji odstavek 24. člena Uredbe 910/2014/EU);
5. ne prekliče kvalificiranih potrdil v primerih iz prvega odstavka 34. člena tega zakona;
6. ne prekliče kvalificiranih potrdil v primeru iz drugega odstavka 34. člena tega zakona;
7. izvede preklic v nasprotju s tretjim odstavkom 35. člena tega zakona;
8. nima določenega načina obveščanja iz tretjega odstavka 34. člena tega zakona;
9. ne zagotovi informacij o veljavnosti ali preklicu izdanih kvalificiranih potrdil (četrti odstavek 24. člena Uredbe 910/2014/EU);
10. izda kvalificirano potrdilo za elektronski podpis, ki ne izpolnjuje zahtev iz Priloge I Uredbe 910/2014/EU (prvi odstavek 28. člena Uredbe 910/2014/EU);
11. ponovno aktivira kvalificirana potrdila za elektronski podpis, potem ko so bila že preklicana (četrti odstavek 28. člena Uredbe 910/2014/EU);
12. pri začasni razveljavitvi kvalificiranega potrdila za elektronski podpis ne ukrepa v skladu z drugim, tretjim, četrtim ali petim odstavkom 36. člena tega zakona;
13. omogoči ustvarjanje kvalificiranega elektronskega podpisa z napravo, ki ne izpolnjuje zahtev iz Priloge II Uredbe 910/2014/EU (prvi odstavek 29. člena Uredbe 910/2014/EU);
14. zagotavlja potrjevanje veljavnosti kvalificiranih elektronskih podpisov, ne da bi izpolnjeval zahteve iz prvega odstavka 32. člena Uredbe 910/2014/EU;
15. zagotavlja kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov, ne da bi izpolnjeval zahteve iz prvega odstavka 33. člena Uredbe 910/2014/EU;
16. zagotavlja kvalificirano storitev hrambe kvalificiranih elektronskih podpisov, ne da bi izpolnjevala zahteve iz prvega odstavka 34. člena Uredbe 910/2014/EU;
17. izda kvalificirano potrdilo za elektronski žig, ki ne izpolnjuje zahtev iz Priloge III Uredbe 910/2014/EU (prvi odstavek 38. člena Uredbe 910/2014/EU);
18. ponovno aktivira kvalificirana potrdila za elektronski žig, potem ko so bila že preklicana (četrti odstavek 38. člena Uredbe 910/2014/EU);
19. omogoči ustvarjanje kvalificiranega elektronskega žiga z napravo, ki ne izpolnjuje zahtev iz Priloge II Uredbe 910/2014/EU (prvi odstavek 39. člena Uredbe 910/2014/EU);

20. zagotavlja potrjevanje veljavnosti in hrambo kvalificiranih elektronskih žigov, ne da bi izpolnjevala zahteve iz 40. člena Uredbe 910/2014/EU;
21. izda kvalificirani elektronski časovni žig v nasprotju z zahtevami iz 42. člena Uredbe 910/2014/EU;
22. zagotavlja kvalificirane storitve elektronske priporočene dostave v nasprotju z zahtevami iz 44. člena Uredbe 910/2014/EU;
23. izda kvalificirano potrdilo za avtentikacijo spletišč, ki ne izpolnjuje zahtev iz Priloge IV Uredbe 910/2014/EU (prvi odstavek 45. člena Uredbe 910/2014/EU);
24. ne hrani osebnih in drugih podatkov iz 27. člena tega zakona še deset let po prenehanju veljavnosti izdanega kvalificiranega potrdila ali deset let po koncu postopka, če se postopek ni končal z izdajo kvalificiranega potrdila.

(4) Z globo od 2.000 do 15.000 eurov se za prekršek iz prejšnjega odstavka kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost.

(5) Z globo od 1.000 do 5.000 eurov se kaznuje odgovorna oseba pravne osebe, odgovorna oseba samostojnega podjetnika posameznika ali odgovorna oseba posameznika, ki samostojno opravlja dejavnost, ki stori prekršek iz prvega ali tretjega odstavka tega člena.

(6) Z globo od 2.000 do 20.000 eurov se za prekršek kaznuje ponudnik storitev zaupanja ali kvalificiranih storitev zaupanja, ki kot pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, dejavnost še naprej opravlja, čeprav mu je nadzorni organ delno ali v celoti prepovedal opravljanje dejavnosti.

(7) Z globo od 1.000 do 5.000 eurov se kaznuje odgovorna oseba pravne osebe, odgovorna oseba samostojnega podjetnika posameznika ali odgovorna oseba posameznika, ki samostojno opravlja dejavnost, ki stori prekršek iz prejšnjega odstavka.

53. člen
(prekrški v javnem sektorju)

(1) Z globo od 2.000 do 10.000 eurov se v javnem sektorju kaznuje pravna oseba, če ta kot ponudnik elektronskih storitev:
1. ne prizna sredstva elektronske identifikacije za dostop in uporabo elektronske storitve, ki jo nudi, čeprav so izpolnjeni pogoji iz 6. člena Uredbe 910/2014/EU;
2. ne prizna sredstva elektronske identifikacije za dostop in uporabo elektronske storitve, ki jo nudi (prvi odstavek 14. člena tega zakona);
3. pred uporabo sredstva elektronske identifikacije srednje ali visoke ravni zanesljivosti ne preveri veljavnosti sredstva elektronske identifikacije ali na drug način zagotovi, da se uporablja veljavno sredstvo elektronske identifikacije (drugi odstavek 14. člena tega zakona), ali določi raven zanesljivosti v nasprotju s 15. členom tega zakona;
4. ne prizna naprednih elektronskih podpisov, naprednih elektronskih podpisov, ki temeljijo na kvalificiranem potrdilu za elektronske podpise, in kvalificiranih elektronskih podpisov, ki so vsaj v formatih ali uporabljajo metode, ki so opredeljeni v izvedbenih aktih iz petega odstavka 27. člena Uredbe 910/2014/EU, pa za uporabo spletne storitve, ki jo zagotavlja organ javnega sektorja ali

se zagotavlja v njegovem imenu, zahteva napredni elektronski podpis (prvi odstavek 27. člena Uredbe 910/2014/EU);
5. ne prizna naprednih elektronskih podpisov, ki temeljijo na kvalificiranem potrdilu, in kvalificiranih elektronskih podpisov, ki so vsaj v formatih ali uporabljajo metode, ki so opredeljeni v izvedbenih aktih iz petega odstavka 27. člena Uredbe 910/2014/EU, pa za uporabo spletne storitve, ki jo zagotavlja organ javnega sektorja ali se zagotavlja v njegovem imenu, zahteva napredni elektronski podpis, ki temelji na kvalificiranem potrdilu (drugi odstavek 27. člena Uredbe 910/2014/EU);
6. ne prizna naprednih elektronskih žigov, naprednih elektronskih žigov, ki temeljijo na kvalificiranem potrdilu za elektronske žige, in kvalificiranih elektronskih žigov, ki so vsaj v formatih ali uporabljajo metode, ki so opredeljene v izvedbenih aktih iz petega odstavka 37. člena Uredbe 910/2014/EU, pa za uporabo spletne storitve, ki jo zagotavlja organ javnega sektorja ali se zagotavlja v njegovem imenu, zahteva napredni elektronski žig (prvi odstavek 37. člena Uredbe 910/2014/EU);
7. ne prizna naprednih elektronskih žigov, ki temeljijo na kvalificiranem potrdilu, in kvalificiranih elektronskih žigov, ki so vsaj v formatih ali uporabljajo metode, ki so opredeljeni v izvedbenih aktih iz petega odstavka 37. člena Uredbe 910/2014/EU, pa za uporabo spletne storitve, ki jo zagotavlja organ javnega sektorja ali se zagotavlja v njegovem imenu, zahteva napredni elektronski žig, ki temelji na kvalificiranem potrdilu (drugi odstavek 37. člena Uredbe 910/2014/EU).

(2) Z globo od 1.000 do 4.000 eurov se v javnem sektorju za prekršek iz prejšnjega odstavka kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost.

(3) Z globo od 1.000 do 4.000 eurov se v javnem sektorju za prekršek iz prvega odstavka tega člena kaznuje tudi odgovorna oseba pravne osebe, odgovorna oseba samostojnega podjetnika posameznika oziroma posameznika, ki samostojno opravlja dejavnost, ali odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti.

54. člen
(nezakonita uporaba sredstva elektronske identifikacije in nezakonita uporaba kvalificiranega potrdila)

(1) Z globo od 1.000 do 4.000 eurov se kaznuje imetnik sredstva elektronske identifikacije, če sredstva elektronske identifikacije ne uporablja osebno in s skrbnostjo dobrega gospodarja (prvi odstavek 4. člena tega zakona).

(2) Z globo od 500 do 1.000 eurov se kaznuje imetnik kvalificiranega potrdila, če kvalificiranega potrdila in podatkov, ki so potrebni za njegovo uporabo, ne uporablja in hrani s skrbnostjo dobrega gospodarja ali gospodarstvenika (drugi odstavek 4. člena tega zakona).

55. člen
(višina globe v hitrem prekrškovnem postopku)

Za prekrške iz tega zakona se sme v hitrem postopku izreči globa tudi v znesku, ki je višji od najnižje prepisane globe, določene s tem zakonom.

7. PREHODNA DOLOČBA

56. člen
(uporaba kvalificiranih potrdil za elektronski podpis, ki so izdana tudi za namen avtentikacije)

(1) Fizična oseba lahko za namene elektronske identifikacije in avtentikacije za dostop do elektronskih storitev v javnem sektorju iz 14. člena tega zakona uporablja kvalificirano potrdilo za elektronski podpis še pet let po uveljavitvi tega zakona, če:
– je kvalificirano potrdilo izdal ponudnik kvalificiranih storitev zaupanja, ki je bil ob sprejemu zakona registriran v Republiki Sloveniji in vpisan v nacionalni zanesljivi seznam,
– je bilo kvalificirano potrdilo izdano tudi za namen avtentikacije in
– je iz kvalificiranega potrdila mogoče samodejno, na avtomatiziran način, nedvoumno ugotoviti identiteto imetnika.

(2) Če drugi predpis zahteva uporabo sredstva elektronske identifikacije, se kot ustrezno šteje tudi kvalificirano potrdilo iz prejšnjega odstavka.

8. KONČNE DOLOČBE

57. člen
(začetek preverjanja interesa za certificiranje kvalificiranih naprav za ustvarjanje kvalificiranega elektronskega podpisa)

Javnost se po 42. členu tega zakona prvič pozove k priglasitvi interesa za certificiranje kvalificiranih naprav za ustvarjanje kvalificiranega elektronskega podpisa v dveh letih po uveljavitvi tega zakona.

58. člen
(začetek uporabe EŠEI v kvalificiranih potrdilih)

Izdajanje kvalificiranih potrdil z uporabo EŠEI v skladu z 21. členom tega zakona se začne v dveh letih po uveljavitvi podzakonskih aktov iz 61. člena tega zakona.

59. člen
(sprememba zakona in razveljavitev predpisa)

(1) V Zakonu o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14) se črtajo:

– v naslovu besedilo "in elektronskem podpisu",

– v prvem odstavku 1. člena za besedo "tehnologije" besedilo "in uporabo elektronskega podpisa v pravnem prometu",

– drugi odstavek 1. člena,
– tretja, četrta, peta, deseta, dvanajsta, trinajsta, štirinajsta, petnajsta, šestnajsta, sedemnajsta, osemnajsta, devetnajsta in dvajseta točka 2. člena;
– tretje poglavje.

(2) Z dnem uveljavitve tega zakona preneha veljati Uredba o izvajanju Uredbe (EU) o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (Uradni list RS, št. 46/16).

60. člen
(uskladitev področnih predpisov)

(1) Predpisi, ki določajo uporabo storitev zaupanja v skladu z Uredbo 910/2014/EU, s tem zakonom in podzakonskimi akti, se uskladijo s tem zakonom v petih letih po njegovi uveljavitvi.

(2) Če predpis določa obveznost uporabe varnega elektronskega podpisa, overjenega s kvalificiranim digitalnim potrdilom, se šteje, da se zahteva kvalificirani elektronski podpis.

61. člen
(izdaja podzakonskih aktov)

(1) Vlada podrobneje določi način vodenja nacionalnega zanesljivega seznama po 22. členu Uredbe 910/2014/EU.

(2) Rok za izdajo podzakonskih predpisov po tem zakonu je šest mesecev po uveljavitvi tega zakona.

62. člen
(začetek veljavnosti)

Ta zakon začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije.

IV. OBRAZLOŽITVE

1. SPLOŠNE DOLOČBE

K 1. (vsebina in namen zakona)

Predlog člena določa vsebino, ki jo zakon ureja. Gre za urejanje osebne elektronske identitete, ki jo dodeljuje Republika Slovenija, in sredstev elektronske identifikacije, s katerimi se dokazuje to elektronsko identiteto ter na tej elektronski identiteti temelječo shemo elektronske identifikacije v skladu z zahtevami iz Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (UL L št. 257 z dne 28. 8. 2014, str. 73, v nadaljnjem besedilu: Uredba 910/2014/EU) za priglasitev shem elektronske identifikacije. Pri tem velja poudariti, da je bila v letu 2016 za izvajanje Uredbe 910/2014/EU že sprejeta Uredba o izvajanju Uredbe 910/2014/EU (Uradni list RS, št. 46/16), ki pa jo bo predlagani zakon nadomestil.

Z zakonom se urejajo tudi storitve zaupanja v delu, kjer Uredba 910/2014/EU to omogoča, z njim se določijo tudi pristojni organi in kazenske določbe za izvajanje Uredbe 910/2014/EU. V tem delu zakon ne predvideva različne obravnave storitev zaupanja glede na vrsto izdajatelja.

K 2. členu (pomen izrazov)

V predlaganem členu so opredeljeni pomeni izrazov, ki so uporabljeni v tem zakonu. Glede na v slovenskem pravnem redu neposredno uporabljivost Uredbe 910/2014/EU pa izrazi, ki jih ta opredeljuje (kot na primer "sredstvo elektronske identifikacije", "elektronski dokument", "avtentikacija", "elektronska identifikacija", "identifikacijski podatki osebe", "shema elektronske identifikacije", "kvalificirano potrdilo za elektronski podpis", "zanašajoča se stranka", "ponudnik kvalificiranih storitev zaupanja", "zaprt sistem" in "zanesljivi seznam"), neposredno veljajo in posledično niso opredeljeni.

K 3. členu (enotna številka elektronske identifikacije)

V skladu z Izvedbeno uredbo komisije (EU) 2015/1501 z dne 8. septembra 2015 o interoperabilnostnem okviru v skladu z osmim odstavkom 12. člena Uredbe 910/2014/EU, ki v specifikaciji podatkov za enolično identifikacijo fizične ali pravne osebe za čezmejno poslovanje zahteva določitev takega enoličnega identifikatorja, ki ga je ustvarila država članica pošiljateljica v skladu s tehničnimi specifikacijami za čezmejno identifikacijo in je časovno čim bolj obstojen, je na podlagi davčne številke fizične ali pravne osebe predlagan nov identifikator z imenom Enotna številka elektronske identifikacije (v nadaljnjem besedilu: EŠEI). Pri tem je EŠEI za fizično osebo sestavljen iz predpone "11" in davčne številke, za poslovni subjekt pa iz prepone "21" in njegove davčne številke. Pri tem pojasnjujemo, da se izraz "poslovni subjekt" uporablja, kot je to določeno v davčni zakonodaji, torej vključuje fizične osebe z dejavnostjo in pravne osebe, saj z vidika elektronskega poslovanja ni potrebe po ločevanju fizične osebe z dejavnostjo in pravne osebe.

Njena uporaba se enotno predvideva tako na področju storitev zaupanja kot tudi elektronske identifikacije, s čimer se kar najbolj poenostavljajo sistemi, ki bodo zagotavljali enotno interoperabilno infrastrukturo za čezmejno poslovanje in nacionalne storitve. Davčna številka je predlagana kot osnova zaradi že obstoječih sistemov izdajanja kvalificiranih potrdil za elektronski podpis, ki je že več kot desetletje v uporabi pri večini ponudnikov storitev zaupanja. Tako se ponudnikom zagotavlja minimalno administrativno breme, ki je potrebno za uskladitev njihovih sistemov s predvidenim zakonom. Pri tem je treba poudariti, da je davčna številka

fizičnih oseb v skladu z Zakonom o davčnem postopku davčna tajnost, zato se ta pri čezmejnem elektronskem poslovanju prikazuje v preračunani obliki, kar smo upoštevali. Ker elektronske identifikacije do zdaj v svojem pravnem redu nismo imeli, davčna številka se je torej v okviru elektronskega poslovanja uporabljala brez pravne podlage, saj je bila vzpostavljena za druge namene (drugi odstavek 33. člena Zakon o davčnem postopku navaja, da se "davčna številka uporablja za enotno opredelitev in povezavo podatkov v evidencah, ki jih vodi Finančna uprava Republike Slovenije"), s predlaganim zakonom vzpostavljamo pravno podlago za uporabo te številke za identifikacijo posameznika pri elektronskem poslovanju.

V četrtem odstavku pa je dana pravna podlaga za uredbo, v kateri se določita oblika preračunane številke EŠEI in način preračunavanja.

K 4. členu (skrbnost ravnanja imetnika)

Z namenom preprečevanja zlorab in kraje identitete predlog člena vzpostavlja obveznost za imetnika sredstva elektronske identifikacije, da ga uporablja osebno in s skrbnostjo dobrega gospodarja, kar v skladu s prvim odstavkom 6. člena Obligacijskega zakonika pomeni, da mora ravnati s skrbnostjo, ki se v pravnem prometu zahteva pri ustrezni vrsti obligacijskih razmerij (skrbnost dobrega gospodarstvenika oziroma skrbnost dobrega gospodarja). Glede na pravno teorijo se ta standard uporablja za subjekte v obligacijskih razmerjih, ki imajo položaj laika, to je neprofesionalne osebe, njihovo ravnanje pa se presoja po najpogostejšem ravnanju subjektov, ki imajo enake značilnosti kot tisti, čigar ravnanje presojamo v enakih okoliščinah. Kot merilo pa je treba upoštevati starost, izobrazbo, pričakovano ravnanje razumnega človeka v danem položaju in drugo.

S smiselno enakim namenom je v drugem odstavku vzpostavljena enaka obveznost tudi za imetnika kvalificiranega potrdila.

2. OSEBNA ELEKTRONSKA IDENTITETA IN SREDSTVA ELEKTRONSKE IDENTIFIKACIJE

S predlaganim poglavjem se določa osebna elektronska identiteta v Republiki Sloveniji, ki se uporablja za identifikacijo pri elektronskem poslovanju z organi javnega sektorja. Posameznik ima zgolj eno osebno elektronsko identiteto, vendar pa ima lahko več sredstev elektronske identifikacije, s katerimi to identiteto dokazuje, saj se tudi v prihodnje predvideva obstoj različnih tehnoloških rešitev, ki bodo uporabljene v različnih uporabniških scenarijih. Smiselnost več sredstev elektronske identifikacije je v tem, da so sredstva tehnološko različna, prav tako pa so različnih ravni zanesljivosti, zato se bodo posledično uporabljale pri različnih elektronskih storitvah. Osebna elektronska identiteta je preko sredstva elektronske identifikacije uporabna za čezmejno elektronsko poslovanje v skladu z Uredbo 910/2014/EU, kar pa sicer ni zahteva same uredbe, saj ta formalno ne zahteva, da države EU uvajajo kakršno koli izdajanje sredstva elektronske identifikacije. Kljub temu pa v Republiki Sloveniji uvajamo sredstvo elektronske identifikacije, ker želimo slovenskim državljanom in državljankam omogočiti čezmejno poslovanje in dostop do elektronskih storitev javnega sektorja z nacionalno izdanim sredstvom elektronske identifikacije na podlagi nacionalne elektronske identitete. Prizadevamo pa si tudi za uporabo sredstev elektronske identifikacije za elektronske storitve zasebnega sektorja, torej ponudnikov elektronskih storitev, s čimer država zagotovi izredno pomembno infrastrukturno storitev za celotno prihodnje elektronsko poslovanje. Osebno elektronsko identiteto dobi državljan oziroma državljanka ter tujec, ki ima v Republiki Sloveniji stalno ali začasno prebivališče, na lastno pobudo in torej ni obvezna. Zaradi jasnih ciljev na področju informacijske

družbe, doseganja vse večjega obsega elektronskega poslovanja, Ministrstvo za javno upravo stremi k cilju, da bi sredstva elektronske identifikacije imelo čim več državljanov in državljank.

