Ponudnik storitev zaupanja Rekono.TSP
Pravila delovanja
(Certification Practice Statement)

Ljubljana, 6. april 2020
Verzija 1.0 (javna)

Zaščita dokumenta

Skrbnik dokumenta:

Odobritelj dokumenta: **direktor podjetja Rekono**

Področje veljavnosti: **delovna področja podjetja Rekono, vezana na izvajanje storitev e-identifikacije Rekono in oddaljenega e-podpisa Rekono.Sign**

Nadzor različic dokumenta

Izvirni dokument je shranjen v elektronski obliki, različice dokumenta so pod nadzorom. Morebitne papirne ali elektronske kopija tega dokumenta lahko obstaja 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:

Razl.	Datum	Opis / opomba
1.0	06.04.2020	Obsega storitve zaupanja za: • digitalna potrdila za fizične osebe za napreden elektronski podpis • digitalna potrdila za pravne osebe za napreden elektronski pečat • digitalna potrdila za avtentikacijo • napreden elektronski časovni žig

Kazalo

1. UVOD 10
1.1. Pregled 10
1.2. Naziv dokumenta in identifikacijske oznake digitalnih potrdil 13
1.3. Udeleženci infrastrukture javnih ključev 15
1.3.1. Overitelji 15
1.3.2. RekonoRA (Registration Authority - RA) 17
1.3.3. Naročniki in imetniki digitalnih potrdil 17
1.3.4. Tretje osebe 18
1.3.5. Ostali udeleženci 18
1.4. Namen uporabe digitalnih potrdil 18
1.4.1. Dovoljena uporaba digitalnih potrdil 18
1.4.2. Nedovoljena uporaba digitalnih potrdil 19
1.5. Upravljanje s pravili delovanja 19
1.5.1. Organizacija, ki upravlja s pričujočim dokumentom 19
1.5.2. Kontaktni podatki 19
1.5.3. Oseba, ki ugotavlja ustreznost Politike 19
1.5.4. Postopek odobritve politike delovanja overitelja 19
1.6. Definicije in okrajšave 19
2. objave in repozitorij 25
2.1. Repozitorij 25
2.2. Objave informacij o digitalnih potrdilih 25
2.3. Čas in pogostost objav 25
2.4. Dostop do podatkov v repozitoriju 25
3. Prepoznavanje in preverjanje istovetnosti 26
3.1. Določanje imen 26
3.1.1. Vrste imen 26
3.1.2. Potreba po smiselnosti imen 29
3.1.3. Anonimnost imetnikov in uporaba psevdonimov 29
3.1.4. Pravila za interpretacijo različnih oblik imen 29
3.1.5. Edinstvenost imen 29
3.1.6. Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk 29
3.2. Prva registracija 30
3.2.1. Metode dokazovanja lastništva zasebnega ključa 30
3.2.2. Preverjanje istovetnosti organizacije 30
3.2.3. Preverjanje istovetnosti za fizične osebe 30
3.2.4. Podatki o imetnikih digitalnih potrdil, ki se ne preverjajo 30
3.2.5. Preverjanje pooblastil 30
3.2.6. Merila za medsebojno povezovanje 30

3.3. Preverjanje istovetnosti pri obnovi digitalnega potrdila 31
3.3.1. Preverjanje istovetnosti pri rutinski obnovi digitalnih potrdil 31
3.3.2. Preverjanje istovetnosti pri obnovi digitalnega potrdila po preklicu 31
3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila ... 31
4. Upravljanje z digitalnimi potrdili 32
4.1. Vloga za izdajo digitalnega potrdila 32
4.1.1. Kdo lahko zaprosi za izdajo digitalnega potrdila 32
4.1.2. Postopek obdelave vlog in odgovornosti 32
4.2. Obdelava vloge za izdajo digitalnega potrdila 32
4.2.1. Postopki identifikacije in avtentikacije 32
4.2.2. Odobritev ali zavrnitev izdaje digitalnega potrdila 33
4.2.3. Čas za obdelavo vloge za izdajo digitalnega potrdila 33
4.3. Izdaja digitalnega potrdila 33
4.3.1. Postopki overitelja ob izdaji digitalnega potrdila 33
4.3.2. Obvestilo imetniku o izdaji digitalnega potrdila 34
4.4. Prevzem digitalnega potrdila 34
4.4.1. Postopek potrditve prevzema digitalnega potrdila 34
4.4.2. Objava digitalnega potrdila 34
4.4.3. Obveščanje drugih udeležencev o izdaji digitalnega potrdila 34
4.5. Uporaba ključev in digitalnih potrdil 34
4.5.1. Uporaba ključev in digitalnih potrdil s strani imetnikov 34
4.5.2. Uporaba digitalnih potrdil s strani tretjih oseb 35
4.6. Obnova digitalnih potrdil brez spremembe ključev 35
4.7. Obnova digitalnih potrdil 35
4.7.1. Okoliščine obnove digitalnih potrdil 35
4.7.2. Kdo lahko zahteva obnovo digitalnega potrdila 35
4.7.3. Obdelava zahtevkov za obnovo digitalnega potrdila 36
4.7.4. Obvestilo imetnikov o izdaji novega digitalnega potrdila 36
4.7.5. Postopek potrditve prevzema novega digitalnega potrdila 36
4.7.6. Objava obnovljenega digitalnega potrdila 36
4.7.7. Obveščanje drugih uporabnikov o izdaji digitalnega potrdila 36
4.8. Sprememba digitalnega potrdila 36
4.8.1. Okoliščine, v katerih se izvede sprememba digitalnih potrdil 36
4.8.2. Kdo lahko zahteva spremembo digitalnih potrdil 36
4.8.3. Obdelava zahtevkov za spremembo digitalnih potrdil 36
4.8.4. Obvestilo imetniku o izdaji spremenjenega digitalnega potrdila 36
4.8.5. Postopek potrditve prevzema spremenjenega digitalnega potrdila 36

4.8.6. Objava spremenjenega digitalnega potrdila 37
4.8.7. Obveščanje drugih udeležencev o izdaji spremenjenega digitalnega potrdila 37
4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila 37
4.9.1. Okoliščine preklica 37
4.9.2. Kdo lahko zahteva preklic 38
4.9.3. Postopki za preklic 38
4.9.4. Čas za posredovanje vloge za preklic 38
4.9.5. Čas od vloge za preklic do preklica 39
4.9.6. Obveza preverjanja registra preklicanih potrdil 39
4.9.7. Pogostost objav registrov preklicanih potrdil 39
4.9.8. Dovoljene zakasnitve sprotnega preverjanja statusa digitalnih potrdil 39
4.9.9. Storitev sprotnega preverjanja statusa digitalnih potrdil 39
4.9.10. Obveza sprotnega preverjanja statusa digitalnih potrdil 39
4.9.11. Ostale oblike objavljanja preklicanih digitalnih potrdil 39
4.9.12. Posebne zahteve glede zlorabe ključa 39
4.9.13. Okoliščine za začasno ukinitev veljavnosti (suspenz) digitalnega potrdila 40
4.9.14. Kdo lahko zahteva suspenz ali ukinitev suspenza digitalnega potrdila 40
4.9.15. Postopki za suspenz ali ukinitev suspenza digitalnega potrdila 40
4.9.16. Omejitve obdobja začasne ukinitve veljavnosti 40
4.10. Storitve objavljanja statusa digitalnih potrdil 40
4.10.1. Tehnične lastnosti storitve 40
4.10.2. Razpoložljivost storitve dostopa do registra preklicanih potrdil 40
4.10.3. Dodatne možnosti 40
4.11. Trajanje naročniškega razmerja 40
4.12. Varnostno kopiranje in odkrivanje zasebnega ključa 41
5. fizično varovanje, organizacijski varnostni ukrepi in zahteve za osebje .. 42
5.1. Fizično varovanje 42
5.2. Organizacijski varnostni ukrep 42
5.2.1. Organizacija ponudnika storitev zaupanja 42
5.2.2. Število oseb, potrebnih za izvedbo postopka 43
5.2.3. Preverjanje istovetnosti operativnega osebja 43
5.2.4. Nezdružljivost nalog 43
5.3. Zahteve za osebje overitelja 43
5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje 43
5.3.2. Preverjanje primernosti osebja 43
5.3.3. Usposabljanje osebja 44

5.3.4. Pogostost dodatnih usposabljanj 44
5.3.5. Kroženje med delovnimi mesti 44
5.3.6. Ukrepi ob kršitvah pooblastil 44
5.3.7. Zahteve za pogodbene in zunanje izvajalce 44
5.3.8. Dokumentacija za osebje overitelja 44
5.4. Postopki zbiranja in upravljanja revizijskih sledi 44
5.4.1. Vrste beleženih dogodkov 44
5.4.2. Pogostost pregleda revizijskih dnevnikov 45
5.4.3. Obdobje hranjenja revizijskih dnevnikov 45
5.4.4. Zaščita revizijskih dnevnikov 45
5.4.5. Varnostne kopije revizijskih dnevnikov 46
5.4.6. Način zbiranja revizijskih dnevnikov 46
5.4.7. Obveščanje povzročitelja dogodka 46
5.4.8. Ocena in odprava ranljivosti 46
5.5. Arhiviranje podatkov 46
5.5.1. Vrste arhiviranih podatkov 46
5.5.2. Čas hrambe 47
5.5.3. Zaščita arhiva 47
5.5.4. Varnostna kopija arhiva 47
5.5.5. Zahteva za časovno žigosanje zapisov 47
5.5.6. Arhiviranje (notranje / zunanje) 47
5.5.7. Postopek za dostop do arhivskih podatkov in njihova verifikacija 47
5.6. Obnova digitalnega potrdila overitelja 47
5.7. Postopki v primeru ogrožanja zasebnega ključa in okrevalni načrt .. 48
5.7.1. Postopki za odzivanje na varnostne incidente in nepravilnosti . 48
5.7.2. Uničenje programske, strojne opreme ali podatkov 48
5.7.3. Ogrožanje overiteljevega zasebnega ključa 48
5.7.4. Okrevalni načrt v primeru naravne ali druge nesreče 48
5.8. Prenehanje delovanja overitelja 48
6. TEhnične varnostne zahteve 49
6.1. Tvorjenje in namestitev para ključev 49
6.1.1. Tvorjenje para ključev 49
6.1.2. Prenos zasebnega ključa imetniku 49
6.1.3. Prenos imetnikovega ključa overitelju 49
6.1.4. Dostop do overiteljevega javnega ključa 50
6.1.5. Dolžina asimetričnih ključev 50
6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov 50
6.1.7. Nameni ključev in digitalnih potrdil (X.509 v3 keyUsage) 50

6.2. Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov 51
6.2.1. Standardi za kriptografski modul 51
6.2.2. Nadzor zasebnega ključa z (n od m) pooblaščenimi osebami .. 51
6.2.3. Odkrivanje (ang. Escrow) zasebnega ključa 51
6.2.4. Varnostno kopiranje zasebnih ključev 51
6.2.5. Arhiviranje zasebnega ključa 52
6.2.6. Prenos zasebnega ključa v kriptografski modul in iz njega 52
6.2.7. Hranjenje overiteljevega zasebnega ključa v kriptografskem modulu 52
6.2.8. Postopek za aktiviranje zasebnega ključa 52
6.2.9. Postopek za dezaktiviranje zasebnega ključa 53
6.2.10. Postopek za uničenje zasebnega ključa 53
6.2.11. Stopnja varnosti kriptografskih modulov 53
6.3. Ostali vidiki upravljanja s pari ključev 53
6.3.1. Arhiviranje javnega ključa 53
6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil 53
6.4. Aktivacijski podatki 54
6.4.1. Generiranje in nameščanje aktivacijskih podatkov 54
6.4.2. Zaščita aktivacijskih podatkov 54
6.4.3. Drugi vidiki aktivacijskih podatkov 54
6.5. Varnostne zahteve za računalnike 54
6.5.1. Specifične varnostne zahteve za računalnike 54
6.5.2. Nivo varnostne zaščite računalnikov 54
6.6. Tehnični nadzor življenjskega cikla overitelja 54
6.6.1. Nadzor razvoja sistema 54
6.6.2. Upravljanje varnosti 54
6.6.3. Varnostna ocena (angl. Security Ratings) življenskega cikla 54
6.7. Varnostne kontrole na ravni računalniškega omrežja 55
6.8. Časovno žigosanje 55
7. profil digitalnih potrdil in registrov preklicanih potrdil 56
7.1. Profil digitalnih potrdil 56
7.1.1. Različica digitalnih potrdil 56
7.1.2. Razširitvena polja 56
7.1.3. Identifikacijske oznake (angl. object identifiers) algoritmov 58
7.1.4. Oblike imen 58
7.1.5. Omejitve imen 58
7.1.6. Identifikacijska oznaka digitalnega potrdila 58
7.1.7. Uporaba omejitve imen 58
7.1.8. Specifični podatki o politiki (angl. Policy Qualifiers extension) . 58

7.1.9. Procesiranje oznake kritičnosti razširitvenih polj digitalnega potrdila 58
7.2. Profil registra preklicanih digitalnih potrdil 59
7.2.1. Različica 59
7.2.2. Razširitvena polja registrov preklicanih potrdil 59
7.3. Profil OCSP 59
8. preverjanje skladnosti in ostale oblike nadzora 60
9. ostale poslovne in pravne zadeve 61
9.1. Cenik 61
9.1.1. Cena izdaje in upravljanja digitalnih potrdil 61
9.1.2. Cena dostopa do digitalnih potrdil v javnem imeniku 61
9.1.3. Cena dostopa do registra preklicanih potrdil 61
9.1.4. Cena ostalih storitev 61
9.1.5. Pravica vračila 61
9.2. Finančna odgovornost 61
9.2.1. Zavarovanje odgovornosti 61
9.2.2. Druge oblike zavarovanja 61
9.2.3. Zavarovanja ali jamstva za končne uporabnike 61
9.3. Zaupnost poslovnih informacij 61
9.3.1. Obseg zaupnih poslovnih informacij 61
9.3.2. Informacije izven obsega zaupnih poslovnih informacij 62
9.3.3. Odgovornost za zagotavljanje zaupnosti poslovnih informacij . 62
9.4. Varovanje osebnih podatkov 62
9.4.1. Načrt zagotavljanja varovanja osebnih podatkov 62
9.4.2. Obseg varovanih osebnih podatkov 62
9.4.3. Osebni podatki, ki se ne obravnavajo kot zaupni 62
9.4.4. Odgovornost glede varovanja osebnih podatkov 62
9.4.5. Privolitev posameznika za uporabo osebnih podatkov 62
9.4.6. Posredovanje osebnih podatkov v sodnih in upravnih postopkih 63
9.4.7. Druge okoliščine posredovanja osebnih podatkov 63
9.5. Zaščita intelektualne lastnine 63
9.6. Odgovornost in jamstva 63
9.6.1. Odgovornost in jamstva overitelja 63
9.6.2. Odgovornost in jamstva prijavne službe 64
9.6.3. Odgovornost in jamstva imetnikov digitalnih potrdil 64
9.6.4. Odgovornost in jamstva tretjih oseb 64
9.6.5. Odgovornost in jamstva drugih udeležencev 64
9.7. Zanikanje odgovornosti 64
9.8. Omejitve odgovornosti 65

9.9. Poravnava škode 66
9.10. Začetek in prenehanje veljavnosti 66
9.10.1. Začetek veljavnosti 66
9.10.2. Prenehanje veljavnosti 66
9.10.3. Učinek in posledice prenehanja veljavnosti 66
9.11. Obvestila in komuniciranje z udeleženci 66
9.12. Spreminjanje dokumenta 66
9.12.1. Postopek uveljavitve sprememb 66
9.12.2. Postopek obveščanja in rok za pripombe 67
9.12.3. Spremembe, ki zahtevajo novo identifikacijsko oznako politike 67
9.13. Reševanje sporov 67
9.14. Veljavna zakonodaja 67
9.15. Skladnost s pravnimi akti 67
9.16. Splošne določbe 68
9.16.1. Ostali obvezujoči dokumenti 68
9.16.2. Prenos pravic in obveznosti 68
9.16.3. Spremembe okoliščin delovanja 68
9.16.4. Uveljavljanje (povračila stroškov v primeru sporov in izjeme) ... 68
9.16.5. Višja sila 68
9.17. Ostale določbe 68

1. UVOD

Pričujoči dokument opisuje pravila delovanja ponudnika storitev zaupanja Rekono.TSP, ki jih upravlja Rekono d.o.o.

