



**Ponudnik storitev zaupanja Rekono.TSP
Pravila delovanja za POŠTA®CA
(Certification Practice Statement)**

Verzija: 1.0
Datum izdaje: 08. Junij 2023
Datum uveljavitve: 29. Junij 2023

Zaščita dokumenta

© podjetje Rekono d.o.o.

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

Nadzor različic dokumenta

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

Zgodovina sprememb dokumenta:

Razl.	Datum	Opis / opomba
1.0	08.06.2023	Prva izdaja dokumenta Rekono.TSP Pravila delovanja za POŠTA®CA.

Kazalo

1.	UVOD.....	7
1.1.	Pregled	7
1.2.	Naziv dokumenta in identifikacijske oznake digitalnih potrdil	8
1.3.	Udeleženci infrastrukture javnih ključev	17
1.3.1.	Ponudniki storitev	17
1.3.2.	Registracijska pisarna ponudnika storitev	20
1.3.3.	Naročniki in imetniki digitalnih potrdil	20
1.3.4.	Tretje osebe	21
1.3.5.	Ostali udeleženci.....	21
1.4.	Namen uporabe digitalnih potrdil.....	21
1.4.1.	Dovoljena uporaba digitalnih potrdil	21
1.4.2.	Nedovoljena uporaba digitalnih potrdil	21
1.5.	Upravljanje s pravili delovanja	21
1.5.1.	Organizacija, ki upravlja s pričujočim dokumentom.....	21
1.5.2.	Kontaktne podatke ponudnika storitev zaupanja Rekono.TSP...	21
1.5.3.	Oseba, ki ugotavlja ustreznost Politike.....	22
1.5.4.	Postopek odobritve pravil delovanja ponudnika storitev	22
1.6.	Pojmi in kratice	22
2.	Objave in repozitorij	23
2.1.	Repozitorij	23
2.2.	Objave informacij o digitalnih potrdilih	23
2.3.	Čas in pogostost objav	23
2.4.	Dostop do podatkov v repozitoriju	23
3.	Prepoznavanje in preverjanje istovetnosti	24
3.1.	Določanje imen	24
3.2.	Prva registracija.....	24
3.3.	Preverjanje istovetnosti pri obnovi digitalnega potrdila	24
3.4.	Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila	24
4.	Upravljanje z digitalnimi potrdili.....	25
4.1.	Vloga za izdajo digitalnega potrdila	25
4.2.	Obdelava vloge za izdajo digitalnega potrdila	25
4.3.	Izdaja digitalnega potrdila	25
4.4.	Prevzem digitalnega potrdila.....	25
4.5.	Uporaba ključev in digitalnih potrdil.....	25
4.6.	Obnova digitalnih potrdil brez spremembe ključev	25
4.7.	Obnova digitalnih potrdil	25
4.8.	Sprememba digitalnega potrdila	25
4.9.	Začasna ukinitve veljavnosti in preklic digitalnega potrdila	25
4.9.1.	Okoliščine preklica.....	25