K 5. členu (osebna elektronska identiteta)

S predlaganim členom se vpeljuje institut osebne elektronske identitete fizične osebe, katere namen je izkazovanje istovetnosti fizične osebe pri elektronskem poslovanju. Osebno elektronsko identiteto, ki je glede na opredelitev izrazov niz identifikacijskih podatkov fizične osebe, dodeljenih s strani države, za uporabo v elektronskem poslovanju, pridobi oseba s pridobitvijo prvega sredstva elektronske identifikacije, pri čemer je treba poudariti, da bodo konkretna sredstva opredeljena ločeno (v uredbi ali drugih zakonih). Trenutno so operativno predvidena tri sredstva, in sicer digitalni potrdili na biometrični osebni izkaznici (visoke in nizke ravni zanesljivosti) ter virtualna elektronska identiteta (to je na podlagi rešitve SMS-PASS). V prihodnje bo sredstvo elektronske identifikacije lahko izdano na katerem koli dodatnem nosilcu (na primer mobilnem telefonu, USB-pametnem ključku, platformi veriženja blokov in podobno), tehnologiji ali navsezadnje tudi na že obstoječih dokumentih (na primer dovoljenju za bivanje in tako dalje), če se za to ugotovi potreba in zagotovijo zmožnosti glede na prihodnji razvoj na tem področju.

V skladu s tretjim odstavkom ima oseba eno elektronsko identiteto, enako kakor ima v fizičnem svetu eno osebno identiteto (identiteta je tisto, kar človeka določa kot osebo), ki jo lahko dokazuje z enim ali več sredstvi elektronske identifikacije, ki jih oseba ima ali uporablja hkrati (na primer odvisno od ravni zanesljivosti, tehnološke rešitve, enostavnosti postopka avtentikacije). Pri tem je treba poudariti, da se elektronska identiteta uporablja le za identifikacijo pri elektronskem poslovanju in ni namenjena neposrednemu sklepanju pravnih poslov v elektronski obliki, temu je namreč namenjen elektronski podpis.

Četrti odstavek določa, da osebno elektronsko identiteto lahko pridobi oseba, ki dopolni šest let, preneha pa ob smrti osebe ali ob izgubi statusa osebe, ki je podlaga za pridobitev osebne elektronske identitete.

V skladu s petim in šestim odstavkom pa osebno elektronsko identiteto lahko poleg državljana Republike Slovenije pridobi tudi tujec, ki ima v Republiki Sloveniji prijavljeno stalno ali začasno prebivališče.

K 6. členu (sredstva elektronske identifikacije za osebno elektronsko identiteto)

Ker gre za obširnejšo, podrobnejšo in tehnično tvarino, je s predlaganim členom vladi dana pravna podlaga, da glede na nosilec sredstva elektronske identifikacije in predpise, ki ga določajo, predpiše sredstva elektronske identifikacije, ki so izdana z namenom dokazovanja osebne elektronske identitete iz prejšnjega predlaganega člena, prav tako pa predpiše tudi njihovo obliko, raven zanesljivosti, čas veljavnosti, najnižjo starost, pri kateri oseba lahko pridobi sredstvo elektronske identifikacije, organe, pristojne za sprejem vlog in preverjanje istovetnosti, način izdaje, preklica in začasne razveljavitve ter tehnične specifikacije posameznega sredstva elektronske identifikacije. Prav tako vlada z uredbo določi, katera posamezna sredstva elektronske identifikacije se uporabljajo tudi za čezmejno poslovanje. Prvi pogoj "glede na nosilec sredstva elektronske identifikacije in predpise, ki slednjega določajo", je vsebovan iz razloga, ker so določeni pogoji, ki veljajo za "nosilca sredstev elektronske identifikacije", namreč na področju posameznih nosilcev (na primer osebne izkaznice) že predpisani z zakonom ali podzakonskim aktom (tako Zakon o osebni izkaznici določa obliko, veljavnost in podobno za osebno izkaznico), zato ti pogoji ne morejo biti dodatno predmet vladne uredbe.

Trenutno so operativno predvidena tri sredstva, in sicer digitalni potrdili na biometrični osebni izkaznici (visoke in nizke ravni zanesljivosti) ter virtualna elektronska identiteta (to je na podlagi rešitve SMS-PASS). V prihodnje bo sredstvo elektronske identifikacije lahko izdano na katerem koli dodatnem nosilcu (na primer mobilnem telefonu, USB-pametnem ključku, platformi veriženja blokov in tako dalje), tehnologiji ali navsezadnje tudi na že obstoječih dokumentih (na primer kartica ZZZS, dovoljenje za bivanje in tako dalje), če se za to ugotovi potreba in zagotovijo zmožnosti glede na prihodnji razvoj na tem področju.

Tako Slovenija kot tudi drugod po EU in v svetu sledijo najbolj široko uporabljeni tehnologiji infrastrukture javnih ključev (angl. PKI – public key infrastructure). Vendar v skladu z načelom čim večje tehnološke nevtralnosti dopušča tudi druge tehnološke rešitve ob zavedanju, da se elektronska identifikacija uporablja v uradnih postopkih, v katerih se velikokrat izmenjujejo zavezujoče informacije in osebni podatki.

K 7. členu (ravni zanesljivosti sredstev elektronske identifikacije)

Predlog člena določa, da se ravni zanesljivosti in zahteve za določanje ravni zanesljivosti, kot so določene v Uredbi 910/2014/EU in njenih izvedbenih aktih (gre za Izvedbeno uredbo Komisije (EU) 2015/1501 z dne 8. septembra 2015 o interoperabilnostnem okviru v skladu z osmim odstavkom 12. člena Uredbe 910/2014/EU in njeno Prilogo), uporabljajo tudi za določanje ravni zanesljivosti sredstev elektronske identifikacije na nacionalni ravni. Navedeni koncept je bil vpeljan z namenom uporabe že določenega okvira za določanje ravni zanesljivosti, ki ga določa Uredba 910/2014/EU, hkrati pa omogoča poenotenje in interoperabilnost, ki je ključni pogoj za široko uporabo sredstev elektronske identifikacije pri čezmejnem in nacionalnem elektronskem poslovanju. 8. člen Uredbe 910/2014/EU določa, da shema elektronske identifikacije, priglašena v skladu z 9(1) členom te uredbe, določa nizko, srednjo in/ali visoko raven zanesljivosti, dodeljeno sredstvom elektronske identifikacije, izdanim v okviru te sheme. Nizka, srednja in visoka raven zanesljivosti izpolnjujejo naslednja merila:

a) nizka raven zanesljivosti se nanaša na sredstvo elektronske identifikacije v okviru sheme elektronske identifikacije, ki zagotavlja omejeno stopnjo zaupanja v izkazano ali zagotavljano identiteto osebe in za katero je značilno sklicevanje na tiste tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je zmanjšati nevarnost zlorabe ali spreminjanja identitete;

b) srednja raven zanesljivosti se nanaša na sredstvo elektronske identifikacije v okviru sheme elektronske identifikacije, ki zagotavlja srednjo stopnjo zaupanja v izkazano ali zagotavljano identiteto osebe in za katero je značilno sklicevanje na tiste tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je znatno zmanjšati nevarnost zlorabe ali spreminjanja identitete;

c) visoka raven zanesljivosti se nanaša na sredstvo elektronske identifikacije v okviru sheme elektronske identifikacije, ki zagotavlja višjo stopnjo zaupanja v izkazano ali zagotavljano identiteto osebe kot sredstva elektronske identifikacije srednje ravni zanesljivosti in za katero je značilno sklicevanje na tiste tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je preprečiti nevarnost zlorabe ali spreminjanja identitete. Podrobnejše minimalne tehnične specifikacije in postopke za ravni zanesljivosti za sredstva elektronske identifikacije določa Izvedbena uredba Komisije (EU) 2015/1502.

K 8. členu (obdobje veljavnost sredstva elektronske identifikacije)

Glede na hiter razvoj tehnologije in dejstvo, da je dokazovanje istovetnosti imetnika v elektronskem svetu eden največjih izzivov, predvsem z vidika potencialnih zlorab (kraja identitete), je ključno, da se veljavnost osebnega elektronskega identifikacijskega dokumenta

prilagaja tehnološkim razvojnim ciklom in standardom. Pri slednjem so posebno pomembni varnostni standardi uporabljenih algoritmov in ocena varnostnega tveganja. V predlaganem členu je upoštevaje zgornjo argumentacijo in veljavnost osebnih izkaznic večine populacije (državljani, stari od 18 do 70 let), saj bo eden izmed nosilcev sredstva elektronske identifikacije tudi osebna izkaznica, določena veljavnost sredstva elektronske identifikacije deset let od dneva njegove izdaje.

K 9. členu (izdajatelj sredstva elektronske identifikacije)

1. člen Uredbe 910/2014/EU v točki a določa, da se sredstva elektronske identifikacije v okviru sheme elektronske identifikacije izdajo s strani države članice priglasiteljice, po pooblastilu države članice priglasiteljice, ali neodvisno od države članice priglasiteljice, vendar jih ta država članica priznava. Člen določa, da bo izdajatelj sredstva elektronske identifikacije ministrstvo, pristojno za centralno storitev za spletno prijavo in elektronski podpis.

Drugi odstavek določa pravico vpogleda izdajatelja sredstva elektronske identifikacije v dokumentacijo, ki jo za potrebe izdaje, preklica in začasne razveljavitve sredstva elektronske identifikacije hranijo organi, pristojni za sprejem vlog in preverjanje istovetnosti, saj je to pogoj za izvajanje nadzora nad ustreznostjo vodenja postopkov sprejema vlog in preverjanje istovetnosti, ki so med najpomembnejšimi v celotnem postopku izdaje sredstva elektronske identifikacije in posledično najpomembnejši za zaupanje v verodostojnost sredstva elektronske identifikacije. Mišljen je dostop do dokumentacije, pomembne za izdajatelja sredstva elektronske identifikacije, ki jamči skladnost z zahtevami, ki jih za izdajo elektronske identitete določajo Uredba 910/2014/EU in njeni podzakonski akti (Uredba za določitev ravni zanesljivosti). Ne gre za nadzor v smislu inšpekcijskega nadzora, slednje opravlja nadzorni organ – trenutno Uprava RS za informacijsko varnost (kot je določeno v 47. členu), ki je trenutno opredeljen kot nadzorni organ tako za storitve zaupanja kot za elektronsko identifikacijo in bo opravljal nadzor nad postopki upravnih enot za podeljevanje elektronske identitete z vidika Uredbe 910/2014/EU.

K 10. členu (identifikacija fizične osebe ob izdaji sredstva elektronske identifikacije)

V predlaganem členu so za izdajanje sredstva elektronske identifikacije določeni izdajateljevi postopki preverjanja in avtentikacije za izdajo sredstva elektronske identifikacije za vse tri ravni zanesljivosti (nizka, srednja in visoka). Postopki preverjanja ravni zanesljivosti izhajajo iz Izvedbene uredbe, sprejete na podlagi tretjega odstavka 8. člena Uredbe 910/2014/EU, s katero je Komisija določila minimalne tehnične specifikacije, standarde in postopke, na podlagi katerih se določijo nizka, srednja in visoka raven zanesljivosti za sredstva elektronske identifikacije.

Ob tem še pojasnjujemo, da Uvodna izjava št. 16 Uredbe 910/2014/EU določa, da bi ravni zanesljivosti morale označevati stopnjo zaupanja, ki jo sredstvo elektronske identifikacije zagotavlja pri ugotavljanju identitete osebe, s čimer se zagotovi, da je oseba, ki izkazuje določeno identiteto, dejansko oseba, ki ji je bila ta identiteta dodeljena. Raven zanesljivosti je odvisna od stopnje zaupanja v izkazano ali zagotavljano identiteto osebe, ki jo zagotavlja sredstvo elektronske identifikacije, pri čemer se upoštevajo tudi relevantni postopki (na primer dokazovanje in preverjanje identitete ob prijavi), upravljanje sredstva elektronske identifikacije, avtentikacija ter upravljanje in organizacija izdajatelja, način avtentikacije.

Drugi odstavek dopolnjuje omejene načine identifikacij iz prvega odstavka tako, da omogoča pridobitev sredstva elektronske identifikacije tudi v primerih, ko na primer posameznik nima veljavne javne listine, ki je opremljena s fotografijo, ker jo je izgubil, ker je potekla njena veljavnost ali pa ker je sploh še ni pridobil. Takšen dopolnilni način je sicer mogoč, vendar pa

se zanj zahteva najvišji standard identifikacije posameznika v državi, standard izdajanja javnih listin za prehod meje.

K 11. členu (evidenca imetnikov sredstev elektronske identifikacije)

Določba je potrebna zaradi pravne varnosti posameznikov pri obdelavi njihovih podatkov, prav tako pa določitev obdelave osebnih podatkov s strani državnih organov v zakonu predvidevata Zakon o varstvu osebnih podatkov (ZVOP-1) in Splošna uredba o varstvu podatkov. Predlagani člen izdajatelju sredstva elektronske identifikacije daje neposredno pravno podlago za vodenje evidence imetnikov sredstev elektronske identifikacije za vsako sredstvo elektronske identifikacije posebej. Evidenco imetnikov sredstev elektronske identifikacije mora izdajatelj imeti na voljo, če želi zagotavljati delovanje sredstev elektronske identifikacije, člen pa evidenco opredeljuje, da se zagotovi najmanjši obseg podatkov, ki so lahko uvrščeni v takšno evidenco.

V drugem odstavku je z vidika varstva osebnih podatkov ter ob upoštevanju načela sorazmernosti naveden nabor podatkov, ki naj jih ta evidenca vsebuje. Ker je predlagatelj ob pregledovanju možnosti zmanjšanja števila podatkov, ki jih evidenca vsebuje, ugotovil, da je razlog za razpolaganje z naslovom prebivališča to, da se določena sredstva izdajajo tako, da se potrditvene kode pošljejo na fizični naslov posameznika, se je odločil, da tega podatka ne bo hranil na zalogo in ga bo obdeloval le, če ga bo res potreboval. Smiselno enako velja tudi za naslov elektronske pošte in telefonsko številko, ki pa sta nekoliko specifična, saj se v praksi izkaže, da imetniki mnogokrat pričakujejo, da izdajatelj ima njihov elektronski naslov ali telefonsko številko, in pričakujejo tovrstno komunikacijo oziroma za potrebe posameznih obdelav v času razpolaganja s posameznim sredstvom elektronske identifikacije izdajatelju podajo svoje podatke. Predlog zakona torej predvideva možnost, da če imetnik poda te podatke, izdajatelj podatke lahko vključi v osnovno evidenco imetnikov.

Ker vedno hitrejši razvoj elektronskih storitev omogoča različna sredstva elektronske identifikacije, ki imajo različne ravni zanesljivosti, predlagatelj v tretjem odstavku zavezuje vlado k razmisleku o tem, ali bi bilo mogoče posamezno sredstvo elektronske identifikacije zagotoviti tudi z manjšim naborom podatkov. Vključevanje vsakega sredstva elektronske identifikacije v zakon zaradi tehnične narave opredelitve vsakega sredstva ne bi bilo smiselno. Smiselnost je vprašljiva predvsem zaradi dejstva, da se z zakonom omejijo osebni podatki, ki jih je mogoče obdelovati za zagotavljanje sredstev elektronske identifikacije. Tako je v tretjem odstavku z vidika načela sorazmernosti vladi dana pravna zaveza za določitev manjšega nabora podatkov posamezne evidence imetnikov sredstev elektronske identifikacije, če tehnični razlogi omogočajo, da je nabor lahko manjši, kot je določen v prejšnjem odstavku. S tem se uresničuje načelo *de minimis* pri zbiranju osebnih podatkov – ne več, kot je treba.

Nadalje člen določa, da se evidenca imetnikov sredstev elektronske identifikacije na podlagi EMŠO ali davčne številke povezuje s centralnim registrom prebivalstva. Iz centralnega registra prebivalstva se v evidenco sredstev elektronske identifikacije pošljejo podatki o davčni številki ali EMŠO, osebnem imenu, stalnem prebivališču ali stalnem naslovu v tujini, začasnem prebivališču ali začasnem naslovu v tujini in naslovu za vročanje, državljanstvu ter datumu smrti posameznika. Določeni podatki se iz centralnega registra prebivalstva v evidenco sredstev elektronske identifikacije pošljejo ob sprejemu vloge in ob vsaki spremembi navedenih podatkov v centralnem registru prebivalstva. Za varnost elektronske identifikacije oziroma preverjanje pravilnosti podatkov je namreč nujno uparjanje podatkov z javnimi registri, za kar se na tem mestu zagotavlja izrecna zakonska podlaga. Podobno ureditev je že do zdaj vseboval veljavni ZEPEP.

Podatki se hranijo deset let po koncu veljavnosti sredstva elektronske identifikacije.

EMŠO je vključen v povezovanje zaradi dejstva, da se pri izdaji sredstev elektronske identifikacije, ki so izdana na osebni izkaznici, lahko pridobi le EMŠO in ne davčna številka, pri čemer pa je EMŠO potreben za ugotovitev starosti bodočega imetnika sredstva elektronske identifikacije. Ker po izvedeni povezavi z registrom iz četrtega odstavka in po določitvi ustrezne starosti izdajatelj ne potrebuje več EMŠO, ga tudi izbriše.

Pri sredstvih elektronske identifikacije visoke ravni zanesljivosti Uredba 910/2014/EU zahteva dokazilo, da je bilo sredstvo izdano osebi, ki se je identificirala z veljavnim dokumentom, zato sedmi odstavek določa povezljivost evidence imetnikov sredstev elektronske identifikacije z uradnimi evidencami iz prve alineje točke c prvega odstavka predlaganega 10. člena tega zakona tako, da se na podlagi številke javne listine v evidenco imetnikov sredstev elektronske identifikacije na posamezno zahtevo organa za sprejem vloge prenesejo podatki o tem, ali je javna listina veljavna. Izdajatelj mora namreč ves čas veljavnosti sredstva elektronske identifikacije imeti vsa dokazila, na podlagi katerih je določeno sredstvo izdal. Določila so ne le že predvidena v našem pravnem redu (preko Uredbe 910/2014/EU), temveč tudi potrebna, saj gre pri sredstvih elektronske identifikacije visoke ravni zanesljivosti za sredstvo, s katerim je mogoče izvajati z vidika varnosti identitete najbolj potencialno problematične postopke.

Pri predlaganem členu tako poskušamo slediti enemu izmed temeljnih načel varstva osebnih podatkov – načelu sorazmernosti. Za vsak osebni podatek, ki se od posameznika zahteva, je treba utemeljeno izkazati potrebnost obdelave podatka za dosego konkretnega (zakonitega) cilja. Nesorazmerno oziroma glede na namen prekomerno zbiranje osebnih podatkov namreč pomeni večje tveganje za kršitve in zlorabe osebnih podatkov, obenem pa na upravljavca nalaga večje breme za pravilno zavarovanje.

K 12. členu (podatki na sredstvu elektronske identifikacije)

Z vidika varstva osebnih podatkov ter v skladu z načelom sorazmernosti predlagani člen taksativno našteva podatke, ki jih sredstvo elektronske identifikacije lahko vsebuje. Predlagatelj je v času priprave zakona poglobljeno razmišljal o možnostih zmanjševanja števila podatkov, ki so na sredstvu elektronske identifikacije, in dosegel res minimalni nabor – izdajatelj, osebno ime imetnika, identifikacijska oznaka sredstva – to kar najbolj zmanjšuje možnost pridobivanja podatkov iz samega sredstva.

Z vidika načela sorazmernosti je v primerih, ko je tehnično mogoče izdati sredstvo elektronske identifikacije tako, da to ne potrebuje določenih podatkov, dodatno dana vladi pravna zaveza, da z uredbo predpiše, da posamezno sredstvo elektronske identifikacije nekaterih podatkov ne vsebuje.

