



**Ponudnik storitev zaupanja Rekono.TSP;
Pravila delovanja za
kvalificirani elektronski časovni žig
(RekonoQTSA Pravila delovanja)**

Ljubljana, 6.maj.2022

Verzija: 1.2

Zaščita dokumenta

© podjetje Rekono d.o.o.

Vse pravice pridržane. Reprodukcijska po delih ali v celoti na kakršenkoli način in v kateremkoli mediju ni dovoljena brez pisnega dovoljenja avtorja. Kršitve se sankcionirajo v skladu z avtorsko pravno in kazensko zakonodajo.

Nadzor različic dokumenta

Izvirni dokument je shranjen v elektronski obliki, različice dokumenta so pod nadzorom. Morebitne papirne ali elektronske kopije tega dokumenta lahko obstajajo za namene razdeljevanja tistim, ki jim je dokument namenjen oz. se morajo z njim seznaniti v okviru izvajanja delovnih nalog. Kopije dokumenta niso nadzorovane in jih mora bralec obravnavati kot take.

Zgodovina sprememb dokumenta:

Datum	Različica	Opis / opomba
14.04.2020	1.0	Prva verzija
12.05.2020	1.1	Uskladitev z izrazi eIDAS ("napredni elektronski pečat" spremenjen v "napredni elektronski žig").
06.05.2022	1.2	Dopolnjen opis v pregledu Rekono storitev. Dopolnjen opis dostopa do javnih ključev ponudnika storitev zaupanja. Spremenjeno obdobje uporabe zasebnega ključa enot za časovno žigosanje na največ 1 leto in 30 dni. Dopolnjen opis uporabljenih algoritmov. TSU RSA ključi generirani po 1.6.2022 so dolžine 3072 bitov.

Kazalo

1.	Uvod	6
2.	Prestavitev pravil delovanja storitve časovnega žiga in splošne zahteve .	7
2.1.	Pregled	7
2.2.	Naziv dokumenta in identifikacijske oznake.....	9
2.3.	Udeleženci in namen uporabe	10
2.3.1.	Storitev časovnih žigov	11
2.3.2.	Naročniki	11
2.3.3.	Tretje osebe	12
2.4.	Obveznosti in odgovornosti.....	12
2.4.1.	Obveznosti ponudnika storitev zaupanja.....	12
2.4.2.	Obveznosti overitelja do naročnikov in tretjih oseb storitve časovnega žiga	12
2.4.3.	Obveznosti naročnikov	13
2.4.4.	Obveznosti tretjih strani	13
2.4.5.	Finančna odgovornost	13
2.4.6.	Omejitve odgovornosti ponudnika storitev	14
2.5.	Obveščanje naročnikov in tretjih strani	14
3.	Pravila in pogoji delovanja storitve časovnih žigov	15
3.1.	Pravila delovanja overitelja.....	15
3.2.	Upravljanje s pravili delovanja	15
3.2.1.	Organizacija, ki upravlja s pričujočim dokumentom.....	15
3.2.2.	Kontaktne podatki.....	15
3.2.3.	Postopek odobritve politike delovanja overitelja	15
3.3.	Interna organizacija.....	15
3.3.1.	RekonoPMA (Policy Management Authority (PMA)).....	16
3.3.2.	RekonoOA (Operations Authority (OA))	16
3.3.3.	RekonoRA (Registration Authority - RA)	17
3.4.	Osebe in organizacijski varnostni ukrepi.....	17
3.4.1.	Organizacija ponudnika storitev zaupanja	17
3.4.2.	Število oseb, potrebnih za izvedbo postopka.....	17
3.4.3.	Preverjanje istovetnosti operativnega osebja	18
3.4.4.	Nezdružljivost nalog	18
3.4.5.	Zahteve za osebe overitelja	18
3.5.	Upravljanje s sredstvi	19
3.6.	Upravljanje kriptografskih ključev storitve časovnega žiga.....	19
3.6.1.	Generiranje kriptografskih ključev.....	19
3.6.2.	Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov	19
3.6.3.	Potrdilo javnega ključa storitve časovnega žiga.....	19

3.6.4.	Dostop do javnih ključev ponudnika storitev zaupanja	20
3.6.5.	Obdobje uporabe in obnova parov ključev ponudnika storitev..	20
3.6.6.	Konec obdobja uporabe zasebnih ključev in uničenje.....	21
3.6.7.	Nadzor življenjskega cikla strojnega varnostnega modula.....	21
3.7.	Časovno žigosanje	21
3.7.1.	Zahteva za izdajo elektronskega časovnega žiga	22
3.7.2.	Oblika in vsebina časovnega žiga	22
3.7.3.	Sinhronizacija časa z UTC	23
3.8.	Fizično varovanje in kontrola okolja	23
3.9.	Operativno upravljanje varnosti sistemov	23
3.10.	Varnostne kontrole na ravni računalniškega omrežja	23
3.10.1.	Postopki za odzivanje na varnostne incidente in nepravilnosti.	24
3.11.	Zbiranje dokazov	24
3.12.	Upravljanje kontinuitete poslovanja	24
3.13.	Prenehanje delovanja ponudnika storitev	24
4.	Dodatki.....	26
4.1.	Definicije in okrajšave	26
4.2.	Reference	30

1. UVOD

V okviru podjetja Rekono d.o.o. deluje ponudnik storitev zaupanja Rekono.TSP, ki izvaja kvalificirane in nekvalificirane storitve zaupanja. Pričujoči dokument opisuje pravila delovanja ponudnika storitev zaupanja Rekono.TSP za storitev kvalificiranega elektronskega časovnega žiga RekonoQTSA.

2. PRESTAVITEV PRAVIL DELOVANJA STORITVE ČASOVNEGA ŽIGA IN SPLOŠNE ZAHTEVE

2.1. Pregled

Rekono d.o.o. je vzpostavil in upravlja infrastrukturo javnih ključev Rekono.TSP, ki deluje kot ponudnik storitev zaupanja za kvalificirani elektronski časovni žig in druge storitve zaupanja, kot so overjanje digitalnih potrdil za kvalificirani elektronski podpis, kvalificirani elektronski žig, napredni elektronski podpis, napredni elektronski žig, elektronsko avtentikacijo in izdajanje naprednih elektronskih časovnih žigov.

Rekono.TSP deluje kot javni ponudnik storitev zaupanja 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 ter EN 319 421, EN 319 422 in EN 391 401.

Definicije in okrajšave uporabljene v pričujočem dokumentu so povzete po uredbi eIDAS [6] in ETSI TR 119 001 [7]. Glej tudi 4.1.

Pričujoči dokument, Rekono.TSP Pravila delovanja za kvalificirani elektronski časovni žig (v nadaljevanju RekonoQTSA Pravila delovanja), vsebuje pogoje uporabe in opis pravil ter postopkov, ki jih izvaja Rekono d.o.o. za izvajanje storitve kvalificiranega elektronskega časovnega žiga. RekonoQTSA Pravila delovanja vsebujejo poleg navedenega tudi opis tehničnih lastnosti in operativnih postopkov upravljanja infrastrukture IT, ki jo Rekono d.o.o. uporablja za izvajanje in upravljanje storitve kvalificiranega elektronskega žiga.

