Certifikatska agencija POŠTA®CA

Politika POŠTA®CA za kvalificirane elektronske časovne žige

Javni del notranjih pravil delovanja

Verzija 2.0

Datum izdaje 28.6.2019

POŠTA SLOVENIJE, d.o.o. | Slomškov trg, 2500 Maribor | info.postarca@posta.si | postarca.posta.si

Zgodovina dokumenta

Verzija	Datum	Opis
1.1	01.07.2017	Uskladitev z ETSI EN 319 421 in ETSI EN 319 401.
2.0	30.06.2019	Enolična imena strežnikov časovnega žiga Sprememba telefonske številke Uredniški in tipografski popravki

Izdaje politike POŠTA ® CA za časovni žig		
Izdaja	**Datum**	**Opis izdaje**
Verzija 1.1	01.07.2017	Politika POŠTA®CA za kvalificiran časovni žig **OID 1.3.6.1.4.1.15284.2.1.1;**
Verzija 2.0	28.06.2019	Politika POŠTA®CA za kvalificirane elektronske časovne žige **OID 1.3.6.1.4.1.15284.2.1.2;**

1 PREDSTAVITEV

1.1 Pregled

V okviru POŠTE SLOVENIJE d.o.o., Maribor (v nadaljevanju: ***organizacija***) deluje ponudnik kvalificiranih storitev zaupanja, Certifikatska agencija Pošte Slovenije, krajše overitelj POŠTA®CA (v nadaljevanju ***overitelj***). Overitelj izdaja različne vrste potrdil in elektronske časovne žige različnim naročnikom (posameznikom, pravnim in fizičnim osebam, registriranim za opravljanje dejavnosti, …) v skladu z *Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1993/93/ES*, *ETSI EN 319 421- Policy and Security Requirements for Trust Service Providers issuing Time-Stamps* ter drugimi akti, navedenimi v poglavju 1.3.1.

Overitelj objavlja:

- politike, ki opisujejo overiteljeva pravila opravljanja storitve kvalificiranega elektronskega časovnega žiga, znane kot javni del notranjih pravil delovanja (ang. TSA Practice Statement – v nadaljevanju: politika).

Politika opisuje tehnične lastnosti in nivo varnosti overiteljeve infrastrukture ter postopke, ki jih overitelj uporablja za upravljanje infrastrukture storitve časovnega žiga. Politika vsebuje vse bistvene določbe, ki vplivajo na odnos med overiteljem in naročniki storitve kvalificiranega elektronskega časovnega žiga ter tretjimi osebami, ki se na časovni žig upravičeno zanašajo.

Oblika politike je harmonizirana z ETSI EN 319 421 in ETSI EN 319 401. Poglavja, ki niso relevantna za delovanje overitelja, so označena s komentarjem *ni predpisano*, ki označuje, da je bilo poglavje izključeno iz dokumenta po tehtni presoji overitelja, oziroma da je vsebinsko zajeto v ostalih poglavjih dokumenta. S tem se ohranja primerljivost z referenčnimi dokumenti ter politikami drugih overiteljev v Republiki Sloveniji in svetu.

Pričujoči dokument opisuje javni del notranjih pravil delovanja overitelj POŠTA®CA za storitev kvalificiranega elektronskega časovnega žiga. Opis pravil delovanja je namenjen vsem, ki potrebujejo informacije za oceno zaupanja v časovne žige, ki jih izdaja overitelj. Za dodatne informacije, ki niso podane v politiki, se lahko zainteresirani obrnejo na kontaktne osebe, navedene v poglavju **Error! Reference source not found.**.

Časovni žigi, ki jih izdaja overitelj POŠTA®CA temeljijo na uporabi kriptografije javnih ključev, digitalnih potrdil, zanesljivega časovnega vira ter naprednega elektronskega žiga ustvarjenega s tehnologijo digitalnega podpisa.

