PRAVILNIK O IZVAJANJU KVALIFICIRANE STORITVE ZAUPANJA POTRJEVANJA VELJAVNOSTI KVALIFICIRANIH ELEKTRONSKIH ŽIGOV

Oznaka dok.:	0613/3/4
Veljavnost od:	30. maj 2020
Verzija:	4
Datum verzije:	27.5.2020
Avtor:	Ana Kalan
Stopnja zaupnosti:	Javno
Odgovorna oseba:	Pavel Reberc, direktor

Pregled predhodnih izdaj

Izdaja	Številka dokumenta	Verzija	Datum	Opis spremembe	Spremembe pripravil	Spremembe odobril
1	0613/3/1	V1	14.4.2017	Začetna izdaja - Skupni pravilnik o izvajanju kvalificirane storitve zaupanja potrejevanja veljavnosti kvalificiranih elektronskih podpisov in elektronskih žigov	Ana Kalan	Pavel Reberc
2.	0613/3/2	V2	19.6.2017	Dokument vsebuje samo pravilnik o izvajanju kvalificirane storitve zaupanja potrjevanja veljavnosti kvalificiranih elektronskih žigov	Ana Kalan	Pavel Reberc
3.	0613/3/3	V3	30.6.2017	Popravek pravopisnih napak	Pavel Reberc	Pavel Reberc
4.	0613/3/4	V4	27.5.2020	Dodana stran ”Pregled predhodnih izdaj”, nova verzija standarda	Marija Stojanović-Grujić	Pavel Reberc

JAVNI DEL NOTRANJIH PRAVIL EIUS D.O.O.

POLITIKA O IZVAJANJU KVALIFICIRANE STORITVE ZAUPANJA POTRJEVANJA VELJAVNOSTI KVALIFICIRANIH ELEKTRONSKIH ŽIGOV

Politika za Kvalificirano storitev zaupanja potrjevanja veljavnosti kvalificiranih elektronskih žigov,

CPOID: 1.3.6.1.4.1.50183.3.1

1. UVOD

1.1 EIUS d.o.o. je ponudnik kvalificiranih storitev zaupanja (QTSP), ki za izvajanje svojih storitev priporočene elektronske dostave, elektronskega podpisovanja, elektronskega žigosanja, elektronskega časovnega žigosanja, validacije in drugih storitev uporablja najvarnejše tehnologije, vključno z uporabo varnih nosilcev podatkov.

1.2 Družba izvaja storitve zaupanja v skladu z veljavnim pravnim redom Republike Slovenije in Evropske unije, še posebej pa v skladu z Uredbo (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 (t.i. uredba eIDAS) ter v skladu s tehničnimi zahtevami, smernicami in mednarodnimi standardi, še posebej ETSI SR 019 050, EN 319 401 v2.2.1 , EN 319 421 v1.1.1 ETSI TS 119 101 V1.1.1 (2016-03), .

1.3 Ta pravilnik ureja določila glede:

- osebja družbe (pristojnosti, naloge, pooblastila in zahtevani pogoji posameznih članov osebja) ter
- načina izvajanja storitev zaupanja.

1.4 Evidentiranje in razvrstitev sredstev informacijskega sistema in komunikacijskega omrežja, fizično varovanje, upravljanje s komunikacijami, obvladovanje dostopov do informacij in sistemov, načrtovanje neprekinjenega poslovanja ter nadzor so podrobneje urejeni z akti na področju informacijske varnosti.

1.5 Skladno z uredbo eIDAS družba izvaja kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih žigov.

Storitev kreiranja kvalificiranih elektronskih žigov izpolnjuje naslednje zahteve:

- kvalificiran elektronski žig je enolično povezan z ustvarjalcem žiga;
- s kvalificiranim elektronskim žigom je mogoče identificirati ustvarjalca žiga;
- kvalificiran elektronski žig je bil ustvarjen na podlagi podatkov za ustvarjanje kvalificiranega elektronskega žiga, ki jih ustvarjalec žiga z visoko stopnjo zaupanja in pod svojim nadzorom lahko uporablja za ustvarjanje kvalificiran elektronskega žiga, in
- je povezan s podatki, na katere se nanaša, in sicer tako, da je mogoče zaslediti vsako naknadno spremembo teh podatkov.

Storitev potrjevanja veljavnosti kvalificiranih elektronskih žigov izpolnjuje naslednje zahteve:

- je bilo potrdilo, na katerem temelji žig, v času podpisa kvalificirano potrdilo za elektronski žig, ki je skladno s Prilogo I uredbe EIDAS;
- je kvalificirano potrdilo izdal ponudnik kvalificiranih storitev zaupanja in je bil veljaven v času žiga;

- podatki za potrjevanje veljavnosti žiga ustrezajo podatkom, predloženim zanašajočim se strankam;
- je enolični nabor podatkov, ki predstavlja podpisnika potrdila, pravilno predložen zanašajočim se strankam;
- je zanašajoči se stranki jasno sporočeno, če je bil v času žiga uporabljen psevdonim;
- je bil kvalificiran elektronski žig ustvarjen z napravo za ustvarjanje kvalificiranega elektronskega podpisa;
- celovitost podpisanih podatkov ni ogrožena;
- so bile v času podpisa izpolnjene zahteve iz člena 26.
- Sistem za potrjevanje veljavnosti kvalificiranega elektronskega žiga zanašajoči se stranki zagotavlja pravilne rezultate postopka potrjevanja veljavnosti in ji omogoča odkrivanje vseh zadevnih varnostnih vprašanj.
- kvalificiran elektronski žig je enolično povezan s podpisnikom;
- s kvalificiranim elektronskim žigom je mogoče identificirati podpisnika;
- kvalificiran elektronski žig je bil ustvarjen na podlagi podatkov za ustvarjanje kvalificiranega elektronskega podpisa, ki jih podpisnik z visoko stopnjo zaupanja lahko uporablja izključno pod svojim nadzorom, in
- s podatki, ki so na ta način podpisani, je kvalificiran elektronski žig povezan tako, da je opazna vsaka naknadna sprememba podatkov.

2. OPIS KVALIFICIRANE STORITVE POTRJEVANJA VELJAVNOSTI KVALIFICIRANIH ELEKTRONSKIH ŽIGOV

a) Naročniki

Naročniki so pravne osebe in fizične osebe, ki uporabljajo kvalificirane storitve zaupanja in imajo z družbo eIUS d.o.o. sklenjeno pogodbeno razmerje.

b) Tretje osebe

Tretje osebe so pravne ali fizične osebe, ki se zanašajo na podatke, ki jih družba zagotavlja na podlagi opravljene kvalificirane storitve zaupanja ter v konkretnem primeru niso uporabnik storitve.

c) Namen uporabe in nedovoljena uporaba

(1) Storitev potrjevanja veljavnosti kvalificiranih elektronskih žigov se lahko uporablja za preverjanje žigov izvedenih po tehnično podprtih standardih.

(2) Prepovedano je izvajanje kvalificiranih storitev zaupanja v nasprotju z določili tega pravilnika ali veljavnih predpisov ali izven obsega dovoljene uporabe, določene s tem pravilnikom.

d) Pooblaščene kontaktne osebe

Naročniki in tretje osebe se lahko za vsa vprašanja v zvezi s tem pravilnikom ali izvajanjem kvalificirane storitve zaupanja obrnejo na pooblaščene osebe ponudnika kvalificiranih storitev zaupanja, ki so dosegljive na spodnjem naslovu in spodaj navedenih telefonskih številkah:

Pavel Reberc, eIUS d.o.o., Vrtna ulica 22, Ljubljana tel. 01 426 53 76.

e) Dostopnost za invalide

Storitve zaupanja in izdelki za končne uporabnike, ki se uporabljajo pri zagotavljanju teh storitev, so dostopni invalidom.

f) Objava informacij

(1) Ponudnik kvalificiranih storitev zaupanja vsa obvestila v zvezi s svojim delovanjem ter druge pomembne dokumente javno objavi na spletnih straneh družbe na naslovu http://vep.si/ .

