PRAVILNIK O IZVAJANJU KVALIFICIRANE STORITVE ZAUPANJA KVALIFICIRANE STORITVE ZAUPANJA ELEKTRONSKE PRIPOROČENE DOSTAVE

Oznaka dok.:	0613/2/6
Veljavnost od:	10. junij 2021
Verzija:	6
Datum verzije:	10.6.2021
Avtor:	Pavel Reberc
Stopnja zaupnosti:	Javno
Odgovorna oseba:	Pavel Reberc, direktor

Pregled predhodnih izdaj

Izdaja	Številka dokumenta	Verzija	Datum	Opis spremembe	Spremembe pripravil	Spremembe odobril
1	0613/2/1	V1	12.4.2017	Začetna izdaja	Ana Kalan	Pavel Reberc
2.	0613/2/2	V2	19.6.2017	Popravek pravopisnih napak	Ana Kalan	Pavel Reberc
3.	0613/2/3	V3	30.6.2017	Popravek pravopisnih napak	Pavel Reberc	Pavel Reberc
4.	0613/2/4	V4	24.5.2019	Novi standardi	Pavel Reberc	Pavel Reberc
5.	0613/2/5	V5	27.5.2020	Dodana stran ”Pregled predhodnih izdaj”	Marija Stojanović-Grujić	Pavel Reberc
6.	0613/2/6	V6	10.6.2021	Dopolnitev glede splošnih zahtev	Pavel Reberc	Pavel Reberc

JAVNI DEL NOTRANJIH PRAVIL EIUS D.O.O.

POLITIKA O IZVAJANJU KVALIFICIRANE STORITVE ZAUPANJA KVALIFICIRANE STORITVE ZAUPANJA ELEKTRONSKE PRIPOROČENE DOSTAVE

Politika za kvalificirano storitev zaupanja elektronske priporočene dostave,

CPOID : 1.3.6.1.4.1.50183.4.1

1. UVOD

1.1 EIUS d.o.o. je ponudnik kvalificiranih storitev zaupanja, ki za izvajanje svojih storitev zaupanja elektronske priporočene dostave, kvalificiranega elektronskega podpisovanja, kvalificiranega elektronskega žigosanja, kvalificiranega 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), ETSI EN 319 522-1 V1.1.1 (2018-09) , ETSI EN 319 522-2 V1.1.1 (2018-09), ETSI EN 319 521 V1.1.1 (2019-02) .

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 elektronske priporočene dostave, ki omogoča prenos dokumentov z elektronskimi sredstvi, zagotavlja dokaze o ravnanju s prenesenimi podatki, vključno z dokazilom o oddaji in prejemu podatkov, ter prenesene podatke varuje pred izgubo, krajo, poškodbo ali kakršno koli nepooblaščeno spremembo.

Storitev družbe izpolnjuje naslednje zahteve:

a) zagotavlja jo eden ali več ponudnikov kvalificiranih storitev zaupanja;
b) z visoko stopnjo zaupanja zagotavlja identifikacijo pošiljatelja;
c) zagotavlja identifikacijo naslovnika pred dostavo podatkov;
d) oddaja in prejem podatkov je zavarovana z kvalificiranim elektronskim podpisom ali kvalificiranim elektronskim žigom ponudnika kvalificiranih storitev zaupanja, tako da je izključena možnost spremembe podatkov, ne da bi bila ta sprememba zaznana;
e) vsaka sprememba podatkov, potrebna za pošiljanje ali prejem podatkov, se jasno sporoči pošiljatelju in naslovniku podatkov;

f) s kvalificiranim elektronskim časovnim žigom se navedeta datum in čas oddaje, prejema in vseh sprememb podatkov.

2. OPIS KVALIFICIRANE STORITVE ZAUPANJA

a) Naročniki

Naročniki so pravne osebe in fizične osebe, ki uporabljajo storitve zaupanja elektronske priporočene dostave (e-dostave) v vlogi pošiljatelja ali prejemnika, ter uporabniki z e-dostavo povezanih storitev ustvarjanja in preverjanje kvalificiranih elektronskih podpisov ter ustvarjanja in preverjanja kvalificiranih elektronskih časovnih žigov.

b) Tretje osebe

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

c) Namen uporabe in nedovoljena uporaba

(1) E-dostava se lahko uporablja v postopkih kot so npr. sodni, upravni, delovnopravni, arbitražni in drugi postopki oziroma drugih pogodbenih ali nepogodbenih komunikacijah.

(2) Prepovedano je izvajanje 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 storitve zaupanja obrnejo na pooblaščene osebe ponudnika storitev zaupanja, ki so dosegljive na spodnjem naslovu in spodaj navedenih telefonskih številkah:

Pavel Reberc, Eius d.o.o., Grudnovo nabrežje 15, 1000 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 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: splošni pogoji, uporabniška navodila, cenik, obvestila, in sicer na spletni strani ponudnika družbe.