K 13. členu (uporaba sredstva elektronske identifikacije)

Predlog člena navaja, da je informacijska rešitev za uporabo sredstev elektronske identifikacije informacijska rešitev, ki omogoča avtentikacijo uporabnika in preverjanje veljavnosti sredstev elektronske identifikacije. Storitev bo v skladu z drugim odstavkom na voljo tudi zasebnemu sektorju (storitev, ki omogoča, da informacijski sistemi uporabijo avtenticirajo uporabnika in preverijo veljavnost posameznega sredstva elektronske identifikacije posameznika). S tem se poskuša zagotoviti široka uporaba sredstev elektronske identifikacije, zaradi poenotenja poslovanja posameznikov pa se poskuša dvigniti stopnja digitalizacije. Zasebni sektor bo tako lahko prostovoljno uporabljal informacijske rešitve za uporabo sredstva elektronske identifikacije v okviru priglašene sheme za identifikacijo ter bo imel možnost preverjanja EŠEI, kadar je to potrebno za spletne storitve ali elektronske transakcije. Zasebni sektor bo s to storitvijo lahko preveril EŠEI, če ga bo imel na voljo iz kakšnega drugega pravnega naslova (ali preko soglasja

ali z drugo zakonsko podlago), javnemu sektorju pa tretji odstavek omogoča pridobitev EŠEI na podlagi identifikacijske oznake sredstva.

K 14. členu (sredstvo elektronske identifikacije za dostop do elektronskih storitev v javnem sektorju)

Predlog člena določa, da organ javnega sektorja (v skladu s 3. točko 2. člena predloga zakona je to državni organ, organ samoupravne lokalne skupnosti, javna agencija, javni sklad, javni zavod ali druga oseba javnega prava, nosilec javnega pooblastila ali izvajalec javne službe), ki za dostop in uporabo elektronske storitve, ki jo nudi, v skladu s 6. členom Uredbe 910/2014/EU zahteva uporabo sredstev elektronske identifikacije srednje ali visoke ravni zanesljivosti, v ta namen prizna tudi sredstva elektronske identifikacije, ki so izdana na podlagi tega zakona, ravni zanesljivosti, ki je enaka ali višja od zahtevane ravni zanesljivosti.

O tem govori Uvodna izjava št. 15 Uredbe 910/2014/EU, ki določa, da bi obveznost priznavanja sredstev elektronske identifikacije morala zadevati le tista sredstva, katerih raven zanesljivosti identitete ustreza ravni, ki je enaka ali višja od zahtevane ravni za to spletno storitev. Poleg tega bi bilo treba to obveznost uporabljati le, kadar organ javnega sektorja uporablja srednjo ali visoko raven zanesljivosti glede dostopa do te spletne storitve.

V skladu z drugim odstavkom mora pred uporabo sredstva elektronske identifikacije srednje ali visoke ravni zanesljivosti vsak organ javnega sektorja v sistemu za samodejno strojno preverjanje preveriti veljavnost sredstva elektronske identifikacije ali drugače zagotoviti, da se uporablja veljavno sredstvo elektronske identifikacije, kar lahko ključno pripomore k dodatni varnosti imetnikov z vidika kraje identitete.

K 15. členu (zahtevana raven zanesljivosti sredstva elektronske identifikacije za dostop do elektronskih storitev v javnem sektorju)

Predlog člena sledi določbi 6. člena Uredbe 910/2014/EU, ki zahteva, da vsi organi javnega sektorja za dostop do svojih elektronskih storitev omogočijo uporabo in priznajo vsa priglašena sredstva elektronske identifikacije ter da morajo vsi organi javnega sektorja določiti najnižjo raven zanesljivosti sredstvom elektronske identifikacije za dostop do elektronskih storitev, ki jih nudijo. Glede na Uvodno izjavo št. 16 Uredbe 910/2014/EU bi ravni zanesljivosti morale označevati stopnjo zaupanja, ki jo sredstvo elektronske identifikacije zagotavlja pri ugotavljanju identitete posameznika, s čimer se zagotovi, da je posameznik, ki izkazuje določeno identiteto, dejansko posameznik, ki mu je bila ta identiteta dodeljena. Raven zanesljivosti je odvisna od stopnje zaupanja v izkazano ali zagotavljano identiteto posameznika, ki jo zagotavlja sredstvo elektronske identifikacije, pri čemer se upoštevajo vsa merila, določena z Uredbo 910/2014/EU in Izvedbeno uredbo Komisije (EU) 2015/1502.

Prvi odstavek tako določa, da organ javnega sektorja za dostop in uporabo posamezne elektronske storitve iz prejšnjega člena določi raven zanesljivosti v skladu z Uredbo 910/2014/EU in njenimi izvedbenimi akti.

Drugi odstavek v skladu z Uredbo 910/2014/EU določa, da se raven zanesljivosti določi na podlagi ocene tveganja, da identiteta uporabnika, ki dostopa do elektronske storitve in jo uporablja, ni enaka identiteti, ki se izkazuje pri dostopu do storitve, ter določa merila za njeno določitev.

V tretjem odstavku so merila za ocenjevanje ocene tveganje, v četrtem odstavku pa je vladi dana pravna podlaga, da v pomoč ocenjevanju tveganja določi podrobnejšo specifikacijo uporabe meril in načina določanja ravni zanesljivosti.

K 16. členu (obdelava in varstvo podatkov pri elektronskih storitvah v javnem sektorju)

Predlog člena ureja obdelavo in varstvo podatkov pri elektronskih storitvah v javnem sektorju.

Celotno poslovanje ministrstva, pristojnega za centralno storitev za spletno prijavo in elektronski podpis, stremi k spodbujanju uporabe centralne storitve za spletno prijavo in elektronski podpis, je pa treba vedeti, da se nekateri ponudniki kompleksnejših elektronskih storitev trudijo svoje storitve zagotavljati tudi z uporabo svojih storitev, ki jih želijo optimizirati na način, da zagotavljajo identifikacijo in avtentikacijo posameznika neposredno v svojih informacijskih sistemih zaradi boljše uporabniške izkušnje ali pa zaradi večje zanesljivosti sistema. Takšna avtentikacija ni mogoča brez povezave med imetnikom sredstva elektronske identifikacije in samim sredstvom, zato se v tem členu določi izrecna zakonska podlaga za obdelavo osebnih podatkov, ki so za to potrebni. Konkretno se v prvem odstavku vzpostavi pravna podlaga za hrambo in obdelavo identifikacijske oznake sredstva elektronske identifikacije, z omejitvijo, da je to mogoče le za namene identifikacije, avtentikacije ali preverjanja identifikacijskih podatkov fizične osebe.

Organ javnega sektorja, ki ima za zagotavljanje elektronskih storitev pravico hraniti in obdelovati osebno ime fizične osebe, lahko v skladu s predlaganim členom hrani in obdeluje tudi EŠEI fizične osebe, če ga potrebuje za elektronsko identifikacijo, avtentikacijo ali preverjanje identifikacijskih podatkov fizične osebe.

Če fizična oseba nima EŠEI, lahko organ uporabi za namene iz prvega odstavka najmanjši nabor drugih identifikacijskih podatkov iz minimalnega nabora podatkov za fizično osebo, kot jih določa Izvedbena uredba Komisije (EU) 2015/1501 z dne 8. septembra 2015 o interoperabilnostnem okviru v skladu s členom 12(8) Uredbe 910/2014/EU, ki še vedno omogočajo doseganje istega namena.

Z navedenim členom se tako v skladu s predpisi s področja varstva osebnih podatkov daje javnemu sektorju pravna podlaga za obdelavo osebnih podatkov.

K 17. členu (preklic sredstva elektronske identifikacije)

V skladu s točko g prvega odstavka 9. člena Uredbe 910/2014/EU mora država članica priglasiteljica priglasiti Komisiji informacije glede ureditve začasne razveljavitve ali preklica priglašene elektronske identifikacijske sheme, avtentikacije ali zadevnih ogroženih delov.

Predlagani člen tako nalaga izdajatelju sredstva elektronske identifikacije preklic sredstva elektronske identifikacije takoj oziroma najpozneje v 24 urah v primerih, taksativno navedenih v prvem odstavku

V drugem odstavku je določeno, da po preklicu izdajatelj sredstva elektronske identifikacije onemogoči nadaljnjo uporabo sredstva elektronske identifikacije oziroma zagotovi informacijo o preklicu v svojem sistemu za samodejno strojno preverjanje veljavnosti sredstva elektronske identifikacije.

Izdajatelj sredstva elektronske identifikacije mora najpozneje v 24 urah obvestiti imetnika preklicanega sredstva elektronske identifikacije (razen v primeru, ko je imetnik umrl). Podatke o preklicu preda tretji osebi, ki jih zahteva, ali jih javno objavi.

Navedeni člen je z nalaganjem obveznosti preklica v primeru nastanka tveganega položaja namenjen čim večji omejitvi tveganja za zlorabo identitete, ki po podatkih narašča, posledice pa so lahko zelo hude.

K 18. členu (dolžnosti imetnikov pri preklicu sredstev elektronske identifikacije)

Predlagani člen imetniku sredstva elektronske identifikacije nalaga, da zahteva preklic svojega sredstva elektronske identifikacije, če so bili podatki, nosilec sredstva elektronske identifikacije ali naprave ali informacijski sistem imetnika sredstva elektronske identifikacije spremenjeni, izgubljeni, odtujeni ali ogroženi tako, da to vpliva na veljavnost oziroma raven zanesljivosti sredstva elektronske identifikacije, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v sredstvu elektronske identifikacije ali v evidenci sredstev elektronske identifikacije, ki vplivajo na veljavnost oziroma raven zanesljivosti sredstva elektronske identifikacije.

Tudi ta člen je enako kot prejšnji z nalaganjem obveznosti preklica v primeru nastopa tveganega stanja namenjen čim večji omejitvi tveganja za pojav zlorabe identitete, ki po podatkih narašča, posledice pa so lahko zelo hude.

K 19. členu (učinek preklica sredstva elektronske identifikacije)

S predlaganima prejšnjima členoma se je vpeljal preklic sredstev elektronske identifikacije, s tem predlaganim členom pa se ureja njegov učinek. Preklic sredstva elektronske identifikacije učinkuje med imetnikom sredstva elektronske identifikacije in izdajateljem tega sredstva od trenutka preklica dalje. Preklic sredstva elektronske identifikacije učinkuje med tretjimi osebami in izdajateljem sredstva elektronske identifikacije od trenutka objave, ali če preklic še ni javno objavljen, od trenutka, ko tretje osebe zanj zvedo. Čas preklica se evidentira v evidenci sredstev elektronske identifikacije.

K 20. členu (začasna razveljavitev sredstva elektronske identifikacije)

S predlaganim členom se določa možnost začasne razveljavitve sredstva elektronske identifikacije, ki pomeni neveljavnost sredstva elektronske identifikacije v času njegove razveljavitve. Navedeno je na primer zaradi primerov, ko imetnik založi oziroma se trenutno ne spomni, kje je sredstvo elektronske identifikacije oziroma njegov nosilec, vendar ni prepričan, ali ga je trajno izgubil. Možnost začasne razveljavitve sredstva elektronske identifikacije izhaja iz točke g prvega odstavka 9. člena Uredbe 910/2014/EU.

Pri predlaganem členu smo se zgledovali po 28. členu Uredbe 910/2014/EU, ki se sicer nanaša na kvalificirano potrdilo za elektronski podpis. Ta v petem odstavku določa, da države članice lahko določijo nacionalna pravila o začasni razveljavitvi kvalificiranega potrdila za elektronski podpis, pri čemer morata biti izpolnjena naslednja pogoja:

a) če je kvalificirano potrdilo za elektronski podpis začasno razveljavljeno, to potrdilo za čas začasne razveljavitve preneha veljati ter

b) obdobje začasne razveljavitve se jasno navede v podatkovni zbirki potrdil, v tem času pa mora biti iz storitve, ki zagotavlja informacije o statusu potrdila, razvidno, da je kvalificirano potrdilo začasno razveljavljeno.

O tem tudi Uvodna izjava št. 53 Uredbe 910/2014/EU (ki sicer govori o začasni razveljavitvi kvalificiranih potrdil), ki navaja, da je začasna razveljavitev kvalificiranih potrdil uveljavljena

operativna praksa ponudnikov storitev zaupanja v več državah članicah, ki se razlikuje od preklica potrdila in pomeni začasno prenehanje njegove veljavnosti. Zaradi pravne varnosti mora biti vedno jasno navedeno, da je potrdilo začasno razveljavljeno. Ponudniki storitev zaupanja bi zato morali jasno navesti status potrdila, v primeru njegove začasne razveljavitve pa tudi natančno obdobje, za katero je potrdilo začasno razveljavljeno. Ta uredba ponudnikom storitev zaupanja ali državam članicam ne bi smela nalagati uporabe začasne razveljavitve, morala pa bi zagotavljati pravila o preglednosti, kadar in kjer je taka praksa na voljo.

Navedeni člen skupaj z uvodno izjavo je bil torej zgled za oblikovanje predlaganega člena. Tako drugi odstavek določa, da se začasna razveljavitev izvede le na podlagi izrecne zahteve imetnika sredstva elektronske identifikacije. V skladu s tretjim odstavkom lahko začasna razveljavitev traja največ 48 ur. Če imetnik v tem roku ne zahteva vzpostavitve veljavnosti sredstva elektronske identifikacije, izdajatelj prekliče to sredstvo.

Izdajatelj sredstva elektronske identifikacije pošlje podatke o začasni razveljavitvi tretji osebi, ki jih zahteva, ali jih javno objavi. Pri tem mora biti jasno razvidno, da gre za začasno razveljavitev.

Izdajatelj sredstva elektronske identifikacije pri ureditvi začasne razveljavitve smiselno upošteva določila tega zakona, ki se nanašajo na preklic sredstva elektronske identifikacije.

K 21. členu (priglasitev sheme elektronske identifikacije)

Predlog člena določa, da pristojni organ (ki je ministrstvo, pristojno za informacijsko družbo) kot sheme elektronske identifikacije priglasi tista sredstva elektronske identifikacije, ki imajo v Uredbi 910/2014/EU določen namen čezmejne uporabe.

3. STORITVE ZAUPANJA

K 22. členu (začetek zagotavljanja nekvalificirane storitve zaupanja)

Čeprav Uredba 910/2014/EU tega ne zahteva, pa zgolj z vidika preglednosti stanja na trgu in obveščenosti o dejanskem stanju ponudbe predlog člena določa, da ponudniki kvalificiranih storitev zaupanja pred začetkom zagotavljanja nekvalificirane storitve zaupanja obvestijo nadzorni organ za storitve zaupanja najmanj osem dni pred začetkom izvajanja te storitve, ki uvrsti storitev zaupanja na seznam nekvalificiranih storitev zaupanja.

K 23. členu (oprema za zagotavljanje nekvalificirane storitve zaupanja)

Z namenom zagotavljanja čim boljše kakovosti, varnosti in transparentnosti izvajanja nekvalificiranih storitev zaupanja, predvsem za vse uporabnike storitev zaupanja in zanašajoče se stranke, je s predlogom člena določena obveznost, da če ponudnik kvalificiranih storitev zaupanja za izvajanje nekvalificiranih storitev zaupanja uporablja strojno oziroma programsko opremo, ki se uporablja tudi za izvajanje kvalificiranih storitev zaupanja, mora ponudnik na tej strojni oziroma programski opremi izvajati postopke v skladu z zahtevami za kvalificirano storitev zaupanja.

K 24. členu (uporaba EŠEI pri kvalificiranih potrdilih)

Predlog člena opredeljuje uporabo EŠEI pri kvalificiranih potrdilih, ki tako poenoti identifikacijo fizične in pravne osebe v vseh kvalificiranih potrdilih. Glede EŠEI glej tudi obrazložitev k 3. členu.

Tako je v prvem odstavku določeno, katere podatke še vsebuje kvalificirano potrdilo za elektronski podpis, če je fizični osebi mogoče določiti EŠEI.

V drugem odstavku je določeno, katere podatke kvalificirano potrdilo za elektronski podpis, ki se izdaja za fizično osebo pri poslovnem subjektu, še vsebuje, če je poslovnemu subjektu mogoče določiti EŠEI.

V tretjem odstavku je določeno, katere podatke kvalificirano potrdilo za elektronski žig še vsebuje, če je poslovnemu subjektu mogoče določiti EŠEI.

V četrtem odstavku je določeno, katere podatke kvalificirano potrdilo za avtentikacijo spletišč še vsebuje, če je fizični osebi ali poslovnemu subjektu mogoče določiti EŠEI.

V petem odstavku je vladi dana pravna podlaga, da določi tehnične specifikacije za zapis EŠEI v kvalificirano potrdilo ter za dostop do storitve za pridobivanje oziroma preverjanje EŠEI na podlagi identifikacijskih podatkov kvalificiranega potrdila iz tega člena.

K 25. členu (evidenca imetnikov kvalificiranih potrdil za elektronski podpis)

Določba je potrebna zaradi pravne varnosti posameznikov pri obdelavi njihovih podatkov, prav tako pa določitev obdelave osebnih podatkov v državnih organih v zakonu predvidevata Zakon o varstvu osebnih podatkov (ZVOP-1) in Splošna uredba o varstvu podatkov. Predlagani člen z namenom varovanja osebnih podatkov imetnika ob upoštevanju načela sorazmernosti taksativno našteva, katere podatke naj vsebuje evidenca imetnikov kvalificiranih potrdil za elektronski podpis, ki jo vodi ponudnik kvalificiranih storitev zaupanja, registriran v Republiki Sloveniji za identifikacijo in preverjanje identifikacijskih podatkov fizične osebe, za katero se izdaja kvalificirano potrdilo za elektronski podpis, ter za izdajo kvalificiranega potrdila za elektronski podpis in zagotavljanje njegove uporabe.

Predlagatelj je podatke pregledal in ugotovil, v katerih delih bi lahko določene podatke hranil. Odločitev je smiselno enaka, kot je bila za podatke o imetnikih sredstva elektronske identifikacije iz 11. člena.

V tretjem odstavku je določeno, kateri podatki se še vodijo v evidenci imetnikov kvalificiranih potrdil za elektronski podpis fizične osebe pri poslovnem subjektu, za katero se izdaja kvalificirano potrdilo za elektronski podpis.

Četrti odstavek določa, da določila tega člena smiselno veljajo tudi v primeru izdaje kvalificiranega potrdila za avtentikacijo spletišč, če je imetnik fizična oseba.

Tudi pri tem predlaganem členu se poskuša slediti enemu izmed temeljnih načel varstva osebnih podatkov – načelu sorazmernosti. Za vsak osebni podatek, ki se od posameznika zahteva, je treba utemeljeno izkazati potrebnost obdelave podatka za dosego konkretnega (zakonitega) cilja. Nesorazmerno oziroma glede na namen prekomerno zbiranje osebnih podatkov namreč pomeni večje tveganje za kršitve in zlorabe osebnih podatkov, obenem pa na upravljavca nalaga večje breme za pravilno zavarovanje.

K 26. členu (evidenca imetnikov kvalificiranih potrdil za elektronski žig)

Predlagani člen z namenom varovanja osebnih podatkov ob upoštevanju načela sorazmernosti taksativno našteva, katere podatke naj vsebuje evidenca, ki jo vodi ponudnik kvalificiranih storitev zaupanja, registriran v Republiki Sloveniji, za identifikacijo in preverjanje identifikacijskih podatkov poslovnega subjekta in pooblaščenega predstavnika poslovnega subjekta, za katerega se izdaja kvalificirano potrdilo za elektronski žig.

Podatki iz drugega odstavka se v večini nanašajo na poslovni subjekt, njegova šesta točka pa vsebuje osebne podatke pooblaščenega predstavnika poslovnega subjekta, ki je tudi oseba, ki kvalificirano potrdilo prevzame in je zanj odgovorna. Posledično se tudi potrebujejo osnovni podatki, potrebni za njeno identifikacijo.

Tretji odstavek določa, da določila tega člena, ki veljajo za kvalificirana potrdila za elektronski žig, smiselno veljajo tudi v primeru izdaje kvalificiranega potrdila za avtentikacijo spletišč, če je imetnik poslovni subjekt.

K 27. členu (hramba podatkov o imetniku kvalificiranega potrdila)

Predlagani člen ureja hrambo podatkov o imetniku kvalificiranega potrdila. Ta je določena na deset let po prenehanju veljavnosti izdanega kvalificiranega potrdila ali deset let po koncu postopka, če se postopek ni končal z izdajo kvalificiranega potrdila. S tem se sledi Uvodni izjavi št. 61 Uredbe 910/2014/EU, ki navaja, da bi ta uredba morala zagotoviti dolgoročno hrambo informacij, da se zagotovi pravna veljavnost elektronskih podpisov in elektronskih žigov v daljšem časovnem obdobju ter da se jih lahko potrdi ne glede na prihodnje tehnološke spremembe.