1.1. Pregled

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

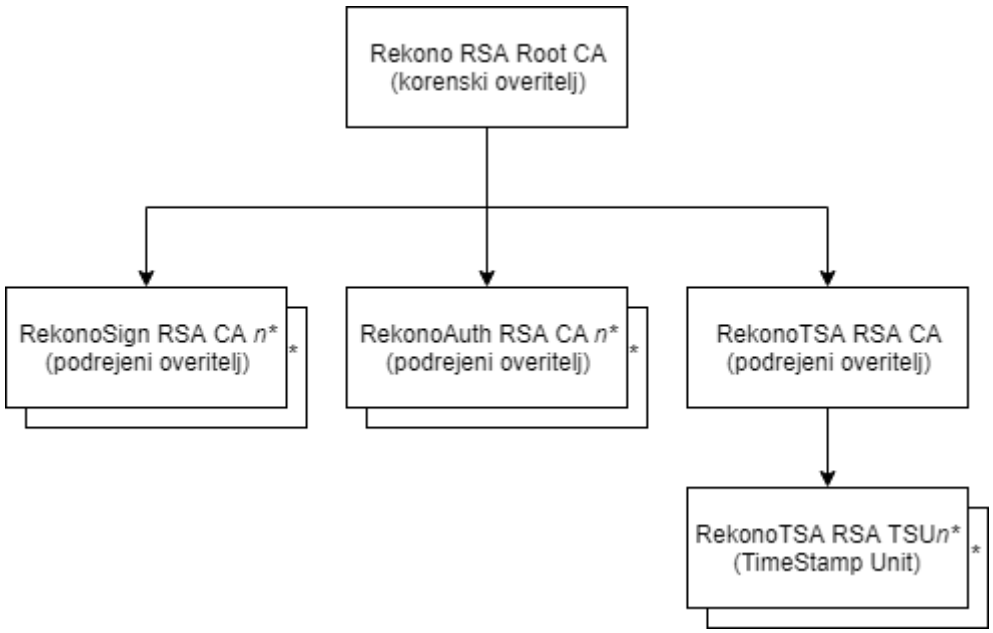
Pričujoči dokument, Rekono.TSP Pravila delovanja, vsebuje pogoje uporabe in opis pravil ter postopkov, ki jih izvaja Rekono d.o.o. za opravljanje storitev zaupanja, ki obsega registracijo naročnikov, izdajanje, obnovo in preklic digitalnih potrdil, objavo statusa digitalnih potrdil ter izdajanje naprednih elektronskih časovnih žigov. Rekono.TSP 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 storitev zaupanja.

Struktura dokumenta Rekono.TSP Pravila delovanja je usklajena z RFC 3647 [1]. Določena poglavja RFC 3647, ki niso uporabna za Rekono.TSP, so navedena, vendar namenoma puščena prazna in zato vsebujejo besedilo "Namenoma puščeno prazno".

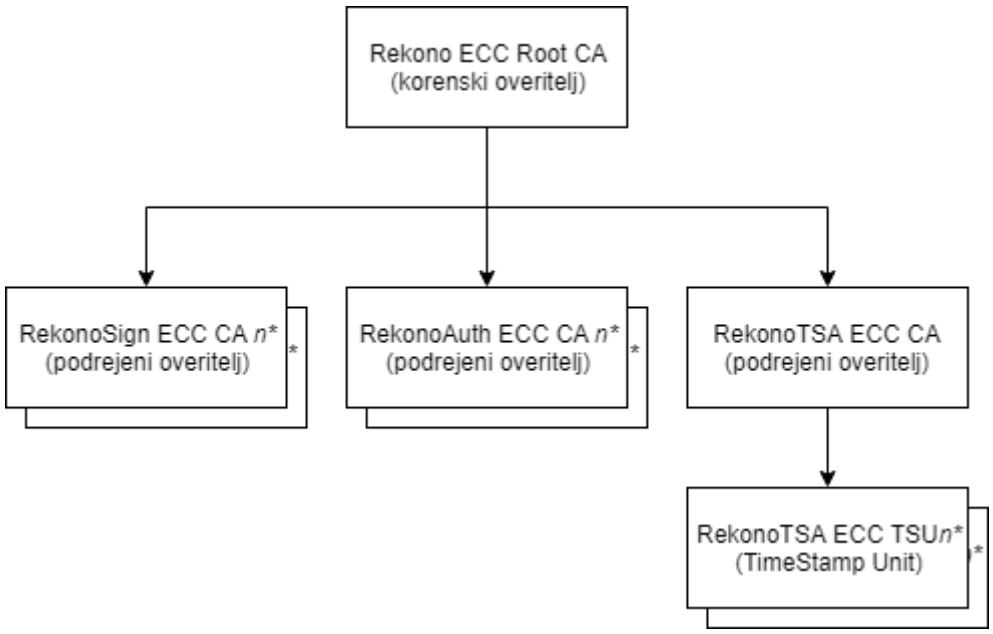
Vsebina dokumenta Rekono.TSP Pravila delovanja je usklajena z RFC 3647, [1], RFC 5280 [3], EN 319 401 [5] in EN 319 411-1 [2].

Za potrebe izvajanja storitev zaupanja ima Rekono d.o.o. vzpostavljeno lastno infrastrukturo javnih ključev Rekono.TSP, ki obsega korenskega overitelja, več podrejenih overiteljev ter registrov preklicanih digitalnih potrdil in izdajatelja elektronskih časovnih žigov. V okviru Rekono.TSP sta vzpostavljeni dve verigi zaupanja, in sicer veriga zaupanja, ki uporablja asimetrične ključe RSA in veriga zaupanja, ki uporablja asimetrične ključe ECC.

Sledeča slika prikazuje PKI hierarhijo overiteljev Rekono.TSP v verigi zaupanja z RSA ključi.



Sledeča slika prikazuje PKI hierarhijo overiteljev Rekono.TSP v verigi zaupanja z ECC ključi.



Overitelji Rekono.TSP verige zaupanja z RSA ključi in verige z ECC ključi imajo razločevalna imena kot je navedeno v spodnjih tabelah.

Opomba: Oznaka *n** v razločevalnih imenih podrejenih overiteljev pomeni številčno oznako instance podrejenega overitelja (npr.: "RekonoSign ECC CA1"). Za vsakega od podrejenih overiteljev je lahko ena ali več instanc, ki se praviloma nahajajo na različnih lokacijah. Instance posameznega podrejenega overitelja so med seboj enakovredne.

Tabela: Veriga zaupanja z RSA ključi

Korenski overitelj v verigi zaupanja z RSA ključi
CN=Rekono RSA Root CA,OI=VATSI-60762802,O=Rekono d.o.o.,C=SI
Podrejeni overitelji v verigi zaupanja z RSA ključi
CN=RekonoSign RSA CA*n**,OI=VATSI-60762802,O=Rekono d.o.o.,C=SI
CN=RekonoAuth RSA CA*n**,OI=VATSI-60762802,O=Rekono d.o.o.,C=SI
CN=RekonoTSA RSA CA,OI=VATSI-60762802,O=Rekono d.o.o.,C=SI

Tabela: Veriga zaupanja z ECC ključi

Korenski overitelj v verigi zaupanja z ECC ključi
CN=Rekono ECC Root CA,OI=VATSI-60762802,O=Rekono d.o.o.,C=SI
Podrejeni overitelji v verigi zaupanja z ECC ključi
CN=RekonoSign ECC CA*n**,OI=VATSI-60762802,O=Rekono d.o.o.,C=SI
CN=RekonoAuth ECC CA*n**,OI=VATSI-60762802,O=Rekono d.o.o.,C=SI
CN=RekonoTSA ECC CA,OI=VATSI-60762802,O=Rekono d.o.o.,C=SI

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

Overitelj Rekono.TSP izdaja digitalna potrdila naročnikom (glej tudi 1.3.3), ki so lahko:

- fizične osebe;
- fizične osebe, identificirane v povezavi s pravno osebo;
- pravni osebi, ki je lahko funkcija, organizacija, enota ali oddelek, opredeljen v povezavi s pravno osebo.

Pričujoči dokument, Rekono.TSP Pravila delovanja, opredeljuje sledeče kategorije digitalnih potrdil. izdane s strani overiteljev Rekono.TSP:

1. Digitalna potrdila za napredni elektronski podpis ustvarjen s storitvijo za digitalni podpis na daljavo RekonoSign
2. Digitalna potrdila za napredni elektronski žig ustvarjen s storitvijo za digitalni podpis na daljavo RekonoSign
3. Digitalna potrdila za storitev elektronskega časovnega žiga RekonoTSU
4. Digitalna potrdila za elektronsko avtentikacijo

V sledeči tabeli je podan pregled kategorij digitalnih potrdil, overiteljev, imetnikov in namen uporabe.

Opomba: Oznaka *[CA]* pri navedbi overiteljev v spodnji pomeni overitelja v vseh verigah zaupanja in vse instance.

Digitalno potrdilo	Overitelji	Imetniki	Namen uporabe
RekonoSign	RekonoSign *[CA]*	fizične osebe imetniki računa Rekono.ID	napredni elektronski podpis

RekonoSeal	RekonoSign *[CA]*	fizične osebe imetniki računa Rekono.ID, identificirane v povezavi s pravno osebo	napredni elektronski pečat
RekonoAuth	RekonoAuth *[CA]*	fizične osebe imetniki računa Rekono.ID	elektronska avtentikacija
RekonoTSU	RekonoTSA *[CA]*	strežniki storitve elektronskega časovnega žiga	elektronski časovni žig
RekonoOCSP	Rekono Root *[CA]* RekonoSign *[CA]* RekonoAuth *[CA]* RekonoTSA *[CA]*	Strežniki storitve OCSP	OCSP
RekonoPKI	Rekono Root *[CA]* RekonoSign *[CA]* RekonoAuth *[CA]* RekonoTSA *[CA]*	Infrastrukturna potrdila za upravljanje sistemov v okviru Rekono.TSP	Digitalni podpis

Vsaka kategorija digitalnih potrdil, ki je opredeljena v tem dokumentu, ima dodeljeno enolično identifikacijsko oznako (OID, Object Identifier) politike, v skladu s katero je bilo posamezno digitalno potrdilo izdano (glej poglavje 1.2).

1.2. Naziv dokumenta in identifikacijske oznake digitalnih potrdil

Naziv dokumenta, sl:	Rekono.TSP Pravila delovanja
Naziv dokumenta, en.:	Certification Practice Statement of the Rekono.TSP
Verzija:	1.0
Datum:	06.04.2020

Vsaka kategorija digitalnih potrdil 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.).

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

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 z RSA ključi:

Digitalno potrdilo	Identifikacijska oznaka (CertPolicyId)
RekonoSign	1.3.6.1.4.1.54579.1.1.1.1 iso.org.dod.internet.private.enterprise.rekono-pen(54579). rekono-pki(1).oids(1).dp-rsa(1).esign(1)
RekonoSeal	1.3.6.1.4.1.54579.1.1.1.2 iso.org.dod.internet.private.enterprise.rekono-pen(54579). rekono-pki(1).oids(1).dp-rsa(1).eseal(2)
RekonoAuth	1.3.6.1.4.1.54579.1.1.1.3 iso.org.dod.internet.private.enterprise.rekono-pen(54579). rekono-pki(1).oids(1).dp-rsa(1).auth(3)
RekonoTSU	1.3.6.1.4.1.54579.1.1.1.4 iso.org.dod.internet.private.enterprise.rekono-pen(54579). rekono-pki(1).oids(1).dp-rsa(1).tsu(4)
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 z ECC ključi:

Digitalno potrdilo	Identifikacijska oznaka (CertPolicyId)
RekonoSign	1.3.6.1.4.1.54579.1.1.2.1 iso.org.dod.internet.private.enterprise.rekono-pen(54579). rekono-pki(1).oids(1).dp-ecc(2).esign(1)
RekonoSeal	1.3.6.1.4.1.54579.1.1.2.2 iso.org.dod.internet.private.enterprise.rekono-pen(54579). rekono-pki(1).oids(1).dp-ecc(2).eseal(2)
RekonoAuth	1.3.6.1.4.1.54579.1.1.2.3 iso.org.dod.internet.private.enterprise.rekono-pen(54579). rekono-pki(1).oids(1).dp-ecc(2).auth(3)
RekonoTSU	1.3.6.1.4.1.54579.1.1.2.4 iso.org.dod.internet.private.enterprise.rekono-pen(54579). rekono-pki(1).oids(1).dp-ecc(2).tsu(4)
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 elektronskim časovnim žigom, ki so izdani v verigi zaupanja z RSA ključi:

RFC 3161 polje	Identifikacijska oznaka (TSAPolicyId)
TSTInfo policy	1.3.6.1.4.1.54579.1.1.3.1 iso.org.dod.internet.private.enterprise.rekono-pen(54579). rekono-pki(1).oids(1).ts-rsa(3).tsp(1)

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

RFC 3161 polje	Identifikacijska oznaka (TSAPolicyId)
TSTInfo policy	1.3.6.1.4.1.54579.1.1.4.1 iso.org.dod.internet.private.enterprise.rekono-pen(54579). rekono-pki(1).oids(1).ts-ecc(4).tsp(1)

Sledeče identifikacijske oznake (OIDs) so dodeljene digitalnim potrdilom, ki se uporabljajo interno za upravljanje infrastrukture in sistemov v okviru Rekono.TSP:

Digitalno potrdilo	Identifikacijska oznaka (CertPolicyId)
RekonoPKI	1.3.6.1.4.1.54579.1.1.0. {id} iso.org.dod.internet.private.enterprise.rekono-pen(54579). rekono-pki(1).oids(1).pki(0).{id} Opomba: vrednost {id} se dodeli interno.