1.1.1 Osnovne definicije

Izraz	Definicija
Digitalni podpis	Je niz podatkov, ki je dodan ali kriptografska transformacija podatkov, ki omogoča prejemniku preveriti pristnost podatkov in identifikacijo podpisnika ter ščiti pred ponarejanjem.
Elektronski žig	Pomeni niz podatkov v elektronski obliki, ki so dodani k drugim podatkom v elektronski obliki ali so z njimi logično povezani, da se zagotovita izvor in celovitost povezanih podatkov.
Napredni elektronski žig	Pomeni elektronski žig, ki izpolnjuje zahteve: a) enolično je povezan z ustvarjalcem žiga; b) z njim je mogoče identificirati ustvarjalca žiga;

	c) ustvari se na podlagi podatkov za ustvarjanje elektronskega žiga, ki jih ustvarjalec žiga z visoko stopnjo zaupanja in pod svojim nadzorom lahko uporablja za ustvarjanje elektronskega žiga, in d) povezan je s podatki, na katere se nanaša, in sicer tako, da je mogoče zaslediti vsako naknadno spremembo teh podatkov.
Informacijski sistem	Je sistem za oblikovanje, pošiljanje, prejemanje, shranjevanje in druge obdelave podatkov v elektronski obliki.
Potrdilo (ali digitalno potrdilo)	Je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa ali elektronskega žiga z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto.
Oprema za elektronsko podpisovanje	Je strojna ali programska oprema ali njuna specifična sestavina, ki jo overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem oz. se uporablja za oblikovanje ali preverjanje elektronskih podpisov.
Overitelj	Je fizična ali pravna oseba, ki izdaja digitalna potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskim podpisovanjem.
Naprava za ustvarjanje elektronskega žiga	Pomeni konfigurirano programsko ali strojno opremo, ki se uporablja za ustvarjanje elektronskega žiga.
Elektronski časovni žig (ali časovni žig)	Pomeni podatke v elektronski obliki, ki druge podatke v elektronski obliki povezujejo z določenim trenutkom in tako zagotavljajo dokaz, da so slednji podatki v tistem trenutku obstajali.
Kvalificirani elektronski časovni žig	Kvalificirani elektronski časovni žig izpolnjuje naslednje zahteve: a) datum in čas povezuje s podatki tako, da je mogoče razumno izključiti možnost spremembe podatkov, ne da bi bila ta sprememba zaznana; b) temelji na točnem časovnem viru, povezanem z univerzalnim koordiniranim časom; c) podpisan je z naprednim elektronskim podpisom ali ožigosan z naprednim elektronskim žigom ponudnika kvalificiranih storitev zaupanja ali z drugo enakovredno metodo.
Žeton časovnega žiga (angl. time-stamp token, TST)	Podatkovni objekt, ki povezuje podatek, ki je bil preoblikovan s kriptografskimi algoritmi, s točnim časom, s čimer je vzpostavljen dokaz, da je podatek obstajal pred tem časom.
Overitelj časovnega žiga (angl. time-stamping authority)	Overitelj, ki opravlja storitev izdajanja žetonov časovnega žiga.
Javni del notranjih pravil delovanja overitelja časovnega žiga	Dokument, ki opisuje overiteljeva pravila opravljanja storitve časovnega žiga.

(angl. TSA practice statement)	
Servis časovnega žiga (angl. TSA system)	Produkti in elementi informacijske tehnologije, ki jih overitelj uporablja za opravljanje storitve časovnega žiga.
Strežnik časovnega žiga (angl. time-stamping unit)	Sklop strojne in programske opreme, ki ima kot samostojna enota v določenem trenutku aktiven le en ključ za podpisovanje žetonov časovnega žiga.
Koordiniran univerzalni čas (angl. Coordinated Universal Time)	Koordiniran univerzalni čas določen v mednarodnem standardu za meritve časa, ITU-R Recommendation TF.460-5.