4.9.2.	Kdo lahko zahteva preklic	26
4.9.3.	Postopki za preklic	27
4.9.4.	Čas za posredovanje vloge za preklic.....	27
4.9.5.	Čas od vloge za preklic do preklica.....	27
4.9.6.	Obveza preverjanja registra preklicanih potrdil.....	27
4.9.7.	Pogostost objav registrov preklicanih potrdil	27
4.9.8.	Dovoljene zakasnitve sprotnega preverjanja statusa digitalnih potrdil	28
4.9.9.	Storitev sprotnega preverjanja statusa digitalnih potrdil	28
4.9.10.	Obveza sprotnega preverjanja statusa digitalnih potrdil.....	28
4.9.11.	Ostale oblike objavljanja preklicanih digitalnih potrdil	28
4.9.12.	Posebne zahteve glede zlorabe ključa.....	28
4.9.13.	Okoliščine za začasno ukinitve veljavnosti (suspenz) digitalnega potrdila	28
4.9.14.	Kdo lahko zahteva suspenz ali ukinitve suspenza digitalnega potrdila	28
4.9.15.	Postopki za suspenz ali ukinitve suspenza digitalnega potrdila	28
4.9.16.	Omejitve obdobja začasne ukinitve veljavnosti	28
4.10.	Storitve objavljanja statusa digitalnih potrdil	28
4.10.1.	Tehnične lastnosti storitve	28
4.10.2.	Razpoložljivost storitve dostopa do seznama preklicanih potrdil	29
4.10.3.	Dodatne možnosti	29
4.11.	Trajanje naročniškega razmerja.....	29
4.12.	Varnostno kopiranje in odkrivanje zasebnega ključa	30
5.	Fizično varovanje, organizacijski varnostni ukrepi in zahteve za osebje	31
6.	Tehnične varnostne zahteve	32
6.1.	Tvorjenje in namestitve para ključev.....	32
6.2.	Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov	32
6.3.	Ostali vidiki upravljanja s pari ključev	32
6.4.	Aktivacijski podatki	32
6.5.	Varnostne zahteve za računalnike	32
6.6.	Tehnični nadzor življenjskega cikla overitelja	32
6.7.	Varnostne kontrole na ravni računalniškega omrežja	32
6.8.	Časovno žigosanje	32
7.	Profil digitalnih potrdil in registrov preklicanih potrdil	33
8.	Preverjanje skladnosti in ostale oblike nadzora	34
9.	Ostale poslovne in pravne zadeve	35
9.1.	Cenik.....	35

9.1.1.	Cena izdaje in upravljanja digitalnih potrdil	35
9.1.2.	Cena dostopa do digitalnih potrdil v javnem imeniku	35
9.1.3.	Cena dostopa do registra preklicanih potrdil	35
9.1.4.	Cena ostalih storitev.....	35
9.1.5.	Pravica vračila.....	35
9.2.	Finančna odgovornost	35
9.2.1.	Zavarovanje odgovornosti	35
9.2.2.	Druge oblike zavarovanja	35
9.2.3.	Zavarovanja ali jamstva za končne uporabnike.....	35
9.3.	Zaupnost poslovnih informacij.....	35
9.3.1.	Obseg zaupnih poslovnih informacij.....	35
9.3.2.	Informacije izven obsega zaupnih poslovnih informacij.....	36
9.3.3.	Odgovornost za zagotavljanje zaupnosti poslovnih informacij.....	36
9.4.	Varovanje osebnih podatkov	36
9.4.1.	Načrt zagotavljanja varovanja osebnih podatkov.....	36
9.4.2.	Obseg varovanih osebnih podatkov.....	36
9.4.3.	Osebni podatki, ki se ne obravnavajo kot zaupni.....	36
9.4.4.	Odgovornost glede varovanja osebnih podatkov	36
9.4.5.	Privolitev posameznika za uporabo osebnih podatkov.....	36
9.4.6.	Posredovanje osebnih podatkov v sodnih in upravnih postopkih	36
9.4.7.	Druge okoliščine posredovanja osebnih podatkov.....	36
9.5.	Zaščita intelektualne lastnine.....	37
9.6.	Odgovornost in jamstva	37
9.6.1.	Odgovornost in jamstva ponudnika storitev	37
9.6.2.	Odgovornost in jamstva prijavnih služb.....	38
9.6.3.	Odgovornost in jamstva imetnikov digitalnih potrdil.....	38
9.6.4.	Odgovornost in jamstva tretjih oseb.....	39
9.6.5.	Odgovornost in jamstva drugih udeležencev	40
9.7.	Zanikanje odgovornosti	40
9.8.	Omejitve odgovornosti.....	40
9.9.	Poravnava škode	41
9.10.	Začetek in prenehanje veljavnosti.....	41
9.10.1.	Začetek veljavnosti.....	41
9.10.2.	Prenehanje veljavnosti	41
9.10.3.	Učinek in posledice prenehanja veljavnosti.....	41
9.11.	Obvestila in komuniciranje z udeleženci	41
9.12.	Spreminjanje dokumenta	41
9.12.1.	Postopek uveljavitve sprememb	41
9.12.2.	Postopek obveščanja in rok za pripombe	41