1.3. Udeleženci infrastrukture javnih ključev

1.3.1. Overitelji

Overitelji digitalnih potrdil in izdajatelji elektronskih časovnih žigov, ki delujejo v okviru Rekono.TSP izvajajo storitve zaupanja v skladu s temi Rekono.TSP Pravili delovanja in dotično zakonodajo.

Rekono d.o.o. ima za izvajanje storitev zaupanja vzpostavljeno lastno infrastrukturo javnih ključev Rekono.TSP s korenskimi in podrejenimi izdajatelji ter izdajatelji časovnih žigov.

Korenski overitelji Rekono.TSP imajo samopodpisano digitalno potrdilo, ki je bilo izdano v okviru nadzorovanega postopka generiranja overiteljevih kriptografskih ključev (angl. Root Key Generation Ceremony). Korenski overitelji izdajajo le potrdila podrejenim overiteljem Rekono.TSP in potrdila za upravljanje korenskih overiteljev.

Podrejeni overitelji Rekono.TSP izdajajo digitalna potrdila naročnikom, ki so lahko fizične osebe ali pravne osebe (glej 1.3.3).

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

- RekonoPMA - POE za upravljanje (angl. Policy Management Authority – PMA)
- RekonoOA - POE za operativno delovanje (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.

1.3.1.1. RekonoPMA (Policy Management Authority (PMA))

Osebje RekonoPMA je odgovorno za:

- razvoj in vzdrževanje Rekono.TSP Pravil delovanja;
- razvoj in vzdrževanje drugih javnih dotičnih dokumentov (splošna pravila uporabe storitve …);
- potrditev osebja RekonoOA in RekonoRA;
- nadzor skladnosti delovanja z Rekono.TSP 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.

1.3.1.2. RekonoOA (Operations Authority (OA))

Osebje RekonoOA je odgovorno za:

- generiranje kriptografskih ključev storitev zaupanja v okviru Rekono.TSP, varno upravljanje zasebnih kriptografskih ključev storitev zaupanja in distribucijo javnih ključev overiteljev oziroma digitalnih potrdil overiteljev;
- vzpostavitev postopkov in informacijske podpore za delovanje storitev;
- izvedbo preklica digitalnih potrdil na zahtevo naročnikov oziroma imetnikov digitalnih potrdil;
- 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 Rekono.TSP Pravili delovanja;

- sodelovanje z RekonoPMA pri pripravi sprememb in novih verzij pravil delovanja;

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

1.3.2. RekonoRA (Registration Authority - RA)

Naloge RA v okviru storitev zaupanja so preverjanje identitete naročnikov oziroma imetnikov, obdelava vlog oziroma zahtevkov ter odobritev ali zavrnitev vlog oziroma zahtevkov za izdajo digitalnih potrdil.

Digitalna potrdila, ki jih izdajajo overitelji Rekono.TSP, lahko pridobijo le fizične ali pravne osebe, ki imajo račun Rekono.ID ustrezne ravni zanesljivosti.

Vsi postopki preverjanja identitete, pridobitve Rekono računa ustrezne ravni zanesljivosti in upravljanje identitete se izvajajo preko storitve Rekono (https://idp.rekono.si). Pridobitev, upravljanje in uporaba digitalnih potrdil, ki jih izdajajo overitelji Rekono.TSP so neločljivo povezani z Rekono računom, ki zagotavlja vse funkcije RA in tako predstavlja RekonoRA.

1.3.3. Naročniki in imetniki digitalnih potrdil

Naročnik je stranka, ki zahteva digitalno potrdilo v imenu ene ali več fizičnih oseb ali v imenu pravne osebe. Na primer, organizacija zahteva digitalna potrdila za svoje zaposlene. Imetnik digitalnega potrdila je entiteta, ki je identificirana kot imetnik zasebnega ključa, ki je povezan z javnim ključem, vsebovanem v digitalnem potrdilu, in je naveden kot v polju Imetnik (angl. Subject) digitalnega potrdila.

Naročnik ali imetnik digitalnega potrdila je lahko:

- fizična oseba;
- fizična oseba, identificirana v povezavi s pravno osebo oziroma organizacijo, ki ima status pravne osebe;
- pravna oseba, ki je lahko organizacija, enota ali oddelek, opredeljen v okviru organizacije.

Kadar je naročnik hkrati imetnik, je odgovoren za vse obveznosti v povezavi z uporabo digitalnega potrdila.

Kadar deluje naročnik v imenu več imetnikov (na primer, ko pravna oseba zahteva digitalna potrdila za zaposlene), nosi naročnik polno odgovornost v odnosu do overitelja za vse obveznosti glede uporabe zasebnega kriptografskega ključa, povezanega z javnim ključem v digitalnem potrdilu. V primeru, ko je imetnik fizična oseba, identificirana v povezavi s pravnim

subjektom, morata biti z obveznostmi seznanjena naročnik (pravna oseba) in imetnik (fizična oseba). Naročnik in imetnik (fizična oseba) morata potrditi strinjanje vsak za svoj del pogojev uporabe storitev zaupanja.

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

1.3.4. Tretje osebe

Tretje osebe so entitete, ki vključujejo fizične osebe (posameznike) in/ali pravne osebe, ki se zanašajo na digitalna potrdila, izdana s strani overiteljev Rekono.TSP, ne glede na to, ali so naročnik digitalnega potrdila ali ne.

Za preverjanje veljavnosti prejetega digitalnega potrdila morajo tretje osebe vedno preveriti status v zadnjem izdanem registru preklicanih digitalnih potrdil (CRL) ali preko storitve sprotnega preverjanja statusov digitalnih potrdil (OCSP).

1.3.5. Ostali udeleženci

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.

1.4. Namen uporabe digitalnih potrdil

1.4.1. Dovoljena uporaba digitalnih potrdil

Digitalna potrdila, ki jih izdajajo overitelji Rekono.TSP, se lahko uporabljajo, kot je za posamezno kategorijo digitalnih potrdil navedeno v sledeči tabeli.

Digitalno potrdilo	Dovoljena uporaba
RekonoSign	Za ustvarjanje naprednega elektronskega podpisa na sistemu za digitalni podpis na daljavo RekonoSign in za preverjanje veljavnosti elektronskega podpisa.
RekonoSeal	Za ustvarjanje naprednega elektronskega pečata na sistemu za digitalni podpis na daljavo RekonoSign in za preverjanje veljavnosti elektronskega pečata.
RekonoAuth	Za elektronsko avtentikacijo oziroma kot sredstvo elektronske identifikacije v okviru elektronske identitete oziroma računa Rekono. Opomba: Digitalna potrdila RekonoAuth so tehnološko nevtralna, to so standardna digitalna potrdila X.509, ki jih lahko imetnik po svoji presoji uporablja tudi za elektronsko avtentikacijo v povezavi z drugimi sistemi.
RekonoTSU	Za izdajanje elektronskih časovnih žigov na sistemih Rekono.TSP.

	Storitev elektronskih časovnih žigov je dostopna oziroma se uporablja le v povezavi z ustvarjanjem naprednega elektronskega podpisa ali naprednega elektronskega žiga na sistemu za digitalni podpis na daljavo RekonoSign.
RekonoOCSP	Za storitve OCSP overiteljev Rekono.TSP.
RekonoPKI	Za upravljanje infrastrukture in sistemov v okviru Rekono.TSP

1.4.2. Nedovoljena uporaba digitalnih potrdil

Vsa digitalna potrdila, izdana s strani overiteljev Rekono.TSP, se lahko uporabljajo le v skladu z Rekono.TSP Pravili delovanja ter zakonodajo in predpisi Republike Slovenije. Glej tudi 9.14.

1.5. Upravljanje s pravili delovanja

1.5.1. Organizacija, ki upravlja s pričujočim dokumentom

Z dokumentom upravlja Rekono d.o.o.

1.5.2. Kontaktni podatki

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

1.5.3. Oseba, ki ugotavlja ustreznost Politike

Namenoma puščeno prazno.

1.5.4. Postopek odobritve politike delovanja overitelja

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

1.6. 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: 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 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: 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 povezan je s podatki, na katere se nanaša, in sicer tako, da je mogoče zaslediti vsako naknadno spremembo teh podatkov.
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 storitev zaupanja	Pomeni fizično ali pravno osebo, ki zagotavlja eno ali več storitev zaupanja kot ponudnik kvalificiranih ali nekvalificiranih storitev zaupanja.
Kvalificirana storitev zaupanja	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.
Imetnik potrdila **(angl. Subject)**	Je subjekt, opredeljen v digitalnem potrdilu v polju *Subject*. Imetnik je lahko fizična oseba (angl. natural person) ali poslovni subjekt oziroma pravna oseba (angl. legal person).
Naročnik potrdila **(ang. Subscriber)**	Fizična oseba ali poslovni subjekt, ki zahteva izdajo digitalnega potrdila v imenu enega ali več imetnikov ali v svojem imenu. Naročnik je hkrati imetnik, kadar podpiše vlogo za izdajo digitalnega potrdila v svojem imenu.

Druge definicije in izrazi:

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.
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.

Strežnik časovnega žiga **(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
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)

2. OBJAVE IN REPOZITORIJ

2.1. Repozitorij

Rekono.TSP uporablja notranje in javne repozitorije.

Javni repozitoriji so dostopni na sledečih spletnih naslovih:

Javne spletne strani:	https://www.rekono.si https://tsp.rekono.si http://pki.rekono.si

2.2. Objave informacij o digitalnih potrdilih

Overitelj Rekono.TSP objavlja:

- sezname preklicanih digitalnih potrdil (angl. Certificate Revocation Lists, CRL);
- digitalna potrdila korenskih in podrejenih overiteljev;
- pravila delovanja in druge javne dokumente ponudnika storitev zaupanja;
- navodila za pridobitev, preklic in obnovo digitalnih potrdil;
- ostale pogoje uporabe storitev Rekono.TSP;
- ostale javne informacije, povezane z izvajanjem storitev zaupanja.

2.3. Čas in pogostost objav

Seznami preklicanih digitalnih potrdil so objavljeni po izdaji novega seznama, kot je določeno v poglavju 4.9.7. Vse ostale informacije so objavljene takoj, ko pride do sprememb ali ko postanejo dostopne ponudniku storitev zaupanja.

2.4. Dostop do podatkov v repozitoriju

V javnih repozitorijih so objavljene samo javne informacije, ki so dostopne samo za branje. Repozitoriji imajo vzpostavljene ustrezne tehnične varnostne mehanizme za zaščito pred nepooblaščenimi spremembami podatkov ter mehanizme za zagotavljanje razpoložljivosti podatkov.

3. PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI

3.1. Določanje imen

3.1.1. Vrste imen

Za ime subjekta se v digitalnih potrdilih uporablja overjeno ime naročnika, kot je za posamezno kategorijo digitalnih potrdil navedeno v nadaljevanju tega poglavja. Overjeno ime subjekta je v digitalnem potrdilu zapisano v atributih, ki so del celotnega X.501 razločevalna imena (angl. Distinguished Name, DN). Posamezni atributi razločevalnega imena so v skladu z RFC 5280 vpisani v obliki `UTF8String` ali `PrintableString`.

Razločevalno ime je v digitalnih potrdilih RekonoSign in RekonoAuth za fizične osebe zapisano v sledeči obliki:

Atribut razločevalnega imena	Vrednost
Country Name (C=), obvezen	ISO 3166-1 Alpha-2 koda države (npr. SI).
Description	Vrsta digitalnega potrdila (npr. RekonoSign). Opomba: Polje ni obvezno. Vsebina je informativna in sama po sebi ne opredeljuje zaupanja v potrdilo.
Surname (SN=), obvezen	Priimek imetnika
Given Name (givenName =), obvezen	Ime imetnika
Common Name (CN=), obvezen	Ime in priimek imetnika digitalnega potrdila.
Serial Number (serialNumber=), obvezen	Enolična oznaka, ki jo določi overitelj.

Razločevalno ime je v digitalnih potrdilih RekonoSign in RekonoAuth za fizične osebe, identificirane v povezavi s pravnim subjektom, zapisano v sledeči obliki:

Atribut razločevalnega imena	Vrednost
Country Name (C=), obvezen	ISO 3166-1 Alpha-2 koda države (npr. SI).

Organization Name (O=), obvezen	Polni ali kratki naziv poslovnega subjekta
Organization Identifier (organizationIdentifier =), obvezen	Davčna številka poslovnega subjekta (v obliki EN 319 412-1, npr. VATSI-60762802)
Description	Vrsta digitalnega potrdila (npr. RekonoSign). Opomba: Polje ni obvezno. Vsebina je informativna in sama po sebi ne opredeljuje zaupanja v potrdilo.
Surname (SN=), obvezen	Priimek imetnika
Given Name (givenName =), obvezen	Ime imetnika
Common Name (CN=), obvezen	Ime in priimek imetnika digitalnega potrdila.
Serial Number (serialNumber=), obvezen	Enolična oznaka, ki jo določi overitelj.

Razločevalno ime je v digitalnih potrdilih RekonoSeal zapisano v sledeči obliki:

Atribut razločevalnega imena	Vrednost
Country Name (C=), obvezen	SI
Organization Name (O=), obvezen	Polni ali kratki naziv poslovnega subjekta
Organization Identifier (organizationIdentifier =), obvezen	Davčna številka poslovnega subjekta (v obliki EN 319 412-1, npr. VATSI-60762802)
Description	Vrsta digitalnega potrdila (npr. RekonoSeal). Opomba: Polje ni obvezno. Vsebina je informativna in sama po sebi ne opredeljuje zaupanja v potrdilo.
Common Name (CN=), obvezen	Naziv poslovnega subjekta oziroma naziv, ki predstavlja subjekt (ni treba, da je polno registrirano ime)

Razločevalno ime je v digitalnih potrdilih RekonoTSU zapisano v sledeči obliki:

Atribut razločevalnega imena	Vrednost
Country Name (C=), obvezen	SI
Organization Name (O=), obvezen	Polni ali kratki naziv poslovnega subjekta
Organization Identifier (organizationIdentifier =), obvezen	Davčna številka poslovnega subjekta (v obliki VATSI-60762802)
Common Name (CN=), obvezen	Splošni naziv storitve elektronskega časovnega žiga

Razločevalno ime je v digitalnih potrdilih RekonoOCSP zapisano v sledeči obliki:

Atribut razločevalnega imena	Vrednost
Country Name (C=), obvezen	SI
Organization Name (O=), obvezen	Rekono d.o.o.
Organization Identifier (organizationIdentifier =), obvezen	VATSI-60762802
Common Name (CN=), obvezen	Splošni naziv storitve OCSP

Razločevalno ime je v digitalnih potrdilih RekonoPKI zapisano v sledeči obliki:

Atribut razločevalnega imena	Vrednost
Country Name (C=), obvezen	SI
Organization Name (O=), obvezen	Rekono d.o.o.

Organization Identifier (organizationIdentifier =), obvezen	VATSI-60762802
Organizational Unit (OU=)	RekonoPKI
Common Name (CN=)	Splošni naziv storitve oziroma subjekta

3.1.2. Potreba po smiselnosti imen

Razločevalno ime digitalnega potrdila sestavlja nabor atributov v skladu z RFC 5280 [3] in EN 319 412 Parts 1 to 3 [8] [9] [10]. Glej tudi poglavje 3.1.1.