2.1 Elektronska priporočena dostava

Definicije:
Varen elektronski predal – je uporabnikov naslov za (kvalificirano) storitev zaupanja elektronske priporočene dostave, ki ima obliko naslov@domena, naslov je omejen na 64 znakov, domena pa je iz nabora podprtih domen (vep.si, vepmail.com). (glej referenčni standard RFC5322 – sekcija 3.2.3 in 3.4.1) .
Dostop do vsebine varnega elektronskega predala je zaščiten. Za dostop je potrebna avtentikacija s kvalificiranim potrdilom za elektronski podpis, dodatno pa tudi z geslom (za namene administracije).

Varen elektronski predal omogoča varno, zanesljivo in pravno veljavno izmenjavo elektronskih dokumentov, uporablja se v sodnih postopkih, upravnih postopkih, ter povsod tam kjer se zahteva višja stopnja varnosti – zanesljivost, zaupnost in identifikacija udeležencev.

Nosilec predala – je oseba povezana s kvalificiranim potrdilom za elektronski podpis, potrdilo pa je bilo uporabljeno za registracijo varnega elektronskega predala. Nosilec predala ima možnost spreminjanja nastavitev in pooblaščanja dodatnih oseb za dostop do varnega elektronskega predala.

Oseba zaupanja – je imetnik kvalificiranega potrdila za elektronski podpis, ki ni nosilec predala (tisti, ki je predal registriral) a ima pravico dostopa v posamezen varen elektronski predal. V primeru, da ima nosilec predala več kvalificiranih potrdil za elektronski podpis, se dodatna potrdila štejejo kot potrdila osebe zaupanja. S potrdilom osebe zaupanja je možno prejemat in pošiljat pošiljke, ni pa možno spreminjati nastavitev varnega elektronskega predala.

Opis:
Storitve zaupanja elektronske priporočene dostave omogoča prenos podatkov med uporabniki z elektronskimi sredstvi, zagotavlja dokaze o ravnanju s prenesenimi podatki, vključno z dokazilom o oddaji in prejemu podatkov, ter prenesene podatke varuje pred izgubo, krajo, poškodbo ali kakršno koli nepooblaščeno spremembo, ter izpolnjuje zahteve za kvalificirano storitev zaupanja elektronske priporočene dostave po uredbi EIDAS[1].

Podatkom, poslanim in prejetim s storitvijo zaupanja elektronske priporočene dostave, se ne odvzameta pravni učinek in dopustnost kot dokaz v pravnih postopkih le zato, ker so v elektronski obliki ali ne izpolnjujejo zahtev za kvalificirano storitev zaupanja elektronske priporočene dostave.

1 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 zvezi s podatki, poslanimi in prejetimi s kvalificirano storitvijo zaupanja elektronske priporočene dostave, se domneva, da so podatki celoviti, da jih je poslal njihov pošiljatelj in prejel njihov naslovnik, katerih identiteta je ugotovljena, ter da so točni glede datuma in časa oddaje in prejema podatkov, navedenih v okviru kvalificirane storitve zaupanja elektronske priporočene dostave.

Storitev se uporablja pri elektronskemu vročanju dokumentov v civilnih sodnih postopkih, v upravnih postopkih in povsod tam, kjer se zahteva visoka stopnja zanesljivosti, varnosti in veljavnosti za dostavo dokumentov po elektronski poti.

Storitev zaupanja elektronske priporočene dostave izpolnjuje naslednje zahteve:

- zagotavlja jo ponudnik kvalificiranih storitev zaupanja (EIUS d.o.o.);
- z visoko stopnjo zaupanja zagotavljaja identifikacijo pošiljatelja (Z uporabo kvalificiranih elektronskih potrdil za elektronski podpis in dodatno možnostjo uporabe gesel);
- zagotavljajo identifikacijo naslovnika pred dostavo podatkov (imenik uporabnikov sistema VEP, avtentikacija in avtorizacija z uporabo kvalificiranega elektronskega potrdila za elektronski podpis);
- oddaja in prejem podatkov je zavarovana s kvalificiranim elektronskim podpisom ponudnika kvalificiranih storitev zaupanja tako, da je izključena možnost spremembe podatkov, ne da bi bila ta sprememba zaznana;
- vsaka sprememba podatkov, potrebna za pošiljanje ali prejem podatkov, se jasno sporoči pošiljatelju in naslovniku podatkov;
- s kvalificiranim elektronskim časovnim žigom se navedeta datum in čas oddaje, prejema in vseh sprememb podatkov;

Sistem omogoča pošiljanje sporočil in priponk - dokumentov. Od običajne elektronske pošte se sistem razlikuje po tem, da se mora uporabnik za uporabo sistema predhodno registrirati, ob prijavi se legitimira z kvalificiranim elektronskim potrdilom za elektronski podpis.
Poslane pošiljke se lahko dodatno časovno žigosajo, kar zagotavlja enolično identifikacijo časa pošiljanja.