9.12.3.	Spremembe, ki zahtevajo novo identifikacijsko oznako politike	42
9.13.	Reševanje sporov	42
9.14.	Veljavna zakonodaja	42
9.15.	Skladnost s pravnimi akti.....	42
9.16.	Splošne določbe	42
9.16.1.	Ostali obvezujoči dokumenti	42
9.16.2.	Prenos pravic in obveznosti.....	42
9.16.3.	Spremembe okoliščin delovanja	43
9.16.4.	Uveljavljanje (povračila stroškov v primeru sporov in izjeme)...	43
9.16.5.	Višja sila	43
9.17.	Ostale določbe	43

1. UVOD

1.1. Pregled

Pričujoči dokument opisuje pravila delovanja ponudnika kvalificiranih in nekvalificiranih storitev zaupanja Rekono.TSP za izvajanje preklica in objavo statusa potrdil izdajatelj potrdil POŠTA@CA.

Kvalificirani ponudnik storitve zaupanja, Certifikatska agencija Pošte Slovenije, krajše overitelj POŠTA@CA, je bil ustanovljen v okviru POŠTE SLOVENIJE d.o.o., Maribor (v nadaljevanju Pošta Slovenije). Overitelj POŠTA@CA je izdajal različne vrste digitalnih potrdil (kvalificirana potrdila in normalizirana potrdila) različnim končnim uporabnikom v skladu z Zakon o elektronski identifikaciji in storitvah zaupanja (Uradni list RS, št. 121/21 z dne 23. 7. 2021, v nadaljevanju ZEISZ), Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1993/93/ES (Uredba eIDAS), evropskimi direktivami ter drugimi veljavnimi predpisi in priporočili.

Overitelj POŠTA@CA je z dnem prenehanja izdajanja potrdil naročnikom (28.06.2023) prenesel upravljanje storitve na ponudnika storitev zaupanja Rekono.TSP, ki ga je ustanovil in ga upravlja Rekono d.o.o. Ponudnik storitev zaupanja Rekono.TSP je akreditiran ponudnik storitev zaupanja v skladu z Uredbo eIDAS za overjanje digitalnih potrdil za kvalificirani elektronski podpis, kvalificirani elektronski žig, napredni elektronski podpis, napredni elektronski žig, potrdil za elektronsko avtentikacijo in izdajanje naprednih elektronskih časovnih žigov.

Ponudnik storitev zaupanja Rekono.TSP bo od dneva prevzema overitelja POŠTA@CA do konca poteka veljavnosti vseh potrdil, ki jih je izdal overitelj POŠTA@CA, izvajal preklic potrdil in objavo statusa potrdil. To bo omogočilo nemoteno uporabo potrdil, izdanih s strani overitelja POŠTA@CA, do konca obdobja njihove veljavnosti.

Do konca prenehanja izdaje potrdil overitelja POŠTA@CA je bila v veljavi in se je v celoti uporabljala Politika POŠTA@CA za kvalificirana in normalizirana potrdila, javni del notranjih pravil delovanja. V nadaljevanju Politika POŠTA@CA.

Vsa potrdila overitelja POŠTA@CA so bila izdana po Politiki POŠTA@CA, ki ostane v veljavi kot referenca za potrebe ocene postopkov overitelja POŠTA@CA do datuma prenehanja izdaje potrdil.

Politika POŠTA@CA se preneha uporabljati z datum uveljavitve pričujočih Rekono.TSP Pravil delovanja za POŠTA@CA. Politika POŠTA@CA postane priloga pričujočih Rekono.TSP Pravil delovanja za POŠTA@CA.

Pričujoči dokument, Rekono.TSP Pravila delovanja za POŠTA@CA, vsebuje opis pravil ter postopkov, ki jih izvaja Rekono d.o.o. za opravljanje storitev zaupanja, ki obsega preklic in objavo statusa digitalnih potrdil overitelja POŠTA@CA. Rekono.TSP Pravila delovanja za POŠTA@CA povzema po Politiki POŠTA@CA identifikacijske oznake potrdil POŠTA@CA, namene uporabe potrdil POŠTA@CA ter postopke preklica potrdil. V delih, ki se nanašajo na postopke izdaje potrdil, ki se ne izvajajo več, se sklicuje na Politiko POŠTA@CA. V delih, ki se nanašajo na upravljanje infrastrukture in varnostne kontrole, se sklicuje na Rekono.TSP Pravila delovanja.