3.1.3. Anonimnost imetnikov in uporaba psevdonimov

Namenoma puščeno prazno.

3.1.4. Pravila za interpretacijo različnih oblik imen

Vrste imen in pomen posameznega atributa v razločevalnem imenu digitalnega potrdila so navedeni v poglavju 3.1.1. Razločevalno ime lahko vsebuje dodatna polja, ki pa ne vplivajo na identifikacijo imetnika potrdila.

Vrstni red relativnih imen (RDN) razločevalnega imena (DN) se lahko razlikuje od navedenega v poglavju 3.1.1 in ne vpliva na zaupanje oziroma verodostojnost razločevalnega imena.

Imena so sestavljena iz črk kodne tabele UTF8. V potrdilu so posamezna polja razločevalnega imena zapisana kot ASN.1 `utf8String` ali ASN.1 `printableString`. V primeru nepredvidenih znakov si overitelj pridržuje pravico poiskati ustrezno kombinacijo črk iz kodne tabele ASCII.

3.1.5. Edinstvenost imen

Overitelj za vsako digitalno potrdilo določi enolično razločevalno ime (DN), ki je v digitalnem potrdilu v skladu z RFC 5280 [3] vpisano v potrdilu v polju `Subject`.

Set atributov v razločevalnem imenu (DN) potrdila enolično predstavlja vsakega imetnika digitalnega potrdila. Edinstvenost razločevalnega imena je zagotovljena z atributom `serialNumber`.

3.1.6. Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk

Rekono.TSP si razumno prizadeva za rešitev sporov, ki se lahko pojavijo pri dodeljevanju imen, npr. ponudnik storitev zaupanja lahko kontaktira naročnika in se z njim dogovori, da se sporni del razločevalnega imena spremeni, tako da ne bo v konfliktu z že uporabljenim razločevalnim imenom.

Naročniki ne smejo zahtevati izdaje digitalnega potrdila na ime, ki bi kršilo pravice tretjih oseb (kot npr. ime podjetja, osebno ime, intelektualne pravice ali druge lastninske pravice).

Ponudnik storitev zaupanja lahko po lastni presoji brez obrazložitve zavrne ali zahteva dodatna dokazila, če sumi, da zahtevek krši pravice tretjih oseb (kot npr. ime podjetja, osebno ime, avtorske ali druge lastniške pravice). Če je potrdilo že izdano, ga lahko prekliče.

3.2. Prva registracija

3.2.1. Metode dokazovanja lastništva zasebnega ključa

Dokaz posedovanja zasebnega ključa je zagotovljen z uporabo postopkov na osnovi splošno priznanih standardov, kot so PKCS#10 (Public Key Cryptographic Standard #10), Certificate Management Protocol (CMP) in Netscape SPKI (angl. Signed Public Key and Challenge, SPKAC).

3.2.2. Preverjanje istovetnosti organizacije

Vsi postopki preverjanja istovetnosti se izvajajo preko storitve Rekono.ID. Glej tudi Splošne pogoje uporabe storitve Rekono (https://www.rekono.si/sl/kako-deluje/splosni-pogoji/).

3.2.3. Preverjanje istovetnosti za fizične osebe

Vsi postopki preverjanja istovetnosti se izvajajo preko storitve Rekono.ID. Glej tudi Splošne pogoje uporabe storitve Rekono (https://www.rekono.si/sl/kako-deluje/splosni-pogoji/).

3.2.4. Podatki o imetnikih digitalnih potrdil, ki se ne preverjajo

Vsi podatki, vsebovani v razločevalnem imenu potrdila, ki so v tabelah v poglavju 3.1.1 označeni kot "obvezen", so preverjeni kot del postopka registracije računa Rekono.ID.

3.2.5. Preverjanje pooblastil

Vsi postopki preverjanja pooblastil se izvajajo kot del postopka registracije računa Rekono.ID.

3.2.6. Merila za medsebojno povezovanje

Rekono.TSP izvaja medsebojno priznavanje z drugimi overitelji po lastni presoji. Pred vzpostavitvijo medsebojnega priznavanja bo overitelj izvedel skrbno presojo ujemanja pravil delovanja, za katere se vzpostavlja medsebojno zaupanje ter zahteval dokazila, da ponudnik storitev res izvaja postopke v skladu s svojimi pravili delovanja.

Rekono.TSP lahko po lastni presoji in brez obrazložitve zavrne vzpostavitev medsebojnega zaupanja.

3.3. Preverjanje istovetnosti pri obnovi digitalnega potrdila

3.3.1. Preverjanje istovetnosti pri rutinski obnovi digitalnih potrdil

Vsi postopki preverjanja istovetnosti se izvajajo preko storitve Rekono.ID.

Imetnik lahko na osnovi avtentikacije z računom Rekono.ID kadarkoli pred potekom ali po poteku zadnjega potrdila izvede obnovo svojega potrdila.

V primeru, da so se imetnikovi identifikacijski podatki spremenili, je imetnik dolžan uskladiti podatke svojega računa Rekono.ID. To lahko naredi preko spletne strani za upravljanje računa Rekono.ID (https://idp.rekono.si).

3.3.2. Preverjanje istovetnosti pri obnovi digitalnega potrdila po preklicu

Postopki preverjanja istovetnosti se izvedejo preko storitve Rekono.ID kot ob prvem prevzemu potrdila (glej 3.2.3).

3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila

Postopki preverjanja istovetnosti se izvedejo preko storitve Rekono.ID kot ob prvem prevzemu potrdila (glej 3.2.3).

4. UPRAVLJANJE Z DIGITALNIMI POTRDILI

4.1. Vloga za izdajo digitalnega potrdila

4.1.1. Kdo lahko zaprosi za izdajo digitalnega potrdila

Digitalno potrdilo RekonoSign ali RekonoAuth lahko pridobi vsaka fizična oseba, ki ima registriran račun Rekono.ID ravni zanesljivosti srednja (Rekono 20) ali visoka (Rekono 30).

Digitalno potrdilo RekonoSeal lahko pridobi vsaka pravna oseba, ki ima registriran račun Rekono.ID ravni zanesljivosti srednji (Rekono 20) ali visoka (Rekono 30) in ima sklenjeno pogodbo z Rekono d.o.o.

Digitalna potrdila RekonoTSU se izdajajo izključno za uporabo na strežnikih storitve elektronskega časovnega žiga Rekono.TSP.

Digitalna potrdila RekonoOCSP se izdajajo izključno za uporabo na strežnikih storitve OCSP overiteljev Rekono.TSP.

Digitalna potrdila RekonoPKI se izdajajo izključno za upravljanje infrastrukture Rekono.TSP.

Korenski overitelji Rekono.TSP izdajajo potrdila izključno podrejenim overiteljem Rekono.TSP.

4.1.2. Postopek obdelave vlog in odgovornosti

Rekono.TSP izda digitalna potrdila RekonoSign, RekonoAuth ali RekonoSeal na osnovi prijave z računom Rekono.ID. Račun Rekono.ID vsebuje vse identifikacijske podatke naročnika oziroma imetnika, ki so potrebni za izdajo digitalnega potrdila. Preverjanje identifikacijskih podatkov je bilo izvedeno ob registraciji računa Rekono.ID ali kasneje kot del postopkov storitve Rekono.ID za potrjevanje identitete. Storitvi Rekono.Sign in Rekono.ID imata vzpostavljeno medsebojno zaupanje, zato ponovno preverjanje identifikacijskih podatkov ni potrebno.

Potrdila korenskega overitelja, podrejenih overiteljev, RekonoOCSP in RekonoTSU se izdajo v okviru internih postopkov Rekono.TSP.

4.2. Obdelava vloge za izdajo digitalnega potrdila

4.2.1. Postopki identifikacije in avtentikacije

Glej 4.1.2 Postopek obdelave vlog in odgovornosti.

4.2.2. Odobritev ali zavrnitev izdaje digitalnega potrdila

Digitalno potrdilo RekonoSign, RekonoSeal ali RekonoAuth lahko pridobi vsaka pravna ali fizična oseba, ki ima račun Rekono.ID ustrezne ravni zanesljivosti. Dodatna odobritev ni potrebna.

4.2.3. Čas za obdelavo vloge za izdajo digitalnega potrdila

Namenoma puščeno prazno.

4.3. Izdaja digitalnega potrdila

4.3.1. Postopki overitelja ob izdaji digitalnega potrdila

Postopek izdaje digitalnega potrdila RekonoSign ali RekonoSeal se izvede ob vsakem ustvarjanju naprednega elektronskega podpisa ali naprednega elektronskega žiga, ki se izvedeta preko storitve za digitalni podpis na daljavo RekonoSign na sledeči način:

- Pred izvedbo postopka digitalnega podpisa se uporabnik prijavi z računom Rekono.ID na storitev RekonoSign.
- Storitev RekonoSign na strojnem varnostnem modulu (HMS) tvori zasebni ključ uporabnika, ter pridobi potrdilo javnega ključa od zadevnega overitelja Rekono.TSP.
- Storitev RekonoSign uporabi tvorjeni zasebni ključ in pridobljeno potrdilo za ustvarjanje napredenega elektronskega podpisa ali naprednega elektronskega žiga.
- Digitalno potrdilo se shrani v repozitoriju storitve RekonoSign.
- Zasebni ključ uporabnika se po izvedbi digitalnega podpisa briše iz HSM, na katerem je bil tvorjen.
- Ob prvi uporabi storitve se uporabnik seznani s pogoji uporabe digitalnih potrdil. Pred nadaljevanjem postopka mora potrditi strinjanje s pogoji uporabe.

Postopek izdaje digitalnega potrdila RekonoAuth se izvede preko spletne strani RekonoSign na sledeči način:

- Uporabnik se prijavi z računom Rekono.ID na storitev RekonoSign.
- Ob prvi uporabi storitve se uporabnik seznani s pogoji uporabe digitalnih potrdil. Pred nadaljevanjem postopka mora potrditi strinjanje s pogoji uporabe. Izjava o strinjanju s pogoji uporabe se podpiše s potrdilom RekonoSign po zgoraj opisanem postopku. Podpisana izjava se shrani v repozitoriju storitve RekonoSign.
- Uporabnik na spletni strani izbere povezavo za prevzem potrdila RekonoAuth. Na prikazani spletni strani vpiše osebno geslo, s katerim želi zaščititi prevzeti zasebni ključ in pripadajoče potrdilo javnega ključa.

- Storitev RekonoSign tvori zasebni ključ in pridobi RekonoAuth potrdilo javnega ključa. Tvorjeni zasebni ključ in potrdilo shrani v datoteko v obliki PKCS#12, ki jo zaščiti z osebnim geslom imetnika.
- Storitev RekonoSign ponudi uporabniku možnost, da prenese datoteko PKCS#12. Datoteka PKCS#12 se po prenosu k uporabniku briše in se nikdar ne hrani ali arhivira na strani storitve RekonoSign ali overitelja Rekono.TSP.
- Uporabnik lahko zasebni ključ in potrdilo, vsebovano v datoteki PKCS#12, uvozi v spletni brskalnik na napravo, kot je na primer pametna kartica.

4.3.2. Obvestilo imetniku o izdaji digitalnega potrdila

Naročnik bo prejel obvestilo o izdaji digitalnega potrdila v okviru postopka prevzema digitalnega potrdila (glej poglavje 4.3.1).

4.4. Prevzem digitalnega potrdila

Naročnik bo prejel vse digitalna potrdila med postopkom prevzema digitalnega potrdila (glej poglavje 4.3.1.).

4.4.1. Postopek potrditve prevzema digitalnega potrdila

Naročnik mora ob prevzemu digitalnega potrdila RekonoAuth preveriti verodostojnost digitalnega potrdila na osnovi korenskega digitalnega potrdila overitelja Rekono.TSP in najkasneje v roku sedmih (7) koledarskih dni obvestiti overitelja o morebitnih napakah. V nasprotnem primeru velja, da so podatki točni in uporabnik prevzema vso odgovornost za točnost podatkov v digitalnem potrdilu.

Če podatki niso točni, mora naročnik v najkrajšem možnem času, vendar ne kasneje kot v sedmih (7) koledarskih dneh, napako sporočiti overitelju Rekono.TSP na kontaktni naslov, naveden v poglavju 1.5.2.

4.4.2. Objava digitalnega potrdila

Overitelj ne objavlja digitalnih potrdil v javnem imeniku.

4.4.3. Obveščanje drugih udeležencev o izdaji digitalnega potrdila

Namenoma puščeno prazno.

4.5. Uporaba ključev in digitalnih potrdil

4.5.1. Uporaba ključev in digitalnih potrdil s strani imetnikov

Naročniki morajo uporabiti digitalna potrdila v skladu z zahtevami, navedenimi v poglavju 1.4.

Zasebne ključe lahko uporabljajo le imetniki, katerim je bilo izdano digitalno potrdilo pripadajočega javnega ključa.

Naročniki morajo skrbeti za varnost svojih zasebnih ključev in preventivno skrbeti, da preprečijo nepooblaščeno uporabo.

4.5.2. Uporaba digitalnih potrdil s strani tretjih oseb

Tretje osebe morajo omejiti zanašanje na digitalna potrdila oziroma pripadajoče javne ključe le na namene uporabe, kot je določeno v poglavju 1.4. Tretje osebe morajo poleg tega:

- Biti seznanjene z zahtevami Rekono.TSP Pravil delovanja in jih dosledno upoštevati;
- Pred uporabo preveriti status digitalnih potrdil v registru preklicanih potrdil ali storitvi OCSP;
- Nemudoma obvestiti overitelja Rekono.TSP ob sumu ali znani zlorabi kateregakoli digitalnega potrdila, ki ga je izdal katerikoli od overiteljev Rekono.TSP.

4.6. Obnova digitalnih potrdil brez spremembe ključev

Obnova digitalnega potrdila brez spremembe ključev ni podprta, se ne uporablja in ni dovoljena.

4.7. Obnova digitalnih potrdil

Obnova digitalnega potrdila je proces, v katerem overitelj izda naročniku novo digitalno potrdilo. Novo digitalno potrdilo vsebuje iste identifikacijske oznake naročnika kot staro potrdilo in nov javni ključ.

4.7.1. Okoliščine obnove digitalnih potrdil

Obnova potrdila se izvede:

- Po preklicu digitalnega potrdila, če uporabnik zahteva izdajo novega;
- Po poteku veljavnosti digitalnega potrdila ali po poteku časovnega obdobja uporabe zasebnega ključa, če je to obdobje krajše kot je obdobje veljavnosti digitalnega potrdila.

Zasebni ključi RekonoSign in RekonoSeal se uporabijo le za en digitalni podpis in se ne hranijo, zato se obnova potrdil izvede ob vsakem zahtevku za elektronski podpis ali elektronski žig.

4.7.2. Kdo lahko zahteva obnovo digitalnega potrdila

Obnovo digitalnega potrdila lahko zahteva naročnik oziroma isti subjekti kot prvo izdajo digitalnega potrdila (glej poglavje 4.1.1).