1.1.2 Okrajšave

Kratica	Pomen
CA	angl. Certification Authority – overitelj digitalnih potrdil
CN	angl. Common Name – X.500 domače ime imetnika digitalnega potrdila
CRL	angl. Certificate Revocation List – lista preklicanih digitalnih potrdil
DN	angl. Distinguished Name- razločevalno ime X.500
EAL	angl. Evaluation Assurance Level – standard označevanja varnostnih nivojev v računalniških sistemih
FIPS	angl. United State Federal Information Processing Standards – oznaka standarda s področja informacijskega procesiranja
PKCS	angl. Public Key Cryptographic Standars – kriptografski standardi na področju javnih ključev
PKIX-CMP	angl. Public Key Infrastructure (based on) X.509 Certificate Management Protocols – protokol za izmenjavo ključev in upravljanje certifikatov
OID	Identifikacijska oznaka v skladu z mednarodnim standardom, ITU-T recommendation X.208 (ASN.1).
UTC	Koordiniran univerzalni čas določen v mednarodnem standardu za meritve časa, ITU-R Recommendation TF.460-5.

1.1.3 Dodatne definicije

Posamezni izrazi imajo v nadaljevanju tega dokumenta naslednji pomen:

- **Organizacija** je lahko državni organ, organ samoupravnih lokalnih skupnosti, pravna oseba, fizična oseba, ki samostojno opravlja dejavnost, odvetniki, notarji in drugi pravni subjekti , ki so registrirani za opravljanje dejavnosti.
- **Objava overitelja** je javna objava na spletnih straneh overitelja ali v medijih
- **Obvestila overitelja** so vsa navodila, pojasnila, seznami, pogoji, posamezna obvestila, priporočila, standardi in drugi dokumenti, ki jih določi ali priporoči overitelj in jih objavi ali kako drugače posreduje naročnikom in imetnikom digitalnih potrdil ali tretjim osebam.

- **Digitalna identiteta, digitalni ID** (angl. Digital Identity, Digital ID) je par ključev – zasebni in javni – ter digitalno potrdilo javnega ključa overitelja, izdano od overitelja digitalnih potrdil.
- **Naročnik storitve kvalificiranega elektronskega časovnega žiga** je vsaka organizacija, ki v skladu s to politiko uporablja storitev kvalificiranega elektronskega časovnega žiga (v nadaljevanju: časovni žig).

1.2 Identifikacijski podatki

Overitelja v okviru Pošte Slovenije predstavljajo naslednji identifikacijski in kontaktni podatki:

Naslov:	Pošta Slovenije d. o. o. POŠTA®CA Slomškov trg 10 2000 Maribor
Telefon:	02 449 2941
Fax:	02 449 2807
Spletna stran:	http://postarca.posta.si/
E-mail	info.postarca@posta.si
Pomoč uporabnikom:	080 44 40

Identifikacijska oznaka pričujoče politike POŠTA®CA overitelja časovnega žiga je:

PolicyIdentifier OID: 1.3.6.1.4.1.15284.2.1.2

Enolična imena strežnikov časovnega žiga POŠTA®CA overitelja so:

cn=TSA1-2019, cn=POSTArCA G2, organizationIdentifier=VATSI-25028022, o=POSTA SLOVENIJE d.o.o.,c=SI
cn=TSA2-2019, cn=POSTArCA G2, organizationIdentifier=VATSI-25028022, o=POSTA SLOVENIJE d.o.o.,c=SI

1.3 Naročniki in namen uporabe (User Community and applicability)

Pričujoči dokument ne določa nobenih omejitev glede uporabe žetonov časovnega žiga, ki jih POŠTA®CA overitelj časovnega žiga izdaja po tej politiki. Overitelj lahko brez omejitev izda žeton časovnega žiga za zagotavljanje dolgoročne veljavnosti elektronskega podpisa, kot tudi za uporabo v vse ostale namene, kjer je iz zakonskih, tehničnih ali drugih razlogov potreben elektronski časovni žig (arhiviranje elektronskih dokumentov, elektronski obrazci, ...).

Uporaba storitve časovnega žiga je dovoljena vsem naročnikom, ki imajo z overiteljem podpisano pogodbo ali sklenjen dogovor o uporabi storitve časovnega žiga.

Tehnični pogoji uporabe POŠTA®CA storitve časovnega žiga so dostopni na zahtevo na kontaktnih naslovih, navedenih v poglavju **Error! Reference source not found.**.