Kvalificirani elektronski časovni žigi, izdani po teh RekonoQTSA Pravilih delovanja, so jasno označeni z identifikacijskimi oznakami, navedenimi v poglavju 2.2 Naziv dokumenta in identifikacijske oznake.

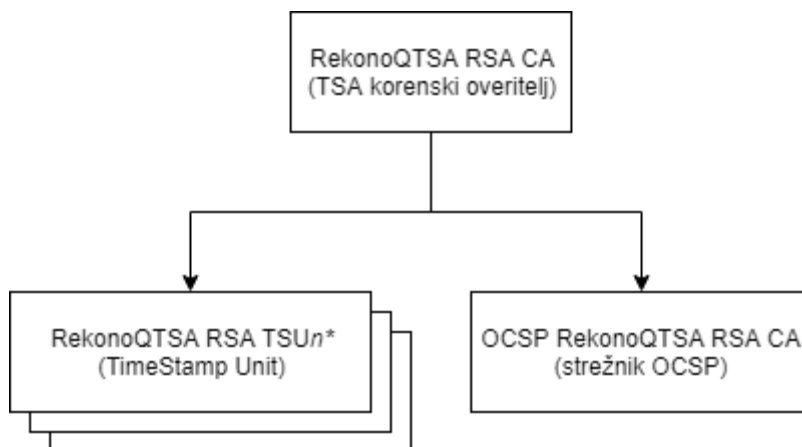
Za potrebe izvajanja storitev zaupanja ima Rekono d.o.o. vzpostavljeno lastno infrastrukturo javnih ključev Rekono.TSP, ki obsega korenskega overitelja za izdajanje potrdil enotam za časovno žigosanje. V okviru storitve RekonoQTSA sta vzpostavljeni dve verigi zaupanja, in sicer veriga zaupanja, ki uporablja asimetrične ključe RSA (Rivest–Shamir–Adleman) in veriga zaupanja, ki uporablja asimetrične ključe ECC (Elliptic-curve cryptography).

Korenski overitelj RekonoQTSA, oziroma njegovo potrdilo javnega ključa v posamezni verigi zaupanja, predstavlja digitalno identiteto storitve (angl. Service digital identity) ter izhodišče zaupanja (angl. Trust Anchor) za preverjanje digitalnih potrdil enot za časovno žigosanje ter časovnih žigov.

Korenski overitelj RekonoQTSA izdaja digitalna potrdila le enotam za časovno žigosanje za izdajanje kvalificiranih elektronskih časovnih žigov v okviru ponudnika storitev zaupanja Rekono.TSP in strežnikom OCSP za preverjanje statusa potrdil.

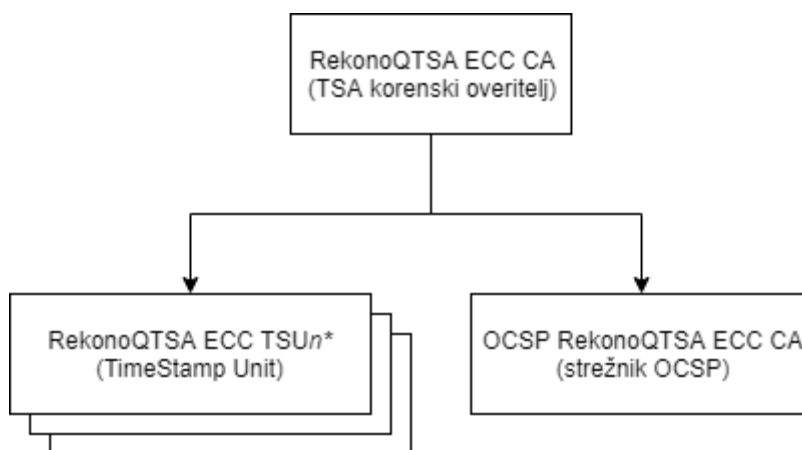
Slika 1 prikazuje PKI hierarhijo oziroma verigo zaupanja s ključi RSA.

Slika 1 - PKI veriga zaupanja s ključi RSA



Slika 2 prikazuje PKI hierarhijo oziroma verigo zaupanja s ključi ECC.

Slika 2 - veriga zaupanja s ključi ECC



RekonoQTSA uporablja več enot za časovno žigosanje, ki se praviloma nahajajo na različnih lokacijah. Oznaka n^* v razločevalnih imenih pomeni številčno oznako instance enote za časovno žigosanje (npr.: "RekonoQTSA ECC TSU1"). Enote za časovno žigosanje so med seboj enakovredne. Vsaka enota za časovno žigosanje ima lasten zasebni ključ za napreden elektronski žig in digitalno potrdilo pripadajočega javnega ključa. Napreden elektronski žig je realiziran z uporabo asimetrične kriptografije in tehnologije digitalnih podpisov.

Korenski overitelj in enota za časovno žigosanje verige zaupanja s ključi RSA in verige s ključi ECC imajo razločevalna imena, kot je navedeno v spodnjih tabelah (Tabela 1 in Tabela 2).

Tabela 1 – Razločevalna imena v verigi zaupanja s ključi RSA

TSA korenski overitelj v verigi zaupanja s ključi RSA
CN=RekonoQTSA RSA CA, OI=VATSI-60762802, O=Rekono d.o.o., C=SI
Enote za časovno žigovanje v verigi zaupanja s ključi RSA
CN=RekonoQTSA RSA TSUn*, OI=VATSI-60762802, O=Rekono d.o.o., C=SI

Tabela: Veriga zaupanja s ključi ECC

Tabela 2 - Razločevalna imena v verigi zaupanja s ključi ECC

TSA korenski overitelj v verigi zaupanja s ključi ECC
CN=RekonoQTSA ECC CA, OI=VATSI-60762802, O=Rekono d.o.o., C=SI
Enote za časovno žigovanje v verigi zaupanja s ključi ECC
CN=RekonoQTSA ECC TSUn*, OI=VATSI-60762802, O=Rekono d.o.o., C=SI

Opomba: Oznaka *OI* v razločevalnih imenih je okrajšava za Organization Identifier (organizationIdentifier).

Pričujoči dokument, Pravila delovanja RekonoQTSA, opredeljuje sledeče kategorije digitalnih potrdil, izdane s strani overitelja RekonoQTSA:

1. Digitalna potrdila RekonoQTSU za napredni elektronski žig za overjanje kvalificiranih elektronskih žigov
2. Digitalna potrdila RekonoOCSP za overjanje statusa potrdil RekonoQTSU

Vsaka vrsta digitalnih potrdil, ki je opredeljena v tem dokumentu, ima dodeljeno enolično identifikacijsko oznako (OID, Object Identifier) (glej poglavje 2.2).

2.2. Naziv dokumenta in identifikacijske oznake

Naziv dokumenta, sl: RekonoQTSA Pravila delovanja
Verzija: 1.2
Datum: 06.05.2022

Vsak izdani elektronski časovni žig vsebuje enolično identifikacijsko oznako, ki je v skladu z RFC 3161 vpisana v parameter *policy* v polju *TSTInfo* (glej RFC 3161 [4], poglavje 2.4.2.).

Vsako potrdilo enote za časovno žigovanje vsebuje enolično identifikacijsko oznako (OID), ki je v skladu z RFC 5280 [3] v vsakem izdanem digitalnem potrdilu vpisana v polje *id-ce-certificatePolicies*, parameter *policyIdentifier* (glej RFC 5280 [3], poglavje 4.2.1.4.).