4.7.3. Obdelava zahtevkov za obnovo digitalnega potrdila

Obnova digitalnega potrdila se izvede kot prvi prevzem.

4.7.4. Obvestilo imetnikov o izdaji novega digitalnega potrdila

Enako kot je navedeno v poglavju 4.3.2.

4.7.5. Postopek potrditve prevzema novega digitalnega potrdila

Enako kot je navedeno v poglavju 4.4.1.

4.7.6. Objava obnovljenega digitalnega potrdila

Enako kot je navedeno v poglavju 4.4.2.

4.7.7. Obveščanje drugih uporabnikov o izdaji digitalnega potrdila

Enako kot je navedeno v poglavju 4.4.3.

4.8. Sprememba digitalnega potrdila

Sprememba digitalnega potrdila je postopek, ki omogoča naročnikom, da zaprosijo za digitalno potrdilo s spremenjenimi identifikacijskimi podatki. Sprememba digitalnega potrdila zahteva izdajo novega digitalnega potrdila za nov javni ključ in se izvaja po istem postopku kot prva izdaja.

4.8.1. Okoliščine, v katerih se izvede sprememba digitalnih potrdil

Naročnik lahko zahteva spremembo digitalnega potrdila, kadar so se spremenili podatki, vsebovani v digitalnem potrdilu, kot na primer ime ali priimek.

4.8.2. Kdo lahko zahteva spremembo digitalnih potrdil

Spremembo digitalnega potrdila lahko zahteva naročnik oziroma isti subjekti kot prvo izdajo digitalnega potrdila (glej poglavje 4.1.1).

4.8.3. Obdelava zahtevkov za spremembo digitalnih potrdil

Enako kot ob prvi izdaji potrdila (glej poglavje 4.2).

4.8.4. Obvestilo imetniku o izdaji spremenjenega digitalnega potrdila

Enako kot je navedeno v poglavju 4.3.2.

4.8.5. Postopek potrditve prevzema spremenjenega digitalnega potrdila

Enako kot je navedeno v poglavju 4.4.1.

4.8.6. Objava spremenjenega digitalnega potrdila

Enako kot je navedeno v poglavju 4.4.2.

4.8.7. Obveščanje drugih udeležencev o izdaji spremenjenega digitalnega potrdila

Enako kot je navedeno v poglavju 4.4.3.

4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila

Postopek se uporablja za predčasno ukinitev (preklic) ali začasno ukinitev (suspenz) veljavnosti digitalnega potrdila.

Preklic digitalnega potrdila pomeni dokončno ukinitev veljavnosti digitalnega potrdila. Razveljavitev preklica ni možna.

Začasna ukinitev pomeni začasno ukinitev veljavnosti digitalnega potrdila. Digitalno potrdilo, ki je v stanju začasne ukinitve, se lahko dokončno prekliče ali pa razveljavi začasno ukinitev.

V obeh primerih, to je, če je digitalno potrdilo preklicano ali začasno ukinjeno, se status potrdila objavi v registru preklicanih potrdil. V primeru razveljavitve začasne ukinitve se status briše iz registra preklicanih digitalnih potrdil.

4.9.1. Okoliščine preklica

Overitelj lahko oziroma mora izvesti preklic digitalnega potrdila v sledečih primerih:

- Če to zahteva naročnik ali imetnik digitalnega potrdila;
- Če overitelj izve, da je imetnik potrdila preminil ali izgubil svoje poslovne sposobnosti ali prenehal obstajati ali če so spremenjene okoliščine, ki imajo pomemben učinek na veljavnost digitalnega potrdila;
- Kadar je katera od informacij, vsebovanih v potrdilu, nepravilna ali obstaja sum o tem;
- Kadar je zasebni ključ, povezan s potrdilom, ogrožen ali pa za to obstaja sum (ni potrebno za RekonoSign, ker se podpisni ključ takoj po uporabi uniči);
- Kadar je kateri od aktivacijskih podatkov, kot sta geslo ali PIN, uporabljen za zaščito zasebnega ključa, ogrožen ali pa za to obstaja sum (ni potrebno za RekonoSign, ker se podpisni ključ takoj po uporabi uniči in ni potrebno geslo ali PIN);
- Če je bil račun Rekono, s katerim se imetnik prijavlja na storitev Rekono.Sign, ogrožen ali pa za to obstaja sum;
- Če overitelj preneha z delovanjem ali mu je delovanje prepovedano in njegove dejavnosti ni prevzel drug overitelj;

- Če preklic odredi pristojno sodišče ali upravni organ;
- Če overitelj ugotovi, da digitalno potrdilo ni bilo izdano v skladu z Rekono.TSP Pravili delovanja;
- Če naročnik ali imetnik digitalnega potrdila krši določbe Rekono.TSP Pravil delovanja ali veljavne zakonodaje ali predpisov.

4.9.2. Kdo lahko zahteva preklic

Preklic digitalnega potrdila lahko zahteva:

- naročnik ali imetnik digitalnega potrdila;
- pooblaščeni zastopnik v imenu naročnika (pravne osebe), ki je zahteval izdajo digitalnega potrdila;
- osebje Rekono.TSP;
- osebje Rekono.ID; ali
- pristojno sodišče ali upravni organ.

4.9.3. Postopki za preklic

Zahtevo za preklic lahko naročnik ali imetnik digitalnega potrdila poda na sledeče načine:

- pošlje elektronsko pošto na naslov support@rekono.si
    - elektronsko sporočilo mora biti poslano z naslova, ki ga ima imetnik registriranega v računu Rekono
    - zahtevek bo preverjen s povratnim klicem službe za podporo Rekono na telefonsko številko, ki jo ima imetnik registrirano v računu Rekono
- pošlje sporočilo preko spletne strani https://www.rekono.si, obrazec za pomoč (Help)
    - zahtevek bo preverjen s sporočilom na elektronski poštni naslov, naveden v zahtevku; in
    - s povratnim klicem službe za podporo Rekono na telefonsko številko, ki jo ima imetnik registrirano v računu Rekono
- pooblaščena oseba naročnika (pravne osebe) pošlje digitalno podpisan elektronski zahtevek v obliki PDF, ki mora biti overjen z digitalnim potrdilom zakonitega zastopnika, preko elektronske pošto na naslov support@rekono.si.

4.9.4. Čas za posredovanje vloge za preklic

Subjekt, ki se zaveda okoliščin, ki zahtevajo preklic digitalnega potrdila, mora zahtevati preklic takoj, ko je to možno, brez nepotrebnega odlašanja.

4.9.5. Čas od vloge za preklic do preklica

V vseh primerih bo preklicano potrdilo objavljeno v registru preklicanih potrdil najkasneje do konca naslednjega delovnega dne od trenutka, ko overitelj prejme veljaven zahtevek za preklic. Delovni dan se šteje vsak dan od ponedeljka do petka, razen dela prostih dni v Republiki Sloveniji.

4.9.6. Obveza preverjanja registra preklicanih potrdil

Tretja stran oziroma vsak subjekt, ki se zanaša na digitalna potrdila, ki jih izdajajo overitelji Rekono.TSP, mora pred uporabo preveriti status digitalnega potrdila v zadnjem veljavnem registru preklicanih potrdil.

Če noben od veljavnih registrov preklicanih potrdil ni dostopen, zaradi napake v sistemu, nedelovanja storitve ali drugega vzroka, mora biti uporaba potrdila zavrnjena.

Tretja stran oziroma vsak subjekt, ki dostopa do registra preklicanih potrdil, mora preveriti njegovo verodostojnost na osnovi overiteljevega digitalnega potrdila in preveriti, da obdobje veljavnosti registra ni poteklo.

4.9.7. Pogostost objav registrov preklicanih potrdil

Overitelj Rekono.TSP posodobi register preklicanih potrdil najkasneje v roku 60 minut, ko izvede preklic digitalnega potrdila, ali vsaj enkrat vsakih 24 ur.

Korenski overitelj [Rekono CA Root] posodobi register preklicanih potrdil takoj, ko izvede preklic digitalnega potrdila, ali vsaj enkrat vsakih 365 dni.

4.9.8. Dovoljene zakasnitve sprotnega preverjanja statusa digitalnih potrdil

Namenoma puščeno prazno.

4.9.9. Storitev sprotnega preverjanja statusa digitalnih potrdil

Namenoma puščeno prazno.

4.9.10. Obveza sprotnega preverjanja statusa digitalnih potrdil

Namenoma puščeno prazno.

4.9.11. Ostale oblike objavljanja preklicanih digitalnih potrdil

Namenoma puščeno prazno.

4.9.12. Posebne zahteve glede zlorabe ključa

Namenoma puščeno prazno.

4.9.13. Okoliščine za začasno ukinitev veljavnosti (suspenz) digitalnega potrdila

Začasna ukinitev veljavnosti (suspenz) se lahko uporabi le v internih postopkih overitelja.

4.9.14. Kdo lahko zahteva suspenz ali ukinitev suspenza digitalnega potrdila

Namenoma puščeno prazno.

4.9.15. Postopki za suspenz ali ukinitev suspenza digitalnega potrdila

Namenoma puščeno prazno.

4.9.16. Omejitve obdobja začasne ukinitve veljavnosti

Obdobje začasne ukinitve veljavnosti v okviru internih postopkov overitelja ni omejeno.

4.10. Storitve objavljanja statusa digitalnih potrdil

4.10.1. Tehnične lastnosti storitve

Status digitalnih potrdil se objavlja kot register preklicanih potrdil X.509 Certificate Revocation List (CRL) v skladu z RFC 5280 [3] in po protokolu OCSP v skladu z RFC 6960.

Registri preklicanih potrdil so dostopni po protokolu http. Spletni naslovi registrov preklicanih potrdil so v skladu z RFC 5280 [3] navedeni v razširitvenem polju `cRLDistributionPoints` (X.509 CRL Distribution Points), vsebovanem v vsakem izdanem digitalnem potrdilu.

Storitev OCSP je dostopna na spletnem naslovu, ki je naveden v razširitvenem polju `id-pe-authorityInfoAccess, id-ad-ocsp`.

4.10.2. Razpoložljivost storitve dostopa do registra preklicanih potrdil

Dostop do registra preklicanih digitalnih potrdil in storitve OCSP je mogoč 24ur vse dni v letu.

4.10.3. Dodatne možnosti

Namenoma puščeno prazno.

4.11. Trajanje naročniškega razmerja

Naročniško razmerje so konča po preteku ali preklicu zadnjega naročnikovega digitalnega potrdila.

4.12. Varnostno kopiranje in odkrivanje zasebnega ključa

Overitelji Rekono.TSP ne izvajajo hrambe ali varnostnega kopiranja zasebnih ključev imetnikov.

5. FIZIČNO VAROVANJE, ORGANIZACIJSKI VARNOSTNI UKREPI IN ZAHTEVE ZA OSEBJE

5.1. Fizično varovanje

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.

5.2. Organizacijski varnostni ukrep

5.2.1. 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.

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

Operativna vloga	Odgovornosti
Skrbniki HSM	Osebe zadolžene za upravljanje strojnih varnostnih modulov (HSM) in logičnih particij HSM. Obsega štiri nivoje vlog: • Varnostni skrbnik HSM • Sistemski skrbnik HSM • Varnostni skrbnik logične particije HSM • Uporabnik logične particije HSM
Varnostni skrbnik	Osebe zadolžene za upravljanje nastavitev programske opreme overitelja ter dodajanje in upravljanje pooblastil oseb z vlogo Skrbnik.
Skrbnik	Osebe zadolžene za upravljanje digitalnih potrdil v okviru programske opreme overitelja.
Skrbnik varnostnih kopij kriptografskih materialov	Osebe zadolžene za hrambo varnostnih kopij kriptografskih ključev overitelja in po potrebi drugih varnostno občutljivih podatkov.
Sistemski skrbnik	Osebe zadolžene za upravljanje IT okolja, v katerem delujejo sklopi programske opreme overitelja.

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

5.2.2. 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.

5.2.3. Preverjanje istovetnosti operativnega osebja

Člani osebja RekonoOA z zaupno vlogo so varnostno preverjeni, preden so imenovani za delo kot člani operativnega osebja.

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

5.2.4. Nezdružljivost nalog

Rekono.TSP zagotavlja delitev dolžnosti operativnega osebja in s tem nezdružljivost nalog z dodelitvijo zaupanja vrednih nalog, navedenih v poglavju 5.2.1 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).

5.3. Zahteve za osebje overitelja

5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje

Rekono.TSP dodeljuje zaupanja vredne operativen vloge zaposlenim in po potrebi zunanjim izvajalcem (glej tudi 5.3.7). Primernost posameznika za določeno operativno vlogo odobri RekonoPMA.

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

5.3.2. Preverjanje primernosti osebja

Preverjanje primernosti osebja se izvaja v skladu z internimi akti Rekono d.o.o.

5.3.3. Usposabljanje osebja

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

5.3.4. Pogostost dodatnih usposabljanj

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

5.3.5. Kroženje med delovnimi mesti

Namenoma puščeno prazno.

5.3.6. Ukrepi ob kršitvah pooblastil

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

5.3.7. 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.

5.3.8. Dokumentacija za osebje overitelja

Operativnemu osebju overitelja so, glede na njihovo vlogo, na voljo interni priročniki, originalna dokumentacija programske in strojne opreme.

5.4. Postopki zbiranja in upravljanja revizijskih sledi

Overitelj ima vzpostavljen stalen nadzor delovanja svoje infrastrukture, v okviru katerega se beležijo revizijske sledi dovoljene in nedovoljene uporabe ter dostopov do infrastrukture Rekono.TSP.

5.4.1. Vrste beleženih dogodkov

Overitelj beleži naslednje vrste dogodkov:

- dogodki na operacijskem sistemu, programski in strojni opremi overitelja;
- dogodki v zvezi s ključi overitelja;

- dogodki v zvezi z imetniškimi ključi in digitalnimi potrdili - izdaja, prevzem, obnova, preklic;
- dogodki v zvezi z varnostno politiko in upravljanjem informacijskega sistema overitelja;
- dogodki v zvezi z varnostno politiko in upravljanjem komunikacijskega sistema.

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.

Overitelj 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 overitelja ter fizično lokacijo;
- kadrovske spremembe operativnega osebja overitelja.

5.4.2. Pogostost pregleda revizijskih dnevnikov

Operativno osebje overiteljev pregleduje dnevnike beleženih dogodkov ob vsakem prejetem opozorilu iz nadzornih sistemov. Pregled vključuje:

- pregled zapisov v dnevniku;
- analizo in poročanje o relevantnih dogodkih - razreševanje problemov.

Operativno osebje overitelja izvaja redne preglede beleženih dogodkov, in sicer najmanj enkrat letno. Redni pregled vključuje:

- zbiranje in združevanje dnevnikov od zadnjega rednega pregleda;
- pregled zapisov v dnevniku in izdelava poročila o relevantnih dogodkih;
- izdelava arhivskih kopij dnevnikov.