1.3.1 Interpretacija in usklajenost

Overitelj deluje v skladu z:

- Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1993/93/ES (Uredba eIDAS, Uradni list Evropske unije, L 257/73);
- Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov);
- Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 98/2004 – UPB-1, 61/2006-ZEPT);
- Zakonom o varstvu osebnih podatkov (Ur.l. RS, št. 94/2007-UPB1 -ZVOP-1);
- drugimi veljavnimi predpisi na območju Republike Slovenije;
- ETSI EN 319 421- Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;
- ETSI EN 319 422- Time-stamping protocol and electronic time-stamp profiles

2 OBVEZNOSTI IN ODGOVORNOSTI

2.1 Obveznosti overitelja časovnega žiga

2.1.1 Splošne

Overitelj časovnega žiga mora zagotoviti:

- izvajanje vseh postopkov v skladu z navedbami v pričujoči politiki (POŠTA®CA Overitelj časovnega žiga, Javni del notranjih pravil delovanja) ter veljavno zakonodajo Republike Slovenije;
- izvajanje vseh postopkov skladno z določili in postopki pričujoče politike tudi kadar storitev v imenu overitelja opravlja podizvajalec;
- izvajanje dodatnih obveznosti, ki so neposredno navedene v žetonu časovnega žiga ali vključene preko reference.

2.1.2 Obveznosti overitelja do naročnikov in tretjih oseb storitve časovnega žiga

Overitelj časovnega žiga jamči:

- da se bo po svojih najboljših močeh trudil zagotoviti neprekinjen dostop 24 ur, 7 dni v tednu do strežnikov časovnega žiga z izjemo napovedanih prekinitev delovanja zaradi tehničnih posegov na infrastrukturi overitelja, nepredvidenih okvar in drugih dogodkov izven nadzora overitelja oziroma višje sile;
- da UTC čas, ki je vsebovan v vsakem izdanem žetonu časovnega žiga, ne odstopa več kot +/- 1s;
- da izdani žetoni časovnega žiga ne vsebujejo napačnih podatkov ali napak.

2.2 Obveznosti naročnikov storitve časovnega žiga

Naročniki storitve časovnega žiga morajo:

- ob prevzemu žetona časovnega žiga preveriti, da je bil pravilno ustvarjen in da zasebni ključ s katerim je bil ustvarjen ni bil preklican;
- upoštevati obveznosti iz politike overitelja digitalnih potrdil;

- upoštevati overiteljeve tehnične pogoje za uporabo storitve časovnega žiga.

2.3 Obveznosti tretje strani

Tretje strani, ki se zanašajo na časovni žig, ki ga je izdal overitelj, so dolžne:

- zaupati časovnemu žigu le v okvirih, določenih v pričujoči politiki;
- preveriti veljavnost digitalnega podpisa na žetonu časovnega žiga;
- preveriti da zasebni ključ s katerim je bil podpis žetona časovnega žiga ustvarjen v času do preverjanja podpisa ni bil preklican;
- skrbno prebrati pričujoči dokument ter se seznaniti z odgovornostjo in omejitvami odgovornosti overitelja;
- upoštevati morebitne obveznosti, določila ali omejitve objavljene drugje.

2.4 Odgovornost

2.4.1 Odgovornost overitelja časovnega žiga

Overitelj odgovarja za vsak izdan žeton časovnega žiga za vse obveznosti, navedene v točki 2.1, vsakemu naročniku storitve časovnega žiga ali tretji strani, ki se upravičeno zanaša na časovni žig.