K 28. členu (hramba podatkov za potrjevanje veljavnosti elektronskega podpisa, elektronskega žiga in elektronskega časovnega žiga)

Predlagani člen določa hrambo podatkov za potrjevanje veljavnosti elektronskega podpisa, elektronskega žiga in elektronskega časovnega žiga. Če predpis določa, da se hrani elektronski dokument, zapis ali podatek, ki je elektronsko podpisan, elektronsko žigosan ali elektronsko časovno žigosan, mora tisti, ki mora dokument, zapis ali podatek hraniti, hraniti tudi podatke za potrjevanje veljavnosti elektronskega podpisa, elektronskega žiga ali elektronskega časovnega žiga. Podatki za potrjevanje veljavnosti se hranijo enako dolgo kot navedeni elektronski dokumenti, zapisi ali podatki. S tem se sledi Uvodni izjavi št. 61 Uredbe 910/2014/EU, ki navaja, da bi ta uredba morala zagotoviti dolgoročno hrambo informacij, da se zagotovi pravna veljavnost elektronskih podpisov in elektronskih žigov v daljšem časovnem obdobju ter da se jih lahko potrdi ne glede na prihodnje tehnološke spremembe.

K 29. členu (identifikacija ob izdaji kvalificiranih potrdil)

V predlaganem členu je urejen način preverjanja istovetnosti in preverjanja pravilnosti podatkov, potrebnih za izdajo kvalificiranega potrdila. Določba je namenjena določitvi ureditve po Uredbi 910/2014/EU, ki se glede teh vprašanj sklicuje na posebnosti nacionalne zakonodaje.

V predlogu člena je predvsem iz razloga čim večje gotovosti o istovetnosti prave identitete izbrana možnost, ki jo opredeljuje točka a prvega odstavka 24. člena Uredbe 910/2014/EU. V skladu z navedenim ponudnik kvalificirane storitve zaupanja za namene izdaje kvalificiranega potrdila za elektronski podpis ali avtentikacijo spletišč fizični osebi izvede preverjanje istovetnosti fizične osebe v skladu s prvo alinejo točke b prvega odstavka 10. člena tega zakona, torej identifikacijo, ki je potrebna za pridobitev sredstva elektronske identifikacije srednje ravni zanesljivosti, kar vključuje posledično tudi drugi odstavek 10. člena, ki določa posebne vrste identifikacije. Glej obrazložitev 10. člena.

Drugi odstavek določa postopek preverjanja za izdajo kvalificiranega potrdila za elektronski podpis fizične osebe pri poslovnem subjektu, tudi v skladu s točko a prvega odstavka 24. člena Uredbe 910/2014/EU.

V tretjem odstavku pa se določa postopek preverjanja za izdajo kvalificiranega potrdila za elektronski žig ali avtentikacijo spletišč poslovnemu subjektu, tudi v skladu s točko a prvega odstavka 24. člena Uredbe 910/2014/EU.

Četrti odstavek opredeli delo prijavne službe.

K 30. členu (preverjanje podatkov v verodostojnih virih v Republiki Sloveniji)

Ponudniki kvalificiranih storitev zaupanja imajo za namene iz 29. člena po predlaganem členu pravico brezplačno pridobiti ali preveriti podatke v verodostojnem viru, kar bo znižalo njihova administrativna bremena, povečalo varnost in zmanjšalo tveganja kraje identitete ter posledično zagotovilo večje zaupanje javnosti v elektronsko poslovanje. Glede verodostojnih virov glej obrazložitev k 31. členu.

K 31. členu (verodostojni vir v Republiki Sloveniji)

Predlagani člen določa verodostojne vire podatkov v Republiki Sloveniji. O državljanih Republike Slovenije je to centralni register prebivalstva, o tujcih v Republiki Sloveniji sta to centralni register prebivalstva in davčni register ter o poslovnih subjektih, registriranih v Republiki Sloveniji, je to poslovni register Slovenije.

K 32. členu (povezovanje evidenc imetnikov kvalificiranih potrdil)

Predlagani člen predvideva povezovanje evidenc imetnikov kvalificiranih potrdil, in sicer je v njem podrobneje opredeljen postopek njihovega povezovanja s centralnim registrom prebivalstva, davčnim registrom in poslovnim registrom. Za preverjanje pravilnosti podatkov je namreč nujno uparjanje podatkov z javnimi registri, za kar je potrebna izrecna zakonska podlaga.

Zaradi varstva osebnih podatkov se povezovanje lahko izvede le, če ponudnik kvalificiranih potrdil že ima na voljo ali davčno številko ali EMŠO, kar je podatek, ki ga za izmenjavo podatkov obravnava drugi odstavek. Zaradi minimalne obdelave podatkov je drugi odstavek potreben že v primeru izdaje kvalificiranega potrdila za elektronski podpis, ki ga bo vsebovala osebna izkaznica, ko gre za postopek, ko prijavna služba nima na voljo davčne številke, ima pa EMŠO. Po pridobitvi podatkov se EMŠO izbriše.

K 33. členu (notranja pravila)

S predlaganim členom se določa obveznost ponudnika kvalificiranih storitev zaupanja, da posluje v skladu s svojimi notranjimi pravili, ki morajo vsebovati javni in zaupni del in ki jih ta opredeli v skladu z zahtevami Uredbe 910/2014/EU za ponudnike kvalificiranih storitev zaupanja in standardov, na podlagi katerih je skladnost njegovega poslovanja certificiral organ za ugotavljanje skladnosti.

K 34. členu (preklic kvalificiranih potrdil)

Predlagani člen tako nalaga ponudniku kvalificiranih storitev zaupanja preklic kvalificiranega potrdila za elektronski podpis, elektronski žig ali avtentikacijo spletišč (v nadaljnjem besedilu: kvalificirano potrdilo) v skladu s svojimi notranjimi pravili, ki urejajo preklice potrdil takoj oziroma v skladu s tretjim odstavkom 24. člena Uredbe 910/2014/EU. Da bi se izognili nezaželeni uporabi oziroma morebitnim zlorabam uporabe, predlagani člen tako v prvem odstavku taksativno našteva stanja, v katerih ponudnik kvalificiranih storitev zaupanja opravi preklic.

Drugi odstavek določa obveznost imetnika kvalificiranega potrdila, kdaj mora zahtevati preklic svojega kvalificiranega potrdila.

Prav tako mora ponudnik kvalificiranih storitev zaupanja v skladu s tretjim odstavkom v svojih notranjih pravilih določiti, kdaj in kako se obvešča o izdaji oziroma preklicu kvalificiranega potrdila.

Predlagani člen je z nalaganjem obveznosti preklica v primeru nastopa tveganega stanja namenjen čim večji omejitvi tveganja za pojav zlorabe kvalificiranih potrdil.

K 35. členu (učinek preklica kvalificiranih potrdil)

Predlog člena glede preklica kvalificiranega potrdila določa, da učinkuje med imetnikom kvalificiranega potrdila in ponudnikom kvalificiranih storitev zaupanja od trenutka preklica. Preklic potrdila učinkuje med tretjimi osebami in ponudnikom kvalificiranih storitev zaupanja od trenutka objave, ali če preklic še ni javno objavljen, od trenutka, ko tretje osebe zanj zvedo. Čas preklica se evidentira v evidenci kvalificiranih potrdil.

K 36. členu (začasna razveljavitev kvalificiranih potrdil za elektronski podpis in elektronski žig)

S predlaganim členom se vpeljuje možnost, ki jo omogoča 28. člen Uredbe 910/2014/EU. Ta v petem odstavku določa, da države članice lahko določijo nacionalna pravila o začasni razveljavitvi kvalificiranega potrdila za elektronski podpis, pri čemer morata biti izpolnjena naslednja pogoja: a) če je kvalificirano potrdilo za elektronski podpis začasno razveljavljeno, to potrdilo za obdobje začasne razveljavitve preneha veljati ter (b) obdobje začasne razveljavitve se jasno navede v podatkovni zbirki potrdil, v tem času pa mora biti iz storitve, ki zagotavlja informacije o statusu potrdila, razvidno, da je kvalificirano potrdilo začasno razveljavljeno.

Tako se vpeljuje možnost začasne razveljavitve kvalificiranega potrdila za elektronski podpis in elektronski žig in pomeni neveljavnost kvalificiranega potrdila samo v določenem obdobju. Navedeno na primer zaradi primerov, ko imetnik založi oziroma se trenutno ne spomni, kje je navedeno kvalificirano potrdilo, vendar ni prepričan, ali je trajno izginilo. Izvede se le na podlagi izrecne zahteve imetnika kvalificiranega potrdila.

Ponudnik kvalificiranih storitev zaupanja mora, če omogoča začasno razveljavitev kvalificiranega potrdila, pogoje in postopke v zvezi z začasno razveljavitvijo urediti v svojih notranjih pravilih, kot to določa drugi odstavek.

Četrti odstavek opredeljuje trajanje začasne razveljavitve, ki lahko traja največ 48 ur. Če imetnik v tem roku ne zahteva vzpostavitve veljavnosti kvalificiranega potrdila, ponudnik storitve prekliče kvalificirano potrdilo.

Ponudnik kvalificiranih storitev zaupanja mora v skladu s petim odstavkom pri ureditvi začasne razveljavitve smiselno upoštevati določila tega zakona in Uredbe 910/2014/EU, ki se nanašajo na preklic kvalificiranih potrdil.

O začasni razveljavitvi kvalificiranih potrdil tudi Uvodna izjava št. 53 Uredbe 910/2014/EU navaja, da je začasna razveljavitev kvalificiranih potrdil uveljavljena operativna praksa ponudnikov storitev zaupanja v več državah članicah, ki se razlikuje od preklica potrdila in pomeni začasno prenehanje njegove veljavnosti. Zaradi pravne varnosti mora biti vedno jasno navedeno, da je potrdilo začasno razveljavljeno. Ponudniki storitev zaupanja bi zato morali jasno navesti status potrdila, v primeru njegove začasne razveljavitve pa tudi natančno obdobje, za katero je potrdilo začasno razveljavljeno. Ta uredba ponudnikom storitev zaupanja ali državam

članicam ne bi smela nalagati uporabe začasne razveljavitve, morala pa bi zagotavljati pravila o preglednosti, kadar in kjer je taka praksa na voljo.

K 37. členu (zaposleni pri ponudniku kvalificiranih storitev zaupanja)

Ker točka b drugega odstavka 24. člena Uredbe 910/2014/EU določa, da ponudniki kvalificiranih storitev zaupanja zaposlujejo osebje in po potrebi podizvajalce, ki imajo potrebno strokovno znanje, izkušnje in kvalifikacije ter so zanesljivi in ki so se udeležili ustreznega usposabljanja v zvezi z varnostjo in pravili o varstvu osebnih podatkov ter uporabljajo upravne in upravljavske postopke, ki so v skladu z evropskimi ali mednarodnimi standardi, se s predlogom tega člena nadrobneje predstavi navedena zahteva.

Podobno določbo glede izobrazbe je vsebovala že na podlagi ZEPEP sprejeta Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje, po kateri smo se tudi zgledovali pri konkretizaciji člena o ustreznosti izobrazbe Uredbe 910/2014/EU. Glede na kompleksnost področja je zahteva glede izobrazbe potrebna in smiselna.

K 38. členu (uporaba podatkov za ustvarjanje kvalificiranega elektronskega podpisa)

Predlog člena vzpostavlja pogoje za ustvarjanje kvalificiranega elektronskega podpisa. Vsaka uporaba podatkov za ustvarjanje kvalificiranega elektronskega podpisa mora z vidika varnosti oziroma zagotovitve, da ima podpisnik izključni nadzor nad uporabo svojih podatkov za ustvarjanje elektronskega podpisa (v skladu z Uvodno izjavo št. 51 Uredbe 910/2014/EU ter točko c 26. člena 910/2014/EU), od podpisnika zahtevati prostovoljno, specifično, ozaveščeno, razumljivo, nedvoumno in zanesljivo dejanje za predstavitev napravi za ustvarjanje kvalificiranega elektronskega podpisa (na primer vnos gesla, prstni odtis).

Če dejanje za predstavitev vključuje tudi voljo podpisnika za več podpisov, se podatki za ustvarjanje kvalificiranega elektronskega podpisa uporabijo tudi za te konkretne podpise. Predlagatelj predlaga konkretizacijo, da se informacijski sistemi razvijejo tako, da lahko posameznik opredeli, katere dokumente želi podpisati, potem pa to stori s pomočjo informacijskega sistema, ne da bi moral za vsak posamezni podpis vnašati geslo – svojo voljo izrazi še s tem, ko dokument predhodno izbere.

K 39. členu (časovna veljavnost kvalificiranega potrdila)

Predlagani člen določa najdaljšo veljavnost kvalificiranega potrdila, ki je največ deset let od dneva njegove izdaje. S tem sledimo stanju tehnike na področju kriptiranja in varnosti različnih danes znanih algoritmov, s katerimi zagotavljamo, da se elektronski podpisi ne morejo potvoriti, hkrati pa omogočamo imetnikom čim daljšo uporabo konkretnega sredstva.

K 40. členu (ponudnik kvalificiranih storitev zaupanja v državnih organih)

Po predlogu člena ponudnik kvalificiranih storitev zaupanja Republika Slovenija (tako imenovani SI-TRUST), ki deluje v okviru ministrstva, pristojnega za centralno storitev za spletno prijavo in elektronski podpis, izvaja kvalificirane storitve zaupanja za potrebe državnih organov. Informacijske rešitve za elektronsko poslovanje v podporo poslovanju državnih organov, ki vključujejo tudi uporabo kvalificiranih storitev zaupanja, uporabljajo kvalificirane storitve zaupanja ponudnika kvalificiranih storitev zaupanja Republika Slovenija in njemu podrejenih ali od njega potrjenih drugih ponudnikov kvalificiranih storitev zaupanja. S tem zagotavljamo enotno podporo elektronskemu poslovanju državnih organov.

K 41. členu (prijavna služba ponudnika kvalificiranih storitev zaupanja Republika Slovenija)

Predlog člena v prvem odstavku določa, da naloge v zvezi s prijavo in preverjanjem istovetnosti imetnikov v postopkih izdaje in upravljanja kvalificiranih potrdil ponudnika kvalificiranih storitev zaupanja Republika Slovenija lahko opravljajo državni organi. Državni center za storitve zaupanja SI-TRUST, ki deluje v okviru Ministrstva za javno upravo Republike Slovenije ter izdaja kvalificirana digitalna potrdila za posameznike, poslovne subjekte in državne organe, bo tako v svojih notranjih pravilih določil pogoje in način izvajanja nalog prijavne službe. Člen omogoča široko mrežo prijavnih služb v različnih državnih organih, kar bo omogočilo čim večjo predvsem geografsko dostopnost do storitev zaupanja.

Tretji odstavek določa pravico ponudnika kvalificiranih storitev zaupanja Republika Slovenija vpogleda v dokumentacijo, ki jo v postopkih izdaje in upravljanja kvalificiranih potrdil hranijo prijavne službe. To je pogoj za izvajanje nadzora nad ustreznostjo vodenja postopkov sprejema vlog in preverjanjem istovetnosti, ki so med najpomembnejšimi v celotnem postopku izdaje kvalificiranih potrdil in posledično najpomembnejši za zaupanje v verodostojnost kvalificiranih potrdil.

K 42. členu (preverjanje interesa za certificiranje kvalificiranih naprav za ustvarjanje kvalificiranega elektronskega podpisa)

Predlog člena določa, da ministrstvo, pristojno za informacijsko družbo, z javnim pozivom vsaj vsaki dve leti pozove javnost k priglasitvi interesa za certificiranje kvalificiranih naprav za ustvarjanje kvalificiranega elektronskega podpisa. Uredba 910/2014/EU zahteva za kvalificirani elektronski podpis uporabo naprave za ustvarjanje kvalificiranega elektronskega podpisa, ki izpolnjuje zahteve iz Priloge II. Te naprave morajo biti ustrezno certificirane v skladu s 30. členom 910/2014/EU, pri čemer mora država zagotoviti ustrezno pravno okolje in imenovati ustrezne organe za certificiranje. Glede na to, da v Sloveniji do zdaj nismo imeli ponudnika naprav, ki bi bil zainteresiran za certifikacijo, država, da bi se izognila nepotrebnim stroškom, ni vzpostavila okvira in imenovala ustreznega organa za certifikacijo. Ta člen zagotavlja, da država preverja interes in po potrebi vzpostavi okvir za certificiranje naprav.

K 43. členu (vpis v nacionalni zanesljivi seznam)

Glede vpisa v nacionalni zanesljivi seznam predlog člena določa, da pristojni organ ponudnika storitev zaupanja in kvalificirane storitve zaupanja, ki jih želi zagotavljati, vpiše v nacionalni zanesljivi seznam, če so za to izpolnjeni vsi pogoji iz tega zakona in Uredbe 910/2014/EU – o zanesljivih seznamih podrobneje njen 22. člen. O tem tudi Uvodna izjava št. 45 Uredbe 910/2014/EU, ki v interesu omogočanja učinkovitega postopka za vključitev ponudnikov kvalificiranih storitev zaupanja in kvalificiranih storitev zaupanja, ki jih ti zagotavljajo, na zanesljive sezname navaja, da bi bilo treba v ta namen spodbujati predhodno sodelovanje med bodočimi ponudniki kvalificiranih storitev zaupanja in pristojnim nadzornim organom, da se spodbudi ustrezna skrbnost, potrebna za začetek zagotavljanja kvalificiranih storitev zaupanja. Uvodna izjava št. 46 nadalje tudi, da so zanesljivi seznami bistveni elementi za krepitev zaupanja med udeleženci na trgu, saj je iz njih razvidno, da je imel ponudnik storitev v trenutku nadzora kvalificiran status.

Drugi odstavek določa, da pristojni organ (to je v skladu s predlogom zakona organ, pristojen za informacijsko varnost) s potrdilom obvesti ponudnika kvalificiranih storitev o vpisu iz prvega odstavka.

V tretjem odstavku je določena pristojnost navedenega organa, da v primeru, ko ponudnik storitve zaupanja ali kvalificirane storitve zaupanja, ki jih želi zagotavljati, ne izpolnjujejo vseh pogojev, o tem izda odločbo.

Zoper odločbo iz prejšnjega odstavka ni pritožbe, zagotovljeno pa je sodno varstvo v upravnem sporu. ZEPEP je do sedaj sicer določal pritožbeni postopek na način, da v njem odloča vlada (peti odstavek 41. člena), vendar je bila sprememba določena zaradi sistemskega ukinjanja vlade kot pritožbenega organa.

K 44. členu (sprememba ali odvzem kvalificiranega statusa v nacionalnem zanesljivem seznamu)

S predlaganim členom se pristojnemu organu (to je v skladu s predlogom zakona organ, pristojen za informacijsko varnost) daje pristojnost odločanja o spremembi ali odvzemu kvalificiranega statusa ponudnika kvalificiranih storitev zaupanja ali kvalificiranih storitev zaupanja, ki jih ta zagotavlja, iz nacionalnega zanesljivega seznama.

Zoper odločbo pristojnega organa ni pritožbe, zagotovljeno pa je sodno varstvo v upravnem sporu.

4. CENTRALNA STORITEV ZA SPLETNO PRIJAVO IN ELEKTRONSKI PODPIS

K 45. členu (centralna storitev za spletno prijavo in elektronski podpis)

Predlog člena opredeljuje centralno storitev za spletno prijavo in elektronski podpis, ki je informacijska rešitev, preko katere se posameznik lahko identificira in avtenticira z uporabo sredstev elektronske identifikacije; preko katere lahko elektronsko podpiše dokument z uporabo potrdila za elektronski podpis; ki zagotavlja funkcionalnost čezmejne avtentikacije in zagotavlja ustvarjanje pooblastil v elektronski obliki za identifikacijo in avtentikacije pooblaščenca in njihovo uporabo v pravnem prometu.

V skladu s 34.a členom Zakona o državni upravi (Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14 in 51/16) je za zagotavljanje centralne storitve za spletno prijavo in elektronski podpis pristojno ministrstvo za javno upravo.

Drugi, tretji in četrti odstavek določajo, kdo in pod kakšnimi pogoji lahko uporablja centralno storitev za spletno prijavo in elektronski podpis.