5.4.3. Obdobje hranjenja revizijskih dnevnikov

Revizijski dnevniki programske opreme za upravljanje digitalnih potrdil se hranijo najmanj tri (3) mesece na sistemih overitelja in sistemu za hrambo podatkov, kot je določeno v 5.5.2.

Operativni dnevniki programske opreme in sistemov se hranijo najmanj en (1) mesec na sistemih overitelja in najmanj eno (1) leto na sistemu za hrambo podatkov.

5.4.4. Zaščita revizijskih dnevnikov

Dnevniki se hranijo v ustreznem varnostnem območju. Lokacija varnostne kopije je vsaj 25 km oddaljena od primarnega operativnega prostora.

Dostop do dnevnikov beleženih dogodkov je dovoljen samo pooblaščenim osebam:

- operativnemu osebju overitelja v okviru delovnih nalog,
- pristojnim inšpekcijskim organom.

Za operativne dnevnike na operacijskem sistemu in programski opremi so uporabljene zaščite, kot jih dopušča operacijski sistem.

Za revizijske dnevnike programske opreme za upravljanje digitalnih potrdil so uporabljeni kriptografski mehanizmi zaščite integritete zapisov.

5.4.5. Varnostne kopije revizijskih dnevnikov

Varnostna kopija revizijskih dnevnikov oziroma sledi se izvaja v okviru rednega dnevnega varnostnega kopiranja sistemov overitelja. Kopija operativnih in revizijskih dnevnikov se hrani na oddaljeni lokaciji.

5.4.6. Način zbiranja revizijskih dnevnikov

Zbiranje operativnih in revizijskih dnevnikov oziroma sledi se na informacijskih sistemih izvaja avtomatsko.

Zbiranje revizijskih sledi sledečih dogodkov se izvaja ročno za/pri:

- Fizični dostop zunanjih izvajalcev oziroma oseb, ki niso del operativnega osebja overitelja Rekono.TSP, v prostore overitelja;
- Spremembe konfiguracij na informacijskih sistemih overitelja;
- Nadgradnje programske in strojne opreme;
- Vzdrževalni posegi (napovedani in nenapovedani) na sistemih overitelja;
- Odstopanja od normalnega delovanja, ugotovljena ob pregledu revizijskih in sistemskih dnevnikov;
- Spremembe osebja overitelja;
- Uničenje informacij in/ali medijev.

5.4.7. Obveščanje povzročitelja dogodka

Povzročitelj dogodka ni obveščen.

5.4.8. Ocena in odprava ranljivosti

Rekono.TSP izvaja oceno ranljivosti kot del postopkov obdelave revizijskih dnevnikov.

5.5. Arhiviranje podatkov

5.5.1. Vrste arhiviranih podatkov

Rekono.TSP arhivira sledeče zapise:

- Informacije določene v poglavju 5.4.1;
- Digitalna potrdila in stanje preklicanih potrdil;

- Poročila o varnostnih pregledih overiteljeve infrastrukture.

5.5.2. Čas hrambe

Rekono.TSP hrani revizijske dnevnike vsaj sedem (7) let. Digitalna potrdila in stanje preklica so shranjeni vsaj trideset (30) let.

5.5.3. Zaščita arhiva

Dostop do Rekono.TSP arhivskih podatkov je dovoljen operativnemu osebju overitelja na podlagi potrebe po vedenju.

5.5.4. Varnostna kopija arhiva

Varnostna kopija arhiva se izvaja v okviru rednega dnevnega varnostnega kopiranja sistemov overitelja. Kopija se hrani na oddaljeni lokaciji. Za prenos medijev med primarno lokacijo overitelja in rezervno lokacijo je zagotovljen varen transport.

5.5.5. Zahteva za časovno žigosanje zapisov

Arhivirani zapisi so časovno označeni ob njihovem nastanku z uporabo sistemske ure sistema, na katerem je dogodek nastal. Sistemske ure vseh informacijskih sistemov so usklajene z zanesljivim zunanjim virom z uporabo protokola NTP.

5.5.6. Arhiviranje (notranje / zunanje)

Arhiviranje se izvaja znotraj Rekono.TSP kot tudi zunaj v prostorih, ki nudijo enakovredno zaščito.

5.5.7. Postopek za dostop do arhivskih podatkov in njihova verifikacija

Dostop do arhivskih podatkov je dovoljen na podlagi potrebe po vedenju v skladu z zaupanja vrednimi vlogami operativnega osebja overitelja.

Arhivirani podatki so na voljo za vpogled vsaki strani, ki izrazi interes in dokaže, da je razkritje potrebno. Oceno upravičenosti za vsak primer posebej izvede RekonoPMA.

5.6. Obnova digitalnega potrdila overitelja

Obnova overiteljevih zasebnih ključev bo izvedena vsaj 5 let pred potekom digitalnega potrdila ali prej. Ob obnovi overiteljevih zasebnih ključev bo generiran nov par kriptografskih ključev in novo digitalno potrdilo overitelja.

5.7. Postopki v primeru ogrožanja zasebnega ključa in okrevalni načrt

5.7.1. 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.

5.7.2. Uničenje programske, strojne opreme ali podatkov

V primeru okvare strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ overitelja ni bil uničen, bodo storitve overitelja vzpostavljene nazaj v najkrajšem možnem času. V primeru uničenja zasebnega ključa overitelja velja postopek, opisan v točki 5.7.3.

5.7.3. Ogrožanje overiteljevega zasebnega ključa

V primeru, da je zasebni ključ overitelja ogrožen, bo Rekono.TSP preklical vsa digitalna potrdila, ki so trenutno veljavna.

5.7.4. Okrevalni načrt v primeru naravne ali druge nesreče

V primeru naravne ali druge nesreče, pri kateri zasebni ključ overitelja ni bil uničen, bodo storitve overitelja vzpostavljene nazaj v najkrajšem možnem času. Postopki overitelja so podrobneje opredeljeni v zaupnem delu notranjih pravil delovanja overitelja.

V primeru uničenja zasebnega ključa overitelja velja postopek, opisan v točki 5.7.3.

5.8. Prenehanje delovanja overitelja

V primeru prenehanja delovanja bo overitelj:

- Obvestil vse trenutne naročnike vsaj devetdeset (90) dni pred namenom prenehanja delovanja;
- Preklical vsa veljavna potrdila ob ali po izteku odpovednega roka;
- Zagotovil razpoložljivost in dostop do registrov preklicanih potrdil vsaj za obdobje šest (6) mesecev po prenehanju delovanja;
- Zagotovil, da bodo arhivi shranjeni vsaj trideset (30) let od zadnjega dneva delovanja.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Tvorjenje in namestitev para ključev

6.1.1. Tvorjenje para ključev

Zasebni podpisni kriptografski ključi overiteljev Rekono.TSP so ustvarjeni na strojnem varnostnem modulu (angl. Hardware Security Module, HSM) v okviru nadzorovanega postopka (angl. Key Generation Ceremony).

Postopek tvorjenja kriptografskih ključev korenskih overiteljev se izvaja s sledečimi kontrolami:

- postopek se izvede ob prisotnosti zunanje verodostojne priče (kvalificirani presojevalec ali notar);
- izdelan je bil podroben zapisnik izvedbe postopka, ki ga je overila oziroma potrdila verodostojna priča (kvalificirani presojevalec ali notar).

Postopki tvorjenja kriptografskih ključev podrejenih izdajateljev so bili izvedeni s sledečimi kontrolami:

- postopek izvede osebje RekonoOA ob prisotnosti in pod nadzorom vsaj ene osebe RekonoPMA, ki nima aktivne vloge pri izvedbi postopka, ki potrdi, da je bil postopek izveden, kot je zabeleženo v zapisniku postopka;
- izdelan je bil podroben zapisnik izvedbe postopka.

Imetniški par kriptografskih ključev, napreden elektronski podpis ali napreden elektronski pečat se tvori v stojnem kriptografskem modulu storitve RekonoSign.

Imetniški par ključev za avtentikacijo oziroma za potrdilo RekonoAuth se tvori v programskem kriptografskem modulu programske opreme za upravljanje digitalnih potrdil.

6.1.2. Prenos zasebnega ključa imetniku

Zasebni ključ za RekonoSign ali RekonoSeal se takoj po uporabi uniči z mehanizmi strojnega varnostnega modula.

Zasebni ključ imetnika za potrdilo RekonoAuth se prenese uporabniku v obliki PKCS#12 datoteke. Datoteka PKCS#12 je zaščitena z geslom, ki ga v okviru postopka prevzema potrdila določi uporabnik.

6.1.3. Prenos imetnikovega ključa overitelju

Imetniški javni ključ se prenese overitelju v okviru postopka izdaje digitalnega potrdila. Javni ključ se prenese v obliki PKCS#10.

6.1.4. Dostop do overiteljevega javnega ključa

Overiteljev javni ključ je objavljen v overiteljevem digitalnem potrdilu, ki je javno objavljen v repozitorijih Rekono.TSP.

6.1.5. Dolžina asimetričnih ključev

Asimetrični ključi v verigi zaupanja z RSA ključi so sledečih dolžin:

- Korenski overitelji uporabljajo RSA ključe dolžine 3072 bit-ov.
- Podrejeni overitelji uporabljajo RSA ključe dolžine 3072 bit-ov.
- Imetniška RSA ključi so dolžine 2048 bit-ov.
- Kriptografski ključi strežnikov elektronskega časovnega žiga in strežnikov OCSP morajo biti RSA dolžine vsaj 2048 bit-ov.

Asimetrični ključi v verigi zaupanja z ECC ključi so iz NIST FIPS186-3 družine krivulj sledečih dolžin:

- Korenski overitelji uporabljajo ECC ključe secp384r1.
- Podrejeni overitelji uporabljajo ECC ključe secp384r1.
- Imetniški ECC ključi so secp256r1 ali secp384r1.
- Kriptografski ključi strežnikov elektronskega časovnega žiga in strežnikov OCSP morajo biti ECC ključi secp256r1 ali secp384r1.

6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov

Vsi parametri kriptografskih ključev se generirajo v okviru kriptografskih modulov, v katerih se ključi tvorijo.

6.1.7. Nameni ključev in digitalnih potrdil (X.509 v3 keyUsage)

Rekono.TSP določa namen uporabe kriptografskih ključev in digitalnih potrdil v polju `keyUsage`. Polje `keyUsage` se uporablja v skladu z RFC 5280 [3].

Poleg polja `keyUsage` se za dodatno določanje uporablja tudi polje `extKeyUsage`, v katerem se lahko določi dodatni namen uporabe. Polje `extKeyUsage` se uporablja v skladu z RFC 5280 [3].

Podpisovanje digitalnih potrdil in registrov digitalnih potrdil je dovoljeno le s ključi overiteljev Rekono.TSP. Digitalna potrdila overiteljev Rekono.TSP imajo `keyUsage` polje, ki vsebuje sledeče namene uporabe:

- keyCertSign
- cRLSign

Pregled uporabe polja keyUsage je podan v sledeči tabeli. Uporaba polja ektKeyUsage je odvisna oziroma prilagojena posamezni aplikaciji (na primer strežniki SSL, strežnik varnega časovnega žiga) in je opredeljena v poglavju 7.1.

Digitalno potrdilo	Polje keyUsage	Polje extKeyUsage
Overitelji	keyCertSign, cRLSign	
RekonoSign	nonRepudiation	
RekonoSeal	nonRepudiation	
RekonoAuth	digitalSignature	clientAuth
RekonoTSU	digitalSignature	timeStamping
RekonoOCSP	digitalSignature	OCSPSigning
RekonoPKI	digitalSignature in/ali keyEncipherment	serverAuth in/ali clientAuth

6.2. Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov

6.2.1. Standardi za kriptografski modul

Generiranje ključev overiteljev in njihova uporaba se izvaja v strojnem varnostnem kriptografskem modulu, skladnem s FIPS 140-2 Level 3.

Generiranje ključev strežnikov elektronskega časovnega žiga ter strežnikov OCSP in njihova uporaba se izvaja v strojnem varnostnem kriptografskem modulu, skladnem s FIPS 140-2 Level 3.

Generiranje in uporaba imetniških ključev za napreden elektronski podpis in napreden elektronski žig se izvaja v strojnem varnostnem kriptografskem modulu, skladnem s FIPS 140-2 Level 3.

6.2.2. Nadzor zasebnega ključa z (n od m) pooblaščenimi osebami

Kot opisano v poglavju 0.

6.2.3. Odkrivanje (ang. Escrow) zasebnega ključa

Rekono.TSP ne podpira odkrivanja zasebnega ključa.

6.2.4. Varnostno kopiranje zasebnih ključev

Rekono.TSP ne izvaja varnostnega kopiranja zasebnih ključev imetnikov.

6.2.5. Arhiviranje zasebnega ključa

Namenoma puščeno prazno.

6.2.6. Prenos zasebnega ključa v kriptografski modul in iz njega

Overiteljevi zasebni ključi so ustvarjeni v strojnem varnostnem modulu (HSM) in so lahko aktivirani samo znotraj strojnega varnostnega modula.

Zasebni ključi strežnikov za elektronski časovni žig so ustvarjeni v strojnem varnostnem modulu (HSM) in so lahko aktivirani samo znotraj strojnega varnostnega modula.

Zasebni ključi imetnikov za napreden elektronski podpis in napreden elektronski žig se tvorijo za vsak digitalni podpis posebej, in se takoj po uporabi brišejo iz HSM.

Zasebni ključi imetnikov za avtentikacijo se takoj po tvorjenju prenesejo k imetnikom v obliki PKCS#12 datoteke. Imetniki lahko uvozijo ključe iz PKCS#12 datoteke v svoj programski ali strojni kriptografski modul z uporabo gesla, ki so ga določili ob prevzemu potrdila.

6.2.7. Hranjenje overiteljevega zasebnega ključa v kriptografskem modulu

Rekono.TSP je v okviru nadzorovanega postopka (angl. Key Generation Ceremony) izdelal varnostno kopijo zasebnih ključev overiteljev. Varnostne kopije so zaščitene s pametnimi karticami in z mehanizmi strojnega kriptografskega modula. Ob povrnitvi ključa iz varnostne kopije je potrebna odobritev dveh oseb. Odobritev se izvaja na osnovi avtentikacije s pametno kartico.

6.2.8. Postopek za aktiviranje zasebnega ključa

Zasebni ključi storitev Rekono.TSP in se lahko aktivira le po načelu štirih oči.

Zasebni ključi imetnikov potrdil RekonoSign za elektronski podpis na daljavo ali elektronski pečat na daljavo se generirajo v strojnem varnostnem modulu (HSM) po uspešni avtentikaciji imetnika z računom Rekono.ID in takoj po izvedbi podpisa uničijo.

Imetniki aktivirajo zasebni ključ z avtentikacijskimi mehanizmi programskega ali strojnega kriptografskega modula, ki ga uporabljajo.