(2) Dokumenti, ki so javno dostopni, so: politike, splošni pogoji, uporabniška navodila, cenik, obvestila, in sicer na spletni strani ponudnika družbe.

2.1 Ustvarjanje žigov

Aplikacija za ustvarjanje kvalificiranih elektronskih žigov je sestavljena iz treh komponent:

- Podpisne komponente, ki se izvaja na uporabnikovem osebnem računalniku in posreduje zahtevke za podpis, prejete iz strežniških modulov, do naprave za elektronsko podpisovanje (pametne kartice) preko programske opreme proizvajalce pametne kartice (angl. »middleware«)
- Strežniških modulov, ki pripravljajo podatke za podpisovanje v predpisani XML obliki z natačno definirano strukturo in jih prikazujejo uporabniku (npr. elektronske pošiljke, priponke, elektronski obrazci, ...)
- Spletne aplikacije, ki uporabniku omogoča podpis poljubnega PDF/A dokumenta ter pošiljanje le-tega poljubnemu uporabniku storitev varnega vročanja ponudnika EIUS d.o.o.

2.2 Preverjanje žigov

Rešitev za preverjanje kvalificiranih elektronskih žigov je sestavljena iz dveh komponent:

- modula za preverjanje žigov dokumentov ponudnika storitev zaupanja EIUS d.o.o., ki se izvaja znotraj aplikacij zaupanja ponudnika v skladu s politiko poslovnih procesov (npr. preverjanje žiga elektronske pošilje, ...),

- spletne aplikacije za preverjanje žigov dokumentov ponudnika, v katero lahko uporabniki sami odložijo svoj dokument za preverjanje žiga, če npr. dokument shranijo na lokalni računalnik in ga izbrišejo v aplikaciji zaupanja.

Aplikacija za preverjanje preverjanje kvalificiranih elektronskih žigov izvede vse s standardi predpisane postopke preverjanja kvalificiranega elektronskega žiga in uporabniku, na zahtevo, izda poročilo o preverjenem žigu, skladno z zahtevami uredbe eIDAS in standard ETSI EN 319 102-1
.

Postopek preverjanja kvalificiranega elektronskega žiga dokumenta poteka na naslednji način:

1. Uporabnik se prijavi v aplikacijo zaupanja ponudnika eIUS d.o.o. in izbere ali naloži dokument, katrega podpis želi preveriti.

2. Uporabnik sproži preverjanje elektronskega podpisa dokumenta.

3. Aplikacija preveri elektronski podpis skladno s politiko preverjanja elektronskih podpisov ter uporabniku prikaže rezultat preverjanja ter mu omogoči prenos poročila o preverjanju v obliki PDF dokumenta, podpisanega s strani ponudnika storitev zaupanja eIUS d.o.o.

2.3 Splošne zahteve za aplikacijo

2.3.1 Uporabniški vmesnik

UI 1: Uporabniški vmesnik storitve za ustvarjanje in validacije podpisov je zasnovan tako, da uporabniku na jasen in predvidljiv način omogoča uporabo funkcionalnosti podpisovanja in validacije žigov. Uporabnik je čez vse postopke, ki vsebujejo podpisovanje ali preverjanje podpisov voden z jasnimi koraki in oznakami na ekranu (npr. »podpiši in pošlji pošiljko«, “podpiši in shrani” za podpisovanje povratnice in prevzema pošiljke na disk«, ...)

Kjer je možno, je kompleksnost podpisovanja in preverjanja žigov skrita pred uporabnikom na tak način, da se vse napredne odločitve o obliki in načinih izvajanja operacije ustvarjanja in validacije žigov nastavljene na razumne privzete vrednosti, ki ustrezajo veliki večini uporabnikov.

Konkretno:

- Aplikacija za podpisovanje se namesti na uporabnikov osebni računalnik brez nepotrebnih vprašanj o namestitvi, na uporabnikov domači imenik, in zato ne potrebuje administratorskih pravic za namestitev. Aplikacija ne potrebuje dodatnih nastavitev, saj se vse odločitve sprejemajo v programski opremi na strežniku, ki preko aplikacije za podpisovanje zahteva uporabnikov žig v ustrezni obliki (PDF, XML) in z ustreznim podpisnim ključem (pripadajočem kvalificiranemu potrdilu za elektronski podpis, s katerim je prijavljen na strežnik). Podpisna aplikacija se skrije v uporabnikovo opravilno vrstico in uporabnika preko balončkov obvešča le o pomembnih dogodkih (npr. podpisujem pošiljko, podpisujem priponko, ...).
- Vse akcije v aplikaciji za podpisovanje so jasno razdeljene na posamezne logične korake in vsebujejo informacije o postopku, ki se bo izvedel (npr. »podpiši in oddaj

pošiljko«, “podpiši in shrani” za podpisovanje povratnice in prevzem pošiljke na lokalni disk«).

- Aplikacija, ki zahteva uporabnikov podpis, ima vgrajena stroga preverjanja vhodnih podatkov in sama dopolni nepopolno vpisane podatke (npr. doda @vep.si pripono pri naslovu prejemnikovega poštnega predala, ipd.).
- Vsa obvestila o napakah se tolmačijo na podlagi številčne oznake napake (angl. »error code«) in prikazujejo razumljivo sporočilo z nasvetom za odpravo težave. Aplikacija ne prikazuje nerazumljivih sporočil, ki jih npr. pripravi operacijski sistem.
- Vse akcije uporabnika povzročijo, da se uporabniku prikaže kratko obvestilo o uspešnosti ali neuspešnosti postopka (npr. »pošiljka uspešno oddana«, »napaka pri pošiljanju pošiljke: prejemnikov naslov ne obstaja«)
- Vsa obvestila aplikacije so opremljena z jasnimi slikovnimi oznakami in barvami, ki uporabniku v hipu nakažejo rezultat operacije (npr. »zelena kljukica – operacija uspešno izvedena«, »rdeč X – operacija neuspešna«)
- Vsi pozivi uporabnikom so opremljeni z gumbom »Prekliči« ali »Nazaj«, kadar je to smiselno.
- Aplikacija ne razkriva več podatkov, kot je to nujno potrebno za izvedbo operacije (npr. »Ali želite poslati pošiljko na janez.novak@vep.si?«, ne prikazuje pa same vsebine pošiljke).
- Aplikacija se ne odloča namesto uporabnika, kadar bi to lahko imelo resne posledice za uporabnika, temveč vse odločitve prepusti uporabniku v potrditev (npr. »Ali res želite podpisati in oddati pošiljko za ...«)

UI 2: Kadar uporabniki prvič vstopijo v aplikacijo, imajo na voljo jasna navodila, ki jim orišejo delovanje aplikacije, razložijo osnove delovanja kvalificiranih potrdil za elektronske podpise in kvalificiranih elektronskih žigov ter uporabniku prikažejo nekaj osnovnih načinov uporabe.

Splošne varnostne zahteve

Aplikacija za podpisovanje in preverjanje podpisa se razvija v skladu z veljavnimi standardni in industrijskimi priporočili za varnostne aplikacije. Uporabljena programska orodja so izbrana tako, da zmanjšujejo možnosti napak, ki jih lahko naredijo razvojni inženirji, saj programska okolja analizirajo izvorno kodo že med samim razvojem in opozarjajo na najpogostejše napake. Izbrani programski jeziki močno zmanjšujejo možnosti nepooblačenega pisanja po spominu in posledično izvajanja neavtorizirane programske kode. Spletne aplikacije sledijo priporočilom OWASP za razvoj varnih spletnih aplikacij.