V postopku vročanja prejemnik sporočila podpiše elektronsko vročilnico s svojim kvalificiranim potrdilom za elektronski podpis, šele nato ima dostop do vsebine pošiljke. Elektronsko podpisana vročilnica se vrne nazaj pošiljatelju in služi kot dokaz o vročitvi.

Registracija uporabnika

Za uporabo varnega elektronskega predala se morajo uporabniki predhodno registrirati in podpisati pogodbo o sklenitvi naročniškega razmerja. Uporabniku se dodeli naslov varnega elektronskega predala (ki ga poljubno izbere sam), registrira se kvalificirano potrdilo, ki ga bo uporabljal pri svojem delu in se poveže z naslovom. Uporabnik se registrira tako, da se prijavi na spletno stran »VEP«, izkaže svojo identiteto s kvalificiranim potrdilom za elektronski podpis, izpolni prijavni obrazec in elektronsko s svojim kvalificirano potrdilom za elektronski podpis podpiše pogodbo za uporabo varnega elektronskega predala.

Ob registraciji uporabnik določi tudi geslo za administracijo predala, ki mora biti dolgo vsaj 6 znakov, vsebovati pa mora velike in male črke ter številke ali interpunkcijo. Geslo se hrani v sistemu v kriptirani obliki. V primeru, da se registrira pravna oseba, mora pogodbo podpisat zakoniti zastopnik pravne osebe.

V primeru, da oseba vrši registracijo za pravno osebo, se:

- preveri ali dostopa s potrdilom za elektronski podpis zastopnika (z dostopom na poslovni register)
- omogoči možnost dopolnitve pogodbe.

Če sklenitev pogodbe ni mogoča (zaradi zgoraj možnih naštetih razlogov), se opravi registracija po pisni – klasični pošti. Uporabnik prenese vsebino pogodbe v PDF obliki, odpre se predal s statusom »na čakanju«, v katerem ni mogoče prejemat in pošiljat pošte. Predal se aktivira s postopkom aktivacije šele po prejemu pisnega izvoda pogodbe.

Po končanem postopku registracije uporabnik po običajni elektronski pošti prejme obvestilo o uspešnosti odpiranja varnega elektronskega predala, sistem shrani podatke o uporabniku ter javni del ključa uporabnikovega kvalificiranega potrdila za elektronski podpis.

Prijava v sistem

Prijava uporabnika v sistem se izvede z avtentikacijskim postopkom z uporabo kvalificiranega potrdila za elektronski podpis in preverjanjem uporabniškega računa. Sistem VEP preveri potrdilo uporabnika in sicer tako da:

1. Preveri izdajatelja potrdila; izdajatelj potrdila mora biti na seznamu zaupanja vrednih izdajateljev elektronskih potrdil, ki ga vodi Evropska komisija .
2. Pri izdajatelju potrdila preveri veljavnost potrdila glede na politiko preverjanja ki jo je predpisal izdajatelj (preverjanje istovetnosti potrdila, preverjanje veljavnosti po datumu, preverjanje po CRL seznamu), preveri tudi, ali je izdajatelj na seznamu veljavnih izdajateljev (ISSUER, na primer OU=sigen-ca, O=state-institutions, C=si).
3. V sistemu VEP preveri če je uporabnik že registriran (id izdajatelja, id potrdila). Če je uporabnik registriran, se iz podatkov v sistemu samodejno izpolne uporabniško (npr lojze.uporabnik@vep.si) , s klikom na gumb “prijava” je prijava v varni elektronski predal uspešna. Če ima uporabnik odprtih več predalov (na primer je pooblaščenec pri več pravnih osebah), se mu ponudi izborni seznam uporabniških računov za izbor tistega, na katerem želi delati.
4. Če uporabnik še ni registriran, sistem ponudi registracijo uporabnika. Če uporabnik nima kvalificiranega potrdila ga sistem napoti na stran z navodili, kako pridobiti kvalificirano potrdilo.

Prijava – obnova potrdila ali dodatno potrdilo

Kvalificirana potrdila za elektronski podpis imajo omejeno veljavnost, zato je potrebno omogočiti, da uporabnik, ki mu je potrdilo poteklo le-tega zamenja z novim. Prav tako za dostop do varnega elektronskega predala uporabnik lahko uporabi več kvalificiranih potrdil za elektronski podpis – npr. različnih izdajateljev.

Če ob prijavi sistem zazna, da ima uporabnik veljavno digitalno potrdilo za elektronski podpis, vendar to potrdilo še ni dodano med potrdila uporabnikov, mu portal ponudi dve možnosti in sicer:

- Dodajanje osebe zaupanja in

- menjavo certifikata

Dodajanja osebe zaupanja se izvede tako, da uporabnik vnese naslov varnega elektronskega predala, administrator predala pa vpiše geslo za dostop, ki ga je določil ob

registraciji.