2.4.2 Omejitve odgovornosti overitelja časovnega žiga

Overitelj ni odgovoren za škodo (direktno ali posredno), izgube, stroške ter terjatve, ki izhajajo iz ali so nastale zaradi uporabe žetona časovnega žiga ki ga je izdal overitelj, če:

- je bil žeton časovnega žiga izdan kot rezultat napake, neverodostojnosti podatkov ali drugih dejanj naročnika storitve časovnega žiga, ali katere koli druge fizične ali pravne osebe, ki ni povezana z overiteljem;
- je bilo potrdilo strežnika časovnega žiga uporabljeno po preklicu in objavi na listi preklicanih potrdil;
- je naročnik storitve časovnega žiga ali tretja oseba kršil določbe overiteljevih pravil delovanja, pogodbe, dogovora ali veljavnih predpisov;
- je bil žeton časovnega žiga uporabljen v drugačne namene, kot je dovoljeno z overiteljevo politiko ali v nasprotju z veljavnimi predpisi;
- naročnik storitve časovnega žiga ali tretja stran ni ravnal v skladu s predpisanimi postopki v overiteljevi politiki, overiteljevih tehničnih pogojih uporabe storitve časovnega žiga, ali morebitni drugi pogodbi, ali dogovoru;
- je nastala škoda zaradi napake v delovanju strojne ali programske opreme naročnika storitve časovnega žiga ali tretje strani.

2.4.3 Finančna odgovornost

Overitelj ima ustrezno zavarovano svojo odgovornost po ZEPEP ter Uredbi o pogojih za elektronsko poslovanje in elektronsko podpisovanje.

Ob materialni škodi, ki bi nastala zaradi kršitev obveznosti iz 2.1, overitelj jamči za povrnitev škode do višine, kot je to določeno v naslednji tabeli:

800,00 EUR	fizičnim osebam
8.000,00 EUR	pravnim osebam

2.5 Cenik

Overitelj ima cenik svojih storitev objavljen na spletni strani http://postarca.posta.si.

3 POGOJI DELOVANJA OVERITELJA ČASOVNEGA ŽIGA

3.1 Postopki z dokumentacijo

3.1.1 Postopki spreminjanja vsebine dokumentacije

Overitelj bo izvajal uredniške in tipografske popravke katerega koli dela tega dokumenta in skrbel za njihovo objavo, brez posebnega obvestila. Verzije z uredniškimi in tipografskimi popravki bodo objavljene na spletnih straneh overitelja sedem (7) dni pred nastopom veljavnosti popravkov.

Vse ostale spremembe javnega dela notranjih pravil overitelja (nov dokument) bodo objavljene vsaj deset (10) dni pred nastopom veljavnosti novega dokumenta. O teh spremembah bo obveščen pristojni nadzorni organ v skladu z obstoječo zakonodajo. Naročniki in druge zainteresirane osebe bodo o spremembah obveščeni na spletni strani overitelja.

3.1.2 Objavljanje dokumentacije

Pričujoči dokument je dostopen na spletnih straneh overitelja na naslovu http://postarca.posta.si/tsa/dokumenti. Dokument je možno zahtevati tudi preko elektronske pošte, na naslovu info.postarca@posta.si.

3.2 Upravljanje ključev storitve časovnega žiga

3.2.1 Tvorjenje para ključev storitve časovnega žiga

Par ključev za podpisovanje je tvorjen ob namestitvi programske opreme strežnika časovnega žiga. Uporabljena je zaščita, ki velja za prostore overitelja [3.4.2 in 3.4.4], strogo preverjanje istovetnosti pooblaščenih oseb [3.4.3] in strojni šifrirni modul (HSM – Hardware Security Module) [3.2.2].

3.2.2 Zaščita zasebnega ključa storitve časovnega žiga

Zasebni ključ overitelja je bil tvorjen in se uporablja izključno na strojni opremi, ki ustreza varnostnemu nivoju FIPS 140-2 level 3.

3.2.3 Potrdilo javnega ključa storitve časovnega žiga

Za storitev časovnega žiga se uporabljajo normalizirana potrdila za strežnike časovnega žiga overitelja POŠTA®CA.

Javni ključi overitelja časovnega žiga so v obliki X.509 potrdila dostopni v vsakem izdanem žetonu časovnega žiga.

3.2.4 Obnova ključa strežnika časovnega žiga

Obnova ključa strežnika časovnega žiga se izvede pred iztekom obdobja veljavnosti digitalnega potrdila. V postopku obnove se tvori nov par ključev. Digitalno potrdilo strežnika časovnega žiga se hrani trajno, kar omogoča preverjanje veljavnosti podpisa na žetonih časovnega žiga, izdanih pred potekom veljavnosti potrdila.