GSM 1: Pri razvoju programske opreme za podpisovanje in preverjanje žigov so upoštevane tudi naslednje zahteve:

- GSM 1.1: Ponudnik storitev zaupanja EIUS d.o.o. ima izdelano analizo tveganj in pripravljene ukrepe za upravljanje s tveganji.
- GSM 1.2: Delovne postaje razvojnih inženirjev se redno posodobljajo. Programska orodja, ki se uporabljajo za razvoj, so nakupljena po modelu naročnine, kar zagotavlja redne (varnostne) posodobitve orodij in podpornih knjižnic.
- GSM 1.3: Vsa programska oprema uporablja odprte standarde in protokole (npr. REST/JSON, SOAP web services, web sockets, TLS, ...) ter uveljavljene prostodostopne podporne knjižnice (Spring, Hibernate, Angular, ...). Ker so standardi in podporne knjižnice prostodostopne, je vsem uporabnikom na voljo izvorna koda na vpogled.

- GSM 1.4: Aplikacija za podpisovanja uporablja kriptografske knjižnice, ki so del programskih orodij za razvoj (npr. sistemske varnostne knjižnice na Windows in macOS, OpenSSL na Linux) ali priznano varnostno knjižnico BouncyCastle za Java okolje.
- GSM 1.6: Aplikacija za podpisovanje in preverjanje podpisov ne nalaga dinamičnih modulov s spleta; namestitveni paket aplikacije je elektronsko podpisan z elektronskim potrdilom EIUS d.o.o., zato se vanjo ne more vriniti neželena programska oprema.
- GSM 1.7: Med priporočili za delovanje aplikacije za podpisovanje in preverjanje podpisov je tudi osebni požarni zid.

GSM 2: Posebne zahteve:

- GSM 2.1: Vsi namestitveni paketi aplikacije za podpisovanje in preverjanje podpisov na vseh podprtih okoljih so elektronsko podpisani.
- GSM 2.2: Za podpisovanje namestitvenega paketa aplikacije se uporablja namensko potrdilo za podpisovanje aplikacij overitelja elektronskih potrdil DigiCert.
- GSM 2.3, GSM 2.4: Vsi podatki, ki se izmenjujejo med komponentami aplikacije za podpisovanje in preverjanje podpisov se izmenjujejo po varni TLS povezavi z obojestransko avtentikacijo.
- GSM 2.5: Protokol prenosa podatkov med moduli aplikacije za podpisovanje in preverjanje podpisov preprečuje morebitne ponovitvene napade.
- GSM 2.6: Aplikacija za podpisovanje in preverjanje podpisov ne shranjuje nobenih podatkov (npr. podatkov, ki se podpisujejo; osebne številke PIN, ...).

GSM 3: Aplikacija za podpisovanje in preverjanje podpisov uporabniku prikaže povezavo do spletne strani z nasveti za varno uporabo osebnega računalnika in aplikacije.

Celovitost storitev zaupanja

Vse zahteve standarda ETSI EN 319 102-1 so vpeljane v vsej verigi modulov, ki tvorijo storitev zaupanja, in ne samo v aplikaciji za podpis in preverjanje podpisa.

Regulatorne zahteve

Obdelava osebnih podatkov

PD1, PD2: Ponudnik storitev zaupanja EIUS d.o.o. je odgovoren v skladu z veljavnimi predpisi o varstvu podatkov.

Ponudnik storitev zaupanja EIUS d.o.o. ne posreduje drugih podatkov o uporabnikih, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih storitev oz. aplikacij, povezanih s kvalificiranimi elektronskimi časovnimi žigi, ter je ponudnika kvalificiranih storitev zaupanja EIUS d.o.o. imetnik pooblastil za to, ali na zahtevo pristojnega sodišča, prekrškovnega ali upravnega organa.

Podatki se posredujejo tudi brez pisne privolitve, če to določa zakonodaja oz. veljavni predpisi.

Nadzor nad skladnostjo delovanja ponudnika storitev zaupanja EIUS d.o.o. z veljavnimi predpisi izvaja pristojni inšpektorat in akreditirani organi za ugotavljanje skladnosti.

Akreditiran organ za ugotavljanje skladnosti ponudnika storitev zaupanja EIUS d.o.o. revidira najmanj vsakih 24 mesecev. Namen revizije je potrditi, ali ponudnik kvalificiranih storitev zaupanja in kvalificirane storitve zaupanja, ki jih zagotavlja, izpolnjujejo zakonske zahteve.

Notranje preverjanje skladnosti delovanja izvajajo pooblaščene osebe v okviru ponudnika storitev zaupanja EIUS d.o.o..

Prilagoditev storitev zaupanja za osebe s posebnimi potrebami

APD 1: Aplikacije ponudnika storitev zaupanja EIUS d.o.o. omogočajo preklop na poseben način delovanja, ki je namenjen osebam s posebnimi potrebami. Preklop na poseben način delovanja s spletnih strani odstrani elemente, ki motijo bralnike zaslona (slike). Primernost spletnih strani je bila preverjena z orodji, ki so prostodostopna na spletu, in priporočila teh orodij upoštevana.

Zagotavljanje integritete aplikacije

Mehanizmi za zagotavljanje integritete aplikacije za podpis in preverjanje podpisa so podrobneje opisani v dokumentu Politika razvoja in vzdrževanja informacijskih storitev.

Dnevniški zapisi

EL 1: Dnevniški zapisi delovanja aplikacije za podpisovanje in preverjanje podpisov so nastavljeni na podlagi sprejete ocene tveganj in ukrepov za obvladovanje tveganj.

EL 2: Dnevniški zapisi delovanja aplikacije za podpisovanje in preverjanje podpisov so zaščiteni pred nepooblaščenimi spremembami tako, da se periodično časovno žigosajo in shranijo na varen medij.

EL 3, EL 4: Vsi moduli aplikacije za podpisovanje in preverjanje podpisov beležijo zapise v dnevniške datoteke z vsemi potrebnimi podatki. Ker se podpisna aplikacija izvaja na računalniku uporabnika, podatke za dnevniške zapise posreduje krmilni aplikaciji na strežniku.

EL 5, EL 6: Aplikacija za podpisovanje in preverjanje podpisov beleži vsako podpisovanje ter preverjanje podpisa v dnevniške datoteke.

EL 7, EL 8: Aplikacija za podpisovanje in preverjanje podpisov vse zapise v dnevniške datoteke beleži s časom nastanka dogodka, statusom dogodka, opisom dogodka ter oznako komponente in modula, ki je sprožila dogodek.

Zahteve za podpisovanje

SCP 1: Aplikacija za podpisovanje podpira podpise po naslednjih formatih:

- XadES-BASELINE-B
- XadES-BASELINE-T
- PAdES-E-BES

Aplikacija podpira »enveloped« in »detached« podpise.

SCP 2: Aplikacija za podpisovanje prikaže vse pomembne podatke glede na vrsto podpisa.

SCP 3, SCP 4: Aplikacija za podpisovanje prikazuje in podpisuje poljubne PDF dokumente ter XML dokumente, ki se uporabljajo v storitvah zaupanja ponudnika EIUS d.o.o. (elektronske pošiljke, vročilnice, povratnice, ...)

SCP 5 – SCP 9: Aplikacija za podpisovanje je namenjena podpisovanju elektronskih pošiljk (XML) in obrazcev (XML) ter prilog pošiljkam (PDF). Podatke za podpis pripravi aplikacija za elektronske pošiljke, zato aplikacija za podpisovanje vedno podpisuje dokumente podprtega tipa in vsebine.

SCP 10 – SCP 14: Aplikacija za podpis prikaže dokument, ki se podpisuje, uporabniku. Uporabnik sam izbere dokument (pošiljko, obrazec), ki ga bo podpisal. Podpiše se ves dokument ali priponka.

SCP 15 – SCP 17: Uporabnik podpisuje dokumente elektronskega vročanja, ki ne vsebujejo drugih podpisov.

SCP 18: Dokument za podpis se pri prikazu vsebine ne more spreminjati.