Če je uporabniku poteklo kvalificirano potrdilo za varen elektronski podpis in želi dostopati do storitve z novim potrdilom, izbere opcijo menjave potrdila, vnese naslov varnega eklektronskega predala ter geslo, ki ga je določil ob registraciji. Sistem preveri, ali je potrdilo izdano na isto osebo in podatke starega potrdila zamenja z novimi.

Dostava pošiljke - vročanje v varni elektronski predal

Vročanje v varni elektronski predal poteka v naslednjih korakih:
Pošiljatelj sestavi pošiljko neposredno v svojem informacijskem sistemu ali pa z uporabo spletnega portala za sestavljanje pošiljk. Komunikacija poteka po varnem protokolu, ter zagotavljanjem zanesljivega posredovanja sporočil.
Pošiljatelj pošiljko pošlje s klicem storitve za pošiljanje, ki opravi sledeče:

- Klicatelj metode se avtenticira in avtorizira s svojim kvalificiranim potrdilom za elektronski podpis
- Klicatelj posreduje podpisano pošiljko, ki je namenjena za vročanje v predal
- Sistem VEP preveri pošiljko
  - Sintaktična pravilnost: validacija po shemi
  - Vsebinska pravilnost: preverjanje pošiljateljevega časovnega žiga, podpisa
  - Preverjanje obstoja prejemnika
- VEP pošiljatelja obvesti o uspehu pošiljanja tako z vsebino odgovora storitve za pošiljanje kot tudi s sporočilom »potrdilo o prejemu« v pošiljateljev predal, ki je elektronsko podpisano.
- VEP v prejemnikov predal pošlje elektronsko podpisano »Obvestilo naslovniku o prejeti pošiljki«
- VEP prejemnika sporočila po navadni elektronski pošti obvesti o prejemu pošiljke

Proces je grafično prikazan na Sliki 1.

Prejem pošiljke

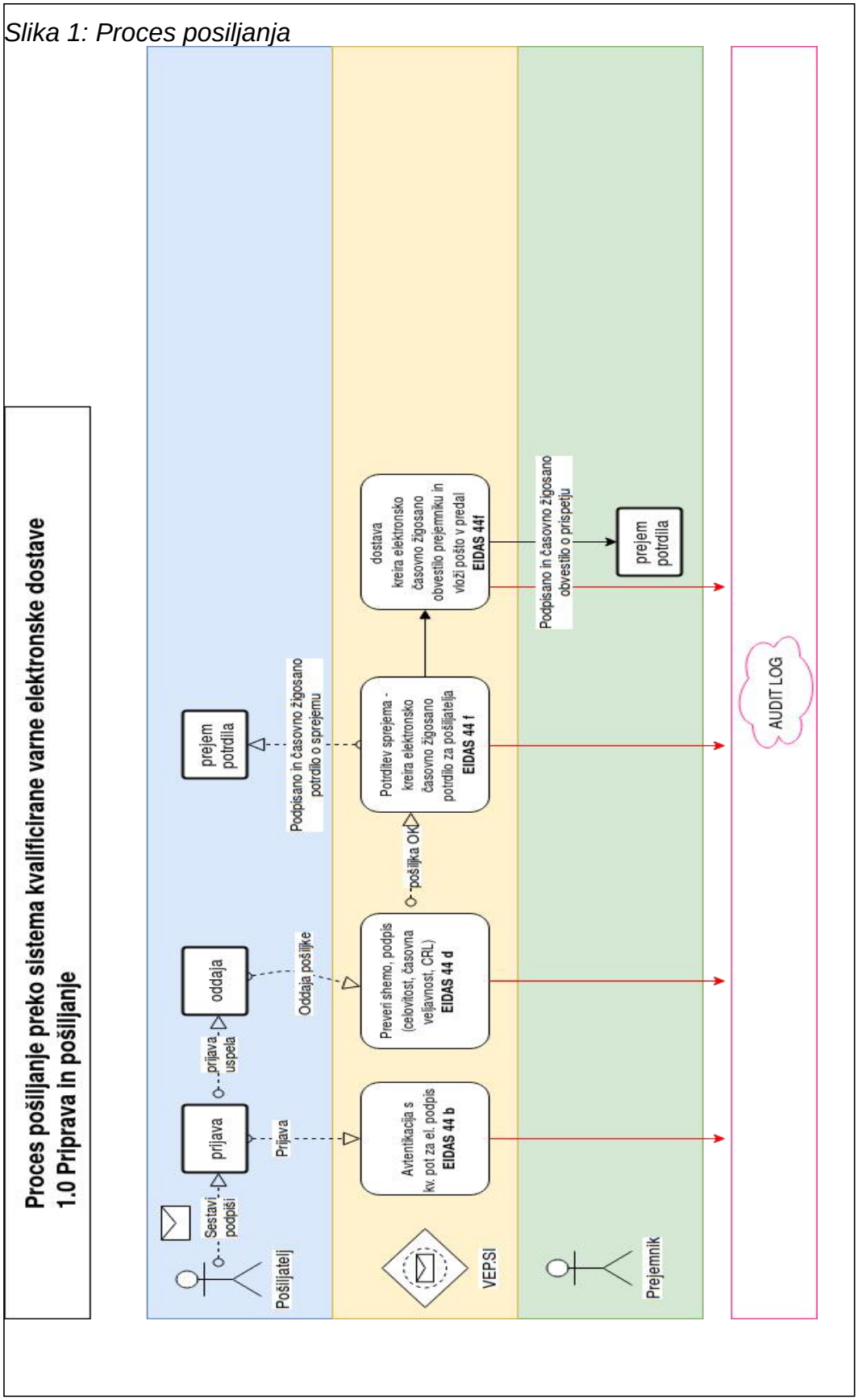
Pošiljke, ki so v uporabnikovem seznamu prejetih pošiljk imajo lahko več statusov. Status pošiljke je lahko „Prejeto“ ali pa „Čaka na prevzem“. Pošiljke s statusom „čaka na prevzem“ uporabnik prevzame na način, ki je odvisen od vrste vročanja. Ob kliku na pošiljko se zgodi sledeče:

- Če je vrsta vročanja „navadno“, se prikaže pošiljka, v podatke o pošiljki se vpiše datum prevzema. Prikaz pošiljke je sestavljen iz podatkov o pošiljki (pošiljatelj, datum pošiljanja, datum prejema, seznama priponk, in vsebina besedila).
- Če vrsta vročanja zahteva potrditev prejema s povratnico – v tem primeru naslovnik v svoj predal prejme obvestilo o pošiljki. Naslovnik bo v pošiljko vpogledal šele takrat, ko bo potrdil prevzem s podpisom (podpisovanje s svojim kvalificiranim potrdilom) vročilnice. Vsebina vročilnice je odvisna od vrste vročitve. Ko uporabnik elektronsko podpiše vročilnico, sistem VEP v njegov predal dostavi vsebino pošiljke s statusom »prejeto«, podpisano vročilnico pa dostavi v pošiljateljev predal.

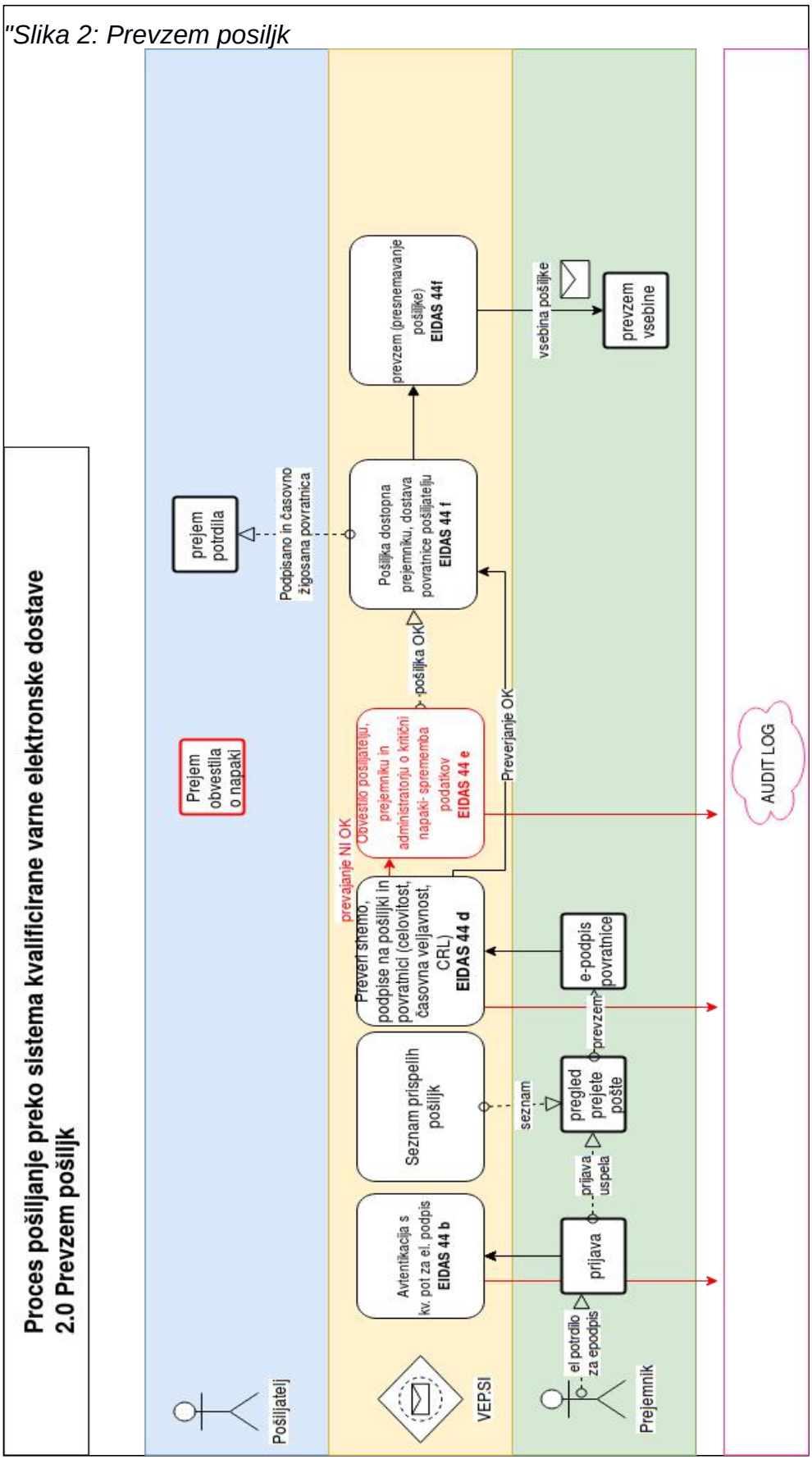
Ne glede na vrsto pošiljanja **sistem vedno preveri veljavnost** elektronskih podpisov, s katerimi so pošiljke podpisane.