Dokument Rekono.TSP Pravila delovanja za POŠTA@CA predstavlja javni del notranjih pravil delovanja ponudnika storitev zaupanja Rekono.TSP. Zaupni del notranjih pravil delovanja ponudnika storitev zaupanja Rekono.TSP predstavlja interni poslovnik za upravljanje storitev in informacijske varnosti podjetja Rekono d.o.o.

Struktura dokumenta Rekono.TSP Pravila delovanja za POŠTA@CA 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 za POŠTA@CA je usklajena z RFC 3647, [1], RFC 5280 [3], EN 319 401 [5], EN 319 411-1 [2], EN 319 411-2 [15] in EN 319 421 [12].

1.2. Naziv dokumenta in identifikacijske oznake digitalnih potrdil

Pričujoči dokument, Rekono.TSP Pravila delovanja za POŠTA@CA, predstavlja pravila delovanja ponudnika storitev zaupanja Rekono.TSP za preklic in objavo statusa potrdil POŠTA@CA, ki so bila izdana po Politiki POŠTA@CA.

Naziv dokumenta, sl:	Rekono.TSP Pravila delovanja za POŠTA@CA
Naziv dokumenta, en.:	Certification Practice Statement of the Rekono.TSP for POŠTA@CA
Verzija:	1.0
Datum izdaje:	08. Junij 2023
Datum uveljavitve:	29. Junij 2023

Rekono.TSP Pravila delovanja za POŠTA@CA veljajo za potrdila, ki so označena z identifikacijskimi oznakami politik (angl. Policy Object Identifiers), navedenimi v spodnji tabeli.

Tabela: identifikacijske oznake potrdil overitelja POŠTA®CA

Kvalificirana potrdila za zaposlene pri pravnih osebah	
1. POŠTA®CA – Napredna kvalificirana potrdila	
Opis:	kvalificirana potrdila z dvema paroma ključev za fizične osebe zaposlene pri pravnih osebah, z obvezno uporabo QSCD naprave
Vrsta:	kvalificirano potrdilo za kvalificirani elektronski podpis
Namen uporabe:	kvalificirani elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.1.1.1.3 qcp-natural-qscd (0.4.0.194112.1.2)
Izdajatelji:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
2. POŠTA®CA – Kvalificirana potrdila z obvezno uporabo QSCD naprave	
Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah. Obvezna je uporaba QSCD naprave.
Vrsta:	kvalificirano potrdilo za kvalificirani elektronski podpis
Namen uporabe:	kvalificirani elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.1.1.1.2.3 qcp-natural-qscd (0.4.0.194112.1.2)
Izdajatelji:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
Opomba	Od objave politike verzije 1.4 se ne izdajajo več. Vsa izdana potrdila ostanejo v uporabi do izteka veljavnosti.
3. POŠTA®CA – Kvalificirana potrdila	
Opis:	osnovna kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah.

Rekono.TSP Pravila delovanja za POŠTA®CA

Vrsta:	kvalificirano potrdilo za elektronski podpis
Namen uporabe:	napredni elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.2.1.2.3 qcp-natural (0.4.0.194112.1.0)
Izdajatelj:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
4. POŠTA®CA – Kvalificirana potrdila, izdana na QSCD napravi	
Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah. Potrdilo je izdano na QSCD napravi.
Vrsta:	kvalificirano potrdilo za kvalificirani elektronski podpis
Namen uporabe:	kvalificirani elektronski podpis
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.3.1.2.2 qcp-natural-qscd (0.4.0.194112.1.2)
Izdajatelj:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
Opomba	Od objave politike verzije 1.4 je namen uporabe kvalificirani elektronski podpis. Pred verzijo 1.4 je bil namen uporabe kvalificirani elektronski podpis, šifriranje in avtentikacija.
5. POŠTA®CA – Kvalificirana potrdila, izdana na oddaljeni QSCD napravi	
Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah, izdana na oddaljeni QSCD napravi
Vrsta:	kvalificirano potrdilo za kvalificirani elektronski podpis
Namen uporabe:	kvalificirani elektronski podpis
Rok veljavnosti:	do tri (3) leta
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.5.1.2.1 qcp-natural-qscd (0.4.0.194112.1.2)
Izdajatelj:	OU=POSTArCA, O=POSTA, C=SI