V petem odstavku je vladi dana pravna podlaga, da določi pogoje in tehnične specifikacije za izvajanje prejšnjih odstavkov. Vlada z uredbo določi tudi cenik storitev za ponudnike elektronskih storitev.

Člen med drugim konkretizira storitev SI-PASS, ki je enotna točka za preverjanje identitete različnih uporabnikov (državljanov, poslovnih subjektov, javnih uslužbencev) ter elektronsko podpisovanje vlog in ostalih dokumentov. SI-PASS se praviloma uporablja v okviru opravljanja posameznih elektronskih storitev (na primer eUprava, eVem).

Predlagani člen v šestem in sedmem odstavku vzpostavlja tudi pravila za pooblastilo v elektronski obliki preko centralne storitve za spletno prijavo in elektronski podpis, ki v skladu s četrto alinejo prvega odstavka zagotavlja ustvarjanje pooblastil v elektronski obliki za identifikacijo in avtentikacije pooblaščenca in njihovo uporabo v pravnem prometu. Sedmi odstavek omogoča vzpostavitev vezi med fizično in elektronsko obliko poslovanja za tiste, ki elektronske oblike niso vešči ali je zaradi katerega koli razloga ne uporabijo.

K 46. členu (obdelava osebnih podatkov in povezovanje centralne storitve za spletno prijavo in elektronski podpis)

Člen z vidika varstva osebnih podatkov in v skladu z načelom sorazmernosti taksativno našteva podatke, ki se lahko hranijo v okviru centralne storitve za spletno prijavo in elektronski podpis za namene njene uporabe in koliko časa se lahko hranijo. Pri tem razlikuje storitev zagotavljanja ustvarjanja pooblastil v elektronski obliki za identifikacijo in avtentikacijo pooblaščenca in njihovo uporabo v pravnem prometu od preostalih treh storitev.

Za uporabo storitve člen konkretizira minimalni nabor podatkov, ki je potreben za izvajanje posamezne storitve, in sicer v prvem odstavku za storitve prvih treh alinej prvega odstavka 45. člena tega zakona in v tretjem odstavku za storitve pooblaščanja, torej četrte alineje prvega odstavka 45. člena tega zakona.

Identifikator uporabniškega računa posameznika, ki je storitev uporabil, je identifikator, ki ga centralna storitev za spletno prijavo in elektronski podpis določi posamezniku, da posameznik lahko uporablja centralno storitev (številka uporabniškega računa oziroma profila).

Zaradi dejstva, da se povezovanje centralne storitve za spletno prijavo in elektronski podpis s centralnim registrom prebivalstva zagotavlja na podlagi davčne številke, člen predvidi tudi izrecen izvzem davčne številke iz EŠEI in njeno uporabo v okviru centralne storitve za spletno prijavo in elektronski podpis.

V okviru pooblastila je vedno naveden obseg pooblastila, ki po svoji vsebini zajema tudi morebitne omejitve uporabe pooblastila in čas veljavnosti pooblastila (poleg identifikatorja ter podpisa). Če pooblaščenec za izvajanja upravnih postopkov v elektronski obliki potrebuje tudi pooblastilo za pridobivanje podatkov o pooblastitelju, mora biti to v pooblastilu posebej navedeno.

Četrti odstavek določa omejitve centralne storitve za spletno prijavo in elektronski podpis v delu, ki omogoča ustvarjanje in hrambo pooblastil. Da ne bi bilo mogoče razumeti določil tega zakona na način, da bi morali organi v smislu 139. člena Zakona o splošnem upravnem postopku pridobivati podatke od centralne storitve za spletno prijavo in elektronski podpis, pa člen tudi izrecno določa, da centralna storitev za spletno prijavo in elektronski podpis v delu, ki omogoča ustvarjanje in hrambo pooblastil, ni uradna evidenca. Nadalje člen tudi določa, da sta pooblastitelj ali pooblaščenec dolžna zagotoviti, da organ, pred katerim se izvaja zastopanje, dobi pooblastilo iz centralne storitve in prav tako ne moreta zahtevati, da ga pridobi organ po uradni dolžnosti.

Peti odstavek določa roke hrambe pooblastila in podatkov iz tretjega odstavka, vendar se omejuje na čas neodzivnosti uporabnika storitve.

V šestem odstavku predlog člena vsebuje izjemo, in sicer da lahko centralna storitev za spletno prijavo in elektronski podpis pri zagotavljanju storitev iz prvih treh alinej prvega odstavka prejšnjega člena obdeluje tudi druge podatke za njihovo pošiljanje ponudnikom elektronskih storitev, vendar izključno na zahtevo posameznika, ki storitev uporablja. Določeno je tudi, kako se za te namene centralna storitev za spletno prijavo in elektronski podpis povezuje s centralnim registrom prebivalstva, davčnim registrom in poslovnim registrom.

V sedmem odstavku je določen režim povezovanja centralne storitve za spletno prijavo in elektronski podpis s centralnim registrom prebivalstva oziroma poslovnim registrom v primeru oblikovanja pooblastila v elektronski obliki, ki je omejen na preverjanje ustreznosti vnesenih podatkov s strani pooblastitelja ali pooblaščenca.

5. PRISTOJNOSTI ORGANOV

K 47. členu (pristojni organi za elektronsko identifikacijo)

S predlaganim členom se za posamezne naloge, povezane z elektronsko identifikacijo, določijo pristojni organi; in sicer so to ministrstvo, pristojno za informacijsko varnost; organ, pristojen za informacijsko varnost; ministrstvo, pristojno za centralno storitev za spletno prijavo in elektronski podpis.

K 48. členu (pristojnosti nadzornega organa za elektronsko identifikacijo)

S predlaganim členom se določijo pristojnosti nadzornega organa za elektronsko identifikacijo, ki je v skladu s 47. členom tega zakona organ, pristojen za informacijsko varnost – po trenutni ureditvi je to Uprava RS za informacijsko varnost. Nadzorni organ tako preverja skladnost delovanja izdajatelja sredstev elektronske identifikacije s predpisi ter v okviru inšpekcijskega nadzorstva inšpektor preverja, ali organi javnega sektorja, ki so ponudniki elektronskih storitev v skladu s 6. členom Uredbe 910/2014/EU, ves čas izvajanja dejavnosti izpolnjujejo zahteve Uredbe 910/2014/EU, tega zakona in na njegovi podlagi izdanih podzakonskih predpisov. Nadzorni organ za elektronsko identifikacijo je hkrati prekrškovni organ s področja elektronske identifikacije.

K 49. členu (pristojni organi za storitve zaupanja)

S predlaganim členom se določijo nadzorni organ za storitve zaupanja, organ, pristojen za vodenje nacionalnega zanesljivega seznama, in organ, ki je pristojen za akreditacijo organov za ugotavljanje skladnosti.

V skladu s predlogom tega zakona je nadzorni organ tisti organ, ki je pristojen za informacijsko varnost (po trenutni ureditvi je to Uprava RS za informacijsko varnost) in izvaja nadzorne naloge v skladu s 17. členom Uredbe 910/2014/EU. Prav tako je isti organ pristojen za vodenje nacionalnega zanesljivega seznama v skladu z 22. členom Uredbe 910/2014/EU. Za akreditacijo organov za ugotavljanje skladnosti je pristojna Slovenska akreditacija.

K 50. členu (pristojnosti nadzornega organa za storitve zaupanja)

S predlaganim členom se določijo pristojnosti nadzornega organa za storitve zaupanja, ki je hkrati prekrškovni organ s področja storitev zaupanja.

K 51. členu (ukrepi nadzornih organov in pravna sredstva)

Predlagani člen določa ukrepe nadzornih organov in pravna sredstva. Pri tem je treba omeniti, da zoper odločbo inšpektorja ni pritožbe, zagotovljeno pa je sodno varstvo v upravnem sporu. ZEPEP je do sedaj sicer določal pritožbeni postopek na način, da v njem odloča vlada (peti odstavek 41. člena), vendar je bila sprememba določena zaradi sistemskega ukinjanja vlade kot pritožbenega organa.

6. KAZENSKE DOLOČBE

K 52. členu (prekrški ponudnika storitev zaupanja) in 53. členu (prekrški v javnem sektorju)

Pomemben del obvezujočih pravnih norm je tudi ustrezno sankcioniranje kršitev. Predlagane kazenske določbe inkriminirajo kot prekrške vse bistvene kršitve zakona. Pri tem sledijo tudi obveznostim, ki izhajajo iz Uredbe 910/2014/EU. Glede razpona kazni predlagane določbe sledijo razponom za sorodne prekrške v Zakonu o varstvu potrošnikov.

Prav tako predlog zakona določa prekrške za odgovorne osebe organov v javnem sektorju (kot je ta opredeljen v 3. točki 2. člena predloga zakona). Pomembna vidika izvajanja predloga zakona in Uredbe 910/2014/EU sta namreč preglednost in odprtost poslovanja javnega sektorja do uporabnikov. Kot je pokazala praksa, je tovrstna kazenska določba v Zakonu o dostopu do informacij javnega značaja močno pripomogla k hitrejši in širši uveljavitvi določb. Prav tako je določba pomembna zaradi zagotavljanja enakosti vseh ponudnikov. Ker kot ponudniki storitev nastopajo tudi organi javnega sektorja, bi bilo namreč diskriminatorno in v nasprotju z enakostjo pred zakonom, da bi bile za povsem enake kršitve prekrškovnim sankcijam izpostavljene samo odgovorne osebe zasebnih ponudnikov, ne pa tudi ponudnikov iz javnega sektorja.

K 54. členu (nezakonita uporaba sredstva elektronske identifikacije in nezakonita uporaba kvalificiranega potrdila)

Zaradi v predlaganem 4. členu zakona vsebovane obveznosti skrbnosti ravnanja imetnika sredstva elektronske identifikacije in imetnika kvalificiranega potrdila se s predlaganim členom kaznujeta imetnik sredstva elektronske identifikacije v primeru nezakonite uporabe izdanega sredstva elektronske identifikacije v nasprotju s prvim odstavkom 4. člena tega zakona ter imetnik kvalificiranega potrdila v primeru nezakonite uporabe izdanega kvalificiranega potrdila v nasprotju z drugim odstavkom 4. člena tega zakona.

K 55. člen (višina globe v hitrem prekrškovnem postopku)

V predlaganem členu je dana pravna podlaga, da se za prekrške iz tega zakona sme v hitrem postopku izreči globa tudi v znesku, ki je višji od najnižje prepisane globe, določene s tem zakonom.

7. PREHODNA DOLOČBA

K 56. členu (uporaba kvalificiranih potrdil za elektronski podpis, ki so izdana tudi za namen avtentikacije)

Predlog člena določa, da lahko fizična oseba za namene elektronske identifikacije in avtentikacije za dostop do elektronskih storitev v javnem sektorju iz 14. člena predloga zakona pod taksativno navedenimi tremi pogoji uporablja kvalificirano potrdilo za elektronski podpis še pet let po uveljavitvi tega zakona.

Trenutno to vprašanje ureja Uredba o izvajanju Uredbe 910/2014/EU, ki v svojem 2. členu vsebuje določbo o uporabi kvalificiranih potrdil za elektronski podpis in da se posledično kot sredstvo elektronske identifikacije lahko uporabi tudi kvalificirano potrdilo za elektronski podpis, ki je izdano tudi za namen avtentikacije, in sicer brez časovne zamejitve, do kdaj se ta potrdila za namen elektronske identifikacije lahko uporabljajo. S sprejetjem predloga zakona se bodo ta potrdila lahko uporabljala le še pet let po njegovi uveljavitvi.

8. KONČNE DOLOČBE

K 57. členu (začetek preverjanja interesa za certificiranje kvalificiranih naprav za ustvarjanje kvalificiranega elektronskega podpisa)

Predlog člena določa, da z dnem uveljavitve predloga zakona začne teči dveletni rok za poziv javnosti k priglasitvi interesa za certificiranje kvalificiranih naprav za ustvarjanje kvalificiranega elektronskega podpisa. S tem se sledi zahtevi 30. člena Direktive 910/2014/EU, ki določa, da skladnost naprav za ustvarjanje kvalificiranega elektronskega podpisa z zahtevami iz Priloge II certificirajo ustrezni javni ali zasebni organi, ki jih imenujejo države članice.

K 58. členu (začetek uporabe EŠEI v kvalificiranih potrdilih)

S predlaganim členom je določen rok za začetek izdajanja kvalificiranih potrdil z uporabo EŠEI (v skladu z 21. členom predloga zakona), ki je dve leti po uveljavitvi podzakonskih aktov iz 61. člena tega zakona.

K 59. členu (sprememba zakona in razveljavitev predpisa)

Predlog zakona razveljavlja zastarele vsebine predpisov in hkrati ustrezne prilagodi evropskim predpisom in obstoječemu stanju na trgu. Predlagani zakon bo torej razveljavil del Zakona o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14; v nadaljnjem besedilu: ZEPEP), ki je do sprejetja Uredbe 910/2014/EU na podlagi evropske Direktive za elektronski podpis 1999/93/ES med drugim urejal področje elektronskega podpisa in elektronskega časovnega žiga. Z začetkom veljavnosti Uredbe 910/2014/EU, ki omenjeni vsebini ureja, pa so te določbe ZEPEP postale obsoletne.

Hkrati pa se z drugim odstavkom določa, da preneha veljati Uredba o izvajanju Uredbe 910/2014/EU, s katero je bila Uredba 910/2014/EU vključena v slovenski pravni red.

K 60. členu (uskladitev področnih predpisov)

Predlog člena nalaga rok za uskladitev predpisov, ki določajo uporabo storitev zaupanja, z Uredbo 910/2014/EU, predlogom zakonom in podzakonskimi akti, in sicer je rok pet let po uveljavitvi zakona.

V drugem odstavku je določeno, da če predpis določa obveznost uporabe varnega elektronskega podpisa, overjenega s kvalificiranim digitalnim potrdilom, se šteje, da se zahteva kvalificirani elektronski podpis, kar je določeno z namenom konkretizacije podpisa v primerih, ko pristojnim organom ne bo uspelo spremeniti svojih predpisov, z vidika pravne varnosti pa je treba vedeti, za kateri podpis gre. Brez tega določila namreč pravno gledano "varnega elektronskega podpisa, overjenega s kvalificiranim digitalnim potrdilom" ni mogoče opredeliti kot katerega od obstoječih. S takšno dikcijo pa je bilo opredeljenih mnogo elektronskih podpisov v našem pravnem redu.

K 61. členu (izdaja podzakonskih aktov)

Predlog člena nalaga Vladi Republike Slovenije pristojnost, da podrobneje določi način vodenja nacionalnega zanesljivega seznama po 22. členu Uredbe 910/2014/EU ter določi rok za izdajo podzakonskih predpisov, ki je šest mesecev po uveljavitvi tega zakona.

K 62. členu (začetek veljavnosti)

Predlog člena določa začetek veljavnosti zakona, ki začne veljati v običajnem roku petnajsti dan po objavi v Uradnem listu Republike Slovenije.

V. PREDLOG ZAKONA RAZVELJAVLJA DOLOČBE VELJAVNIH ZAKONOV

Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14)

1. člen

(1) Ta zakon ureja elektronsko poslovanje, ki zajema poslovanje v elektronski obliki z uporabo informacijske in komunikacijske tehnologije in uporabo elektronskega podpisa v pravnem prometu, kar vključuje tudi elektronsko poslovanje v sodnih, upravnih in drugih podobnih postopkih, če zakon ne določa drugače.

(2) Če ni dogovorjeno drugače, določbe tega zakona, z izjemo določb 4. in 14. člena, ne veljajo v zaprtih sistemih, ki so v celoti urejeni s pogodbami med znanim številom pogodbenih strank.

2. člen

Posamezni izrazi, uporabljeni v tem zakonu, imajo naslednji pomen:

1. podatki v elektronski obliki so podatki, ki so oblikovani, shranjeni poslani, prejeti ali izmenljivi na elektronski način;

2. elektronsko sporočilo je niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto;

3. elektronski podpis je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika;

4. varen elektronski podpis je elektronski podpis, ki izpolnjuje naslednje zahteve:

- da je povezan izključno s podpisnikom;

- da je iz njega mogoče zanesljivo ugotoviti podpisnika;

- da je ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom;

- da je povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi;

5. časovni žig je elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času; varni časovni žig pa elektronsko podpisano potrdilo overitelja, ki izpolnjuje pogoje iz prejšnje točke;

6. pošiljatelj elektronskega sporočila je oseba, ki je sama poslala elektronsko sporočilo ali pa je bilo sporočilo poslano v njenem imenu in v skladu z njeno voljo; posrednik elektronskega sporočila se ne šteje za pošiljatelja tega elektronskega sporočila;

7. naslovnik elektronskega sporočila je oseba, ki ji je pošiljatelj namenil elektronsko sporočilo;

8. prejemnik elektronskega sporočila je oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila;

9. posrednik elektronskega sporočila je oseba, ki za drugo osebo pošlje, prejme, shrani elektronsko sporočilo ali nudi druge storitve v zvezi z elektronskim sporočilom;

10. podpisnik je oseba, ki ustvari ali je v njenem imenu in v skladu z njeno voljo ustvarjen elektronski podpis;

11. informacijski sistem je programska, strojna, komunikacijska in druga oprema, ki deluje samostojno ali v omrežju in je namenjena zbiranju, procesiranju, distribuciji, uporabi in drugi obdelavi podatkov v elektronski obliki;

12. podatki za elektronsko podpisovanje so edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa;

13. sredstvo za elektronsko podpisovanje je nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa;

14. sredstvo za varno elektronsko podpisovanje je sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena tega zakona;

15. podatki za preverjanje elektronskega podpisa so edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa;

16. sredstvo za preverjanje elektronskega podpisa je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa;

17. oprema za elektronsko podpisovanje je strojna ali programska oprema ali njune specifične sestavine, ki jih overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem ali ki se uporabljajo za oblikovanje ali preverjanje elektronskih podpisov;

18. potrdilo je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto;

19. kvalificirano potrdilo je potrdilo iz prejšnje točke, ki izpolnjuje zahteve iz 28. člena tega zakona in ki ga izda overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena tega zakona;

20. overitelj je fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi;

21. (prenehala veljati)

22. (prenehala veljati)

Tretje poglavje
ELEKTRONSKI PODPIS

1. oddelek
Splošne določbe

14. člen

Elektronskemu podpisu se ne sme odreči veljavnosti ali dokazne vrednosti samo zaradi elektronske oblike, ali ker ne temelji na kvalificiranem potrdilu ali potrdilu akreditiranega overitelja, ali ker ni oblikovan s sredstvom za varno elektronsko podpisovanje.

15. člen

Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost.

16. člen

Osebe, ki hranijo dokumente, ki so elektronsko podpisani z uporabo podatkov in sredstev za podpisovanje, morajo hraniti komplementarne podatke in sredstva za preverjanje elektronskega podpisa enako dolgo, kot se hranijo dokumenti.

17. člen

Uporaba podatkov za elektronsko podpisovanje brez vednosti podpisnika ali imetnika potrdila, ki se nanaša na te podatke, je prepovedana.

2. oddelek
Potrdila in overitelji, ki jih izdajajo

18. člen

(1) Overitelj za opravljanje svoje dejavnosti ne potrebuje posebnega dovoljenja.

(2) Overitelj mora začetek opravljanja dejavnosti prijaviti ministrstvu, pristojnemu za informacijsko družbo (v nadaljnjem besedilu: ministrstvo), najmanj osem dni pred začetkom. Ob začetku opravljanja dejavnosti ali ob spremembi dejavnosti mora overitelj ministrstvo seznaniti s svojimi notranjimi pravili glede elektronskega podpisovanja in overjanja ter s svojimi postopki in infrastrukturo.

(3) Overitelj, ki opravlja storitve varnega elektronskega podpisovanja, mora v svojih notranjih pravilih upoštevati varnostne zahteve, določene s tem zakonom in na njegovi podlagi izdanimi podzakonskimi predpisi.

(4) Overitelj mora izpolnjevati zahteve iz svojih notranjih pravil tako ob začetku kot tudi neprekinjeno ves čas izvajanja dejavnosti.

19. člen

(1) Overitelj mora nemudoma obvestiti ministrstvo o vseh okoliščinah, ki ga ovirajo ali mu onemogočajo izvajanje dejavnosti v skladu z veljavnimi predpisi ali njegovimi notranjimi pravili.

(2) Overitelj mora nemudoma obvestiti ministrstvo o možnem začetku stečaja ali prisilne poravnave.