Zasebni ključi imetnikov potrdil RekonoAuth se aktivirajo z mehanizmi kriptografskega modula, ki ga uporablja imetnik. Imetniki morajo varovati zasebni ključ v skladu s sledečimi priporočili:

- zasebni ključ hranijo in uporabljajo na stojnem kriptografskem modulu (npr. čip pametne kartice); ali

- zasebni ključ hranijo in uporabljajo v programskem kriptografskem modulu, ki je zaščiten z geslom (npr. FireFox Software Security Device zaščiten z geslom); ali
- zasebni ključ hranijo in uporabljajo v programskem kriptografskem modulu operacijskega sistema, ki je zaščiten z geslom uporabniškega računa, s katerim dostopajo do operacijskega sistema; ali
- drugimi načini, ki so primerljivi z enim od zgoraj naštetih načinov.

6.2.9. Postopek za dezaktiviranje zasebnega ključa

Zasebni ključi storitev Rekono.TSP se dezaktivirajo ob zaustavitvi aplikacije za upravljanje digitalnih potrdil ali aplikacije storitve za elektronski časovni žig ali storitve za OCSP.

Zasebni ključi imetnikov potrdil RekonoSign za elektronski podpis na daljavo ali elektronski pečat na daljavo se dezaktivirajo takoj po uporabi.

Dezaktiviranje zasebnih ključev imetnikov je pod kontrolo kriptografskega modula na strani imetnikov. Imetniki so dolžni dezaktivirati ključe, kadar niso pod njihovim nadzorom.

6.2.10. Postopek za uničenje zasebnega ključa

Rekono.TSP bo v primeru potrebe izvedel uničenje vseh kopij zasebnih ključev svojih storitev v okviru nadzorovanega postopka.

6.2.11. Stopnja varnosti kriptografskih modulov

Glej 6.2.1.

6.3. Ostali vidiki upravljanja s pari ključev

6.3.1. Arhiviranje javnega ključa

Overitelj Rekono.TSP arhivira overiteljeve in imetniške javne ključe oziroma digitalna potrdila, kot je opisano v poglavju 5.5.4.

6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil

Obdobja uporabe javnih ključev in potrdil so:

- Javni ključ in potrdilo korenskega overitelja: 30 let in 3 mesece
- Javni ključ in potrdilo podrejenih overiteljev: 15 let in 3 mesece
- Javni ključ in potrdilo imetnikov: 5 let
- Javni ključ in potrdilo strežnikov elektronskega časovnega žiga: 5 let
- Zasebni ključ strežnikov elektronskega časovnega žiga: 2 leti
- Javni ključ in potrdilo strežnikov OCSP: 5 let
- Zasebni ključ strežnikov OCSP: 2 leti

6.4. Aktivacijski podatki

6.4.1. Generiranje in nameščanje aktivacijskih podatkov

Namenoma puščeno prazno.

6.4.2. Zaščita aktivacijskih podatkov

Namenoma puščeno prazno.

6.4.3. Drugi vidiki aktivacijskih podatkov

Namenoma puščeno prazno.

6.5. Varnostne zahteve za računalnike

6.5.1. Specifične varnostne zahteve za računalnike

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/).

6.5.2. Nivo varnostne zaščite računalnikov

Operacijski sistemi in drugi uporabljeni produkti so standardni (angl. off-the-shelf) produkti.

6.6. Tehnični nadzor življenjskega cikla overitelja

6.6.1. Nadzor razvoja sistema

Aplikacije in produkti, ki jih uporablja Rekono.TSP, so standardni (angl. off-the-shelf) produkti.

6.6.2. Upravljanje varnosti

Operacijski sistemi, na katerih deluje programska oprema overitelja, so bili varnostno okrepljeni (angl. hardened) v skladu s priporočili najboljše prakse.

Mrežni segmenti, v katerih so nameščeni strežniki overitelja, so ločeni od ostalih omrežij. Varnost med mrežnimi segmenti je zagotovljena z uporabo požarnih zidov z IPS funkcionalnostjo.

Pred vzpostavitvijo produkcijskega okolja je bil izveden preizkus varnosti (angl. vulnerability tests) sistemov Rekono.TSP. Preizkus varnosti se izvaja vsaj vsake 3 mesece.

6.6.3. Varnostna ocena (angl. Security Ratings) življenskega cikla

Namenoma puščeno prazno.

6.7. Varnostne kontrole na ravni računalniškega omrežja

Strežniki storitev Rekono.TSP so postavljeni v DMZ, ki je varovan s požarno pregrado z IPS funkcionalnostjo. Do strežnikov je dovoljen samo eksplicitno specificiran promet.

6.8. Časovno žigosanje

Rekono.TSP izvaja storitev elektronskega časovnega žiga v skladu z EN 319 421 [12] v obsegu za nekvalificirane ponudnike storitev zaupanja.

Storitev elektronskega časovnega žiga je dostopna preko spletnega vmesnika v skladu z RFC 3161 [4]. Dostopna je le drugim strežnikom in storitvam Rekono.TSP, kot je storitev za digitalni podpis na daljavo Rekono.Sign.

Sistemski čas strežnika za elektronske časovne žige se dnevno sinhronizira z uradnim časom UTC preko protokola NTP. Sinhronizacija se izvaja z NTP strežniki UTC(k) laboratorijev, ki so na BIMP listi (https://www.bipm.org).

V primeru večjega odstopanja lokalne ure od referenčnih virov bo, da se zagotovi odstopanje manjše od 1 sekunde, izdajanje časovnih žigov zaustavljeno.

V primeru poteklega potrdila strežnika elektronskega časovnega žiga bo izdajanje časovnih žigov zaustavljeno.

7. PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL

7.1. Profil digitalnih potrdil

7.1.1. Različica digitalnih potrdil

Rekono.TSP CA izdaja X.509 v3 digitalna potrdila skladna z RFC 5280 [3]. Digitalna potrdila vsebujejo naslednja osnovna polja::

X.509 polje	Opis
signature	Overiteljev digitalni podpis
issuer	Edinstveno razločevalno ime overitelja
validity	Obdobje veljavnosti digitalnega potrdila
subject	Edinstveno razločevalno ime imetnika potrdila
subjectPublicKeyInformation	Oznaka algoritma ključa
version	Različica potrdila X.509
serialNumber	Edinstvena serijska številka potrdila

7.1.2. Razširitvena polja

Razširitvena polja so namenjena uporabi dodatnih atributov v X.509 v3 potrdilih. Standardna razširitvena polja so definirana v skladu z RFC 5280, ki dovoljuje tudi uporabo lastnih razširitvenih polj za potrebe overiteljev.

Razširitvena polja v potrdilih korenskih overiteljev so:

X.509 polje	Opis
subjectKeyIdentifier	Zgoščena vrednost imetnikovega javnega ključa
keyUsage	Namen uporabe javnega ključa kot opredeljeno v **Error! Reference source not found.**. Polje je označeno kot kritično.
basicConstraints	Polje ima vrednost *true* v digitalnih potrdilih overiteljev Rekono.TSP. Polje je v potrdilih overiteljev označeno kot kritično.

Razširitvena polja v potrdilih podrejenih overiteljev so:

X.509 polje	Opis
authorityKeyIdentifier	Zgoščena vrednost javnega ključa korenskega overitelja

subjectKeyIdentifier	Zgoščena vrednost javnega ključa
keyUsage	Namen uporabe javnega ključa kot opredeljeno v 6.1.7. Polje je označeno kot kritično.
certificatePolicies: CertPolicyID CPS URI	 anyPolicy OID { 2 5 29 32 0 } Internet naslov do [Rekono.PKI] Pravil delovanja
CRLDistributionPoints	Naslovi, na katerih je objavljen seznam preklicanih potrdil.
basicConstraints	Polje ima vrednost *true* v digitalnih potrdilih overiteljev Rekono.TSP. Polje je v potrdilih overiteljev označeno kot kritično.
authorityInfoAccess	Polje vsebuje http naslov strežnika OCSP.

Razširitvena polja v potrdilih imetnikov so:

X.509 polje	Opis
authorityKeyIdentifier	Zgoščena vrednost overiteljevega javnega ključa
subjectKeyIdentifier	Zgoščena vrednost imetnikovega javnega ključa
keyUsage	Namen uporabe javnega ključa kot opredeljeno v 6.1.7. Polje je v vseh potrdilih označeno kot kritično.
extendedKeyUsage	Razširjeni namen uporabe digitalnih potrdil kot opredeljeno v 6.1.7.
certificatePolicies: CertPolicyID CPS URI	 Identifikacijsko oznaka potrdila v skladu s poglavjem 1.2 Spletni naslov do [Rekono.PKI] Pravil delovanja
CRLDistributionPoints	Naslovi, na katerih je objavljen register preklicanih potrdil.
basicConstraints	Polje ima vrednost *false* v vseh ostalih digitalnih potrdilih imetnikov. Polje je označeno kot kritično.

authorityInfoAccess	Polje vsebuje http naslov potrdila overitelja, ki je izdal digitalno potrdilo in http naslov strežnika OCSP.

Razširitvena polja v potrdilih RekonoTSU so v skladu z RFC 5280 in RFC 3161. Razširitvena polja v potrdilih RekonoOCSP so v skladu z RFC 5280 in RFC 6960.

7.1.3. Identifikacijske oznake (angl. object identifiers) algoritmov

Namenoma puščeno prazno.

7.1.4. Oblike imen

Digitalna potrdila vsebuje razločevalna imena v skladu s standardom X.501. Glej tudi 3.1.1.

7.1.5. Omejitve imen

Namenoma puščeno prazno.

7.1.6. Identifikacijska oznaka digitalnega potrdila

Vsa digitalna potrdila, izdana naročnikom, vsebujejo identifikacijsko oznako politike v polju `certificatePolicies`.

7.1.7. Uporaba omejitve imen

Namenoma puščeno prazno.

7.1.8. Specifični podatki o politiki (angl. Policy Qualifiers extension)

Namenoma puščeno prazno.

7.1.9. Procesiranje oznake kritičnosti razširitvenih polj digitalnega potrdila

Aplikacije morajo procesirati razširitvena polja digitalnega potrdil v skladu s priporočili RFC 5280 [3].

7.2. Profil registra preklicanih digitalnih potrdil

7.2.1. Različica

Registri preklicanih potrdil so v skladu s priporočili RFC 5280 [3]: Certificate and CRL Profile, verzija 2.

Registri preklicanih potrdil vsebujejo naslednja polja:

X.509 polje	Opis
Version	Verzija profila (v2)
Signature	Overiteljev digitalni podpis
Issuer	Edinstveno razločevalno ime overitelja
thisUpdate	Čas izdaje registra
nextUpdate	Čas izdaje naslednjega registra
revokedDigitalna potrdila	Serijske številke preklicanih digitalnih potrdil

7.2.2. Razširitvena polja registrov preklicanih potrdil

Overitelj uporablja X.509 Version 2 CRL razširitvena polja v skladu s priporočili RFC 5280 [3], navedena v naslednji tabeli:

X.509 polje	Opis
CRLNumber	Serijska številka registra
reasonCode	Koda razloga za preklic : (0) unused (1) keyCompromise (2) cACompromise (3) affiliationChanged (4) superseded (5) cessationOfOperation (6) certificateHold
invalidityDate	Datum in ura preklica

7.3. Profil OCSP

Profil OCSP sporočil (zahtevek/odgovor) storitve OCSP je v skladu z RFC2560/RFC6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.

8. PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA

Rekono d.o.o. izvaja notranji pregled delovanja Rekono.TSP enkrat letno.

Zunanjo presojo delovanja Rekono.TSP izvaja neodvisni revizijski in certifikacijski organ. Ocenjevanje in certificiranje se izvajata enkrat letno v skladu z ISO/IEC 27001.

Poročilo presoje oziroma posamezni deli so lahko na voljo za vpogled vsaki strani, ki izrazi interes in dokaže, da je takšno razkritje potrebno. Oceno upravičenosti zahtevka za vpogled za vsak primer posebej izvede RekonoPMA.

9. OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1. Cenik

9.1.1. Cena izdaje in upravljanja digitalnih potrdil

Rekono.TSP storitve se obračunavajo v sklopu storitve Rekono.ID, kot je opredeljeno v splošnih pogojih uporabe storitve Rekono.ID.

9.1.2. Cena dostopa do digitalnih potrdil v javnem imeniku

Namenoma puščeno prazno.

9.1.3. Cena dostopa do registra preklicanih potrdil

Preverjanje statusa potrdil preko seznama preklicanih potrdil ali storitve OCSP je brezplačno za vse naročnike, imetnike in tretje strani.

9.1.4. Cena ostalih storitev

Namenoma puščeno prazno.

9.1.5. Pravica vračila

Rekono.TSP storitve se obračunavajo v sklopu storitve Rekono.ID.

9.2. Finančna odgovornost

9.2.1. Zavarovanje odgovornosti

Namenoma puščeno prazno.

9.2.2. Druge oblike zavarovanja

Namenoma puščeno prazno.

9.2.3. Zavarovanja ali jamstva za končne uporabnike

Namenoma puščeno prazno.

9.3. Zaupnost poslovnih informacij

9.3.1. Obseg zaupnih poslovnih informacij

Za poslovno skrivnost podjetja Rekono se štejejo listine in podatki, ki so z zakonom, statutom, pravili ali drugim splošnim aktom ali sklepom direktorja podjetja Rekono d.o.o. (v nadaljnjem besedilu: direktor) oziroma osebe, ki jo je pisno pooblastil (v nadaljnjem besedilu: pooblaščena oseba), razglašeni za poslovno skrivnost in so tako pomembni, da bi z njihovo izdajo očitno nastale ali bi lahko nastale hujše škodljive posledice.

Ne glede na to, ali so določeni s sklepi iz prejšnjega odstavka, se za poslovno skrivnost štejejo tudi podatki, za katere je očitno, da bi nastala občutna škoda, če bi zanje izvedela nepooblaščena oseba.

9.3.2. Informacije izven obsega zaupnih poslovnih informacij

Informacije, ki so objavljene v digitalnih potrdilih in CRL ali druge informacije v javnih repozitorijih Rekono.TSP, se ne štejejo kot zaupne.

9.3.3. Odgovornost za zagotavljanje zaupnosti poslovnih informacij

Rekono.TSP je odgovoren za zaščito zaupnih informacij v skladu z veljavno zakonodajo (glej 0) in v skladu s pravilnikom Rekono d.o.o. o varovanju poslovnih skrivnosti – Pravilnik o varovanju poslovnih skrivnosti.

9.4. Varovanje osebnih podatkov

9.4.1. Načrt zagotavljanja varovanja osebnih podatkov

Rekono.TSP izvaja varovanje osebnih podatkov v skladu z veljavno zakonodajo (glej 0) in v skladu s pravilnikom Rekono d.o.o. - Pravilnik o postopkih in ukrepih za zavarovanje osebnih podatkov.

9.4.2. Obseg varovanih osebnih podatkov

Vse informacije o imetniku digitalnega potrdila ali naročniku, ki niso objavljene v potrdilu, se štejejo kot zaupne.

9.4.3. Osebni podatki, ki se ne obravnavajo kot zaupni

Informacije, vsebovane v digitalnem potrdilu, CRL ali druge informacije, objavljene v javnih repozitorijih Rekono.TSP, se ne štejejo kot zaupne.