Proces je grafično prikazan na Sliki 2.

Slika 1: Proces posiljanja



"Slika 2: Prevzem posiljk



Interaktivno sestavljanje pošiljke

Sestavljanje pošiljke za vročanje v predpisanem formatu je običajno avtomatizirano opravilo informacijskih sistemov pošiljateljev, ki vročajo dokumente v varne elektronske predale z uporabo strojnega (g2b ali b2b) vmesnika.
V primeru, ko je treba pošiljke sestaviti »ročno«, se uporabi interaktivni vmesnik za sestavljanje varnih elektronskih pošiljk.

Pogoj za sestavljanje pošiljke je uspešna prijava v sistem in veljaven uporabniški račun.

Funkcionalnosti vmesnika za sestavljanje pošiljk:

- Priprava sporočila (besedilna)
- Dodajanje atributov
  - Pošiljatelj sporočila (samodejno) From
  - Prejemnik sporočila To
  - Določitev zadeve Subject
  - Določitev vrste vročitve DeliveryType
  - Določitev identifikatorja dokumenta (SenderDocumentId)
  - Pripenjanje prilog ali ali strukturiranih vsebin z določitvijo tipa vsebine (MIME)
  - Časovno žigosanje
  - Elektronsko podpisovanje
- Vizualizacija pošiljke

Sporočilo pred postopkom priprave samodejno dobi identifikator sporočila MessageId in druge atribute, ki jim je mogoče samodejno nastaviti začetno vrednost.

Priprava pošiljke za vročanje (B2B)

Pošiljatelj sestavi pošiljko neposredno v svojem informacijskem sistemu, z uporabo namenskega programa VEP.SI, z uporabo spletnega portala za sestavljanje pošiljk, ali B2B integracije in klica ustrezne metode. Pošiljka (sporočilo za dostavo) je sestavljena iz vsebine in prilog, ki jih je lahko več. Vsebina pošiljke in priloge so lahko strukturirano besedilo ali druge binarno kodirane vsebine. Sestavljena pošiljka mora imeti predpisano obliko (validacija po XML shemi), da jo varni elektronski predal sprejme. Pošiljka se po sestavljanju elektronsko podpiše s kvalificiranim potrdilom za elektronski podpis enega od priznanih izdajateljev potrdil, s kvalificirano potrdilo za elektronski podpis ponudnika EIUS d.o.o. in opcijsko časovno žigosa.

Pošiljanje e-računov

Uporabniki portala VEP.si lahko preko sistema pošiljajo elektronske račune, ustvarjene v svojih računovodskih programih ali pa neposredno preko spletnega vmesnika vep.si.

Računi so lahko v obliki e-Slog verzije 1.6 ali več, in morajo biti elektronsko podpisani. Uporabnik spremlja status poslanega računa s preklopom na način »eračuni«, možni statusi pa so »v pošiljanju«, »poslano« ali »napaka«. V primeru napake uporabnik lahko ročno sproži ponovno pošiljanje.

pošiljanje elektronske pošiljke

Pošiljanje že oblikovane elektronske pošiljke poteka tako, da se:

- Uporabnika obvesti o ceni storitve
- Preveri oblike pošiljke po XML shemi
- Preverjanje časovnega žiga in elektronskega podpisa

- Preverjanje prejemnika: sistem preveri, če prejemnik obstaja;
- Opcijsko kriptiranje »End-to-end«, da se pošiljka šifrira z javnim ključem prejemnika

Elektronsko podpisovanje

Pošiljke poslane preko sistema VEP se elektronsko podpišejo (žigosajo) s kvalificiranim potrdilom za elektronski podpis ponudnika skladno z zahtevami iz uredbe EIDAS. Sistem omogoča tudi podpisovanje prilog v PDF.