3.2.5 Postopek za uničenje ključev

V postopku uničenja ključev strežnika časovnega žiga so uničene vse kopije ključev. Postopek uničenja ključev je izveden pod strogo kontrolo in zabeležen na trajnem nosilcu podatkov.

3.2.6 Upravljanje s strojnim šifrirnim modulom (HSM – Hardware Security Module)

Strojni šifrirni modul je poslan s strani dobavitelja direktno na naslov overitelja v zapečateni pošiljki. Overitelj ob prejemu pošiljke preveri, da ni poškodovana in ni bila odprta. Po odprtju pošiljke zaupanja vredna in strokovno usposobljena oseba preveri neoporečnost strojnega modula. Strojni modul se stalno hrani v strogo varovanih prostorih overitelja v katere imajo dostop le pooblaščeno osebje overitelja.

Instalacija in aktiviranje strojnega šifrirnega modula je izvedeno s strani overiteljevih pooblaščenih oseb v varovanih prostorih. V postopku aktiviranja in tvorjenja ključev so uporabljeni mehanizmi večkratne avtorizacije. Postopek se izvede v prisotnosti verodostojnih prič.

Zasebni ključ strežnika časovnega žiga je tvorjen in se vedno uporablja le na strojnem šifrirnem modulu. Zasebni ključ se nikdar ne pojavi v nešifrirani obliki izven strojnega šifrirnega modula.

3.3 Časovno žigosanje

3.3.1 Žeton časovnega žiga (angl. Time-stamp token - TST)

Vsak žeton časovnega žiga je izdan varno in vsebuje točen čas. Bistvene lastnosti vsakega izdanega žetona časovnega žiga so:

- vsebuje identifikacijsko oznako politike kot je določena v poglavju 1.2 pričujoče politike;
- vsebuje edinstveno identifikacijsko oznako žetona časovnega žiga;
- vsebuje datum in čas, ko je bil žeton časovnega žiga ustvarjen;
- datum in ura strežnika časovnega žiga sta usklajena s satelitskim sprejemnikom referenčnega časa in je s tem sledljiv glede na čas, ki ga distribuira UTC laboratorij;
- datum in ura vsebovana v žetonu časovnega žiga sta v okviru odstopanj določenih v poglavju 2.1.2 pričujoče politike;
- žeton časovnega žiga je podpisan z zasebnim ključem, ki je bil tvorjen le v ta namen;
- profil žetona časovnega žiga je skladen z RFC 3161;

3.3.2 Sinhronizacija ure z UTC

Ura strežnika časovnega žiga je usklajena s satelitskim sprejemnikom referenčnega UTC časa v okviru odstopanj določenih v poglavju 2.1.2 pričujoče politike. Uskladitev ure strežnika časovnega žiga s časom sprejemnika referenčnega UTC časa se izvaja avtomatsko v skladu s specifikacijo protokola NTP.

Satelitski sprejemnik referenčnega UTC časa je varovan na način, ki preprečuje nepooblaščen dostop.

Overitelj ima vzpostavljen nadzor, ki omogoča zaznavanje odstopanj časa strežnika časovnega žiga od časa referenčnega vira.

3.4 Organizacija in upravljanje

3.4.1 Notranja organizacija in upravljanje varnosti

Organizacija overitelja deluje v okviru Pošte Slovenije d.o.o.

Funkcijo nadzora delovanja operativnega osebja, revidiranja in odobravanja novih različic politike oz. javnega dela notranjih pravil overitelja (CPS) ima poslovodstvo Pošte Slovenije. Kadrovska sestava je potrjena s strani poslovodstva Pošte Slovenije.

Programska in strojna oprema, ki jo overitelj uporablja za opravljanje storitve časovnega žiga, podpira več stopenj pravic oziroma funkcij, ki so dodeljene osebju overitelja glede na njihove naloge. Odvisno od zadolžitev ima osebje sistemske in aplikativne uporabniške račune, omejene na nujno potrebne pravice za opravljanje svojih nalog.