9.4.4. Odgovornost glede varovanja osebnih podatkov

Rekono.TSP je odgovoren za varovanje osebnih podatkov v skladu z veljavno zakonodajo (glej 9.14) in v skladu s pravilnikom Rekono d.o.o. - Pravilnik o postopkih in ukrepih za zavarovanje osebnih podatkov.

9.4.5. Privolitev posameznika za uporabo osebnih podatkov

Naročnik je pred izdajo potrdila v okviru splošnih pogojev seznanjen, kateri osebni podatki bodo vsebovani v potrdilu. Naročnik hkrati s potrditvijo strinjanja s pogoji uporabe poda tudi privolitev za uporabo osebnih podatkov v potrdilu.

Naročnik se s potrditvijo strinjanja s pogoji uporabe podatkov strinja tudi z nameni njihove uporabe. Potrditev hkrati pomeni, da uporabnik z Rekono.TSP sklene pogodbo o izvedbi storitve izdaje potrdila, ki je tudi pravna podlaga za obdelavo naročnikovih podatkov.

9.4.6. Posredovanje osebnih podatkov v sodnih in upravnih postopkih

Zaupne informacije bodo posredovane pristojnim organom v skladu z veljavno zakonodajo (glej 0).

9.4.7. Druge okoliščine posredovanja osebnih podatkov

Rekono d.o.o bo posredoval osebne podatke le v primerih, kot je navedeno v 9.4.6.

9.5. Zaščita intelektualne lastnine

Imetnik vseh intelektualnih pravic na digitalnih potrdilih, elektronskih časovnih žigih in pripadajoči dokumentaciji je Rekono d.o.o.

Naročnik ima za čas, ko ima veljavno sklenjeno naročnino za uporabo digitalnega potrdila, pravico do uporabe digitalnega potrdila, elektronskega časovnega žiga in pripadajoče dokumentacije v skladu s splošnimi pogoji uporabe.

9.6. Odgovornost in jamstva

9.6.1. Odgovornost in jamstva overitelja

Rekono.TSP mora izdati digitalna potrdila, elektronske časovne žige in opravljati druge postopke, povezane z upravljanjem potrdil in infrastrukture Rekono.TSP v skladu s temi Rekono.TSP Pravili delovanja in veljavno zakonodajo (glej 0). Rekono.TSP je odgovoren tudi za postopke in dejanja zunanjih izvajalcev.

Povzetek Rekono.TSP dolžnosti:

- Zagotoviti, da so podatki o naročniku in overitelju v digitalnem potrdilu točni.
- Preveriti identiteto prosilcev pred izdajo digitalnega potrdila preko prijave uporabnika v račun Rekono.ID.
- Zagotavljati točnost in celovitost informacij, objavljenih v javnih repozitorijih.
- Izdati potrdila naročnikom v skladu s temi Rekono.TSP Pravili delovanja.
- Preklicati digitalna potrdila po prejetju zahteve ali iz drugih razlogov v skladu s temi Rekono.TSP Pravili delovanja.
- Izdati in objaviti seznam preklicanih potrdil.
- Zagotoviti dostop do seznama preklicanih potrdil in storitve OCSP.
- Zagotoviti, da se zaposleni in zunanji izvajalci zavedajo določil, ki jih zadevajo, v skladu s temi Rekono.TSP Pravili delovanja.

9.6.2. Odgovornost in jamstva prijavne službe

Naloge RA se izvajajo preko storitve Rekono.ID. Odgovornosti in jamstva Rekono.ID so opredeljeni v Splošnih pogojih uporabe storitve Rekono (https://www.rekono.si/sl/kako-deluje/splosni-pogoji/).

9.6.3. Odgovornost in jamstva imetnikov digitalnih potrdil

Poleg izpolnjevanja obveznosti, ki izhajajo iz Rekono.TSP Pravil delovanja, mora naročnik:

- Zagotavljati zaupnost svojih zasebnih kriptografskih ključev ter upoštevati vse ukrepe, da se preprečijo izguba, razkritje, sprememba ali nepooblaščena uporaba.
- Skrbno varovati kodo (geslo, PIN) za aktiviranje zasebnih ključev.
- Takoj obvestiti Rekono.TSP v primeru kakršnihkoli nepravilnosti ali v primeru spremembe podatkov, vsebovanih v digitalnem potrdilu.
- Izključno uporabljati svoje kriptografske ključe in pripadajoče digitalno potrdilo za namene, navedene v poglavju 1.4.
- V primeru ogrožanja ali suma ogrožanja zasebnega ključa takoj obvestiti Rekono.TSP in preklicati pripadajoče digitalno potrdilo.
- V primeru zlorabe ali suma zlorabe kateregakoli potrdila, ki ga je izdal Rekono.TSP, o tem takoj obvestiti Rekono.TSP.

9.6.4. Odgovornost in jamstva tretjih oseb

Tretje osebe morajo, preden se zanašajo na digitalna potrdila Rekono.TSP, obvezno preveriti veljavnost in status digitalnih potrdil. Poleg tega morajo:

- Zavedati se namena uporabe in omejitev uporabe posameznega digitalnega potrdila ter omejitev odgovornosti Rekono.TSP, kot je opisano v teh Rekono.TSP Pravilih delovanja.
- Omejiti uporabo digitalnih potrdil izključno na namene, navedene v poglavju 1.4.
- Pred vsako uporabo preveriti, da digitalno potrdilo ni bilo preklicano.
- V primeru zlorabe ali suma zlorabe kateregakoli potrdila, ki ga je izdal Rekono.TSP, o tem takoj obvestiti Rekono.TSP.

9.6.5. Odgovornost in jamstva drugih udeležencev

Namenoma puščeno prazno.

9.7. Zanikanje odgovornosti

Razen za jamstva, navedena v 9.6.1, v drugih poglavjih teh Rekono.TSP Pravilih delovanja in v največji meri, kot to dovoljuje veljavna zakonodaja (glej 0.), Rekono.TSP izključuje svojo odgovornost za škodo (direktno ali posredno),

izgubljeni dobiček, izgubljene, uničene ali nedostopne podatke, kakršnekoli druge izgube, stroške ter terjatve, ki izhajajo iz ali so nastale zaradi uporabe digitalnih potrdil overiteljev Rekono.TSP in z njimi povezanih ključev.

Zlasti Rekono.TSP izključuje:

- Vsakršno odgovornost, če je bilo potrdilo izdano kot rezultat napake, neverodostojnosti podatkov, posredovanih s strani naročnika, ali drugih dejanj naročnika oziroma imetnika ali katerekoli druge fizične ali pravne osebe;
- Vsakršno odgovornost, če je bilo digitalno potrdilo uporabljeno po preteku obdobja veljavnosti;
- Vsakršno odgovornost, če je bilo digitalno potrdilo uporabljeno po preklicu in objavi na seznamu preklicanih potrdil;
- Vsakršno odgovornost za morebitno škodo, ki se lahko pojavi ob trenutku, ko Rekono.TSP prejme veljavno zahtevo za preklic, do trenutka objave informacij o preklicu na seznamu preklicanih potrdil v skladu s poglavjem 4.9.5.
- Vsakršno odgovornost, če so bili podatki v digitalnem potrdilu na kakršen koli način spremenjeni;
- Vsakršno odgovornost, če je bil zasebni ključ naročnika/imetnika razkrit ali obstaja sum, da je bil razkrit;
- Vsakršno odgovornost, če je bilo digitalno potrdilo uporabljeno v druge namene, kot je dovoljeno s temi Rekono.TSP Pravili delovanja, ali pa v nasprotju z veljavno zakonodajo (glej 0.);
- Vsakršno odgovornost, če naročnik, imetnik ali tretja oseba ni postopala v skladu s temi Rekono.TSP Pravili delovanja ali morebitno drugo pogodbo;
- Vsakršno odgovornost, če je nastala škoda zaradi napake v delovanju strojne ali programske opreme naročnika/imetnika ali tretje osebe.
- Odgovornost za škodo, ki bi nastala zaradi višje sile kot je opisano v poglavju 9.16.5.

9.8. Omejitve odgovornosti

V primeru škode, ki bi nastala pri uporabi digitalnih potrdil ali elektronskega časovnega žiga brez upoštevanja ali v nasprotju z določbami teh Rekono.TSP Pravili delovanja s strani naročnika, imetnika ali tretjih osebe, Rekono.TSP ne odgovarja za škodo, ki bi pri taki uporabi nastala.

Razen v primerih, kjer bi odgovornost Rekono.TSP nastala zaradi njegovega naklepnega ravnanja ali velike malomarnosti, Rekono.TSP ne prevzema nobene odgovornosti za kakršnokoli škodo, nadomestilo, obveznost povrnitve terjatev ali obveznosti katerekoli vrste v zvezi z izdajo ali uporabo digitalnih potrdil ali elektronskih časovnih žigov.

9.9. Poravnava škode

Vsaka stranka nosi izključno odgovornost za oškodovanje Rekono.TSP ali drugega subjekta za škodo, ki je posledica nepravilne uporabe digitalnega potrdila, ali če ne ravna v skladu s temi Rekono.TSP Pravili delovanja in veljavno zakonodajo (glej 0.).

9.10. Začetek in prenehanje veljavnosti

9.10.1. Začetek veljavnosti

Rekono.TSP Pravila delovanja in drugi dokumenti Rekono.TSP stopijo v veljavo, ko so potrjeni s strani zakonitega zastopnika Rekono d.o.o.

9.10.2. Prenehanje veljavnosti

Veljavnost Rekono.TSP Pravil delovanja ni časovno omejena. Trenutna verzija je veljavna do uveljavitve nove verzije oziroma do prenehanja delovanja Rekono.TSP.

9.10.3. Učinek in posledice prenehanja veljavnosti

Po prenehanju veljavnosti Rekono.TSP Pravil delovanja zaradi objave nove verzije, ki vsebuje nove identifikacijske oznake v polju `certificatePolicies`, vsi subjekti uporabljajo obstoječa potrdila v skladu z verzijo določil Rekono.TSP Pravil delovanja, po kateri so bila izdana. V primeru, da zaradi spremenjenih okoliščin to ne bo več mogoče, bo overitelj ob izdaji nove verzije Rekono.TSP o tem obvestil naročnike.

V primeru, ko nova verzija vsebuje enake identifikacijske oznake v polju `certificatePolicies`, vsi subjekti uporabljajo obstoječa potrdila v skladu z določili nove verzije Rekono.TSP Pravil delovanja.

9.11. Obvestila in komuniciranje z udeleženci

Rekono.TSP objavlja trenutno verzijo teh Rekono.TSP Pravil delovanja in trenutno verzijo vseh ostalih javnih dokumentov na javni spletni strani na naslovu, navedenem v poglavju 2.1. Glej tudi 9.12.2.

9.12. Spreminjanje dokumenta

9.12.1. Postopek uveljavitve sprememb

RekonoPMA pripravi spremembe oziroma predlog sprememb in jih posreduje RekonoOA v pregled oziroma uskladitev. Po končanem usklajevanju sprememb RekonoPMA predloži novo verzjijo pravil delovanja v pregled in odobritev zakonitemu zastopniku Rekono d.o.o.

9.12.2. Postopek obveščanja in rok za pripombe

Vse spremembe Rekono.TSP Pravil delovanja bodo objavljene, kot je opisano v poglavju 2. Rekono.TSP bo preko elektronske pošte obvestil naročnike o spremembah, ki imajo materialen vpliv na naročnike ali tretje strani.

Rekono.TSP se na podlagi lastne presoje odloči, da ne obvesti naročnikov in tretjih strani v primeru sprememb, ki nimajo materialnega vpliva na uporabo digitalnih potrdil ali elektronskega časovnega žiga. V takem primeru bodo spremembe objavljene samo na javni spletni strani na naslovu, navedenem v poglavju 2.1.

9.12.3. Spremembe, ki zahtevajo novo identifikacijsko oznako politike

Identifikacijska oznaka politike digitalnih potrdil, vsebovana v polju `certificatePolicies`, bo spremenjena le v primeru sprememb, ki imajo materialni vpliv na naročnike ali tretje strani. Na primer v primeru spremembe namena uporabe ali sprememb, ki vplivajo na nivo zaupanja v digitalno potrdilo, interpretacijo digitalnih potrdil ali nivo zaupanja v elektronski časovni žig.

9.13. Reševanje sporov

Spori med subjekt (poglavje 1.3.) bodo, če je le mogoče, rešeni sporazumno. Za vse spore, ki niso rešeni sporazumno, je pristojno sodišče v Ljubljani.

9.14. Veljavna zakonodaja

Rekono.TSP deluje v skladu z zakonodajo Republike Slovenije, navedeno v poglavju 9.15.

9.15. Skladnost s pravnimi akti

Rekono.TSP deluje 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;
- zakonom, ki ureja e-identifikacijo in storitve zaupanja;
- splošno uredbo o varstvu podatkov (GDPR);
- zakonom, ki ureja varstvo osebnih podatkov (ZVOP); in
- ostalimi predpisi, ki veljajo na območju Republike Slovenije.

9.16. Splošne določbe

9.16.1. Ostali obvezujoči dokumenti

Ostali obvezujoči dokumenti so:

- Splošni pogoji uporabe storitve Rekono.ID
- Interni akti družbe Rekono d.o.o.

9.16.2. Prenos pravic in obveznosti

Naročnik ali imetnik digitalnega potrdila ne sme v nobenem primeru prenesti pravic in obveznosti uporabe digitalnih potrdil delno ali v celoti na tretjo stran.

9.16.3. Spremembe okoliščin delovanja

Ničnost enega ali več delov teh Rekono.TSP Pravil delovanja ne vpliva na veljavnost drugih določb, če je zagotavljano, da ni materialnega vpliva na nivo zaupanja in uporabo digitalnih potrdil.

9.16.4. Uveljavljanje (povračila stroškov v primeru sporov in izjeme)

Namenoma puščeno prazno.

9.16.5. Višja sila

Višja sila so izredne nepremagljive in nepredvidljive okoliščine, ki nastopijo po sklenitvi pogodbe in so zunaj volje ali sfere pogodbenih strank (v celoti tuje pogodbenim strankam), kot na primer požar, potres, druge elementarne nezgode in podobno.

Za višjo silo štejejo tudi predpisi, posamični akti in dejanja ter drugi ukrepi organov Evropske skupnosti, ki izpolnjujejo pogoje iz prejšnjega odstavka. Za višjo silo štejejo tudi predpisi, posamični akti ali ukrepi organov RS, ki pomenijo vključitev obveznih določb predpisov Evropske skupnosti v pravni red Republike Slovenije ali ki pomenijo izvrševanje neposredno uporabljivih pravil prava te skupnosti, ki izpolnjujejo pogoje za višjo silo iz prejšnjega odstavka.

Nobena stranka ne more uveljavljati zahtevkov, ki ji po tem dokumentu, pogodbi ali po zakonu pripadajo zaradi kršitve druge stranke, če je do ravnanja v nasprotju s pogodbo prišlo zaradi višje sile.

Če je zaradi višje sile začasno onemogočeno izvrševanje kakšne obveznosti po tem dokumentu ali dogovoru, se rok za izvršitev ustrezno podaljša.

9.17. Ostale določbe

Namenoma puščeno prazno.

Dodatek A: 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"