Preverjanje identitete

Preverjanje identitete se izvede s potrdilom za kvalificiran elektronski podpisa po uredbi EIDAS. Če je lastnik kvalificiranega potrdila za elektronski podpis registriran uporabnik VEP, ali ima pooblastilo za dostop, se mu omogoči dostop do VEP.si.

Sporočanje sprememb

Sistem prejemnika in pošiljatelja obvešča o spremembah v pošiljki (REQ-ERDS-4.1.1-06). Spremembe pošiljke lahko izvirajo iz tehničnih razlogov (npr. pretvorba formatov zapisa), napake, ali nepooblaščenega posega tretjih oseb. V vsakem primeru sistem o spremembi obvesti pošiljatelja, prejemnika in sistemskega administratorja po elektronski pošti. Preverjanje, ali je prišlo do spremembe se izvede tako, da se s storitvijo preverjanja elektronskih podpisov in žigov preveri elektronski podpis spooročila.

Dokazila o opravljenih storitvah

Sistem zagotavlja dokazila o opravljenih storitvah v odvisnosti od lastnosti posamezne vrste dostave kot sledi:[2]

Storitev	Rok za dostavo	Potrdilo prejema	Obvestilo prejemniku o prispetju	Neznan prejemnik	Vročilnica	Vročilnica fikcija	Drugo obvestilo o prispetju	Vročilnica fikcija po ZPP 141/6	Obvestilo o fikciji po ZPP 141/6	
(ZPP3 navadno)	0		X	X						
(AR)	15	X	X	X	X	X				
(R)	0		X							
(ZUP)	15	X	X	X	X	X	X			
(ZSReg)	15	X	X	X	X	X				
(ZPP2 osebno)	15	X	X	X	X	X			X	X
(ARA)	15	X	X	X	X	X				

Dokazilo o posameznem dogodku se izdela v obliki elektronsko podpisanega dokumenta, ki ga uporabnik prejme v svoj varen elektronski predal. Dokazila so elektronsko podpisana in časovno žigosana. [3] Dokazila se hranijo skladno s politiko o upravljanju s komunikacijami. V primeru da uporabnik izbriše svoj izvod dokazila, ponudnik za izdajo novega lahko zaračuna nadomestilo. [4]

2 ETSI EN 319 521 V1.1.1, REQ-ERDS-4.1.1-10
3 ETSI EN 319 521 V1.1.1, REQ-ERDS-4.1.1-11 .
4 ETSI EN 319 521 V1.1.1, REQ-ERDS-4.1.1-12

3. SPLOŠNE ZAHTEVE GLEDE PRIPOROČENE ELEKTRONSKE DOSTAVE

3.1 Zaščita pred spremembo vsebine

Sistem vsa poslana sporočila na vhodu opremi z elektronskim žigom temelječim na kvalificiranem potrdilu za elektronski žig ponudnika ter kvalificiranim elektronskim časovnim žigom. V primeru, da sistem v kateremkoli trenutku zazna, da je prišlo do spremembe vsebine, se samodejno pošlje obvestilo o napaki z vsemi relevantnimi podatki pošiljatelju, prejemniku ter skrbniku sistema.

3.2 Identifikacija pošiljatelja in prejemnika

Identifikacija pošiljatelja se izvede na podlagi identifikacijskega sredstva oziroma elektronske identitete z visoko stopnjo zaupanja po uredbi eIDAS (*high*) . Uporabijo se lahko kvalificirana potrdila za e-podpis ponudnikov uvrščenih na varen seznam ali identiteta z visoko stopnjo zaupanja. visoko stopnjo.
Identifikacija prejemnika se izvede na podlagi identifikacijskega sredstva oziroma elektronske identitete s srednjo stopnjo zaupanja po uredbi eIDAS (*substantial*) . Uporabijo se lahko potrdila za e-podpis ponudnikov uvrščenih na varen seznam ali identiteta s srednjo stopnjo zaupanja ali enakovredna dvostopenjska avtentikacija.

3.2 Dokazi o opravljenih transakcijah

Pošiljatelj o poslani pošiljki in poteku dostave prejme dokaze (potrdila), ki so elektronsko podpisan s strani ponudnika kot tudi prejemnika. Samodejno prejemanje potrdil je odvisno od izbrane storitve. V primeru da uporabnik želi dodatna potrdila iz dnevniških zapisov, jih lahko pridobi na zahtevo in proti plačilu od ponudnika ob predložitvi informacij pomembnih za njihovo iskanje (id pošiljke, čas oddaje, naslovnik..).