3.4.2 Varnostni nadzor opreme

Informacijska infrastruktura overitelja se nahaja v varovanih prostorih, ki so fizično zaščiteni pred nepooblaščenim dostopom, uničenjem ali motnjami delovanja. Prostori so pod stalnim nadzorom. Vsi dostopi do prostorov overitelja se beležijo v skladu z načrtom varovanja za PLC Maribor in upravo z Informacijsko varnostno politiko »Vstop v varni sistemski prostor«..

3.4.3 Nadzor osebja

3.4.3.1 Zahteve o ozadju, kvalifikacijah, izkušnjah in odobritvah

Overitelj zaposluje osebje z ustreznimi kvalifikacijami, v skladu s politiko zaposlovanja Pošte Slovenije.

3.4.3.2 Postopki za preverjanje ozadja

Dodatna preverjanja o primernosti kandidatov (angl. security clearance checks) se izvajajo v skladu z varnostno politiko Pošte Slovenije.

3.4.3.3 Izobraževanje osebja

Osebje overitelja se redno izobražuje na naslednjih področjih:

- varnost informacijskih in komunikacijskih sistemov;
- pridobivanja specifičnih znanj za opravljanje svojih funkcij;
- za aplikativno programsko opremo servisa časovnega žiga;
- za obvladovanje postopkov ukrepanja ob incidentih, obnove poslovanja (angl. Business Continuation) ter okrevalnega načrta (angl. Disaster Recovery).

3.4.3.4 Dodatno izobraževanje in pogostost izobraževanja osebja

Osebje overitelja se udeležuje izobraževanj po potrebi, glede na nove operativne zahteve, oziroma vsaj enkrat letno za obnovo znanja.

3.4.3.5 Pogostost in sekvenca menjave dela med pooblaščenim osebjem

Ni predpisano.

3.4.3.6 Sankcije za nedovoljene postopke

Proti osebju overitelja, ki ne izvaja svojih nalog po predpisanih postopkih, se ukrepa v skladu z zakonom, ki urejuje delovna razmerja. V primeru nepravilnosti ali suma nepravilnosti se osebi odvzamejo pooblastila za sisteme ter prekličejo potrdila, izdana osebi za opravljanje funkcije.

3.4.3.7 Zahteve za osebje podizvajalcev

Varnostne zahteve za osebje podizvajalcev so enake kot za osebje overitelja.

3.4.3.8 Dokumentacija za osebje

Overitelj vzdržuje dokumentacijo na spletni strani, kot je opisano v točki 3.1.2. Ta dokumentacija je javno dostopna. Dodatno so osebju overitelja na voljo interni operativni priročniki, originalna dokumentacija programske in strojne opreme ter priročniki iz sklopa izobraževanja, glede na njihovo funkcijo in plan izobraževanja.

3.4.4 Varnostni nadzor prostorov in okolja

To poglavje opisuje varnostni nadzor prostorov in opreme, ki ga izvaja overitelj za zaščito svojega delovanja in je izvaja v skladu z načrtom varovanja za PLC Maribor in Upravo in informacijsko varnostno politiko Pošte Slovenije,

3.4.4.1 Lokacija in konstrukcija prostorov overitelja

Dejavnosti overitelja se izvajajo v varovanih prostorih in na varni lokaciji.

3.4.4.2 Fizični dostop do overitelja

Dostop do posameznih delov infrastrukture overitelja ima le pooblaščeno operativno osebje v skladu z zaupanimi nalogami. Vsi dostopi do prostorov overitelja se beležijo in varujejo v skladu z načrtom varovanja za PLC Maribor in upravo in informacijsko varnostno politiko Vstop v varni sistemski prostor..

3.4.4.3 Napajanje in klimatske naprave

Center overitelja je opremljen s:

- sistemom za neprekinjeno napajanje, za zagotavljanje napajanja kritičnim strežnikom in mrežnim napravam;
- klimatsko napravo za kontrolo temperature in vlage.