Vse identifikacijske oznake (OID) v digitalnih potrdilih imajo predpono 1.3.6.1.4.1.54579. Identifikacijska oznaka je registrirna pri mednarodni organizaciji IANA (<http://www.iana.org/>), ki upravlja identifikacijske oznake za predpono *iso.org.dod.internet.private.enterprise* (1.3.6.1.4.1). OID številka 54579 je pri IANA registrirana na podjetje Rekono d.o.o..

Sledeče identifikacijske oznake (OIDs) so dodeljene kategorijam digitalnih potrdil, ki so izdani v verigi zaupanja s ključi RSA:

Digitalno potrdilo	Identifikacijska oznaka (CertPolicyId)
RekonoQTSU	1.3.6.1.4.1.54579.1.1.1.6 iso.org.dod.internet.private.enterprise.rekono-pen(54579).rekono-pki(1).oids(1).dp-rsa(1).qtsu(6)
RekonoOCSP	1.3.6.1.4.1.54579.1.1.1.5 iso.org.dod.internet.private.enterprise.rekono-pen(54579).rekono-pki(1).oids(1).dp-rsa(1).ocsp(5)

Sledeče identifikacijske oznake (OIDs) so dodeljene kategorijam digitalnih potrdil, ki so izdani v verigi zaupanja s ključi ECC:

Digitalno potrdilo	Identifikacijska oznaka (CertPolicyId)
RekonoQTSU	1.3.6.1.4.1.54579.1.1.2.6 iso.org.dod.internet.private.enterprise.rekono-pen(54579).rekono-pki(1).oids(1).dp-ecc(2).qtsu(6)
RekonoOCSP	1.3.6.1.4.1.54579.1.1.2.5 iso.org.dod.internet.private.enterprise.rekono-pen(54579).rekono-pki(1).oids(1).dp-ecc(2).oscp(5)

Sledeče identifikacijske oznake (OIDs) so dodeljene kvalificiranim elektronskim časovnim žigom, ki so izdani v verigi zaupanja s ključi RSA:

RFC 3161 polje	Identifikacijska oznaka (TSAPolicyId)
TSTInfo policy	1.3.6.1.4.1.54579.1.1.3.2 iso.org.dod.internet.private.enterprise.rekono-pen(54579).rekono-pki(1).oids(1).ts-rsa(3).qtsp(2)

Sledeče identifikacijske oznake (OIDs) so dodeljene elektronskim časovnim žigom, ki so izdani v verigi zaupanja s ključi ECC:

RFC 3161 polje	Identifikacijska oznaka (TSAPolicyId)
TSTInfo policy	1.3.6.1.4.1.54579.1.1.4.2 iso.org.dod.internet.private.enterprise.rekono-pen(54579).rekono-pki(1).oids(1).ts-ecc(4).qtsp(2)

2.3. Udeleženci in namen uporabe

Časovni žigi ustvarjeni v skladu s temi pravili delovanja, RekonoQTSA Pravila delovanja, so namenjeni izpolnjevanju zahtev za dolgoročno veljavnost časovnih žigov (npr. kot je opredeljeno v ETSI EN 319 122 [14]), vendar se lahko

na splošno uporabljajo tudi za druge primere uporabe, ki imajo podobne zahteve.

2.3.1. Ponudnik storitev časovnih žigov (angl. Time-Stamping Authority, TSA)

Storitev kvalificiranih elektronskih časovnih žigov RekonoQTSA, ki deluje v okviru ponudnika storitev zaupanja Rekono.TSP, izvaja storitve v skladu s temi RekonoQTSP Pravili delovanja in dotično zakonodajo.

Rekono d.o.o. ima za izvajanje storitev zaupanja vzpostavljeno lastno infrastrukturo javnih ključev Rekono.TSP s korenskimi overitelji in enotami za časovno žigosanje.

Korenski overitelji RekonoQTSA imajo samopodpisano digitalno potrdilo, ki je bilo izdano v okviru nadzorovanega postopka generiranja overiteljevih kriptografskih ključev (angl. Root Key Generation Ceremony). Korenski overitelji RekonoQTSA izdajajo potrdila le enotam za časovno žigosanje RekonoQTSU in dotičnim strežnikom OCSP.

Enote za časovno žigosanje RekonoQTSU izdajajo kvalificirane elektronske časovne žige naročnikom, ki so lahko fizične osebe ali pravne osebe. Glej tudi 2.3.2.

2.3.2. Naročniki

RekonoQTSA izdaja kvalificirane elektronske časovne žige vsem zainteresiranim strankam, tudi za zaprte sisteme.

Naročnik je lahko fizična oseba ali poslovni subjekt, ki ima z Rekono d.o.o. podpisano pogodbo za uporabo storitve RekonoQTSA ali uporablja druge storitve Rekono.TSA ali Rekono.ID, ki vključujejo kvalificiran elektronski časovni žig RekonoQTSA.

Kadar deluje naročnik v imenu več uporabnikov (na primer, ko pravna oseba zahteva dostop do storitve časovnega žiga za zaposlene), nosi naročnik polno odgovornost v odnosu do ponudnika storitev zaupanja Rekono.TSP za vse obveznosti glede uporabe storitve RekonoQTSA. V primeru, ko je uporabnik fizična oseba, identificirana v povezavi s pravnim subjektom, morata biti z obveznostmi seznanjena naročnik (pravna oseba) in uporabnik (fizična oseba).

Kadar je potrebno, ta dokument razlikuje različne subjekte, ki so vključeni v posamezen postopek ali nosijo določeno odgovornost. Kadar to razlikovanje ni potrebno, se uporablja izraz naročnik.

2.3.3. Tretje osebe

Tretje osebe so entitete, ki vključujejo fizične osebe (posameznike) in/ali poslovne subjekte, ki se zanašajo na elektronske časovne žige, izdane s strani RekonoQTSA, ne glede na to, ali so naročnik storitve ali ne.

Za preverjanje veljavnosti elektronskega časovnega žiga morajo tretje osebe vedno preveriti, da je potrdilo za preverjanje veljavnosti žiga izdano s strani enega od korenskih overiteljev RekonoQTSA ter status potrdila v veljavnem registru preklicanih digitalnih potrdil (CRL) ali preko storitve sprotnega preverjanja statusov potrdil (OCSP).

2.4. Obveznosti in odgovornosti

2.4.1. Obveznosti ponudnika storitev zaupanja

Ponudnik storitev zaupanja Rekono.TSP mora izvajati storitev RekonoQTSA, opravljati druge postopke, povezane z overjanjem časovnih žigov in upravljanjem infrastrukture ponudnika storitev, v skladu s temi RekonoQTSA Pravili delovanja in veljavno zakonodajo.