Beležijo se dokazi dostopa do varnega predala, oddaje pošiljke, prevzema pošiljke, preverjanja veljavnosti podpisov in žigov, brisanja pošiljk, napake pri dostopu in neuspešni poizkusi dostopa ter napake zaradi spremembe vsebine.

3.3 Časovna razpoložljivost dokazov

Ponudnik samodejne dokaze v obliki potrdil hranil vsaj tri mesece, sezname prejetih in poslanih pošiljk 7 let, medtem ko se nadzorni dnevniški zapisi (AUDIT LOG) hranijo trajno.

3.3 Vključevanje tretjih ponudnikov storitev zaupanja

Ponudnik poleg svojih storitev zaupanja v izvajanje kvalificirane storitve priporočene elektronske dostave vključuje tudi kvalificirane ponudnike:
- Halcom d.d.
- Rekono d.o.o.

4. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE

Uvod

(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.

4.1 Zaščita pred izgubo, krajo, okvaro ali nepooblaščenimi spremembami

(1) Ponudnik izvaja splošne varnostne postopke navedene v nadaljevanju, dodatno pa zagotavlja:

- Ob predaji sporočila prejemniku se ponovno izvede preverjanje celovitosti in veljavnosti elektronskih podpisov
- O vseh dostopih se vodijo dnevniški zapisi, ki se dodatno varujejo proti spremembam
- Vsa prejeta sporočila se hranijo v podatkovni bazi ponudnika, ki ima zagotovljeno replikacijo na oddaljeni lokaciji
- ostop do podatkov je mogoč le pooblaščenim osebam na način, ki zagotavlja sledljivost in onemogoča nepooblaščen vpogled ali spremembe podatkov

4.2 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.

4.3 Lokacija in zgradba ponudnika storitev e-dostave

(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.

4.4 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.

4.5 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.

4.6 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.

4.7 Zaščita pred požari

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

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

4.8 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 e, 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).
Poročanje o incidentih se izvaja skladno z akti družbe.

4.9 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.

4.10 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.

4.11 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	1

		• sprememb in dopolnitev zaradi pravnih, tehnoloških ali organizacijskih sprememb ter 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

4.12 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.

4.13 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.

4.14 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.

4.15 Primernost osebja

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

4.16 Dodatno usposabljanje osebja

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

4.17 Zahteve za redna usposabljanja

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

4.18 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.

4.19 Zahteve za zunanje izvajalce

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

4.20 Dostop osebja do dokumentacije

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

5. Varnostni pregledi sistema

5.1 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.

5.2 Pogostost pregledov dnevnikov

Ponudnik storitev zaupanja dnevno opravlja varnostne preglede svoje infrastrukture.

5.3 Čas hrambe dnevnikov

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

5.4 Varnostne kopije dnevnikov

Varnostne kopije dnevnikov se izvajajo dnevno.

5.5 Zbiranje podatkov za dnevnike

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

5.6 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.

6. Dolgoročna hramba podatkov

6.1 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.

6.2 Rok hrambe

Najpomembnejši podatki se hranijo trajno, vsi ostali pa 7 let od nastanka zapisa.

6.3 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.

6.4 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.

6.5 Zahteva po časovnem žigosanju

Podatki se časovno žigosajo enkrat letno.

6.6 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.

6.7 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.

6.8 Postopek v primeru vdorov in zlorabe

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

6.9 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.

7. 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.

8. Prenehanje delovanja ponudnika storitev zaupanja

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

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

9.1 Specifične tehnične varnostne zahteve

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

9.2 Nivo varnostne zaščite

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

9.3 Nadzor razvoja sistema

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

9.4 Upravljanje varnosti

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

9.5 Varnostna kontrola omrežja

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

10. NADZOR

10.1 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.

10.2 Pogostnost nadzora

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

10.3 Področja nadzora

Področja nadzora so določena v aktih na področju informacijske varnosti.

10.4 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.

10.10 Objava rezultatov nadzora

Rezultati izvedbe nadzorov se hranijo pri ponudniku storitev zaupanja.

11.. FINANČNE IN OSTALE PRAVNE ZADEVE

11.1 Cenik

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

12. Finančna odgovornost

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

13. Varovanje poslovnih in osebnih podatkov

13.1 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.

13.2 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.

13.3 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.

14. Obveznosti in odgovornosti

14.1 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.

14.2 Obveznosti in odgovornost naročnika

Uporabnik storitev - pošiljatelj, prejemnik ali tretja oseba oziroma 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.

14.3 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.

14.4 Poravnava škode

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

15. Spremembe in dopolnitve

15.1 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.

15.2 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.

15.3 Veljavna zakonodaja

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

15.4 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.

16. 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, vendar ne prej kot 10.6.2021.

(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, 10.6.2021 Pavel Reberc, direktor