SCP 19 – SCP 22: Dokument, ki se podpisuje, vsebuje oznako tipa dokumenta (text/xml) v podpisu dokumenta.

SCP 23 - SCP 24: Vrste dokumentov (XML, PDF/A), ki se podpisujejo, ne vsebujejo programskih elementov, ki bi lahko spreminjali prikaz dokumenta pred podpisom.

SCP 25 - SCP 26: Uporabniku se prikaže vsebina dokumenta, ki ga podpisuje, ter predstavi posledice, ki jih bo podpis imel (dostava pošiljke na izbrani dokument, plačilo storitve dostave s točnim zneskom).

SCP 27 – SCP 30: Vsi atributi, ki se podpisujejo, so prikazani uporabniku pred podpisom.

SCP 31 – SCP 33: Uporabnik dokumente podpisuje s kvalificiranim potrdilom za elektronski podpis, s katerim se je prijavil v aplikacije storitev zaupanja ponudnika EIUS d.o.o. Pri podpisovanju ne more izbrati drugega kvalificiranega potrdila za elektronski podpis.

SCP 34 - SCP 36: Uporabnikovo kvalificirano potrdilo za elektronsko podpisovanje se preveri pred vstopom v aplikacije storitev zaupanja ponudnika EIUS d.o.o. in uporabniku onemogoči dostop do aplikacije (in posledično podpisovanja), če njegovo kvalificirano potrdilo za elektronski podpis ni veljavno (časovna veljavnost, podpisi v celotni verigi do priznanega korenskega potrdila, status preklica).

SCP 37: Aplikacija za podpis v podpisanih atributih podpisa vsebuje oznako kvalificiranega potrdila za elektronski podpis, ki se je uporabilo za podpis.

SCP 38 – SCP 39: Podpisani dokumenti ne vsebujejo posebnih atributov z zavezami (angl. »committment attributes«).

SCP 40 - SCP 44: Podpisna politika je opredeljena v politikah storitev zaupanja ponudnika EIUS d.o.o. in je uporabnik ne more spremeniti.

SCP 46 – SCP 47: Aplikacija izvede operacijo elektronskega podpisa na dokumente šele po izrecni privolitvi uporabnika (dialog z vprašanjem po potrditvi). Dialog se pojavi po prikazu dokumenta za podpis.

SCP 48: Dokument se v skladu s politiko izvajanja storitev zaupanja ponudnika EIUS d.o.o. časovno žigosa takoj po podpisovanju. Če časovnega žiga ni mogoče pridobiti, dokumenta ni mogoče oddati v sistem in se postopek oddaje (podpisa) dokumenta prekine.

SCP 49 - SCP 53: Uporabnik je pred izdelavo elektronskega podpisa opozorjen in pozvan, da potrdi elektronsko podpisovanje dokumenta.

SCP 54: Dostop do podpisne naprave po vnosu osebne številke je omejen na čas, ki ga določa podpisna naprava. Aplikacija za podpisovanje ne shranjuje osebne številke za dostop do podpisne naprave. Če podpisna naprava ne dovoli izvedbe več podpisov v omejenem časovnem obdobju, mora uporabnik pri vsakem podpisu vpisati osebno številko PIN.

SCP 55 – SCP 56: Uporabniški vmesnik podpisne aplikacije je omejen na prikaz dokumenta za podpis, obveznega nabora podatkov, ki se morejo prikazati uporabniku, ter vnosa osebne številke PIN za dostop do naprave. Podpisna aplikacija ne shranjuje uporabnikovih podatkov za dostop do podpisne naprave.

SCP 57 – SCP 59: Izbrani algoritmi za elektronsko podpisovanje so v skladu z zahtevami ETSI TS 119 312. Trenutno se uporablja zgoščevalna funkcija SHA 256 ter RSA dolžine vsaj 2048 bitov.

SCP 60 - SCP 73: Izbor podprtih politik kvalificiranih potrdil za elektronski podpis uporabnikov zagotavlja, da so izpolnjene vse zahteve SCP 60 – SCP 73. Ker se za vnos osebne številke PIN uporablja programska oprema ponudnika pametnih kartic (»middleware«), so natančna pravila vnosa in spremembe osebne številke PIN opisana v dokumentaciji proizvajalca pametnih kartic.

SCP 74 – SCP 78: Trenutno biometrične naprave niso podprte.

SCP 79 - SCP 81: Podpisna aplikacija uporablja programsko opremo proizvajalca podpisnih kartic; preverjanje avtentičnosti programske opreme proizvajalca kartic se izvaja v operacijskem sistemu, ki naloži programsko opremo. Podpisna aplikacija je elektronsko podpisana, zato se preverjanje avtentičnosti prav tako izvaja v operacijskem sistemu, ki požene programsko opremo.

SCP 82: Podpisna aplikacija uporablja privzeto politiko za vrsto dokumentov, ki se podpisujejo (pošiljka, elektronski obrazec, priponka).

SCP 83 – SCP 84: Podpisna aplikacija prikaže dokument z vsemi podatki, ki so pomembni za podpisnika. Priprava podatkov za podpis se izvrši v podpisni aplikaciji, izračun zgoščevalne funkcije pa v podpisni napravi (pametni kartici).

SCP 85: Prikaz podatkov za podpisovanje ne omogoča spreminjanja podatkov v dokumentu. Podpis se izdela na kopiji dokumenta v aplikaciji.

SCP 86: Zahteve po vrsti podpisne naprave se določajo glede na vrsto podatkov, ki se podpisujejo. Kadar je za podpis potrebna posebna vrsta naprave, se ustrezno naprave preveri iz podatkov v kvalificiranem potrdilu za elektronski podpis in/ali t.i. »trust listi« s seznamom vseh politik izdajatelja konkretnega kvalificiranega potrdila za elektronski podpis.

SCP 87: Izbor podpisne naprave ni v domeni podpisne aplikacije, razen tako, kot je navedeno v zahtevi SCP 86.

SCP 88 – SCP 91: Podatki med programsko opremo podpisne naprave (angl. »middleware«) in aplikacijo za podpisovanje se prenašajo znotraj naslovnega prostora procesa, kjer teče aplikacija za podpisovanje. Podatki med programsko opremo podpisne naprave in podpisno napravo se izmenjujejo v skladu s politiko proizvajalca podpisne naprave.

SCP 92 - SCP 94: Aplikacija za podpisovanje ne omogoča podpisa več združenih dokumentov hkrati.

Zahteve za preverjanje podpisov

SVP 1 – SVP 2: Aplikacija za preverjanje podpisov podpira preverjanje podpisov dokumentov, narejenih po naslednjih standardih:

- XAdES-BASELINE-B (za dokumente po shemah ponudnika storitev zaupanja EIUS d.o.o.)
- XAdES-BASELINE-T (za dokumente po shemah ponudnika storitev zaupanja EIUS d.o.o.)
- PAdES-E-BES

SVP 3 - SVP 7: Aplikacija za preverjanje podpisov izvaja postopek preverjanja podpisa v skladu z zahtevami razdelkov »Validation Process for Basic Signatures« in »Validation process for time-stamps« standarda ETSI 119 102-1.

SVP 8 – SVP 9: Aplikacija za preverjanje podpisov podpira le preverjanje podpisov po implicitni politiki za preverjanje podpisov, saj se zanaša, da bo preverjala le dokumente iz aplikacij zaupanj ponudnika EIUS d.o.o. V primeru, da se v preverjanje pošlje nepodprt dokument, aplikacija uporabnika opozori, da ne more preveriti podpisa.

SVP 10 – SVP 11: Aplikacija za preverjanje podpisov vedno preveri vse podpise dokumenta, ki vsebuje podpis (»detached« podpis znotraj krovnega dokumenta ali »enveloped« podpisa dokumenta).