2.4.2. Obveznosti overitelja do naročnikov in tretjih oseb storitve časovnega žiga

Overitelj časovnih žigov RekonoQTSA pri overjanju časovnih žigov jamči:

- da čas, ki je vsebovan v časovnem žigu, ne odstopa več kot 1s;
- da izdani časovni žigi vsebujejo pravo zgoščeno vrednost, kot je bila poslana v zahtevku in da ne vsebuje napak;
- za zagotavljanje točnosti in celovitosti informacij objavljenih na spletnem mestu ali drugi shrampi ponudnika storitev zaupanja;
- za zagotavljanje dostopnosti javnih shramb za objavo splošnih informacij;
- za izdajanje časovnih žigov naročnikom v skladu s temi RekonoQTSA Pravili delovanja;
- za preklic digitalnih potrdil enot za časovno žigosanje RekonoQTSA v primeru ogrožanja ali suma ogrožanja zasebnih ključev;
- za preklic digitalnih potrdil korenskih overiteljev RekonoQTSA v primeru ogrožanja ali suma ogrožanja zasebnih ključev.

Rekono.TSP si bo prizadeval zagotoviti stalno dostopnost storitev RekonoQTSA 24 ur na dan vse dni v letu, razen v primerih:

- načrtovanih in vnaprej napovedanih prekinitev delovanja zaradi posegov ali vzdrževalnih del na infrastrukturi;
- prekinitev, ki so posledica nenačrtovanih okvar na infrastrukturi;
- prekinitev, ki so posledica nedelovanja infrastrukture izven pristojnosti Rekono.TSP (npr. ponudnikov dostopa do interneta);

- prekinitev, ki so posledica višje sile.

2.4.3. Obveznosti naročnikov

Poleg izpolnjevanja obveznosti, ki izhajajo iz RekonoQTSA Pravil delovanja, morajo naročniki:

- skrbno varovati avtentikacijske podatke za dostop do storitve časovnega žiga, če so jim bili ;
- ob prevzemu časovnega žiga preveriti točnost podatkov, vsebovanih v časovnem žigu, da digitalno potrdilo enote za časovno žigosanje ni preklicano in da je bilo izdano s strani korenskega overitelja RekonoQTSA;
- upoštevati tehnične pogoje za uporabo storitve časovnega žiga;
- spremljati obvestila ponudnika storitev in ravnati v skladu z njimi;
- v primeru, da je naročnik pravna oseba, mora z obveznostmi seznaniti fizične osebe oziroma zaposlene, ki bodo uporabljali storitev časovnega žiga;
- v skladu s pogodbo za uporabo storitve v roku poravnati vse finančne obveznosti do ponudnika storitev.

Naročniki in imetniki sami nosijo vse posledice, ki bi nastale zaradi neupoštevanja teh RekonoQTSA Pravil delovanja, pogodbe ali drugega dogovora med naročnikom ter ponudnikom storitev Rekono.TSP in zadevne zakonodaje.

2.4.4. Obveznosti tretjih strani

Tretje osebe se morajo, preden se zanašajo na časovni žig RekonoQTSA, seznaniti z RekonoQTSA Pravili delovanja.

Poleg tega morajo:

- preveriti veljavnost podpisa na časovnem žigu;
- preveriti, da digitalno potrdilo za preverjanje veljavnosti časovnega žiga ni bilo preklicano;
- preveriti, da je bilo digitalno potrdilo za preverjanje veljavnosti časovnega žiga izdano s strani korenskega overitelja RekonoQTSA;
- spremljati obvestila ponudnika storitev in ravnati v skladu z njimi.

Tretje osebe same nosijo vse posledice, ki bi nastale zaradi neupoštevanja teh RekonoQTSA Pravil delovanja in zadevne zakonodaje.

2.4.5. Finančna odgovornost

2.4.5.1. Zavarovalniško kritje

Ni predpisano.

2.4.5.2. Drugo kritje

Rekono d.o.o. ima kot ponudnik storitev zaupanja stalno rezervacijo sredstev v višini najmanj 20.000,00 EUR za kritje morebitne škode, nadomestil, obveznost povrnitve terjatev ali obveznosti katerekoli vrste v zvezi z izdajo ali uporabo kvalificiranega časovnega žiga.

2.4.6. Omejitve odgovornosti ponudnika storitev

V primeru škode, ki bi nastala pri uporabi časovnih žigov brez upoštevanja ali v nasprotju z določbami teh RekonoQTSA Pravil delovanja s strani naročnika ali tretjih osebe, Rekono.TSP ne odgovarja za škodo, ki bi pri taki uporabi nastala.

2.5. Obveščanje naročnikov in tretjih strani

Rekono.TSP obvešča naročnike in tretje strani o pogojih uporabe storitve časovnega žiga preko spletne strani <https://www.rekono.si>. Poleg pričujočega dokumenta RekonoQTSA Pravila delovanja, so na navedeni spletni strani objavljeni še Splošni pogoji uporabe storitev podjetja Rekono d.o.o., Politika zasebnosti podjetja Rekono d.o.o. in Rekono.TSP Pravila delovanja [13].

Naročniki lahko pridobijo tehnična navodila za integracijo storitve RekonoQTSA z e-poštnim sporočilom na kontaktni naslov naveden v poglavju 3.2.2.

3. PRAVILA IN POGOJI DELOVANJA STORITVE ČASOVNIH ŽIGOV

3.1. Pravila delovanja overitelja

Vsi postopki in aktivnosti, ki jih izvaja ponudnik storitev Rekono.TSP za opravljanje storitve RekonoQTSA, so opisani v pričujočem dokumentu RekonoQTSP Pravila delovanja. Pravila delovanja za napredne storitve, ki jih izvaja Rekono.TSP so vsebovane v dokumentu Rekono.TSP Pravila delovanja [13].

3.2. Upravljanje s pravili delovanja

3.2.1. Organizacija, ki upravlja s pričujočim dokumentom

Z dokumentom upravlja Rekono d.o.o.

3.2.2. Kontaktni podatki

Naslov: Rekono d.o.o.
Ukmarjeva ulica 2
Ljubljana
E-mail: info@rekono.si
Internet: <https://www.rekono.si>

3.2.3. Postopek odobritve pravil delovanja

RekonoQTSP Pravila delovanja oziroma novo različico odobri zakoniti zastopnik podjetja Rekono d.o.o. Dokument se odobri in objavi v elektronski različici v obliki PDF. Odobritev oziroma podpis se izvede s kvalificiranim elektronskim podpisom zakonitega zastopnika.

3.3. Interna organizacija

Rekono d.o.o. ima za upravljanje in izvajanje storitev zaupanja Rekono.TSP projektno organizacijsko strukturo s tremi projektnimi organizacijskimi enotami (POE):

- RekonoPMA - POE za upravljanje storitev zaupanja (angl. Policy Management Authority – PMA)
- RekonoOA - POE za operativno delovanje storitev zaupanja (angl. Operations Authority – OA)
- RekonoRA – POE za registracijo (angl. Registration Authority – RA)

Osebe, ki izvajajo naloge posamezne POE, so stalno zaposleni, začasno zaposleni ali osebe, ki imajo z Rekono d.o.o. pogodbo o izvajanju zadevnih storitev.

Rekono d.o.o. ima sklenjeno pogodbo z OSI d.o.o., Ukmarjeva ulica 2, Ljubljana za izvajanje storitev v okviru nalog RekonoPMA in RekonoOA.