20. člen

(1) Overitelj mora preklicati potrdilo iz 18. točke 2. člena tega zakona v času njegove veljavnosti v skladu s svojimi notranjimi pravili, ki urejajo preklice potrdil, vendar vedno nemudoma:

- če preklic potrdila zahteva imetnik potrdila ali njegov pooblaščenec, ali

- ko overitelj izve, da je imetnik potrdila izgubil poslovno sposobnost, umrl, prenehal obstajati ali da so se spremenile okoliščine, ki bistveno vplivajo na veljavnost potrdila, ali

- če je podatek v potrdilu napačen ali je bilo potrdilo izdano na podlagi napačnih podatkov, ali

- če so bili podatki za preverjanje elektronskega podpisa ali informacijski sistem overitelja ogroženi na način, ki vpliva na zanesljivost potrdila, ali

- če so bili podatki za elektronsko podpisovanje ali informacijski sistem imetnika potrdila ogroženi na način, ki vpliva na zanesljivost oblikovanja elektronskega podpisa in je overitelj s tem seznanjen, ali

- če overitelj preneha z delovanjem ali mu je delovanje prepovedano in njegove dejavnosti ni prevzel drug overitelj, ali

- če preklic odredi pristojno sodišče, sodnik za prekrške ali upravni organ.

(2) Overitelj mora v svojih notranjih pravilih določiti, kdaj in na kakšen način se obvešča o izdaji oziroma preklicu potrdila.

(3) Ne glede na notranja pravila mora overitelj vedno nemudoma obvestiti imetnika preklicanega potrdila. Podatke o preklicu mora posredovati vsaki osebi, ki jih zahteva, ali jih javno objaviti, če overitelj vodi register preklicanih potrdil.

21. člen

Ministrstvo mora nemudoma zagotoviti preklic potrdil overitelja, če overitelj preneha z delovanjem ali je njegovo delovanje prepovedano in njegove dejavnosti ni prevzel drug overitelj, če overitelj potrdila ne prekliče.

22. člen

(1) Imetnik potrdila mora podatke za elektronsko podpisovanje hraniti s skrbnostjo dobrega gospodarja ali dobrega gospodarstvenika in jih uporabljati v skladu z zahtevami tega zakona in na njegovi podlagi izdanih podzakonskih predpisov ter preprečiti nepooblaščen dostop do teh podatkov.

(2) Imetnik potrdila mora zahtevati preklic svojega potrdila, če so bili podatki za elektronsko podpisovanje ali informacijski sistem imetnika potrdila izgubljeni ali ogroženi na način, ki vpliva na zanesljivost oblikovanja elektronskega podpisa, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

23. člen

Če potrdilo vsebuje podatke o tretji osebi, ki ni imetnik potrdila, je tudi ta upravičena zahtevati preklic potrdila iz razlogov, določenih v drugem odstavku prejšnjega člena.

24. člen

(1) Preklic potrdila učinkuje med imetnikom potrdila in overiteljem od trenutka preklica. Preklic potrdila učinkuje med tretjimi osebami in overiteljem od trenutka objave ali, če preklic ni javno objavljen, od trenutka, ko tretje osebe zanj zvedo.

(2) V preklicu potrdila mora biti naveden čas preklica.

(3) Preklic vedno velja od trenutka preklica naprej. Preklic za nazaj ni dovoljen.

25. člen

Za časovni žig in storitve, povezane z njim, se smiselno uporabljajo določbe tega zakona, ki urejajo potrdilo, za varen časovni žig in storitve, povezane z njim, pa določbe tega zakona, ki urejajo kvalificirano potrdilo.

26. člen

Overitelj mora voditi dokumentacijo o varnostnih ukrepih v skladu s tem zakonom in predpisi, izdanimi na njegovi podlagi, ter o vseh izdanih in preklicanih potrdilih tako, da bodo podatki vedno dostopni ter njihova verodostojnost in nespremenljivost vedno preverljiva, in sicer najmanj pet let od posameznega dogodka ali dejanja.

27. člen

(1) Overitelj mora pred prenehanjem delovanja o tem nemudoma obvestiti ministrstvo in imetnike od njega izdanih potrdil, ter zagotoviti, da vse njegove pravice in obveznosti glede izdanih potrdil prevzame drug overitelj ali da prekliče veljavna potrdila.

(2) Vso dokumentacijo, ki jo je doslej vodil, mora predati drugemu overitelju, ki bo prevzel vse pravice in obveznosti prejšnjega overitelja glede izdanih potrdil, oziroma ministrstvu, če takega overitelja ni.

3. oddelek
Kvalificirana potrdila in overitelji, ki jih izdajajo

28. člen

(1) Iz kvalificiranega potrdila mora biti ugotovljivo:

- navedba, da gre za kvalificirano potrdilo;

- ime ali firma in država stalnega prebivališča ali sedeža overitelja;

- ime oziroma psevdonim imetnika potrdila z obvezno navedbo, da gre za psevdonim

- dodatni podatki o imetniku potrdila, ki so predpisani za namen, za katerega se bo potrdilo uporabljalo ki pa ne smejo biti v nasprotju z namenom uporabe psevdonima.

- podatki za preverjanje elektronskega podpisa, ki ustrezajo podatkom za elektronsko podpisovanje pod nadzorom imetnika potrdila;

- začetek in konec veljavnosti potrdila;

- identifikacijska oznaka potrdila;

- varen elektronski podpis overitelja, ki je potrdilo izdal;

- morebitne omejitve v zvezi z uporabo potrdila;

- morebitne omejitve transakcijskih vrednosti, za katere se potrdilo lahko uporablja.

(2) Če ni drugače dogovorjeno, potrdilo ne sme vsebovati podatkov, ki jih varuje poseben zakon.

(3) Kvalificirana potrdila, izdana za potrebe osebnih dokumentov, vsebujejo poleg podatkov iz prvega odstavka tega člena tudi osebno identifikacijsko oznako, ki se lahko v ta namen sklicuje ali poveže s Centralnim registrom prebivalstva. Vlada Republike Slovenije podrobneje določi način določanja osebne identifikacijske oznake, vzpostavitev in vodenje registra osebnih identifikacijskih oznak ter pogoje in način sklicevanja ali povezovanja s Centralnim registrom prebivalstva v skladu s predpisi, ki urejajo varstvo osebnih podatkov.

29. člen

Overitelj, ki izdaja kvalificirana potrdila, mora zagotavljati storitve v zvezi z elektronskim podpisovanjem s skrbnostjo dobrega strokovnjaka.

30. člen

(1) Overitelj, ki izdaja kvalificirana potrdila, mora zagotoviti vodenje registra preklicanih potrdil, ki mora vsebovati zlasti identifikacijsko oznako preklicanega potrdila, da se ga da natančno identificirati. Register ne sme vsebovati podatkov o vzrokih za preklic ali kakršnih koli podatkov, ki niso vsebovani v potrdilu, razen datuma in časa preklica. Register mora biti varno elektronsko podpisan in podpis overjen s kvalificiranim potrdilom z najmanj enako zanesljivostjo kot potrdila, ki se preklicujejo v registru.

(2) Overitelj mora zagotoviti možnost takojšnjega in varnega preklica kvalificiranega potrdila, kot tudi možnost natančne določitve trenutka izdaje in preklica kvalificiranega potrdila.

(3) Overitelj, ki izdaja kvalificirana potrdila in preneha z delovanjem, mora zagotoviti, da drug overitelj, ki izdaja kvalificirana potrdila, vodi preklicana kvalificirana potrdila v svojem registru.

(4) Če overitelj, ki preneha z delovanjem, ne zagotovi hrambe dokumentacije in vodenja preklicanih kvalificiranih potrdil pri drugem overitelju, to zagotovi na njegove stroške ministrstvo.

31. člen

Overitelj, ki izdaja kvalificirana potrdila, mora s pomočjo uradnega osebnega dokumenta s fotografijo za fizične osebe ali z uradno potrjenimi dokumenti za pravne osebe zanesljivo ugotoviti identiteto in druge pomembne lastnosti osebe, ki zahteva potrdilo.

(2) Overitelj iz prejšnjega odstavka lahko ugotovi in preveri identiteto in druge pomembne lastnosti osebe, ki zahteva izdajo kvalificiranega potrdila, tudi na podlagi veljavnega kvalificiranega potrdila, ki ga je izdal overitelj, uvrščen na zanesljivi seznam nadzorovanih overiteljev v skladu z Odločbo Komisije 2009/767/ES z dne 16. oktobra 2009 o vzpostavitvi ukrepov za pospeševanje uporabe postopkov po elektronski poti s pomočjo »enotnih kontaktnih točk« po Direktivi 2006/123/ES Evropskega parlamenta in Sveta o storitvah na notranjem trgu (UL L št. 274 z dne 20. 10. 2009, str. 36), zadnjič spremenjeno z Izvedbenim sklepom Komisije z dne 14. oktobra 2013 o spremembi Odločbe 2009/767/ES v zvezi z vzpostavitvijo, vzdrževanjem in objavo zanesljivih seznamov overiteljev, ki jih nadzorujejo/akreditirajo države članice (UL L št. 306 z dne 16. 11. 2013, str. 21).

(3) Overitelj, ki izdaja kvalificirano potrdilo po postopku iz prejšnjega odstavka, mora pri državnih organih, ki dodeljujejo uradno dodeljene identifikacijske oznake, preveriti naslednje podatke o osebi, ki zahteva izdajo kvalificiranega potrdila: identifikacijsko oznako, ime in priimek imetnika potrdila oziroma firmo in sedež pravne osebe.

(4) Če podatkov iz prejšnjega odstavka overitelj ne more preveriti, se na ta način izdano kvalificirano potrdilo uporablja le v sistemu, v okviru katerega je bilo izdano.

32. člen

(1) Overitelj, ki izdaja kvalificirana potrdila, mora zaposlovati osebje s potrebnim strokovnim znanjem, izkušnjami in usposobljenostjo na področju opravljanih storitev, še posebej na področju upravljanja ter poznavanja tehnologije elektronskega poslovanja in ustreznih varnostnih postopkov, da zagotovi izpolnjevanje vseh določb tega zakona.

(2) Osebje se mora ravnati po administrativnih in upravljavskih postopkih in predpisih, skladnih z uveljavljenimi pravili stroke.

(3) Vlada Republike Slovenije s podzakonskim predpisom določi vrsto in stopnjo zahtevane strokovne izobrazbe, leta izkušenj ter morebitna dodatna opravljena usposabljanja za izpolnjevanje zahtev iz prvega odstavka tega člena.

33. člen

(1) Overitelj mora uporabljati zanesljive sisteme in opremo, ki so zaščiteni pred spreminjanjem in ki zagotavljajo tehnično in kriptografsko varnost postopkov, v katerih se uporabljajo.

(2) Overitelj mora izvajati varnostne ukrepe zoper ponarejanje potrdil ter v primerih, ko overitelj oblikuje podatke za elektronsko podpisovanje, zagotavljati zaupnost podatkov ves čas postopka oblikovanja takih podatkov.

(3) Overitelj ne sme shranjevati podatkov za elektronsko podpisovanje imetnika potrdila.

(4) Overitelj mora za shranjevanje potrdil uporabljati zanesljive sisteme, ki omogočajo enostavno odkrivanje sprememb ter hkrati omogočajo, da:

1. lahko samo pooblaščene osebe vnašajo nove podatke in spreminjajo obstoječe;

2. je omogočeno preverjanje pristnosti podatkov;

3. so potrdila javno dostopna samo, če je overitelj predhodno dobil dovoljenje imetnika potrdila;

4. uporabnik lahko enostavno opazi kakršnekoli tehnične spremembe, ki bi ogrozile izpolnjevanje teh varnostnih zahtev.

(5) Vlada Republike Slovenije s podzakonskim predpisom predpiše podrobnejša merila za izpolnjevanje zahtev iz tega člena.

34. člen

Overitelj, ki izdaja kvalificirana potrdila, mora zavarovati svojo škodno odgovornost. Najnižji znesek zavarovalne vsote predpiše Vlada Republike Slovenije z uredbo.

35. člen

(1) Overitelj, ki izdaja kvalificirana potrdila, mora shranjevati vse pomembne podatke o kvalificiranih potrdilih, še posebej zaradi dokazovanja overitev v sodnih, upravnih in drugih postopkih, vsaj toliko časa, kot bodo hranjeni podatki, podpisani z elektronskim podpisom, na katerega se nanaša kvalificirano potrdilo, najmanj pa pet let od izdaje potrdila.

(2) Za pomembne podatke o kvalificiranih potrdilih se štejejo zlasti podatki o načinu ugotovitve istovetnosti imetnika potrdila, času in načinu izdaje potrdila, vzroku, času in načinu morebitnega preklica potrdila, roku veljavnosti potrdila ter vseh sporočilih, ki se nanašajo na veljavnost potrdila, izmenjanih med overiteljem in imetnikom.

(3) Podatki iz prvega in drugega odstavka tega člena se lahko shranjujejo v elektronski obliki.

36. člen

(1) Overitelj, ki izdaja kvalificirana potrdila, mora osebo, ki zahteva potrdilo, pred izdajo potrdila obvestiti o vseh pomembnih okoliščinah uporabe potrdila.

(2) Obvestilo mora vsebovati:

1. podroben povzetek vsebine veljavnih predpisov ter notranjih pravil in drugih pogojev, ki se nanašajo na uporabo potrdila;

2. podatke o morebitnih omejitvah uporabe potrdila;

3. podatke o obstoju prostovoljne akreditacije;

4. podatke o postopkih za reševanje pritožb in mirno razreševanje sporov;

5. podatke o ukrepih imetnika potrdila, potrebnih za varnost elektronskega podpisovanja in preverjanja elektronskih podpisov, ter o ustrezni tehnologiji;

6. opozorilo, da bo morda potrebno elektronsko podpisane podatke ponovno elektronsko podpisati, in sicer preden bo varnost obstoječega elektronskega podpisa s časom zmanjšana;

7. opozorilo, da mora imetnik kvalificiranega potrdila sam sporočiti spremembe obveznih podatkov kvalificiranega potrdila iz 28. člena tega zakona.

(3) Obvestilo mora biti napisano v lahko razumljivem jeziku ter v pisni obliki.

(4) Ustrezni deli obvestila morajo biti na njihovo zahtevo dostopni tudi tretjim osebam, ki se zanašajo na potrdilo.

4. oddelek
Tehnične zahteve za varno elektronsko podpisovanje

37. člen

(1) Sredstva za varno elektronsko podpisovanje morajo z uporabo ustreznih postopkov in infrastrukture zagotavljati naslednje:

1. podatki za elektronsko podpisovanje morajo biti edinstveni in njihova zaupnost zagotovljena;

2. podatkov za elektronsko podpisovanje ni mogoče v razumnem času ali z razumnimi sredstvi ugotoviti iz podatkov za preverjanje elektronskega podpisa, elektronski podpis pa je učinkovito zaščiten pred poneverjanjem z uporabo trenutno dostopne tehnologije;

3. podpisnik lahko zanesljivo varuje svoje podatke za elektronsko podpisovanje pred nepooblaščenim dostopom.

(2) Sredstvo za varno elektronsko podpisovanje ne sme spremeniti podatkov, ki se podpisujejo ali preprečiti prikaza podatkov podpisniku pred podpisom.

(3) Vlada Republike Slovenije s podzakonskim predpisom predpiše podrobnejša merila za izpolnjevanje zahtev glede sredstev za varno elektronsko podpisovanje iz tega člena.

38. člen

(1) Med postopkom preverjanja varnega elektronskega podpisa mora biti z uporabo ustreznih postopkov in infrastrukture zagotovljeno naslednje:

1. podatki, ki se uporabljajo za preverjanje elektronskega podpisa, morajo biti enaki podatkom, ki so prikazani uporabniku;

2. podpis mora biti zanesljivo preverjen in rezultati preverjanja ter identiteta podpisnika pravilno prikazani uporabniku;

3. uporabnik lahko zanesljivo ugotovi vsebino podpisanih podatkov;

4. pristnost in veljavnost potrdila morata biti preverjeni v času preverjanja podpisa;

5. raba psevdonima mora biti jasno označena;

6. vse spremembe, ki kakorkoli vplivajo na varnost elektronskega podpisa, morajo biti ugotovljene.

(2) Vlada Republike Slovenije s podzakonskim predpisom predpiše podrobnejša merila za izpolnjevanje zahtev glede postopkov in infrastrukture iz prejšnjega odstavka.

5. oddelek
Odgovornost overiteljev

39. člen

(1) Overitelj odgovarja vsaki osebi, ki se upravičeno zanaša na kvalificirano potrdilo, ki ga je overitelj izdal, za:

- točnost podatkov v potrdilu v trenutku izdaje potrdila ter da potrdilo vsebuje vse predpisane podatke za kvalificirano potrdilo;

- zagotovilo, da je imel imetnik potrdila, naveden v potrdilu, v času izdaje potrdila podatke za elektronsko podpisovanje ustrezne podatkom za preverjanje elektronskega podpisa, navedenim ali označenim v potrdilu;

- zagotovilo, da delujejo podatki za elektronsko podpisovanje in podatki za preverjanje elektronskega podpisa komplementarno v primeru, če overitelj oblikuje oboje podatke;

- takojšen preklic potrdila in objavo preklica, če za preklic obstajajo razlogi;

- izpolnjevanje zahtev tega zakona in na njegovi podlagi izdanih podzakonskih predpisov glede varnih elektronskih podpisov in kvalificiranih potrdil.

(2) Overitelj lahko v kvalificiranem potrdilu označi meje uporabnosti ali najvišje transakcijske vrednosti določenega potrdila in ne odgovarja za posledice uporabe potrdila izven tako določenih meja, če so omejitve prepoznavne tretjim osebam.

(3) Overitelj je odgovoren, če ne dokaže, da je škoda nastala brez njegove krivde.

6. oddelek
Nadzor

40. člen

(1) Inšpekcijsko nadzorstvo nad izvajanjem določb tega zakona opravlja ministrstvo.

(2) V okviru inšpekcijskega nadzorstva ministrstvo:

- preverja, ali so zahteve zakona in na njegovi podlagi izdanih podzakonskih predpisov ustrezno prenesene v notranja pravila overiteljev;

- preverja, ali overitelj ves čas izvajanja dejavnosti izpolnjuje zahteve iz tega zakona in na njegovi podlagi izdanih podzakonskih predpisov ter svojih notranjih pravil;

- v primeru zagotavljanja kvalificiranih potrdil nadzoruje uporabo ustreznih postopkov in potrebne infrastrukture;

- nadzoruje zakonitost izdajanja, hranjenja in preklica potrdil;

- nadzoruje zakonitost izvajanja drugih storitev overiteljev.

(3) Ministrstvo vodi elektronski javni register overiteljev v Republiki Sloveniji. V register overiteljev se vpišejo overitelji, če izpolnjujejo pogoje iz tega zakona. V register overiteljev se na njihovo zahtevo vpišejo tudi tuji overitelji, če izpolnjujejo pogoje iz tega zakona za veljavnost njihovih potrdil v Republiki Sloveniji.

(4) Register overiteljev varno elektronsko podpiše ministrstvo. Podatki za preverjanje kvalificiranega potrdila ministrstva se objavijo na spletnih straneh ministrstva skupaj z registrom overiteljev.

41. člen

(1) Pri opravljanju inšpekcijskega nadzorstva je inšpektor upravičen:

- pregledovati dokumentacijo in akte, ki se nanašajo na poslovanje overiteljev;

- pregledovati prostore, v katerih se opravljajo storitve overjanja, ter informacijsko tehnologijo, infrastrukturo in drugo opremo ter tehnično dokumentacijo overiteljev;

- preverjati ukrepe in postopke overitelja.

(2) Inšpektor ima pravico za največ petnajst dni zaseči dokumentacijo, če je to potrebno za zavarovanje dokazov ali za natančno ugotovitev nepravilnosti. O tem mora izdati potrdilo.

(3) Podatke o potrdilih, osebne podatke in podatke, ki so varovani po posebnem zakonu, s katerimi se inšpektor seznani pri izvajanju inšpekcijskega nadzorstva, je dolžan varovati kot tajne.

(4) Inšpektor z odločbo:

- prepove uporabo neprimernih postopkov in infrastrukture;

- začasno prepove delovanje overitelja, delno ali v celoti;

- prepove delovanje overitelja, če overitelj ne izpolnjuje zahtev tega zakona in na njegovi podlagi izdanih predpisov in če milejši ukrepi niso ali ne bi bili uspešni;

- naloži preklic potrdil, če je verjetno, da so bila potrdila ponarejena.