SVP 12 - SVP 13: Aplikacija za preverjanje podpisov uporabniku, na zahtevo, prikaže rezultat preverjanja skupaj s podatki o podpisniku. Uporabnik lahko iz aplikacije prenese elektronsko podpisan PDF dokument z rezultatom in podrobnostmi preverjanja.

SVP 14 – SVA 19: Aplikacija za preverjanje podpisov preverja le podpise, opisane v točkah SVP 1 – SVP 9. Aplikacija za preverjanje podpisov uporablja zanesljiv vir časa za referenčni čas preverjanja.

SVP 20 – SVP 23: Aplikacija za preverjanje podpisov uporabniku prikaže rezultate preverjanje, ki med drugim vsebujejo tudi:

- rezultat preverjanja,
- podrobnosti preverjanja (veljavni elementi, neveljavni elementi)
- podatke o podpisniku.

Zahteve za dopolnitev podpisa

Aplikacija za podpisovanje in kvalificirano storitev za preverjanje podpisov uporablja kvalificiran elektronski časovni žig za potrebe podaljševanja veljavnosti elektronskih podpisov dokumentov.

3. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE

3.1 Splošno

(1) Družba načrtuje in izvaja vse varnostne ukrepe v skladu s standardom ISO/IEC 27001 ter s tehničnimi zahtevami ETSI SR 019 050- Electronic Signatures and Infrastructures (ESI); Rationalized framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures.

(2) Oprema družbe je postavljena v posebnih, ločenih prostorih in je zavarovana z večnivojskim sistemom fizičnega in protivlomnega tehničnega varovanja. Oprema je varovana proti nepooblaščenemu dostopu. Prav tako je zavarovana in zaščitena s protipožarnim sistemom, s sistemom proti izlitju vode, sistemom za prezračevanje in večnivojskim sistemom neprekinjenega napajanja.

(3) Družba shranjuje rezervne in distribucijske nosilce podatkov tako, da je v največji meri preprečena izguba, vdor ali nepooblaščena uporaba ali spreminjanje shranjenih informacij. Tako za obnovitev podatkov kot za arhiviranje pomembnih informacij so zagotovljene rezervne kopije, ki so shranjene na drugem mestu, kot je shranjena programska oprema, za zagotovitev ponovnega delovanja v primerih, ko bi bili uničeni podatki na osnovni lokaciji.

(4) Podroben opis infrastrukture družbe, operativno delovanje, postopki upravljanja z infrastrukturo ter nadzor nad varnostno politiko njenega delovanja je določen z akti na področju informacijske varnosti.

3.2 Fizično varovanje

(1) Oprema ponudnika storitev zaupanja je varovana z večnivojskim sistemom fizičnega in elektronskega varovanja.

(2) Varovanje infrastrukture ponudnika storitev zaupanja se izvaja v skladu s priporočili stroke za najvišji nivo varovanja.

(3) Celoten opis infrastrukture ponudnika storitev zaupanja in postopki upravljanja ter varovanje le-te so določeni z akti na področju informacijske varnosti.

3.3 Lokacija in zgradba ponudnika

(1) Oprema ponudnika storitev zaupanja je postavljena v posebnih, varovanih, ločenih prostorih.

(2) Zavarovana je z večnivojskim sistemom fizičnega in elektronskega varovanja.

(3) Podrobna določila so v aktih na področju informacijske varnosti.

3.4 Fizični dostop do infrastrukture ponudnika storitev zaupanja

(1) Dostop do infrastrukture ponudnika storitev zaupanja je omogočen samo pooblaščenim osebam ponudnika storitev zaupanja skladno z njihovimi nalogami in pooblastili.

(2) Vsi dostopi so varovani v skladu z zakonodajo in priporočili.

(3) Podrobna določila so v aktih na področju informacijske varnosti.

3.5 Napajanje in prezračevanje

(1) Infrastruktura ponudnika storitev zaupanja ima zagotovljeno neprekinjeno napajanje in ustrezne klimatske sisteme.

(2) Podrobna določila so v aktih na področju informacijske varnosti.

3.6 Zaščita pred poplavo

(1) Infrastruktura ponudnika storitev zaupanja ni izpostavljena nevarnostim poplav, razen v primeru višje sile.

(2) Podrobna določila so v aktih na področju informacijske varnosti.

3.7 Zaščita pred požari

(1) Prostori ponudnika storitev zaupanja so varovani pred morebitnim izbruhom požara.

(2) Podrobna določila so v aktih na področju informacijske varnosti.

3.8 Incidenti

(1) Varnostni dogodek je vsak dogodek povezan z varnostjo. Primeri varnostnih dogodkov so pooblaščeni ali nepooblaščeni vstopi v nek objekt, sprememba podatkov s strani pooblaščene ali nepooblaščene osebe.

(2) Varnostni incident je vsak varnostni dogodek, ki se zgodi drugače kot predvidevajo veljavni predpisi ali interni akti, ga krši, ali je posledica višje nepredvidljive sile.

(3) Varnostne incidente razvrščamo v dve različni kategoriji, in sicer:

1. varnostni incidenti, ki ogrožajo integriteto storitev zaupanja (npr. vdor oz. kraja pošiljk, napake pri vzdrževanju, ki ogrozijo celovitost sistemov/strežnikov, fizični dostop nepooblaščene osebe,);

2. varnostni incidenti, ki ne ogrožajo integritete storitev zaupanja (npr. izpad el. napajanja, izpad komunikacijskih vodov, zloraba pooblastil, poskusi vdora, DDOS napadi...).

(4) Če obstaja dvom pri določanju, v katero kategorijo se razvršča varnostni incident, se šteje, da se incident razvršča v prvo kategorijo.

(5) Vsak posameznik, ki zazna ali sumi na varnostni incident, ga je nemudoma dolžan prijaviti. Prijavljanje varnostnih incidentov poteka na kakršenkoli način (osebno, telefonsko, po elektronski pošti, prek spletnega vmesnika ...), ki omogoča čim hitrejše obveščanje ustreznih oseb.

(6) Za varnostne incidente, ki se nanašajo na varovanje življenja in zdravja oseb ali za varnostne incidente, ki se nanašajo na varovanje družbe, se obvešča direktorja ali prokurista in v primeru, ko je potrebno ukrepanje državnih organov se obveščajo pristojne službe (policija, gasilci, reševalci …).

(7) Za varnostne incidente, ki ogrožajo integriteto storitve zaupanja, se obvešča direktorja ali prokurista in inženirja za inf. varnost.

(8) Za varnostne incidente, ki ne ogrožajo integriteto storitve zaupanja, se obvešča direktorja ali prokurista in inženirja za inf. varnost.

(9) Pri vseh varnostnih incidentih, ki ogrožajo storitev zaupanja, prejemniki obvestila o varnostnem incidentu obvestijo direktorja.

(11) Prejemniki obvestila o varnostnem incidentu so dolžni raziskati prijavljene varnostne incidente in sprejeti ali predlagati ustrezne ukrepe, ki preprečujejo ponovitev varnostnega incidenta.

(12) V Evidenci varnostnih incidentov se evidentira vsak varnostni incident. Osnovni podatki o vsakem varnostnem incidentu so:

- naziv ali kratek opis incidenta ali dogodka,
- datum in čas dogodka,
- opis posledic dogodka,
- kategorija incidenta z razlago kriterijev za določitev kategorije,
- izvedeni ukrepi za odpravo incidenta in njegovih posledic.

(13) Evidenca varnostnih incidentov služi kot baza znanja za hitro ukrepanje ob ponovitvi enakih ali podobnih varnostnih incidentov.

(14) Obveščanje o varnostnih dogodkih in incidentih ne nadomesti postopkov in obveščanj po posameznih delovnih področjih (npr. obveščanje za odpravo škode in drugih postopkov, ki jih morajo opraviti delavci po posameznih področjih).

3.9 Hramba nosilcev podatkov

(1) Nosilci podatkov, bodisi v papirnati ali elektronski obliki, se hranijo varno v zaščitenih objektih.