3.3.1. RekonoPMA (Policy Management Authority (PMA))

Osebjje RekonoPMA je odgovorno za:

- razvoj in vzdrževanje RekonoQTSA Pravil delovanja;
- razvoj in vzdrževanje drugih javnih dotičnih dokumentov (splošna pravila uporabe storitve ...);
- potrditev osebjja RekonoOA;
- nadzor skladnosti delovanja z Rekono.QTSA Pravili delovanja in dotično zakonodajo;
- pregled ustreznosti pravil delovanja oziroma politik drugih ponudnikov storitev zaupanja v primeru vzpostavitve navzkrižnega priznavanja (angl. cross certification) ali priznavanja njihovih storitev zaupanja v okviru Rekono.TSP;
- reševanje sporov med subjekti v okviru Rekono.TSP.

3.3.2. RekonoOA (Operations Authority (OA))

Osebjje RekonoOA je odgovorno za:

- generiranje kriptografskih ključev storitev zaupanja RekonoQTSA, varno upravljanje zasebnih kriptografskih ključev storitev zaupanja in distribucijo javnih ključev overiteljev oziroma digitalnih potrdil overiteljev in enot za časovno žigosanje;
- vzpostavitev postopkov in informacijske podpore za delovanje storitev;
- izvedbo preklica digitalnih potrdil enot za časovno žigosanje;
- izdajo in objavo registrov preklicanih digitalnih potrdil (angl. Certificate Revocation List, CRL);
- delovanje storitve za sprotno preverjanje statusa digitalnih potrdil OCSP;
- delovanje storitve elektronskega časovnega žiga;
- upravljanje infrastrukture v skladu z RekonoQTSA Pravili delovanja;
- sodelovanje z RekonoPMA pri pripravi sprememb in novih različic pravil delovanja;

Kadar je potrebno, ta dokument razlikuje različne subjekte in vloge, ki upravljajo s posameznimi sklopi in funkcijami storitev zaupanja Rekono.TSP in RekonoQTSA kot ene od storitev zaupanja v okviru Rekono.TSP. Kadar to razlikovanje ni potrebno, se pojem Rekono.TSP uporablja za sklicevanje na ponudnika storitev kot celoto.

3.3.3. RekonoRA (Registration Authority - RA)

V primeru uporabe storitve časovnega žiga kot samostojne storitve, preverjanje identitete naročnika ne izvaja, ker časovni žigi ne vsebujejo podatkov o naročniku.

Poleg uporabe storitve časovnega žiga kot samostojne storitve, lahko storitve zaupanja Rekono.TSP, vključno s storitvijo RekonoQTSA, uporabljajo fizične ali pravne osebe, ki imajo račun Rekono.ID ustrezne ravni zanesljivosti. Vsi postopki preverjanja identitete, pridobitve računa Rekono ustrezne ravni zanesljivosti in upravljanje identitete se izvajajo preko storitve Rekono (<https://idp.rekono.si>).

3.4. Osebe in organizacijski varnostni ukrepi

3.4.1. Organizacija ponudnika storitev zaupanja

Rekono.TSP ima opredeljeno organizacijsko strukturo, razdelitev nalog ter pooblastil za dostop do infrastrukture in podatkov glede na naloge, ki jih opravlja posamezna oseba.

Osebe overitelja ima operativne vloge za opravljanje zaupanja vrednih nalog razdeljene v sledeče skupne:

- Osebe zadolžene za upravljanje strojnih varnostnih modulov (HSM) in logičnih particij HSM. Zadolžitve so razdeljene v sledeče skupine:
 - Varnostni skrbnik HSM
 - Administrator HSM
 - Varnostni skrbnik logične particije HSM
 - Uporabnik logične particije HSM
- Osebe zadolžene za upravljanje nastavitev programske opreme ter dodajanje in upravljanje pooblastil oseb zadolženih za operativno upravljanje posamezne storitve zaupanja.
- Osebe zadolžene za operativno upravljanje posamezne storitve zaupanja.
- Osebe zadolžene za hrambo varnostnih kopij kriptografskih ključev overitelja in po potrebi drugih varnostno občutljivih podatkov.
- Osebe zadolžene za upravljanje sistemov IT, na katerih delujejo sklopi programske opreme overitelja.

Opomba: Naloge registracijske pisarne (RA) se izvajajo v okviru storitve Rekono.ID.

3.4.2. Število oseb, potrebnih za izvedbo postopka

Dve (2) osebi sta potrebni za izvedbo sledečih nalog:

- Povrnitev varnostne kopije zasebnih ključev overitelja na strojni varnostni modul (HSM).
- Aktiviranje zasebnih ključev overitelja na strojnem varnostnem modulu (HSM).

Ena oseba lahko izvede ostale posamezne naloge glede na dodeljeno operativno vlogo.

3.4.3. Preverjanje istovetnosti operativnega osebja

Člani osebja RekonoOA z zaupno vlogo so imenovani za delo kot člani operativnega osebja s strani RekonoPMA.

Vsak posameznik z zaupno vlogo na programski opremi sistemov Rekono.TSP se ob prijavi na posamezen sistem prijavi z digitalnim potrdilom ali močnim geslom.

3.4.4. Nezdržljivost nalog

Rekono.TSP zagotavlja delitev dolžnosti operativnega osebja in s tem nezdržljivost nalog z dodelitvijo zaupanja vrednih nalog, navedenih v poglavju 3.4.1 različnim osebam.

V primeru, ko ima posamezna oseba več zaupanja vrednih vlog, se za avtentikacijo uporablja princip štirih oči (angl. Four Eyes Principle, also Two-man rule).

3.4.5. Zahteve za osebje overitelja

3.4.5.1. Kvalifikacije, izkušnje in varnostno preverjanje

Rekono.TSP dodeljuje zaupanja vredne operativne vloge zaposlenim in po potrebi zunanjim izvajalcem (glej tudi 3.4.5.5). Primernost posameznika za določeno operativno vlogo potrdi oziroma odobri RekonoPMA.

Člani osebja ne smejo izvajati nalog, ki so v nasprotju interesov z njihovo vlogo v okviru Rekono.TSP.

3.4.5.2. Usposabljanje osebja

Člani osebja overitelja imajo, poleg ustrezne formalne izobrazbe, tudi opravljena dodatna interna ali zunanja izobraževanja in/ali delovne izkušnje glede na specifičnost njihovih nalog.

3.4.5.3. Pogostost dodatnih usposabljanj

Zahteve za usposabljanje osebja so redno pregledane in posodobljene, kadar je to zahtevano za prilagoditev spremembam glede na spremembe tehnologije in različic programske opreme.

3.4.5.4. Ukrepi ob kršitvah pooblastil

Nepooblaščenjena dejanja ali prekrški so obravnavani v skladu z internimi akti Rekono d.o.o.

3.4.5.5. Zahteve za pogodbene in zunanje izvajalce

Osebe, ki izvajajo naloge, so lahko pogodbeni ali zunanji izvajalci (v nadaljevanju zunanji izvajalci), ki imajo z Rekono d.o.o. pogodbo o izvajanju zadevnih storitev.

Kjer so za naloge potrebni zunanji izvajalci, je izvedeno preverjanje usposobljenosti izvajalcev. Vsi zunanji izvajalci morajo podpisati sporazum o varovanju in nerazkrivanju zaupnih podatkov.

3.5. Upravljanje s sredstvi

Rekono d.o.o., ki izvaja storitev zaupanja Rekono.TSP, ima vzpostavljeno upravljanje s sredstvi v skladu z ISO/IEC 27001. Oceno postopkov je izvedel neodvisni revizijski in certifikacijski organ. Ocenjevanje in certificiranje se redno ponavljata v skladu z ISO/IEC 27001.