Rekono.TSP Pravila delovanja za POŠTA®CA

CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI

6. POŠTA®CA – Kvalificirana potrdila s splošnim nazivom z obvezno uporabo QSCD naprave

Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah, z dodatnim splošnim nazivom v polju <i>commonName</i> in obvezno uporabo QSCD naprave
Vrsta:	kvalificirano potrdilo za kvalificirani elektronski podpis
Namen uporabe:	kvalificirani elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.1.4.2.1 qcp-natural-qscd (0.4.0.194112.1.2)
Izdajatelji:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
Opomba	Od objave politike verzije 1.3 se ne izdajajo več. Vsa izdana potrdila ostanejo v uporabi do izteka veljavnosti.

7. POŠTA®CA – Kvalificirana potrdila s splošnim nazivom

Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah, z dodatnim splošnim nazivom v polju <i>commonName</i> .
Vrsta:	kvalificirano potrdilo za elektronski podpis
Namen uporabe:	napredni elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.2.4.2.1 qcp-natural (0.4.0.194112.1.0)
Izdajatelji:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
Opomba	Od objave politike verzije 1.3 se ne izdajajo več. Vsa izdana potrdila ostanejo v uporabi do izteka veljavnosti.

8. POŠTA®CA – Kvalificirana potrdila s splošnim nazivom, izdana na QSCD napravi

Rekono.TSP Pravila delovanja za POŠTA®CA

Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah, z dodatnim splošnim nazivom v polju commonName, izdana na QSCD napravi
Vrsta:	kvalificirano potrdilo za kvalificirani elektronski podpis
Namen uporabe:	kvalificirani elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.3.4.2.1 qcp-natural-qscd (0.4.0.194112.1.2)
Izdajatelji:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
Opomba	Od objave politike verzije 1.3 se ne izdajajo več. Vsa izdana potrdila ostanejo v uporabi do izteka veljavnosti.

Kvalificirana potrdila za fizične osebe

9. POŠTA®CA – Napredna kvalificirana potrdila

Opis:	kvalificirana potrdila z dvema paroma ključev za fizične osebe in obvezno uporabo QSCD naprave
Vrsta:	kvalificirano potrdilo za kvalificirani elektronski podpis
Namen uporabe:	kvalificirani elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.1.2.1.2 qcp-natural-qscd (0.4.0.194112.1.2)
Izdajatelji:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI

10. POŠTA®CA – Kvalificirana potrdila z obvezno uporabo QSCD naprave

Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe in obvezno uporabo QSCD naprave
Vrsta:	kvalificirano potrdilo za kvalificirani elektronski podpis
Namen uporabe:	kvalificirani elektronski podpis, šifriranje in avtentikacija

Rekono.TSP Pravila delovanja za POŠTA®CA

Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.1.2.2.2 qcp-natural-qscd (0.4.0.194112.1.2)
Izdajatelji:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
Opomba	Od objave politike verzije 1.4 se ne izdajajo več. Vsa izdana potrdila ostanejo v uporabi do izteka veljavnosti.
11. POŠTA®CA – Kvalificirana potrdila	
Opis:	osnovna kvalificirana potrdila z enim parom ključev za fizične osebe
Vrsta:	kvalificirano potrdilo za elektronski podpis
Namen uporabe:	napredni elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.2.2.2.2 qcp-natural (0.4.0.194112.1.0)
Izdajatelji:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
12. POŠTA®CA – Kvalificirana potrdila, izdana na QSCD napravi	
Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe, izdana na QSCD napravi
Vrsta:	kvalificirano potrdilo za kvalificirani elektronski podpis
Namen uporabe:	kvalificirani elektronski podpis
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.3.2.2.2 qcp-natural-qscd (0.4.0.194112.1.2)
Izdajatelji:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
Opomba	Od objave politike verzije 1.4 je namen uporabe kvalificirani elektronski podpis. Pred verzijo 1.4 je bil namen uporabe kvalificirani elektronski podpis, šifriranje in avtentikacija.