(2) Varnostne kopije programske opreme in šifriranih baz ponudnika storitev zaupanja se redno obnavljajo in shranjujejo v dveh ločenih in fizično varovanih prostorih, na različnih lokacijah.

3.10 Odstranjevanje odpadkov

(1) Družba zagotavlja varno odstranjevanje in uničevanje dokumentov v fizični in elektronski obliki.

(2) Odstranjevanje odpadkov izvaja posebna komisija v skladu z akti na področju informacijske varnosti.

3.11 Organizacijska struktura ponudnika storitev zaupanja

Organizacijske skupine

(1) Operativno, organizacijsko in strokovno pravilno delovanje ponudnika storitev zaupanja vodi direktor EIUS d.o.o. Pavel Reberc.

(2) Zaposleni pri ponudniku storitev zaupanja so razporejeni v štiri organizacijske skupine, ki pokrivajo naslednja vsebinska področja:

Organizacijska skupina	Vloga	Osnovne naloge	Število oseb
Upravljanje s storitvijo in z informacijskim sistemom	Vodja izvajanja storitev	• Strategija delovanja ponudnika storitev zaupanja • Določevanje varnostnega inženirja • Operativno vodenje ponudnika storitev zaupanja	1

Upravljanje z podatkovne baze	Inženir podatkovne baze	• Upravljanje podatkovne baze (namestitev, vzdrževanje, strukturne spremembe), • Načrtovanje trenutne in bodoče razpoložljivosti, • Spremljanje in izboljšave (optimizacija)	1
Upravljanje sistemske in omrežne infrastrukture	Sistemski inženir (osebje zunanjega izvajalca – Telekom Slovenije d.d.)	• Upravljanje s strojno opremo • Upravljanje z operacijskim sistemom • Skrb za redno vzdrževanje (nadgradnje, dopolnitve) • Upravljanje s telekomunikacijami (sistem za preprečevanje in odkrivanje vdorov, požarna pregrada, ...) • Vzdrževanje varnostnih kopij	več
Informacijska varnost	Varnostni inženir	• Določevanje in izvajanje pravil varnega delovanja sistema • Izvajanje notranjih kontrol • Sodelovanje pri upravljanju incidentov • Svetovanje glede informacijske varnosti	1
Podpora strankam in preizkušanje	Skrbnik strank	• Sprejem strank • Komunikacija s strankami pisno in po telefonu • Sodelovanje pri upravljanju incidentov • Validacija delovanja aplikativne opreme	3
Evidentiranje in dokumentacija	Vodja pisarne	• Sprejem, oddaja in evidentiranje poslovne dokumentacije • Hramba dokumentacije skladno s klasifikacijskim načrtom	1
Skladnost s predpisi	Pravnik	• Spremljanje veljavnih evropskih in slovenskih predpisov, mednarodnih standardov in priporočil • Priprava predlogov potrebnih sprememb in dopolnitev zaradi pravnih, tehnoloških ali organizacijskih sprememb ter	1

		ugotovitev v praksi • Sodelovanje pri upravljanju incidentov • Svetovanje glede skladnega izvajanja nalog	
Varstvo osebnih podatkov	Pooblaščenec za varstvo podatkov	• Spremljanje veljavnih evropskih in slovenskih predpisov, mednarodnih standardov in priporočil na področju varstva podatkov • svetovanje glede ocene učinkov v zvezi z varstvom podatkov in spremljanje njenega izvajanja • svetovanje pri zagotavljanju vgrajene zasebnosti in drugih pomembnih analizah ali aktivnostih na področju varstva podatkov; • spremljanje skladnosti s Splošno uredbo o varstvu podatkov • sodelovanje z IP RS	1
Notranji nadzor	Pooblaščenec za notranji nadzor	• pregledovanje, ocenjevanje, presojanje in preverjanje primernosti ter učinkovitosti kontrol, sistemov in postopkov; • predlogi za izboljšanje sistema upravljanja; • svetovanje glede priprava internih aktov, smernic, izobraževalnih programov, • vodenje za dejavnost potrebnih evidenc in poročil.	1

3.12 Nezdružljivost nalog

Za vsako vlogo je natančno določeno, s katero sme oz. ne sme biti združljiva. V primeru nepredvidene odsotnosti določenih zaposlenih njihove vloge prevzamejo drugi zaposleni, če to skladno z akti na področju informacijske varnosti ni nezdružljivo.

3.13 Nadzor nad osebjem

(1) V družbi nadzor nad delovanjem osebja izvaja Pooblaščenec za notranji nadzor.

(2) Pooblaščenec za notranji nadzor v primeru odkritih pomanjkljivosti odredi ustrezne ukrepe za odpravo teh pomanjkljivosti, ki jih je družba dolžna izvesti, ter nadzoruje izvedbo odrejenih ukrepov.

3.14 Potrebne kvalifikacije in izkušnje osebja

(1) Osebje ponudnika storitev zaupanja ima skladno z zahtevami veljavnih predpisov ter tehničnih standardov in priporočil ustrezne kvalifikacije in izkušnje.
(2) Vse osebje se redno usposablja in pridobiva dodatna znanja s svojega strokovnega področja ter s področij informacijske varnosti in varstva osebnih podatkov ter uporabljajo upravne in upravljavske postopke, ki so v skladu z evropskimi ali mednarodnimi standardi.

3.15 Primernost osebja

Družba zaposluje zadostno število zanesljivo in strokovno usposobljenega osebja, ki preverjeno ni bilo kaznovano za kakršnokoli kaznivo dejanje.

3.16 Dodatno usposabljanje osebja

Osebam, ki opravljajo naloge zgoraj navedenih organizacijskih skupin, se skladno z internimi akti in letnim načrtom redno zagotavlja vse potrebno usposabljanje.

3.17 Zahteve za redna usposabljanja

Osebje se usposablja glede na potrebe oz. novosti v zvezi z delovanjem infrastrukture ponudnika storitev zaupanja.

3.18 Sankcije

Sankcije v primeru nepooblaščenega ali malomarnega izvajanja nalog se za pooblaščene osebe ponudnika storitev zaupanja izvajajo skladno z veljavnimi predpisi in internim pravilnikom o odgovornosti delavcev za kršitve pogodbenih in drugih obveznosti iz delovnega razmerja.

3.19 Zahteve za zunanje izvajalce

Za morebitne zunanje izvajalce veljajo enake zahteve kot za pooblaščene osebe ponudnika storitev zaupanja.

3.20 Dostop osebja do dokumentacije

Pooblaščenim osebam ponudnika storitev zaupanja je na voljo vsa potrebna dokumentacija skladno z njihovimi zadolžitvami in nalogam

4. Varnostni pregledi sistema

4.1 Vrste dnevnikov

(1) Ponudnik storitev zaupanja redno preverja in evidentira vse, kar pomembno vpliva na:

- varnost infrastrukture,
- nemoteno delovanje vseh varnostnih sistemov in
- ali je v vmesnem času prišlo do vdora ali poskusa vdora nepooblaščenih oseb do opreme ali podatkov.

(2) Podrobni podatki o tem so določeni z akti na področju informacijske varnosti.

4.2 Pogostost pregledov dnevnikov

Ponudnik storitev zaupanja dnevno opravlja varnostne preglede svoje infrastrukture.

4.3 Čas hrambe dnevnikov

Najpomembnejši dnevniki se hranijo trajno, vsi ostali pa 6 let od nastanka zapisa.

4.4 Varnostne kopije dnevnikov

Varnostne kopije dnevnikov se izvajajo dnevno.

4.5 Zbiranje podatkov za dnevnike

Podatki se zbirajo bodisi avtomatsko ali pa ročno, odvisno od vrste podatkov.

4.6 Ocena ranljivosti sistema

(1) Analiza dnevnikov in nadzor nad izvajanjem vseh postopkov se izvaja redno s strani pooblaščenih oseb ponudnika storitev zaupanja ali pa samodejno z drugimi varnostnimi mehanizmi na vseh infromacijsko-komunikacijskih napravah ponudnika storitev zaupanja.