3.6. Upravljanje kriptografskih ključev storitve časovnega žiga

3.6.1. Generiranje kriptografskih ključev

Zasebni podpisni kriptografski ključi storitev, ki se uporabljajo za digitalno podpisovanje v okviru storitve časovnega žigosanja, so ustvarjeni v strojnih varnostnih modulih (angl. Hardware Security Module, HSM) v okviru nadzorovanega postopka (angl. Key Generation Ceremony). Postopek se izvede v nadzorovanem okolju pod nadzorom več oseb v skladu s priporočili in prakso za generiranje kriptografskih ključev ponudnikov storitev zaupanja. Postopek generiranja ključev korenskih overiteljev ali enot za časovno žigosanje odobri predsednik RekonoPMA.

3.6.2. Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov

Generiranje ključev korenskih overiteljev RekonoQTSA in enot za časovno žigosanje ter njihova uporaba se izvaja v strojnih varnostnih modulih, ki imajo potrdilo o skladnosti s FIPS 140-2 Level 3.

3.6.3. Potrdilo javnega ključa storitve časovnega žiga

3.6.3.1. Korenski overitelji

Korenski overitelji storitve RekonoQTSA so izdali samopodpisano potrdilo v postopku generiranja ključev (angl. Root Key Ceremony).

Digitalna potrdila korenskih overiteljev RekonoQTSA predstavljajo digitalno identiteto ponudnika storitev zaupanja za kvalificirane elektronske časovne žige RekonoQTSA.

Veljavnost potrdil korenskih overiteljev je dvajset (20) let in tri (3) mesece.

Glej tudi 3.6.1.

3.6.3.2. Enote za časovno žigosanje

Potrdila enot za časovno žigosanje RekonoQTSU izdajo korenski overitelji storitve RekonoQTSA. Potrdila so v skladu z RFC 3161 ter RFC 5280 in vsebujejo dodatno razširitevno polje timeStamping, ki je v skladu z RFC 3161 v potrdilu označeno kot kritično.

Veljavnost potrdil je pet (5) let.

Glej tudi 3.6.1.

3.6.4. Dostop do javnih ključev ponudnika storitev zaupanja

Javni ključi so vsebovani v digitalnih potrdilih korenskih overiteljev RekonoQTSA in enot za časovno žigosanje RekonoQTSU. Digitalno potrdilo posamezne enote za časovno žigosanje je glede na zahtevo uporabnika oziroma zahtevke za izdajo časovnega žiga (glej tudi 3.7.1) vsebovano v izdanem časovnem žigu. Korenska potrdila RekonoQTSU so objavljena na javni spletni strani ponudnika storitev zaupanja Rekono.TSP navedeni v poglavju 2.5. Naročniki ali tretje strani lahko pridobijo potrdila javnih ključev ponudnika storitev tudi preko e-poštnega sporočila poslanega na naslov naveden v poglavju 3.2.2.

3.6.5. Obdobje uporabe in obnova parov ključev ponudnika storitev

3.6.5.1. Korenski overitelji

Obnova para ključev korenskih overiteljev RekonoQTSA se izvede vsaj pet let pred iztekom veljavnosti digitalnega potrdila pripadajočega javnega ključa.

Posamezni zasebni ključ korenskih overiteljev se uporablja za podpisovanje CRL in potrdil OCSP do izteka veljavnosti pripadajočega digitalnega potrdila.

Postopek obnove se izvede na način kot prvo tvorjenje para ključev (glej 3.6.1).

3.6.5.2. Enote za časovno žigosanje

Obnova para ključev enot za časovno žigosanje RekonoQTSU se izvede pred iztekom uporabe zasebnega podpisnega ključa enote za časovno žigosanje. Zasebni podpisni ključ enot za časovno žigosanje se uporablja za podpisovanje časovnih žigov največ eno (1) leto in trideset (30) dni.

Postopek obnove se izvede na način kot prvo tvorjenje para ključev (glej 3.6.1).

3.6.6. Konec obdobja uporabe zasebnih ključev in uničenje

Rekono.TSP jamči, da ne bo uporabljal zasebnih ključev storitve RekonoQTSA po izteku obdobja uporabe.

Zasebni ključi se po izteku obdobja uporabe uničijo na način, da jih ni možno povrniti. Postopek se izvede z mehanizmi varnostnega strojnega modula, na katerem se ključi nahajajo oziroma uporabljajo.

3.6.7. Nadzor življenjskega cikla strojnega varnostnega modula

Rekono.TSP skrbi za varnost strojnega varnostnega modula skozi celo obdobje uporabe, in sicer:

- da je bil dostavljen na naslov Rekono d.o.o. v originalni embalaži izdelovalca in da varnostne nalepke na ohišju niso poškodovane;
- da ni bil ogrožen v času hrambe ali namestitve;
- da je tvorjenje in aktiviranje ključev izvedeno le s strani zaupanja vrednih oseb v nadzorovanem okolju;
- da deluje brez napak;
- da so ključi v strojnem varnostnem modulu uničeni ob koncu uporabe modula.

3.7. Časovno žigosanje

Storitev kvalificiranega elektronskega časovnega žigosanja RekonoQTSA izdaja časovne žige v skladu s profilom za časovne žige, kot je opredeljeno v ETSI EN 319 422 [15] in RFC 3161 [4].

Kvalificirani elektronski časovni žigi imajo naslednje lastnosti:

- vsebuje identifikacijsko oznako (OID) v skladu s temi RekonoQTSA Pravili delovanja;
- vsak kvalificiran elektronski časovni žig vsebuje edinstven identifikator (serialNumber);
- vir časa, ki ga uporablja TSU pri izdelavi časovnih žigov, je povezan z vsaj enim laboratorijem UTC (k) s seznama Bureau International des Poids et Mesures (BIPM, <http://www.bipm.org/>);
- časovni vir se sinhronizira z UTC z odstopanjem, ki ne presega ene (1) sekunde;
- če časovni vir, ki ga uporablja TSU, ni v okviru dovoljenega odstopanja, se časovni žig ne izda;
- zapis časovnega žiga vsebuje vrednost "hash", ki jo naročnik pošlje v svoji zahtevi;

- elektronski časovni žig se podpiše s ključem TSU, ki se uporablja izključno za ta namen;
- ožigosan je z naprednim elektronskim žigom kvalificiranega ponudnika storitev zaupanja za elektronske časovne žige.

3.7.1. Zahteva za izdajo elektronskega časovnega žiga

Zahteva za izdajo elektronskega časovnega žiga, ki jo pošlje naročnik, mora biti v skladu z RFC 3161 [4].

Podatek "hash", za katerega je zahtevan elektronski časovni žig, mora biti eden od naslednjih algoritmov:

- sha-256 (OID: 2.16.840.1.101.3.4.2.1);
- sha-384 (OID: 2.16.840.1.101.3.4.2.2);
- sha-512 (OID: 2.16.840.1.101.3.4.2.3).

Zahteva lahko vsebuje naslednja RFC 3161 razširitvena polja:

- reqPolicy,
- nonce; in
- certReq.