13. POŠTA®CA – Kvalificirana potrdila, izdana na oddaljeni QSCD napravi

Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe, izdana na oddaljeni QSCD napravi
Vrsta:	kvalificirano potrdilo za kvalificirani elektronski podpis
Namen uporabe:	kvalificirani elektronski podpis
Rok veljavnosti:	do tri (3) leta
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.5.2.2.1 qcp-natural-qscd (0.4.0.194112.1.2)
Izdajatelji:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI

14. POŠTA®CA – Kvalificirana potrdila, izdana na profesionalni kartici v sistemu kartice zdravstvenega zavarovanja

Opis:	kvalificirana potrdila z enim parom ključev izdana na profesionalni kartici v sistemu kartice zdravstvenega zavarovanja
Vrsta:	kvalificirano potrdilo za kvalificirani elektronski podpis
Namen uporabe:	kvalificirani elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.4.2.2.2 qcp-natural-qscd (0.4.0.194112.1.2)
Izdajatelji:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI

Kvalificirana potrdila za pravne osebe:

15. POŠTA®CA – Kvalificirana potrdila za pravne osebe z obvezno uporabo QSCD naprave

Opis:	kvalificirana potrdila za pravne osebe z dvema paroma ključev z obvezno uporabo QSCD naprave
Vrsta:	kvalificirano potrdilo
Namen uporabe:	kvalificirani elektronski žig
Rok veljavnosti:	do pet (5) let

Rekono.TSP Pravila delovanja za POŠTA®CA

Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.4.1.1.2.1 qcp-legal-qscd (0.4.0.194112.1.3)
Izdajatelji:	CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
16. POŠTA®CA – Kvalificirana potrdila za pravne osebe	
Opis:	kvalificirana potrdila za pravne osebe z enim parom ključev
Vrsta:	kvalificirano digitalno potrdilo
Namen uporabe:	napredeni elektronski žig
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.4.2.1.2.1 qcp-legal (0.4.0.194112.1.1)
Izdajatelji:	CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
17. POŠTA®CA – Kvalificirana potrdila za pravne osebe, izdana na QSCD napravi	
Opis:	kvalificirano potrdilo za pravne osebe z enim parom ključev, izdano na QSCD napravi
Vrsta:	kvalificirano digitalno potrdilo
Namen uporabe:	kvalificiran elektronski žig
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.4.3.1.2.1 qcp-legal-qscd (0.4.0.194112.1.3)
Izdajatelji:	CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
18. POŠTA®CA – Kvalificirana potrdila za pravne osebe, izdana na oddaljeni QSCD napravi	
Opis:	kvalificirana potrdila za pravne osebe z enim parom ključev, izdana na oddaljeni QSCD napravi
Vrsta:	kvalificirano digitalno potrdilo
Namen uporabe:	kvalificirani elektronski žig
Rok veljavnosti:	do pet (5) let

Rekono.TSP Pravila delovanja za POŠTA®CA

Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.4.5.1.2.1 qcp-legal-qscd (0.4.0.194112.1.3)
Izdajatelj:	CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
Kvalificirana potrdila za spletne strežnike:	
19. POŠTA®CA – Kvalificirana potrdila za spletne strežnike	
Opis:	kvalificirana potrdila za spletne strežnike z enim parom ključev
Vrsta:	kvalificirano potrdilo
Namen uporabe:	overjanje identitete spletnih strežnikov
Rok veljavnosti:	do 825 dni
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.5.2.1.2.1 qcp-web (0.4.0.194112.1.4)
Izdajatelj:	CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
Normalizirana potrdila	
20. POŠTA®CA – Normalizirana potrdila za spletne strežnike	
Opis:	normalizirana potrdila za spletne strežnike z enim parom ključev
Vrsta:	normalizirano potrdilo
Namen uporabe:	overjanje identitete spletnih strežnikov in VPN naprav
Rok veljavnosti:	do tri (3) leta
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.2.1.1.2
Izdajatelj:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI
21. POŠTA®CA – Normalizirana potrdila za storitev časovnega žiga	
Opis:	normalizirana potrdila za strežnike časovnega žiga
Vrsta:	normalizirano potrdilo