(2) Ocena ranljivosti se izvaja na podlagi analize dnevnikov, varnostnih dogodkov in drugih pomembnih podatkov.

5. Dolgoročna hramba podatkov

5.1 Vrste dolgoročno hranjenih podatkov

Ponudnik storitev zaupanja v skladu z določili veljavnih predpisov hrani naslednje gradivo:

- dnevnike,

- zapisnike,
- politike delovanja oz. druge akte s področja informacijske varnosti,
- objave in obvestila ponudnika storitev zaupanja ter
- druge dokumente v skladu z veljavnimi predpisi.

5.2 Rok hrambe

Najpomembnejši podatki se hranijo trajno, vsi ostali pa 6 let od nastanka zapisa.

5.3 Zaščita dolgoročno hranjenih podatkov

(1) Dolgoročno hranjeni podatki so varno shranjeni.

(2) Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v aktih na področju informacijske varnosti.

5.4 Varnostna kopija dolgoročno hranjenih podatkov

(1) Kopija dolgoročno hranjenih podatkov se varno hrani.

(2) Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v aktih na področju informacijske varnosti.

5.5 Zahteva po časovnem žigosanju

Podatki se časovno žigosajo enkrat letno.

5.6 Način zbiranja podatkov

(1) Podatki se zbirajo na način, skladen z vrsto dokumenta.

(2) Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v aktih na področju informacijske varnosti.

5.7 Postopek za dostop do dolgoročno hranjenih podatkov in njihova verifikacija

(1) Dostop do dolgoročno hranjenih podatkov je možen samo pooblaščenim osebam.

(2) Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v aktih na področju informacijske varnosti.

5.8 Postopek v primeru vdorov in zlorabe

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v aktih na področju informacijske varnosti.

5.9 Postopek v primeru okvare programske opreme, podatkov

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v aktih na področju informacijske varnosti.

6. Okrevalni načrt

Zagotovljena je podvojenost kritičnih sistemov in shranjevanje podatkov na geografsko oddaljenih lokacijah. Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v aktih na področju informacijske varnosti.

7. Prenehanje delovanja ponudnika storitev zaupanja

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v aktih na področju informacijske varnosti.

8. Varnostne zahteve za informacijsko-komunikacijsko opremo ponudnika storitev zaupanja

8.1 Specifične tehnične varnostne zahteve

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v aktih na področju informacijske varnosti.

8.2 Nivo varnostne zaščite

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v aktih na področju informacijske varnosti.

8.3 Nadzor razvoja sistema

Družba uporablja programsko opremo priznanih in svetovno uveljavljenih proizvajalcev oziroma vodilnih podjetij ter lastno razvito programsko opremo.

8.4 Upravljanje varnosti

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v aktih na področju informacijske varnosti.

8.5 Varnostna kontrola omrežja

Podrobnejša ureditev je v skladu z veljavnimi predpisi, standardi in priporočili določena v aktih na področju informacijske varnosti.

9. NADZOR

9.1 Splošno

(1) Pri ponudniku storitev zaupanja deluje pooblaščenec za notranji nadzor, ki je strokovnjak z ustreznimi tehnološkimi in pravnimi znanji ter ki ne opravlja operativnih nalog v zvezi s storitvami zaupanja.

(2) Pooblaščenec za notranji nadzor nadzoruje delo družbe na področju izvajanja storitev zaupanja. Organizacijska skupina v primeru odkritih pomanjkljivosti odredi ustrezne ukrepe za odpravo teh pomanjkljivosti, ki jih je družba dolžna izvesti, ter nadzoruje izvedbo odrejenih ukrepov.

9.2 Pogostnost nadzora

Pooblaščenec za notranji nadzor in usklajenost opravi nadzor najmanj enkrat letno.

9.3 Področja nadzora

Področja nadzora so določena v aktih na področju informacijske varnosti.

9.4 Ukrepi ponudnika storitev zaupanja

V primeru ugotovljenih pomanjkljivosti ali napak Pooblaščenec za notranji nadzor odredi ustrezne ukrepe za odpravo teh pomanjkljivosti, ki jih je družba dolžna izvesti, ter nadzoruje izvedbo odrejenih ukrepov. Podrobno je izvajanje ukrepov določeno v aktih na področju informacijske varnosti.

9.10 Objava rezultatov nadzora

Rezultati izvedbe nadzorov se hranijo pri ponudniku storitev zaupanja.

10.. FINANČNE IN OSTALE PRAVNE ZADEVE

10.1 Cenik

Družba določi cenik uporabe svojih storitev, potrebne opreme in infrastrukture ter cenik objavi na spletnih straneh storitve.

11. Finančna odgovornost

Družba z lastnimi sredstvi prevzema odgovornost za kritje škod iz naslova finančne odgovornosti.

12. Varovanje poslovnih in osebnih podatkov

12.1 Splošno

(1) Družba ravna zaupno z:

- z vsemi podatki o delovnem in poslovnem procesu naročnikov in njihovih poslovnih partnerjev, ki so nujno potrebni za opravljanje storitev zaupanja;

- z vsemi zaupnimi podatki, ob tem, da se kot »zaupni podatki« štejejo vsi podatki (ne glede na dejstvo, ali so kot zaupni tudi označeni) komercialne, finančne in tehnične narave ter vsi drugi podatki, ki pri naročniku veljajo kot zaupni ali jih je šteti kot zaupne ter so pripravljeni in posredovani v kakršnikoli obliki (otipljivi ali neotipljivi), vključno s programsko opremo, analizami, preglednicami, podatki, študijami in drugimi dokumenti, ali ustno posredovani;

Kot zaupni podatki iz prejšnjega člena se štejejo še posebej podatki v zvezi s/z:

finančnimi obveznostmi, cenami, kupci/strankami, drugimi sopogodbeniki naročnika, zaposlenimi naročnika, ekonomskim in finančnim stanjem naročnika ter njegovimi poslovnimi in razvojnimi usmeritvami, nameni in cilji, ostalimi podatki, za katere je očitno, da bi naročniku lahko nastala škoda, vključno s škodo, ki ni pravno priznana (npr. nevšečnosti, izguba časa ipd.), če bi zanje izvedele tretje nepooblaščene osebe ipd.

(2) Družba seznani svoje zaposlene:

- z dolžnostjo, da morajo pri svojem delu za družbo ali v zvezi z njim interesom družbe dati prednost pred lastnimi interesi ter da se morajo po svojih najboljših močeh izogibati temu, da bi naročnikom povzročali škodo;
- z določbami Zakona o varstvu osebnih podatkov, drugo slovensko in evropsko zakonodajo na področju varstva osebnih podatkov ter z ukrepi in postopki za zavarovanje osebnih podatkov, ki so v veljavi pri družbi;
- da morajo vse podatke in informacije, ki so opredeljeni kot poslovna skrivnost, skrbno varovati in jih brez izrecnega dovoljenja družbe ne smejo posredovati, razkriti, seznaniti ali omogočiti seznanitve z njimi tretjim osebam, pri čemer so tretje osebe v smislu te točke tudi drugi zaposleni pri družbi, kupci, stranke in drugi pogodbeni sodelavci, razen v obsegu, ki je nujno potreben za izpolnjevanje pogodbenih obveznosti;
- da so dolžni osebne podatke, ne glede na to, na katerega posameznika se nanašajo, ter ne glede na njihovo obliko in lokacijo, skrbno varovati in po svojih najboljših močeh skrbeti za to, da ne pride do namernega ali naključnega neupravičenega uničenja, izbrisa, posredovanja tretjim osebam ali druge obdelave teh podatkov;
- da je obdelava osebnih podatkov (zbiranje, hramba, spreminjanje, posredovanje, izbris in sploh kakršnokoli obdelovanje v zvezi z njimi) dovoljena le v primeru, ko za obdelavo obstaja zakonita podlaga v skladu z zakonodajo, ki ureja varstvo osebnih podatkov ter da je vsaka drugačna obdelava nezakonita;
- da je nepooblaščeno razkritje zaupnih podatkov podlaga za prenehanje poslovnega sodelovanja;
- da izdaja in neupravičena pridobitev poslovne skrivnosti predstavlja kaznivo dejanje;
- da zloraba osebnih podatkov predstavlja kaznivo dejanje.