3.7.2. Oblika in vsebina časovnega žiga

Odgovor (žeton časovnega žiga) na zahtevo za izdajo elektronskega časovnega žiga, ki ga vrne enota za časovno žigovanje, je v skladu z RFC 3161 [4]. V skladu z ETSI EN 319 422 [15] vsebuje vsaj naslednja razširitvena polja:

- accuracy; in
- nonce (če je poslano v zahtevi).

Polje nonce vsebuje isto vrednost, ki je bila v zahtevi za izdajo časovnega žiga, če je bilo polje nonce v zahtevku prisotno.

Odgovor vedno vsebuje tudi:

- identifikacijsko oznako (OID) ponudnika storitev (razširitveno polje TSAPolicyId); in
- qcStatement "esi4-qtstStatement-1" v skladu z ETSI EN 319 422.

Časovni žigi so podpisani z zasebnim ključem enote za časovno žigovanje, na kateri je bil časovni žig ustvarjen. Glede na verigo zaupanja (RSA ali ECC) so časovni žigi podpisani z eno od sledečih podpisnih shem:

- sha256WithRSA (OID: 1.2.840.113549.1.1.11); ali
- ecdsa-with-SHA384 (OID: 1.2.840.10045.4.3.3).

Glede na verigo zaupanja (RSA ali ECC) se uporabljalo sledeči algoritmi za zasebne ključe enot za časovno žigovanje:

- TSU ključi generirani pred 06.05.2022:

- RSA (OID: 1.2.840.113549.1.1.1) dolžine 2048;
- secp384r1/P-384 (OID: 1.3.132.0.34)
- TSU ključki generirani po 06.05.2022:
 - RSA (OID: 1.2.840.113549.1.1.1) dolžine 3072;
 - secp384r1/P-384 (OID: 1.3.132.0.34)

3.7.3. Sinhronizacija časa z UTC

Ura enote za časovno žigosanje (TSU) se sinhronizira z UTC [16] z odstopanjem, ki ne presega ene (1) sekunde. Vir časa, ki ga uporablja TSU pri izdelavi časovnih žigov, je povezan z vsaj enim laboratorijem UTC (k) s seznama Bureau International des Poids et Mesures (BIPM, <http://www.bipm.org/>). Sinhronizacija se izvaja po protokolu NTP.

3.8. Fizično varovanje in kontrola okolja

Varnostni ukrepi na nivoju fizičnega okolja so opisani v interni dokumentaciji ponudnika storitev Rekono d.o.o. Dokumentacija oziroma posamezni deli so lahko na voljo za vpogled vsaki strani, ki izrazi interes in dokaže, da je takšno razkritje potrebno. Oceno je izvedel neodvisni revizijski in certifikacijski organ. Ocenjevanje in certificiranje se redno ponavljata v skladu z ISO/IEC 27001.

3.9. Operativno upravljanje varnosti sistemov

Strojna in programska oprema, ki jo uporablja Rekono.TSP, so standardni (angl. off-the-shelf) produkti, ki so dodatno varnostno okrepljeni po priporočilih CIS Benchmarks (<https://www.cisecurity.org/cis-benchmarks/>).

Varnostni ukrepi na nivoju sistemov, ki jih Rekono.TSP uporablja za izvajanje storitev, so opisani v interni dokumentaciji ponudnika storitev Rekono d.o.o. Dokumentacija oziroma posamezni deli so lahko na voljo za vpogled vsaki strani, ki izrazi interes in dokaže, da je takšno razkritje potrebno. Oceno je izvedel neodvisni revizijski in certifikacijski organ. Ocenjevanje in certificiranje se redno ponavljata v skladu z ISO/IEC 27001.

3.10. Varnostne kontrole na ravni računalniškega omrežja

Računalniška mreža, v kateri so nameščeni sistemi ponudnika storitev zaupanja, je razdeljena na več segmentov. Ločevanje in nadzor mrežnega prometa med segmenti se zagotavlja z uporabo požarnih zidov z IPS funkcionalnostjo. Do posameznih segmentov in strežnikov je dovoljen samo eksplicitno specificiran mrežni promet nujno potreben za posamezno storitev.

3.10.1. Postopki za odzivanje na varnostne incidente in nepravilnosti

Overitelj izvaja postopke za odzivanje na varnostne incidente in nepravilnosti v skladu z ISO/IEC 27001. Oceno postopkov je izvedel neodvisni revizijski in certifikacijski organ. Ocenjevanje in certificiranje se redno ponavljata v skladu z ISO/IEC 27001.

3.11. Zbiranje dokazov

Overitelj beleži naslednje vrste dogodkov:

- dogodki na operacijskem sistemu, programski in strojni opremi ponudnika storitev;
- dogodki v zvezi z zasebnimi ključi, ki se porabljajo za digitalno podpisovanje časovnih žigov;
- dogodki v zvezi z varnostno politiko in upravljanjem informacijskega sistema ponudnika storitev;
- dogodki v zvezi z varnostno politiko in upravljanjem komunikacijskega sistema;
- dogodki v zvezi s sinhronizacijo ure z referenčnimi viri.

Zapis dogodka v elektronski ali pisni obliki vsebuje datum in čas dogodka, in če je tehnično izvedljivo tudi enoličen identifikator osebe, ki je dogodek povzročila.

Rekono.TSP zbira in beleži v elektronski ali pisni obliki tudi podatke, ki vplivajo na varnost, niso pa del komunikacijsko informacijskega sistema overitelja:

- dogodke v zvezi s fizičnim dostopom do sistemov ponudnika storitev zaupanja ter fizično lokacijo;
- kadrovske spremembe osebja ponudnika storitev zaupanja.

3.12. Upravljanje kontinuitete poslovanja

Rekono.TSP ima vzpostavljeno storitev na več ločenih lokacijah in pri več neodvisnih ponudnikih varnih sistemskih prostorov. Upravljanje kontinuitete poslovanja je opredeljeno v internem dokumentu Politika neprekinjenega poslovanja storitev Rekono. Oceno postopkov je izvedel neodvisni revizijski in certifikacijski organ. Ocenjevanje in certificiranje se redno ponavljata v skladu z ISO/IEC 27001.

3.13. Prenehanje delovanja ponudnika storitev

V primeru, če bo Rekono.TSP prenehal z izvajanjem storitev zaupanja, bo o nameri prekinitve delovanja obvestil nacionalni nadzorni organ.

Poleg tega velja naslednje:

- a) Rekono.TSP vzdržuje in po potrebi posodablja načrt prekinitve delovanja.
- b) V primeru, če bo Rekono.TSP prenehal z izvajanjem storitev zaupanja, bo izvedel vsaj sledeče:
 - obvestil vse trenutne naročnike vsaj devetdeset (90) dni pred namenom prenehanja delovanja;
 - uničil vse zasebne ključe, ki se uporabljajo v okviru storitve časovnega žigosanja na način, da ključev ne bo možno povrniti oziroma ponovno uporabiti;
 - preklical potrdila javnih ključev za overjanje časovnih žigov;
 - ukinil avtorizacije dostopa vsem pogodbenim izvajalcem;
 - če bo možno, prenesel naročniške pogodbe za izvajanje storitve časovnega žigosanja na drugega ponudnika storitev zaupanja;
- c) za razumen čas zagotovil objavo potrdil javnih ključev storitve časovnega žigosanja ali prenesel obveznost na drugega ponudnika storitev.