(5) Zoper odločbo iz prejšnjega odstavka je dovoljena pritožba, o kateri odloči Vlada Republike Slovenije. Pritožba zoper odločbo iz druge alinee prejšnjega odstavka ne zadrži njene izvršitve.

(6) Prepoved delovanja ne vpliva na veljavnost pred tem izdanih potrdil.

7. oddelek
Prostovoljna akreditacija

42. člen

(1) Overitelji, ki dokažejo, da izpolnjujejo vse z zakonom in na njegovi podlagi izdanimi podzakonskimi predpisi predpisane pogoje za svoje delovanje, lahko zahtevajo, da jih akreditacijski organ vpiše v register akreditiranih overiteljev.

(2) V register akreditiranih overiteljev se na njihovo zahtevo vpišejo tudi tuji overitelji, če izpolnjujejo pogoje iz tega zakona za veljavnost njihovih potrdil v Republiki Sloveniji.

(3) Overitelji, ki so vpisani v register akreditiranih overiteljev (akreditirani overitelji), lahko poslujejo z navedbo svoje akreditiranosti.

(4) Overitelji, ki so vpisani v register akreditiranih overiteljev, lahko označijo to dejstvo v izdanih potrdilih.

43. člen

(1) Akreditacijski organ vodi javni elektronski register pri njem prostovoljno akreditiranih overiteljev.

(2) Register akreditiranih overiteljev varno elektronsko podpiše akreditacijski organ. Podatki za preverjanje kvalificiranega potrdila akreditacijskega organa se objavijo na spletnih straneh akreditacijskega organa skupaj z registrom akreditiranih overiteljev.

44. člen

(1) Akreditacijski organ izvaja nadzor in ukrepe glede akreditiranih overiteljev.

(2) Akreditacijski organ:

- izdaja splošna priporočila za delovanje overiteljev ter priporočila in standarde za delovanje akreditiranih overiteljev v skladu z zakonom in na njegovi podlagi izdanimi podzakonskimi predpisi;

- preverja, ali so zahteve zakona in na njegovi podlagi izdanih podzakonskih predpisov ustrezno prenesene v notranja pravila akreditiranih overiteljev;

- preverja, ali overitelj ves čas izvajanja dejavnosti izpolnjuje zahteve tega zakona in na njegovi podlagi izdanih podzakonskih predpisov ter svojih notranjih pravil;

- nadzoruje uporabo ustreznih postopkov in infrastrukture pri akreditiranih overiteljih;

- nadzoruje zakonitost izdajanja, hranjenja in preklica potrdil akreditiranih overiteljev;

- nadzoruje zakonitost izvajanja drugih storitev akreditiranih overiteljev.

(3) Akreditacijski organ lahko priporoči:

- spremembo notranjih pravil akreditiranega overitelja;

- akreditiranemu overitelju prenehanje nadaljnje uporabe neprimernih postopkov in infrastrukture.

(4) Če overitelj ne upošteva priporočil akreditacijskega organa, ga akreditacijski organ z odločbo izbriše iz registra akreditiranih overiteljev.

(5) Zoper odločbo iz prejšnjega odstavka je v petnajstih dneh po prejemu odločbe dovoljena pritožba, o kateri odloči minister, pristojen za informacijsko družbo.

(6) Odločbo o pritožbi je minister dolžen izdati v tridesetih dneh po prejemu pritožbe. Odločba o pritožbi je dokončna.

45. člen

(1) Za opravljanje nalog akreditacijskega organa Vlada Republike Slovenije, na predlog ministra, pristojnega za informacijsko družbo, določi pristojni organ za opravljanje nalog akreditacijskega organa ali za opravljanje teh nalog podeli javno pooblastilo, oziroma koncesijo.

(2) Organ iz prejšnjega odstavka ne sme biti overitelj.

8. oddelek
Veljavnost tujih potrdil

46. člen

(1) Kvalificirana potrdila overitelja s sedežem v Evropski uniji so enakovredna domačim kvalificiranim potrdilom.

(2) Kvalificirana potrdila overiteljev s sedežem v tretjih državah so enakovredna domačim:

1. če overitelj izpolnjuje pogoje iz 29. do 36. člena tega zakona in je prostovoljno akreditiran v Republiki Sloveniji ali eni izmed držav članic Evropske unije;

2. če domači overitelj, ki izpolnjuje pogoje iz 29. do 36. člena tega zakona, jamči za taka potrdila enako, kot bi bila njegova;

3. če tako določa dvostranski ali večstranski sporazum med Republiko Slovenijo in drugimi državami ali mednarodnimi organizacijami;

4. če tako določa dvostranski ali večstranski sporazum med Evropsko unijo in tretjimi državami ali mednarodnimi organizacijami.

(3) Potrdila overiteljev s sedežem v Evropski uniji, ki jih po tem zakonu ni mogoče opredeliti kot kvalificirana, se obravnavajo enako kot domača v skladu z določbami tega zakona.

Četrto poglavje
KAZENSKE DOLOČBE

47. člen

(1) Z globo od 2.000 do 20.000 eurov se za prekršek kaznuje overitelj, ki je pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če:

1. ne ugotovi zanesljivo identitete ali drugih pomembnih lastnosti osebe, ki zaprosi za kvalificirano potrdilo (31. člen);

2. izda kvalificirano potrdilo, ki ne vsebuje vseh zahtevanih podatkov oziroma vsebuje podatke, ki jih ne bi smelo vsebovati (28. člen);

3. ne prekliče potrdila ali kvalificiranega potrdila v primerih, ko to zahteva zakon ali njegova notranja pravila (20. in 23. člen);

4. v preklicu ne navede časa preklica potrdila ali kvalificiranega potrdila ali če potrdilo ali kvalificirano potrdilo prekliče za nazaj (20. in 24. člen);

5. prosilca za potrdilo ali kvalificirano potrdilo ne obvesti o vseh predpisanih podatkih (36. člen);

6. pred prenehanjem delovanja ne obvesti ministrstva in ne zagotovi, da skrb za vsa veljavna potrdila ali kvalificirana potrdila prevzame drug overitelj ali jih ne prekliče (27. člen);

7. ne preda vse dokumentacije drugemu overitelju oziroma ministrstvu (27. člen);

8. ne obvesti ministrstva o možnem začetku stečaja ali prisilne poravnave ali o drugih okoliščinah, ki mu preprečujejo izpolnjevanje predpisanih zahtev (19. člen);

9. ne vodi predpisane dokumentacije (26. člen);

10. ne omogoči inšpektorju vpogleda ali zasega svoje dokumentacije ali ne posreduje potrebnih informacij in pojasnil (41. člen);

11. ne prijavi začetka opravljanja dejavnosti ali ne predloži notranjih pravil (18. člen);

12. izdaja kvalificirana potrdila in ne vodi ali pomanjkljivo vodi register preklicanih potrdil (30. člen);

13. izdaja kvalificirana potrdila in ne izvaja ustreznih varnostnih ukrepov za preprečitev nepooblaščenega zbiranja ali kopiranja podatkov za elektronsko podpisovanje s svoje strani ali s strani tretjega (33. člen);

14. navkljub prepovedi opravljanja dejavnosti s strani ministrstva dejavnost še naprej opravlja (41. člen);

15. neupravičeno uporablja označbo akreditiranega overitelja (42. člen).

(2) Z globo od 200 eurov do 400 eurov se kaznuje tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, če stori prekršek iz prejšnjega odstavka.

(3) Če je overitelj posameznik, se za prekršek iz prvega odstavka tega člena kaznuje z globo od 400 eurov do 1.200 eurov.

48. člen

Z globo od 200 eurov do 600 eurov se kaznuje za prekršek imetnik potrdila, če:

1. ne zahteva preklica potrdila ali kvalificiranega potrdila (22. člen);

2. uporablja podatke za elektronsko podpisovanje v nasprotju z zahtevami tega zakona in na njegovi podlagi izdanih podzakonskih predpisov (22. člen).

49. člen

Z globo od 200 eurov do 600 eurov se kaznuje za prekršek posameznik, ki brez vednosti podpisnika ali imetnika potrdila uporabi njegove podatke za elektronsko podpisovanje (17. člen).

****

Na podlagi sedmega odstavka 21. člena Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G in 65/14) izdaja Vlada Republike Slovenije

UREDBO o izvajanju Uredbe (EU) o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES

1. člen

(vsebina)

S to uredbo se določajo pristojni organi in kazenske določbe za izvajanje Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (UL L št. 257 z dne 28. 8. 2014, str. 73; v nadaljnjem besedilu: Uredba 910/2014/EU), uporaba kvalificiranih potrdil za elektronski podpis ter delovanje komisije za elektronsko identifikacijo in storitve zaupanja.

2. člen

(uporaba kvalificiranih potrdil za elektronski podpis)

Kot sredstvo elektronske identifikacije se lahko uporabi tudi kvalificirano potrdilo za elektronski podpis, ki je izdano tudi za namen avtentikacije.

3. člen

(pristojni organi)

(1) Pristojni organ za izvajanje Uredbe 910/2014/EU in te uredbe je ministrstvo, pristojno za informacijsko družbo, ki je odgovorno tudi za izvajanje nadzornih nalog v skladu s 17. členom Uredbe 910/2014/EU.

(2) Pristojni organ za zagotovitev čezmejne avtentikacije prek spleta po točki f) 7. člena Uredbe 910/2014/EU je ministrstvo, pristojno za javno upravo.

(3) Pristojni organ za akreditacijo organov za ugotavljanje skladnosti je Slovenska akreditacija.

4. člen

(komisija za elektronsko identifikacijo in storitve zaupanja)

Za obravnavo strokovnih vprašanj v zvezi z Uredbo 910/2014/EU ter pripravo strokovnih mnenj in stališč minister, pristojen za informacijsko družbo, imenuje komisijo za elektronsko identifikacijo in storitve zaupanja, ki jo sestavljajo predstavniki pristojnih organov iz prejšnjega člena ter zunanji strokovnjaki, predvsem s področja prava, informatike in elektronskih komunikacij. Komisija o svojem delu javnost obvešča z objavo svojih načelnih mnenj in stališč na spletni strani ministrstva, pristojnega za informacijsko družbo.

5. člen

(prekrški)

(1) Z globo od 5.000 do 30.000 eurov se za prekršek kaznuje pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če:

1. ne izpolnjuje varnostnih zahtev za ponudnike storitev v skladu z 19. členom Uredbe 910/2014/EU;

2. uporablja znak zaupanja EU za kvalificirane storitve zaupanja v nasprotju s 23. členom Uredbe 910/2014/EU;

3. začne zagotavljati kvalificirane storitve zaupanja, ne da bi bil njegov kvalificirani status naveden na zanesljivem seznamu (tretji odstavek 21. člena Uredbe 910/2014/EU).

(2) Z globo od 2.000 do 15.000 eurov se za prekršek kaznuje pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če kot ponudnik kvalificiranih storitev zaupanja:

1. ne preveri identitete in drugih posebnih lastnosti osebe, za katero izdaja kvalificirano potrdilo, kakor to določa prvi odstavek 24. člena Uredbe 910/2014/EU;

2. pri zagotavljanju kvalificiranih storitev zaupanja ne izpolnjuje zahtev iz točk (a) do (k) drugega odstavka 24. člena Uredbe 910/2014/EU;

3. pri izdajanju kvalificiranih potrdil ne zabeleži in objavi preklica potrdila ali ne zagotovi informacij o veljavnosti ali preklicu izdanih kvalificiranih potrdil v skladu s tretjim in četrtim odstavkom 24. člena Uredbe 910/2014/EU;

4. pri izdajanju kvalificiranih potrdil izda kvalificirano potrdilo za elektronske podpise, ki ne vsebuje vseh obveznih podatkov v skladu z 28. členom Uredbe 910/2014/EU;

5. omogoči ustvarjanje kvalificiranega elektronskega podpisa z napravo, ki ne izpolnjuje zahtev iz 29. člena Uredbe 910/2014/EU;

6. omogoči ustvarjanje kvalificiranega elektronskega žiga z napravo, ki ne izpolnjuje zahtev iz 39. člena Uredbe 910/2014/EU;

7. zagotavlja potrjevanje veljavnosti kvalificiranih elektronskih podpisov, ne da bi izpolnjeval zahteve iz 32. člena Uredbe 910/2014/EU;

8. zagotavlja kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov, ne da bi izpolnjeval zahteve iz 33. člena Uredbe 910/2014/EU;

9. zagotavlja kvalificirano storitev hrambe kvalificiranih elektronskih podpisov, ne da bi izpolnjeval zahteve iz 34. člena Uredbe 910/2014/EU;

10. izda kvalificirano potrdilo za elektronski žig, ki ne vsebuje vseh obveznih podatkov v skladu z 38. členom Uredbe 910/2014/EU;

11. zagotavlja potrjevanje veljavnosti in hrambo kvalificiranih elektronskih žigov, ne da bi izpolnjeval zahteve iz 40. člena Uredbe 910/2014/EU;

12. izda kvalificirani elektronski časovni žig v nasprotju z zahtevami iz 42. člena Uredbe 910/2014/EU;

13. zagotavlja kvalificirane storitve elektronske priporočene dostave v nasprotju z zahtevami iz 44. člena Uredbe 910/2014/EU;

14. izda kvalificirano potrdilo za avtentikacijo spletišč, ki ne izpolnjuje zahtev iz 45. člena Uredbe 910/2014/EU.

(3) Z globo od 400 do 5.000 eurov se kaznuje odgovorna oseba pravne osebe, odgovorna oseba samostojnega podjetnika posameznika ali odgovorna oseba posameznika, ki samostojno opravlja dejavnost, ki stori prekršek iz prvega ali drugega odstavka tega člena.

PREHODNE IN KONČNA DOLOČBA

6. člen

(prenehanje veljavnosti)

Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06) in Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji (Uradni list RS, št. 99/01 in 42/07) prenehata veljati 30. junija 2016.

7. člen

(roki)

(1) Ministrstvo, pristojno za informacijsko družbo, v skladu s tretjim odstavkom 51. člena Uredbe 910/2014/EU do 1. avgusta 2016 po uradni dolžnosti izda odločbe, s katerimi overitelje, ki do 30. junija 2016 izdajajo kvalificirana potrdila na podlagi Zakona o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14), kot ponudnike kvalificiranih storitev zaupanja vpiše v zanesljivi seznam.

(2) Slovenska akreditacija do 30. marca 2017 vzpostavi postopek akreditacije na področju iz tretjega odstavka 3. člena te uredbe.

(3) Minister, pristojen za informacijsko družbo, do 30. decembra 2016 imenuje komisijo iz 4. člena te uredbe.

8. člen

(prehodni ukrep)

Kvalificiranim potrdilom pravnih oseb, ki so jih do 30. junija 2016 na podlagi Zakona o elektronskem poslovanju in elektronskem podpisu izdali registrirani overitelji in se uporabljajo za elektronski podpis pravnih oseb, se do izteka njihove veljavnosti, vendar ne dlje kot do 1. julija 2017, ne sme odreči veljavnost in dokazna vrednost.

9. člen

(uveljavitev)

Ta uredba začne veljati naslednji dan po objavi v Uradnem listu Republike Slovenije, uporabljati pa se začne 1. julija 2016.

VI. PRILOGE

Predlagatelj prilaga osnutek Uredbe o določitvi sredstev elektronske identifikacije in uporabi centralne storitve za spletno prijavo in elektronski podpis.

OSNUTEK

Na podlagi 3., 6., 11., 12., 15., 24. in 45. člena Zakona o elektronski identifikaciji in storitvah zaupanja (Uradni list RS, št. xx/21) izdaja Vlada Republike Slovenije

U R E D B O

o določitvi sredstev elektronske identifikacije in uporabi centralne storitve za spletno prijavo in elektronski podpis

SPLOŠNE DOLOČBE

1. člen

(predmet uredbe)

(1) Ta uredba ureja obliko preračunavanja enoličnega identifikatorja iz EŠEI.

(2) Ta uredba ureja poslovanje in zagotavljanje javnosti dela, upravljanje dokumentarnega gradiva, posebne primere krajevne pristojnosti, uradna dejanja, uradne zgradbe, prostore in opremo ter zagotavljanje varnosti in nadzor nad izvajanjem uredbe.

2. člen

(pomen izrazov)

Izrazi, uporabljeni v tej uredbi, pomenijo:

1. dokument je izviren ali reproduciran (pisan, risan, tiskan, fotografiran, fotokopiran, fonografski, v elektronski obliki ali kako drugače zapisan) zapis, ki je bil prejet ali je nastal pri delu organa in je pomemben za njegovo poslovanje;
2. izdajatelj sredstev elektronske identifikacije je ministrstvo, pristojno za centralno storitev za spletno prijavo in elektronski podpis (v nadaljnjem besedilu: izdajatelj).

ELEKTRONSKA OSEBNA IZKAZNICA VISOKE RAVNI

3. člen

(splošno)

Izdajatelj zagotovi izdajo sredstva elektronske identifikacije visoke ravni zanesljivosti na osebni izkaznici (v nadaljnjem besedilu: elektronska osebna izkaznica visoke ravni).

4. člen

(tehnične specifikacije)

(1) Elektronska osebna izkaznica visoke ravni je izdana v obliki digitalnega potrdila, shranjenega na čipu osebne izkaznice. Dostop do pripadajočega zasebnega ključa je zaščiten, tako da se za uporabo elektronske osebne izkaznice visoke ravni uporabljajo naslednji varnostni mehanizmi:

– začetno geslo,
– uporabniško geslo,
– koda za ponastavitev uporabniškega gesla.

(2) Tehnične podrobnosti izvedbe elektronske osebne izkaznice visoke ravni so določene v pravilih upravljanja elektronske osebne izkaznice visoke ravni, ki so objavljena na spletnih straneh izdajatelja.

5. člen

(raven zanesljivosti)

Elektronska osebna izkaznica visoke ravni je narejena tako, da zadosti merilom Uredbe 910/2014/EU za sredstva elektronske identifikacije visoke ravni zanesljivosti.

6. člen

(obdobje veljavnosti)

Elektronska osebna izkaznica visoke ravni se izdaja za čas veljavnosti osebne izkaznice in največ za 10 let.

7. člen

(starost ob izdaji)

Elektronsko osebno izkaznico visoke ravni lahko pridobi oseba, ki je dopolnila 12 let.

8. člen

(pristojni organ za sprejem vlog)

(1) Vloge za izdajo elektronske osebne izkaznice visoke ravni sprejemajo upravne enote in diplomatsko-konzularna predstavništva Republike Slovenije.

(2) Identifikacijo fizične osebe s fizično prisotnostjo opravi uradna oseba na upravni enoti ali diplomatsko-konzularnem predstavništvu Republike Slovenije.

(3) Uradna oseba, ki sprejme vlogo, preveri veljavnosti vnesenih podatkov in identificira posameznika tako, kot je določeno v zakonu, ki ureja izdajo sredstev elektronske identifikacije.

9. člen

(postopek izdaje)

(1) Če je vloga popolna, organ, pristojen za sprejem vloge, vlogo preda izdajatelju.

(2) Izdajatelj izda elektronsko osebno izkaznico visoke ravni po naslednjem postopku:

- izdajatelj pripravi podatke za izdelavo digitalnega potrdila in jih pošlje v evidenco osebnih izkaznic;
- pogodbeni izvajalec ministrstva, pristojnega za notranje zadeve, v postopku izdelave osebne izkaznice iz evidence osebnih izkaznic pridobi podatke za izdelavo digitalnega potrdila ter jih preda izdajatelju;
- izdajatelj izdela digitalno potrdilo in ga vrne pogodbenemu izvajalcu ministrstva, pristojnega za notranje zadeve;
- pogodbeni izvajalec ministrstva, pristojnega za notranje zadeve, digitalno potrdilo zapiše na čip osebne izkaznice in določi merila za uporabo elektronske osebne izkaznice visoke ravni (obliko in vrednost začetnega gesla, obliko uporabniškega gesla, obliko in vrednost kode za ponastavitev uporabniškega gesla, dovoljeno število napačnih vnosov uporabniškega gesla …);
- pogodbeni izvajalec ministrstva, pristojnega za notranje zadeve, izdelano osebno izkaznico imetniku vroči v skladu z določili zakona o osebni izkaznici;
- pogodbeni izvajalec ministrstva, pristojnega za notranje zadeve, ovojnico z začetnim geslom imetniku pošlje:
    - na njegov naslov kot navadno poštno pošiljko, in sicer naslednji delovni dan po oddaji osebne izkaznice na pošto, če je imetnik izbral vročitev osebne izkaznice po pošti;
    - na naslov upravne enote v ovojnici z osebno izkaznico, če je imetnik izbral vročitev osebne izkaznice na upravni enoti.