3.4.4.4 Zaščita pred poplavo

V bližini prostorov overitelja ne sme biti vodne napeljave. Prostori se nahajajo na lokaciji, kjer ni možna poplava.

3.4.4.5 Zaščita pred ognjem

Prostori overitelja so opremljeni z detektorji temperature in dima ter gasilnim sistemom.

3.4.4.6 Shranjevanje medijev

Vsi podatkovni mediji za arhiviranje podatkov overitelja so hranjeni na oddaljeni lokaciji v prostorih, ki zagotavljajo vsaj enake pogoje, kot so v centru overitelja.

3.4.4.7 Odstranjevanje odpadkov

Dokumenti v papirni obliki so uničeni v varovanih prostorih overitelja. Vsebina medijev, na katerih se hranijo zaupni podatki, se do fizičnega uničenja hrani v prostorih overitelja. Fizično uničenje izvaja zunanji pogodbeni izvajalec. Dokumentacijo o uničenju nosilcev podatkov vodi glavni administrator.

3.4.4.8 Hranjenje na oddaljeni lokaciji

Overitelj uporablja oddaljeno lokacijo za varno hranjenje podatkov. Mediji ali strojna oprema so na oddaljeni lokaciji shranjene v varovanem območju. V prostorih na oddaljeni lokaciji je zagotovljena vsaj enaka stopnja varnosti, kot v centru overitelja.

3.4.5 Upravljanje infrastrukture

Overitelj ima vzpostavljene procedure upravljanja svoje infrastrukture v skladu z zahtevami ISO 27001 standarda. Procedure so opisane v internih dokumentih, ki so zaupne narave in niso javno dostopni.

3.4.6 Upravljanje dostopa do sistemov

Glej 3.4.4.2.

3.4.7 Vzpostavitev infrastrukture in vzdrževanje

Overitelj izvaja storitev časovnega žiga na zaupanja vredni infrastrukturi, ki izpolnjuje zahteve ETSI EN 319 401. Infrastruktura je pod stalnim nadzorom. Vsi dogodki in spremembe se beležijo, redno pregledujejo in ocenjujejo. Redno se izvajajo pregledi sistemov ter implementirajo sistemski in varnostni popravki.

3.4.8 Ogrožanje servisa časovnega žiga

Ob ogrožanju ključa overitelja bo overitelj po elektronski pošti obvestil:

- celotno osebje overitelja;
- vse naročnike;
- morebitne medsebojno priznane ali podrejene overitelje.

Ob ogrožanju ključa overitelja bo overitelj izvedel naslednje postopke:

- preklical potrdilo ogroženega strežnika časovnega žiga;
- objavil preklic potrdila;
- tvoril nove ključe overitelja.

Ob ogrožanju časovnega vira ali v primeru neusklajenosti časa strežnika časovnega žiga in referenčnega vira UTC časa, bo overitelj zaustavil izdajanje žetonov časovnega žiga ter obvestil vse naročnike in tretje strani. V slučaju večjih odstopanj bo overitelj naročnikom in tretjim stranem zagotovil informacije, ki bodo omogočale prepoznavanje ogroženih žetonov časovnega žiga.

3.4.9 Prenehanje delovanja overitelja časovnega žiga

Overitelj bo v primeru prenehanja delovanja:

- obvestil vse naročnike in javno objavil informacije vsaj 90 dni pred prenehanjem delovanja;
- preklical potrdila strežnikov časovnega žiga in uničil zasebni ključ;
- zagotovil razpoložljivost in dostopnost podatkov potrebnih za preverjanje veljavnosti izdanih žetonov časovnega žiga;
- zagotovil hranjenje arhiviranih podatkov za obdobje deset (10) let po prenehanju delovanja, če veljavni predpisi ne določajo drugače.

3.4.10 Usklajenost z zakonodajo

Glej 1.3.1.

3.4.11 Sistem zbiranja revizijskih beležk

Overitelj ima vzpostavljene mehanizme zbiranja revizijskih beležk za vse dogodke povezane z izdajo žetonov časovnega žiga.

3.5 Organizacijska shema

Glej poglavje 1.1 in poglavje 3.4.1.