12.2 Odgovornost glede varovanja

(1) Družba ne prevzema nobene odgovornosti za vsebino podatkov, ki jih naročnik elektronsko šifrira, podpisuje ali dostavlja in sicer tudi v primeru, da je naročnik spoštoval vse veljavne predpise, vsa določila tega pravilnika in drugih pravil družbe oziroma upošteval vsa njegova navodila.

(2) Družba ne prevzema nobene odgovornosti za posledice, ki nastanejo, ker naročnik ni ravnal v skladu z varnostnimi zahtevami iz tega pravilnika.

12.3 Posredovanje podatkov

(1) Družba ne posreduje drugih podatkov o naročnikih, ki niso navedeni v splošnih pogojih ali tem pravilniku, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih storitev ter je družbo naročnik pooblastil za to ali na zahtevo pristojnega sodišča, prekrškovnega ali upravnega organa.

(2) Podatki se posredujejo tudi brez pisne privolitve, če to določa zakonodaja oz. veljavni predpisi.

13. Obveznosti in odgovornosti

13.1 Obveznosti in odgovornosti ponudnika storitev zaupanja

(1) Ponudnik storitev zaupanja je dolžan:

- delovati v skladu s svojimi internimi akti in ostalimi veljavnimi predpisi in zakonodajo,
- delovati v skladu z mednarodnimi priporočili,
- objavljati vse pomembne dokumente, ki določajo njegovo delovanje;
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti ponudnika storitev zaupanja, ki kakorkoli vplivajo na naročnika,
- spoštovati določila glede varnega ravnanja z osebnimi, poslovnimi in zaupnimi podatki v zvezi z naročnikom.

(2) Ponudnik storitev zaupanja je dolžan:

- zagotoviti primerno fizično varnost prostorov in dostopov do samih prostorov ponudnika storitev zaupanja;
- kot dober gospodar skrbeti za nemoteno delovanje in čim večjo razpoložljivost storitve,
- kot dober gospodar skrbeti za čim večjo dostopnost storitev,

- kot dober gospodar skrbeti za nemoteno delovanje vseh ostalih spremljajočih storitev,
- poskušati odpraviti nastale probleme po najboljših močeh in v najkrajšem času,
- skrbeti za optimizacijo strojne in programske opreme in
- obveščati naročnike o pomembnih zadevah ter
- izpolnjevati vse druge zahteve v skladu s tem pravilnikom.

(3) Ponudnik storitev zaupanja zagotavlja čim večjo dostopnost svojih storitev, in sicer vse dni v letu, pri čemer pa se ne upošteva naslednje primere:

- načrtovane in vnaprej napovedane tehnične ali servisne posege na infrastrukturi,
- nenačrtovane tehnične ali servisne posege na infrastrukturi kot posledica nepredvidenih okvar,
- tehnične ali servisne posege zaradi okvare infrastrukture izven pristojnosti ponudnika storitev zaupanja in
- nedostopnost kot posledica višje sile ali izrednih dogodkov.

(4) Vzdrževalna dela ali nadgradnje infrastrukture mora ponudnik storitev zaupanja najaviti vsaj tri (3) dni pred pričetkom del.

(5) Ponudnik storitev zaupanja je odgovoren za vse navedbe v tem dokumentu in za izvajanje vseh določil iz tega pravilnika.

13.2 Obveznosti in odgovornost naročnika

Poslovni subjekt odgovarja za:

- vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba storitev zaupanja s strani nepooblaščenih oseb,
- vsako drugo škodo, ki izvira iz neupoštevanja določil tega pravilnika in drugih obvestil družbe ter veljavnih predpisov.

13.3 Omejitev odgovornosti

Ponudnik storitev zaupanja ni odgovoren za škodo, ki bi nastala zaradi:

- uporabe storitev zaupanja za namen in na način, ki ni izrecno predviden v tem pravilniku,
- nepravilnega ali pomanjkljivega varovanja gesel, izdajanja zaupnih podatkov in neodgovornega ravnanja naročnika,
- zlorabe oz. vdora v informacijski sistem naročnika,
- nedelovanja ali slabega delovanja informacijske infrastrukture naročnika ali tretjih oseb,
- ravnanja naročnika v nasprotju z obvestili družbe, tem pravilnikom in drugimi predpisi,
- izpada infrastrukture, ki ni v domeni upravljanja ponudnika storitev zaupanja,
- ravnanja naročnikov pri uporabi storitve, in sicer tudi v primeru, če je naročnik spoštoval vsa določila tega pravilnika, obvestila družbe ali druge veljavne predpise,
- uporabe in zanesljivosti delovanja strojne in programske opreme naročnikov.

13.4 Poravnava škode

Za škodo odgovarja stranka, ki je le-to povzročila zaradi neupoštevanja določil iz tega pravilnika in veljavne zakonodaje.

14. Spremembe in dopolnitve

14.1 Postopek za sprejem sprememb in dopolnitev

(1) Spremembe ali dopolnitve tega pravilnika lahko družba objavi v obliki sprememb in dopolnitev tega pravilnika.

(2) Vsak predlog sprememb in dopolnitev je pred potrditvijo direktorja družbe z namenom zagotavljanja zakonitosti, varnosti in kakovosti podvržen tako tehnološkemu kot tudi pravnemu pregledu

(3) Ponudnik storitev zaupanja določi pričetek in konec veljavnosti sprememb in dopolnitev.

(4) Spremembe in dopolnitve se objavijo na www.vep.si.

(5) V primeru, da se spremenijo zakonske določbe ali določbe drugih predpisov, na podlagi katerih je sprejet ta pravilnik, se do uskladitve pravilnika upoštevajo ustrezne spremembe.

(6) Ponudnik storitve zaupanja o vsaki spremembi pri zagotavljanju svojih kvalificiranih storitev zaupanja ter o nameri o prenehanju opravljanja teh dejavnosti obvesti nadzorni organ v roku 45 dni.

14.2 Postopek v primeru sporov

(1) Vse pritožbe naročnikov rešuje interna služba pomoč in podpora naročnikom.

(2) Morebitne spore med družbo in naročnikom rešuje stvarno pristojno sodišče v Ljubljani.

14.3 Veljavna zakonodaja

Za odločanje o vseh spornih in drugih pravnih vprašanjih glede izvajanja storitve ali pogodbenih razmerij z naročniki se uporablja pravo Republike Slovenije.

14.4 Skladnost z veljavno zakonodajo

(1) Nadzor nad skladnostjo delovanja ponudnika storitev zaupanja z veljavno zakonodajo in predpisi izvaja Ministrstvo za javno upravo ter občasno (najmanj vsaki dve leti) izbrani organ za presojo skladnosti.

(2) Notranje preverjanje skladnosti delovanja izvajajo pooblaščene osebe v okviru ponudnika storitev zaupanja.

15. Začetek veljavnosti

(1) Ta pravilnik je sprejet z dnem, ko ga podpiše direktor družbe, uporabljati pa se začne v roku 3 dni po seznanitvi delavcev z aktom..

(2) Ob nastopu dela se mora vsak delavec seznaniti z vsebino tega pravilnika in podpisati izjavo, da je s tem seznanjen. Pisna izjava se hrani v delavčevi personalni mapi. Te izjave podpisujejo tudi vsi zunanji sodelavci (dijaki in študenti, podjemniki in drugi).

V Ljubljani, 27.5.2020 Pavel Reberc, direktor