(2) Elektronska osebna izkaznica visoke ravni postane aktivna, ko imetnik po vnosu začetnega gesla določi uporabniško geslo.

10. člen

(preklic)

(1) Elektronsko osebno izkaznico visoke ravni izdajatelj prekliče, če:

- imetnik zahteva preklic osebne izkaznice tako, kot je določeno v zakonu o osebni izkaznici;
- se imetniku osebna izkaznica prekliče;
- imetnik zahtevek za preklic elektronske osebne izkaznice visoke ravni vloži pri organu, pristojnem za sprejem vlog;
- imetnik v 7 (sedmih) dneh po vložitvi zahtevka za začasno razveljavitev elektronske osebne izkaznice visoke ravni vloge ne umakne;
- izdajatelj pridobi informacijo, na podlagi katere presodi, da obstaja resnična nevarnost za nepooblaščeno uporabo elektronske osebne izkaznice visoke ravni.

11. člen

(začasna razveljavitev)

(1) Elektronsko osebno izkaznico visoke ravni izdajatelj začasno razveljavi, če imetnik potrdila izdajatelju po elektronski poti pošlje zahtevek za začasno razveljavitev elektronske osebne izkaznice visoke ravni. V zahtevku mora imetnik navesti naslednje podatke:

- osebno ime,
- EMŠO,
- naslov stalnega prebivališča,
- telefonsko številko,
- …

(2) Izdajatelj izvede začasno razveljavitev elektronske osebne izkaznice visoke ravni.

(3) Če imetnik pri organu, pristojnem za sprejem vlog, v sedmih dneh ne umakne zahtevka za začasno razveljavitev elektronske osebne izkaznice visoke ravni, izdajatelj elektronsko osebno izkaznico visoke ravni prekliče.

12. člen

(čezmejna uporaba)

Elektronska osebna izkaznica visoke ravni se lahko brez omejitev uporablja za čezmejne elektronske storitve.

ELEKTRONSKA OSEBNA IZKAZNICA NIZKE RAVNI

13. člen

(splošno)

Izdajatelj zagotovi izdajo sredstva elektronske identifikacije nizke ravni zanesljivosti na osebni izkaznici (v nadaljnjem besedilu: elektronska osebna izkaznica nizke ravni).

14. člen

(tehnične specifikacije)

(1) Elektronska osebna izkaznica nizke ravni je izdana v obliki digitalnega potrdila, shranjenega na čipu osebne izkaznice. Dostop do pripadajočega zasebnega ključa ni zaščiten, tako da se za uporabo elektronske osebne izkaznice nizke ravni ne uporabljajo dodatni varnostni mehanizmi.

(2) Tehnične podrobnosti izvedbe elektronske osebne izkaznice nizke ravni so določene v pravilih upravljanja elektronske osebne izkaznice nizke ravni, ki so objavljena na spletnih straneh izdajatelja.

15. člen

(raven zanesljivosti)

Elektronska osebna izkaznica nizke ravni je narejena tako, da zadosti merilom Uredbe 910/2014/EU za sredstva elektronske identifikacije nizke ravni zanesljivosti.

16. člen

(obdobje veljavnosti)

Elektronska osebna izkaznica nizke ravni se izdaja za čas veljavnosti osebne izkaznice in največ za čas 10 let.

17. člen

(starost ob izdaji)

Elektronsko osebno izkaznico nizke ravni lahko pridobi oseba, ki je dopolnila 12 let.

18. člen

(organ, pristojen za sprejem vlog)

(1) Vloge za izdajo elektronske osebne izkaznice nizke ravni sprejemajo upravne enote in diplomatsko-konzularna predstavništva Republike Slovenije.

(2) Identifikacijo fizične osebe s fizično prisotnostjo opravi uradna oseba na upravni enoti ali diplomatsko-konzularnem predstavništvu Republike Slovenije.

(3) Uradna oseba, ki sprejme vlogo, preveri veljavnost vnesenih podatkov in identificira posameznika tako, kot je določeno v zakonu, ki ureja izdajo sredstev elektronske identifikacije.

19. člen

(postopek izdaje)

(1) Če je vloga popolna, organ, pristojen za sprejem vloge, vlogo preda izdajatelju.

(2) Izdajatelj izda elektronsko osebno izkaznico nizke ravni po naslednjem postopku:

- izdajatelj pripravi podatke za izdelavo digitalnega potrdila in jih pošlje v evidenco osebnih izkaznic;
- pogodbeni izvajalec ministrstva, pristojnega za notranje zadeve, v postopku izdelave osebne izkaznice iz evidence osebnih izkaznic pridobi podatke za izdelavo digitalnega potrdila ter jih preda izdajatelju;
- izdajatelj izdela digitalno potrdilo in ga vrne pogodbenemu izvajalcu ministrstva, pristojnega za notranje zadeve;

– pogodbeni izvajalec ministrstva, pristojnega za notranje zadeve, digitalno potrdilo zapiše na čip osebne izkaznice in določi merila za uporabo elektronske osebne izkaznice nizke ravni;
– pogodbeni izvajalec ministrstva, pristojnega za notranje zadeve, izdelano osebno izkaznico imetniku vroči v skladu z določili zakona o osebni izkaznici.

(2) Elektronska osebna izkaznica nizke ravni postane aktivna takoj po izdaji.

20. člen

(preklic)

(1) Elektronsko osebno izkaznico nizke ravni izdajatelj prekliče, če:

– imetnik zahteva preklic osebne izkaznice tako, kot je določeno v zakonu o osebni izkaznici;
– se imetniku osebna izkaznica prekliče;
– imetnik zahtevek za preklic elektronske osebne izkaznice nizke ravni vloži pri organu, pristojnem za sprejem vlog;
– imetnik v 7 (sedmih) dneh po vložitvi zahtevka za začasno razveljavitev elektronske osebne izkaznice nizke ravni vloge ne umakne;
– izdajatelj pridobi informacijo, na podlagi katere presodi, da obstaja resnična nevarnost za nepooblaščeno uporabo elektronske osebne izkaznice nizke ravni.

21. člen

(začasna razveljavitev)

(1) Elektronsko osebno izkaznico nizke ravni izdajatelj začasno razveljavi, če imetnik potrdila izdajatelju po elektronski poti pošlje zahtevek za začasno razveljavitev elektronske osebne izkaznice nizke ravni. V zahtevku mora imetnik navesti naslednje podatke:

– osebno ime,
– EMŠO,
– naslov stalnega prebivališča,
– telefonsko številko,
– …

(2) Izdajatelj začasno razveljavi elektronsko osebno izkaznico nizke ravni.

(3) Če imetnik v 7 (sedmih) dneh pri organu, pristojnem za sprejem vlog, ne umakne vloge za začasno razveljavitev elektronske osebne izkaznice nizke ravni, izdajatelj elektronsko osebno izkaznico nizke ravni prekliče.

22. člen

(čezmejna uporaba)

Elektronska osebna izkaznica nizke ravni se ne uporablja za čezmejne elektronske storitve.

VIRTUALNA ELEKTRONSKA IDENTITETA SREDNJE RAVNI

23. člen

(splošno)

Izdajatelj zagotovi izdajo sredstva elektronske identifikacije srednje ravni zanesljivosti, ki ga je mogoče uporabljati s pošiljanjem sporočil na mobilni telefon (v nadaljnjem besedilu: virtualna elektronska identiteta srednje ravni).

24. člen

(tehnične specifikacije)

(1) Virtualna elektronska identiteta srednje ravni je izdana v obliki niza podatkov, shranjenih na informacijskem sistemu izdajatelja, ki enolično določajo posameznika. Dostop od teh podatkov je zaščiten, tako da se za uporabo virtualne elektronske identitete srednje ravni uporabljajo naslednji varnostni mehanizmi:

- uporabniško ime,
- uporabniško geslo,
- enkratno geslo, poslano kot sporočilo na mobilni telefon imetnika.

(2) Tehnične podrobnosti izvedbe virtualne elektronske identitete srednje ravni so določene v pravilih upravljanja virtualne elektronske identitete srednje ravni, ki so objavljene na spletnih straneh izdajatelja.

25. člen

(raven zanesljivosti)

Virtualna elektronska identiteta srednje ravni je narejena tako, da zadosti merilom Uredbe 910/2014/EU za srednjo raven zanesljivosti.

26. člen

(obdobje veljavnosti)

Virtualna elektronska identiteta srednje ravni se izdaja za pet let.

27. člen

(starost ob izdaji)

Virtualno elektronsko identiteto srednje ravni lahko pridobi oseba, ki je dopolnila 15 let.

28. člen

(organ, pristojen za sprejem vlog)

(1) Vloge za izdajo virtualne elektronske identitete srednje ravni sprejema izdajatelj.

(2) Identifikacijo fizične osebe s fizično prisotnostjo opravi uradna oseba na upravni enoti.

(3) Uradna oseba, ki sprejme vlogo, preveri veljavnosti vnesenih podatkov in identificira posameznika tako, kot je določeno zakonu, ki ureja izdajo sredstev elektronske identifikacije.

29. člen

(vloga)

Vloga se vloži po elektronski poti prek informacijskega sistema izdajatelja.

30. člen

(postopek izdaje)

(1) Če je vloga popolna, organ, pristojen za sprejem vloge, ugotovi identiteto posameznika, tako da:

- posameznika napoti na upravno enoto, kjer uradna oseba izvede identifikacijo fizične osebe s fizično prisotnostjo;
- posameznik izkaže svojo identiteto z uporabo elektronske osebne izkaznice visoke ravni ali
- posameznik izkaže svojo identiteto z uporabo kvalificiranega potrdila za elektronski podpis.

(2) Izdajatelj izda virtualno elektronsko identiteto srednje ravni po naslednjem postopku:

- posameznik se prijavi v centralno storitev za spletno prijavo in elektronski podpis;
- posameznik vpiše telefonsko številko mobilnega telefona;
- izdajatelj pošlje posamezniku enkratno geslo v sporočilu na telefonsko številko mobilnega telefona;
- posameznik v informacijski sistem izdajatelja vpiše enkratno geslo;
- če se identiteta posameznika ugotavlja s fizično prisotnostjo na upravni enoti ali z uporabo elektronske osebne izkaznice visoke ravni, se postopek zaključi po uspešni identifikaciji posameznika;
- če se identiteta posameznika ugotavlja z uporabo kvalificiranega potrdila za elektronski podpis, izdajatelj pošlje posamezniku podatke za aktivacijo na njegov naslov.

(2) Virtualna elektronska identiteta srednje ravni postane aktivna:

- po uspešni identifikaciji posameznika, če se identiteta posameznika ugotavlja s fizično prisotnostjo na upravni enoti ali z uporabo elektronske osebne izkaznice visoke ravni;
- ko imetnik v informacijski sistem izdajatelja vpiše podatke za aktivacijo, če se identiteta posameznika ugotavlja z uporabo kvalificiranega potrdila za elektronski podpis.

31. člen

(preklic)

(1) Virtualno elektronsko identiteto srednje ravni izdajatelj prekliče, če:

- imetnik zahteva preklic virtualne elektronske identitete srednje ravni prek informacijskega sistema izdajatelja;
- izdajatelj pridobi informacijo, na podlagi katere presodi, da obstaja resnična nevarnost za nepooblaščeno uporabo virtualne elektronske identitete srednje ravni.

32. člen

(začasna razveljavitev)

Začasna razveljavitev virtualne elektronske identitete srednje ravni ni dovoljena.

33. člen

(čezmejna uporaba)

Virtualna elektronska identiteta srednje ravni se lahko uporablja za čezmejne elektronske storitve brez omejitev.

DOLOČITEV RAVNI ZANESLJIVOSTI

34. člen

(organ javnega sektorja določi raven zanesljivosti)

Organ javnega sektorja za dostop in uporabo posamezne elektronske storitve določi raven zanesljivosti v skladu z merili, ki so določena v zakonu, pri čemer upošteva smernice za izbiro ravni zanesljivosti, ki so objavljene na portalu nacionalnega interoperabilnostnega okvira (v nadaljnjem besedilu: portal NIO).

EŠEI

35. člen

(preračunavanje EŠEI za čezmejno elektronsko poslovanje)

Za zagotavljanje čezmejnega elektronskega poslovanja v skladu z Uredbo 910/2014/EU se uporablja enolični identifikator, ki se določi tako:

- številki EŠEI se doda šifra države, v katero se enolični identifikator pošlje kot identifikator uporabnika elektronske storitve, pri čemer velja šifra države, kot jo določa Statistični urad Republike Slovenije;
- dobljeni niz podatkov se šifrira po algoritmu AES s ključem, shranjenim na strojnem varnostnem modulu.

36. člen

(specifikacije za zapis EŠEI v kvalificirano potrdilo)

(1) EŠEI fizične osebe se v kvalificirano potrdilo zapiše kot zasebna razširitev kvalificiranega potrdila s posebno oznako.

(2) EŠEI poslovnega subjekta se v kvalificirano potrdilo zapiše kot zasebna razširitev kvalificiranega potrdila s posebno oznako.

37. člen

(dostop do storitve za pridobivanje in preverjanje EŠEI)

(1) Ponudniki elektronskih storitev za zagotavljanje svojih storitev dostopajo do podatkov oziroma preverijo podatke o EŠEI imetnika kvalificiranega potrdila na podlagi identifikacijskih podatkov kvalificiranega potrdila tako, da v ta namen uporabijo spletno storitev za pridobivanje oziroma preverjanje EŠEI.

(2) Spletni naslov sheme spletne storitve se v kvalificirano potrdilo zapiše kot zasebna razširitev kvalificiranega potrdila s posebno oznako.

CENTRALNA STORITEV ZA SPLETNO PRIJAVO IN ELEKTRONSKI PODPIS

38. člen

(namen identifikacije in avtentikacije ter tehnične specifikacije)

(1) Ponudniki elektronskih storitev uporabljajo centralno storitev za spletno prijavo in elektronski podpis za identifikacijo posameznika in njegovo avtentikacijo z uporabo sredstev elektronske identifikacije, če jim to omogoča zakon, ki ureja centralno storitev za spletno prijavo in elektronski podpis, in izpolnjujejo naslednje pogoje:

- ministrstvu, ki zagotavlja delovanje centralne storitve za spletno prijavo in elektronski podpis (v nadaljnjem besedilu: upravljavec centralne storitve), predajo vlogo za uporabo centralne storitve za spletno prijavo in elektronski podpis za identifikacijo in avtentikacijo;
- integracijo s centralno storitvijo za spletno prijavo in elektronski podpis izvedejo v skladu s tehničnimi specifikacijami, kar dokažejo z uspešno integracijo s testnim okoljem upravljavca centralne storitve;
- z upravljavcem centralne storitve podpišejo dogovor o uporabi centralne storitve za spletno prijavo in elektronski podpis.

(2) Storitev se uporablja tako, kot je določeno v tehničnih specifikacijah centralne storitve za spletno prijavo in elektronski podpis za identifikacijo in avtentikacijo, ki so objavljene na portalu NIO.

39. člen

(namen elektronskega podpisovanja in tehnične specifikacije)

(1) Ponudniki elektronskih storitev uporabljajo centralno storitev za spletno prijavo in elektronski podpis za namen elektronskega podpisovanja dokumentov z uporabo potrdila za elektronski podpis, če jim to omogoča zakon, ki ureja centralno storitev za spletno prijavo in elektronski podpis, in izpolnjujejo naslednje pogoje:

- upravljavcu centralne storitve pošljejo vlogo za uporabo centralne storitve za spletno prijavo in elektronski podpis za elektronsko podpisovanje dokumentov;
- integracijo s centralno storitvijo za spletno prijavo in elektronski podpis izvedejo v skladu s tehničnimi specifikacijami, kar dokažejo z uspešno integracijo s testnim okoljem upravljavca centralne storitve;
- z upravljavcem centralne storitve podpišejo dogovor o uporabi centralne storitve za spletno prijavo in elektronski podpis.

(2) Storitev se uporablja tako, kot je določeno v tehničnih specifikacijah centralne storitve za spletno prijavo in elektronski podpis za elektronsko podpisovanje dokumentov, ki so objavljene na portalu NIO.

40. člen

(namen čezmejne avtentikacije in tehnične specifikacije)

(1) Ponudniki elektronskih storitev, registrirani v Republiki Sloveniji, uporabljajo centralno storitev za spletno prijavo in elektronski podpis za čezmejno avtentikacijo v skladu s 6. členom Uredbe 910/2014/EU, če izpolnjujejo naslednje pogoje:

- upravljavcu centralne storitve pošljejo vlogo za uporabo centralne storitve za spletno prijavo in elektronski podpis za čezmejno avtentikacijo;
- integracijo s centralno storitvijo za spletno prijavo in elektronski podpis izvedejo v skladu s tehničnimi specifikacijami, kar dokažejo z uspešno integracijo s testnim okoljem upravljavca centralne storitve;
- z upravljavcem centralne storitve podpišejo dogovor o uporabi centralne storitve za spletno prijavo in elektronski podpis.

(2) Storitev se za ponudnike elektronskih storitev iz prejšnjega odstavka uporablja tako, kot je določeno v drugem odstavku 51. člena te uredbe.

(3) Ponudniki elektronskih storitev, ki niso registrirani v Republiki Sloveniji, uporabljajo centralno storitev za spletno prijavo in elektronski podpis za čezmejno avtentikacijo v skladu s 6. členom Uredbe 910/2014/EU, če izpolnjujejo naslednje pogoje:

- elektronsko storitev vključijo v interoperabilnostni okvir iz 12. člena uredbe 910/2014/EU v državi, v kateri so registrirani;
- integracijo z interoperabilnostnim okvirjem iz prejšnjega odstavka izvedejo v skladu s tehničnimi specifikacijami.

(4) Storitev se za ponudnike elektronskih storitev iz prejšnjega odstavka uporablja tako, kot je določeno v izvedbenih aktih uredbe 910/2014/EU, ki se nanašajo na interoperabilnostni okvir iz 12. člena uredbe 910/2014/EU.

41. člen

(namen ustvarjanja pooblastil in tehnične specifikacije)

(1) Ponudniki elektronskih storitev uporabljajo centralno storitev za spletno prijavo in elektronski podpis za ustvarjanje pooblastil v elektronski obliki za identifikacijo in avtentikacijo pooblaščenca in njihovo uporabo v pravnem prometu, če jim to omogoča zakon, ki ureja centralno storitev za spletno prijavo in elektronski podpis, in izpolnjujejo naslednje pogoje:

- upravljavcu centralne storitve pošljejo vlogo za uporabo centralne storitve za spletno prijavo in elektronski podpis za ustvarjanje pooblastil v elektronski obliki;
- integracijo s centralno storitvijo za spletno prijavo in elektronski podpis izvedejo v skladu s tehničnimi specifikacijami, kar dokažejo z uspešno integracijo s testnim okoljem upravljavca centralne storitve;
- z upravljavcem centralne storitve podpišejo dogovor o uporabi centralne storitve za spletno prijavo in elektronski podpis.

(2) Storitev se uporablja tako, kot je določeno v tehničnih specifikacijah centralne storitve za spletno prijavo in elektronski podpis za ustvarjanje pooblastil v elektronski obliki, ki so objavljene na portalu NIO.

42. člen

(cenik)

Za uporabo storitev iz prejšnjih treh členov se določi cenik, ki je priloga te uredbe.

NADZOR NAD IZVAJANJEM TE UREDBE

43. člen

(izvajanje nadzora)

(1) Nadzor nad izvajanjem te uredbe opravlja isti organ, kot opravlja nadzor nad zakonom, ki ureja elektronsko identiteto in storitve zaupanja.

(2) V primeru kršitev te uredbe inšpektor predlaga ukrepe za izboljšanje poslovanja organa ali odredi odpravo nezakonitosti.

KONČNA DOLOČBA

44. člen

(začetek veljavnosti)

Ta uredba začne veljati petnajsti dan po objavi v Uradnem listu Republike Slovenije.

OPOMBA:

Prilogo cenik bo predlagatelj priložil v času medresorskega usklajevanja uredbe.