4. DODATKI

4.1. Definicije in okrajšave

Splošne definicije so povzete po eIDAS [6] in ETSI TR 119 001 [7]:

Digitalni podpis	Je kriptografska preobrazba niza podatkov ali dodan niz podatkov, ki omogoča prejemniku dokazovanje vira in celovitosti podatkov ter zaščito pred ponarejanjem, npr. s strani prejemnika.
Elektronski podpis	Je niz podatkov v elektronski obliki, ki so dodani k drugim podatkom v elektronski obliki ali so z njimi logično povezani in jih podpisnik uporablja za podpisovanje.
Napredni elektronski podpis	Je elektronski podpis, ki izpolnjuje naslednje zahteve: <ul style="list-style-type: none"> a) enolično je povezan s podpisnikom; b) z njim je mogoče identificirati podpisnika; c) ustvari se na podlagi podatkov za ustvarjanje elektronskega podpisa, ki jih podpisnik z visoko stopnjo zaupanja lahko uporablja izključno pod svojim nadzorom, in d) s podatki, ki so na ta način podpisani, je povezan tako, da je opazna vsaka naknadna sprememba podatkov.
Potrdilo za elektronski podpis	Pomeni elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega podpisa s fizično osebo in potrjuje vsaj ime ali psevdonim te osebe.
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	Je elektronski žig, ki izpolnjuje naslednje zahteve: <ul style="list-style-type: none"> 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

	<p>ustvarjalec žiga z visoko stopnjo zaupanja in pod svojim nadzorom lahko uporablja za ustvarjanje elektronskega žiga, in</p> <p>d) povezan je s podatki, na katere se nanaša, in sicer tako, da je mogoče zaslediti vsako naknadno spremembo teh podatkov.</p>
Ustvarjalec žiga	Pomeni pravno osebo, ki ustvari elektronski žig.
Podatki za ustvarjanje elektronskega žiga	Pomenijo enolične podatke, ki jih ustvarjalec elektronskega žiga uporabi za ustvarjanje elektronskega žiga.
Potrdilo za elektronski žig	Pomeni elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega žiga s pravno osebo in potrjuje ime te osebe.
Informacijski sistem	Je sistem za oblikovanje, pošiljanje, prejemanje, shranjevanje in druge obdelave podatkov v elektronski obliki.
Potrdilo javnega ključa	Je javni ključ imetnika, skupaj z nekaterimi drugimi informacijami postane digitalno podpisan z zasebnim ključem overitelja, ki ga je izdal.
Digitalno potrdilo	Glej "Potrdilo javnega ključa".
Potrdilo	Sinonim za potrdilo javnega ključa oziroma digitalno potrdilo.
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 digitalnih potrdil.
Podatki za ustvarjanje elektronskega podpisa	Pomeni enolične podatke, ki jih podpisnik uporablja za ustvarjanje elektronskega podpisa.
Podatki za preverjanje elektronskega podpisa	So edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa.
Podpisnik	Je fizična oseba, ki ustvari elektronski podpis.

Ponudnik zaupanja	storitev	Pomeni fizično ali pravno osebo, ki zagotavlja eno ali več storitev zaupanja kot ponudnik kvalificiranih ali nekvalificiranih storitev zaupanja.
Kvalificirana zaupanja	storitev	Pomeni storitev zaupanja, ki izpolnjuje zadevne zahteve Uredbe eIDAS [6].
Sredstvo za elektronsko podpisovanje		Je sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz Zakona o elektronskem poslovanju in elektronskem podpisu.
Sredstvo za preverjanje elektronskega podpisa		Je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa.
Naročnik (ang. Subscriber)		Fizična oseba ali poslovni subjekt, ki zahteva dostop do storitve časovnega žiga.
Korenski overitelj		Izdajatelj digitalnih potrdil, ki v okviru overiteljeve infrastrukture javnih ključev predstavlja izhodišče zaupanja (angl. trust point). Korenski izdajatelj se uporablja le za izdajo digitalnih potrdil podrejenim izdajateljem.
Podrejeni overitelj		Izdajatelj digitalnih potrdil, ki mu je digitalno potrdilo izdal korenski oziroma nadrejeni izdajatelj. Podrejeni izdajatelj izdaja digitalna potrdila naročnikom oziroma končnim uporabnikom ali drugim podrejenim izdajateljem.
Poslovni subjekt		Fizične in pravne osebe, ki opravljajo poslovno dejavnost.
Organizacija		Sinonim za poslovni subjekt.
Uporabnik potrdila		Sinonim za imetnika potrdila.
Elektronski 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		Pomeni elektronski časovni žig, ki izpolnjuje zahteve iz člena 42 uredbe eIDAS;
Žeton časovnega žiga (angl. time-stamp token, TST)		Podatkovni niz, 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.

Enota za časovno žigosanje (angl. time-stamping unit, TSU)	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.
Rekono.ID	Storitev Rekono (https://www.rekono.si , https://idp.rekono.si) za elektronsko identifikacijo.

Okrajšave:

ASN.1	Abstract Syntax Notation One
CA	Certification Authority
PKI	Public Key Infrastructure
CRL	Certificate Revocation List (seznam preklicanih digitalnih potrdil)
OID	Object Identifier
PKIX	Internet X.509 Public Key Infrastructure
SHA	Secure Hash Algorithm
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
RDN	Relative Distinguished Name
CN	Common Name
DN	Distinguished Name
PMA	Policy Management Authority
RSA	Asimetrični kriptografski sistem Rivest–Shamir–Adleman
ECC	Asimetrični kriptografski sistem (Elliptic-curve cryptography), ki temelji na algebrski strukturi eliptičnih krivulj nad končnimi polji
HSM	Hardware Security Module (strojni varnostni modul)
DMZ	Demilitarized Zone
IPS	Intrusion prevention system
OCSP	Online Certificate Status Protocol
POE	Projektna organizacijska enota
TSP	Trust Service Provider (ponudnik storitev zaupanja)
NTP	Network time protocol
BIMP	Bureau International des Poids et Mesures (https://www.bipm.org)
UTC	Coordinated Universal Time
TSA	Time-stamp authority
TST	Žeton časovnega žiga (angl. time-stamp token)

- TSU Nabor strojne in programske opreme, ki se upravlja kot enota in ima naenkrat en ključ za podpisovanje časovnih žigov (angl. Time-Stamping Unit)
- OI Organization Identifier (polje organizationIdentifier v razločevalnem imenu potrdila)

4.2. Reference

- [1] RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"
- [2] EN 319 411-1 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements"
- [3] RFC 5280 "Internet X.509 Public Key Infrastructure Certificates and Certificate Revocation List (CRL) Profile"
- [4] RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"
- [5] EN 319 401 "General Policy Requirements for Trust Service Providers"
- [6] eIDAS "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 "
- [7] ETSI TR 119 001 "Definitions and abbreviations"
- [8] EN 319 412 Part1: "Overview and common data structures"
- [9] EN 319 412 Part2: "Certificate profile for certificates issued to natural persons"
- [10] EN 319 412 Part3: "Certificate profile for certificates issued to legal persons"
- [11] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 "on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market"
- [12] EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps"
- [13] Rekono.TSP Pravila delovanja

- [14] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".
- [15] EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
- [16] UTC: Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
- [17] ETSI TS 119 312: "Electronic signatures and Infrastructures (ESI); Cryptographic Suites"