Rekono.TSP Pravila delovanja za POŠTA®CA

Namen uporabe:	overjanje naprednega elektronskega podpisa storitve časovnega žiga
Rok veljavnosti:	do pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.2.4.1.2.1
Izdajatelji:	CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI

22. POŠTA®CA – Normalizirana potrdila za storitev OCSP	
Opis:	normalizirana potrdila za storitev OCSP
Vrsta:	normalizirano potrdilo
Namen uporabe:	overjanje naprednega elektronskega podpisa storitve OCSP
Rok veljavnosti:	do tri (3) leta
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.2.5.1.2.1
Izdajatelji:	OU=POSTArCA, O=POSTA, C=SI CN=POSTArCA G2, OI=VATSI-25028022, O=POSTA SLOVENIJE d.o.o., C=SI

1.3. Udeleženci infrastrukture javnih ključev

1.3.1. Ponudniki storitev

Ponudnik storitev je dolžan izvajati ukrepe in postopke, ki zagotavljajo upravljanje potrdil v skladu s predpisi, ki veljajo na območju RS in notranjimi pravili ponudnika storitev.

V okviru overitelja POŠTA®CA sta vzpostavljena sledeča izdajatelja potrdil:

- POŠTA®CA Root, ki je v okviru postopka vzpostavitve sam sebi podpisal potrdilo (angl. self-signed certificate) in deluje kot korenski izdajatelj, ki izdaja potrdila podrejenim izdajateljem.
- POŠTA®CA G2, ki mu je potrdilo izdal korenski izdajatelj POŠTA®CA Root in deluje kot izdajatelj potrdil uporabnikom.

Digitalno potrdilo overitelja POŠTA®CA Root vsebuje:

Naziv polja		Vrednost v digitalnem potrdilu izdajatelja POŠTA®CA Root
Serial Number	Serijska številka	25 2A 24 F9 00 00 00 00 59 52 22 E6
Issuer	Overitelj	CN=POSTArCA Root

Rekono.TSP Pravila delovanja za POŠTA®CA

		OI=VATSI-25028022 O=POSTA SLOVENIJE d.o.o. C=SI
Subject	Imetnik	CN=POSTArCA Root OI=VATSI-25028022 O=POSTA SLOVENIJE d.o.o. C=SI
Validity: Not Before	Veljavnost od	27. JUN. 10:48:44 2017 GMT
Validity: Not After	Veljavnost do	27. JUN. 11:18:44 2037 GMT
RSA Public Key	Dolžina RSA ključa	3072 bit
Signature Algorithm	Algoritem	sha256RSA
Key identifier	Identifikator ključa	43 89 A6 EB 17 8A 6F 7E
SHA-1 hash:	SHA-1 odtis digitalnega potrdila	7B 5B DA 71 03 1B 4C AA 84 F2 0B 9F 68 6E 11 6F 70 3F EB 45
SHA-256 hash:	SHA-256 odtis digitalnega potrdila	55 27 C5 78 0F 73 EF C1 97 B2 28 6C FC 96 2D A2 9D 3B 8A 00 2C B1 E3 EF 6E 30 78 88 64 7E 7E 6F

Digitalno potrdilo overitelja POŠTA®CA G2 vsebuje:

Naziv polja		Vrednost v digitalnem potrdilu izdajatelja POŠTA®CA G2
Serial Number	Serijska številka	16 D0 1B 84 00 00 00 00 59 52 23 21
Issuer	Overitelj	CN=POSTArCA Root OI=VATSI-25028022 O=POSTA SLOVENIJE d.o.o. C=SI
Subject	Imetnik	CN=POSTArCA G2 OI=VATSI-25028022 O=POSTA SLOVENIJE d.o.o. C=SI
Validity: Not Before	Veljavnost od	27. JUN. 11:52:52 2017 GMT
Validity: Not After	Veljavnost do	27. JUN. 12:22:52 2035 GMT
RSA Public Key	Dolžina RSA ključa	3072 bit
Signature Algorithm	Algoritem	sha256RSA
Key identifier	Identifikator ključa	4B 00 ED F2 0E 97 A3 7C

Rekono.TSP Pravila delovanja za POŠTA®CA

SHA-1 hash:	SHA-1 odtis digitalnega potrdila	D8 A4 42 C1 00 10 F4 59 C1 A4 AA DC A7 50 EA 36 3B 39 8A C2
SHA-256 hash:	SHA-256 odtis digitalnega potrdila	4E A7 7D EB B5 4B 56 69 56 6E B3 F2 C2 85 9F FF 80 3B 04 61 4A E4 6C AA 33 E8 9C CF 9F C0 DC 14

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))

Osebjem 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))

Osebjem 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. Registracijska pisarna ponudnika storitev

Registracijska pisarna (angl. RA-Registration Authority) deluje v organizacijskih enotah Pošte Slovenije. Zadolžena je za sprejemanje zahtevkov za preklic, preverjanje zahtevkov za preklic in posredovanje zahtevkov ponudniku storitev Rekono.TSP.

1.3.3. Naročniki in imetniki digitalnih potrdil

Naročnik digitalnega potrdila je pravna ali fizična oseba, registrirana za opravljanje dejavnosti, ki je zahtevala izdajo digitalnega potrdila v imenu enega ali več imetnikov, ali samostojna fizična oseba. Naročnik je hkrati imetnik, ko je podpisal vlogo za izdajo digitalnega potrdila v svojem imenu.

Imetnik kvalificiranega potrdila za elektronski podpis je fizična oseba ali fizična oseba zaposlena pri pravni osebi, navedena v potrdilu v polju »subject« kot lastnik zasebnega ključa, ki ustreza javnemu ključu, navedenemu v potrdilu. Kvalificirano potrdilo za elektronski podpis je vedno izdano določeni fizični osebi.

V primeru, ko je naročnik pravna oseba, je imetnik pooblaščen fizična oseba, ki uporablja potrdilo kot skrbnik potrdila za elektronske žige. V potrdilu je v polju »subject« naveden polni registriran naziv pravne osebe kot imetnika potrdila.

V primeru, ko je naročnik pravna ali fizična oseba, registrirana za opravljanje dejavnosti in je zahtevala izdajo digitalnega potrdila za spletni strežnik, ki ga poseduje, ali je pod njegovo kontrolo, je imetnik fizična oseba, ki uporablja potrdilo kot skrbnik spletnega strežnika (v polju "subject" je vpisano polno domensko ime spletnega strežnika in polni registrirani naziv pravne osebe).

S podpisom vloge se naročnik zavezuje k doslednemu spoštovanju in upoštevanju javnega dela notranjih pravil overitelja.

Glej tudi dokument Politika POŠTA®CA, poglavje 1.3.3.

1.3.4. Tretje osebe

Tretje osebe uporabljajo javni ključ, vsebovan v potrdilu, ki ga je izdal overitelj.

Tretje osebe so tako subjekti, ki razpolagajo s kakršnim koli potrdilom, kot tudi osebe, ki takšnega potrdila nimajo in se zanašajo na izdano potrdilo.

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

Imetniška potrdila, ki jih je izdal overitelj POŠTA®CA, je dovoljeno uporabljati v skladu z določili za posamezen tip digitalnega potrdila, navedenimi v poglavju 1.2 Naziv dokumenta in identifikacijske oznake potrdil.

Dovoljeni splošni nameni uporabe so :

- šifriranje in dešifriranje dokumentov v elektronski obliki;
- podpisovanje dokumentov v elektronski obliki;
- izkazovanje istovetnosti imetnika;
- storitve, kjer se zahteva uporaba kvalificiranega potrdila overitelja POŠTA®CA.

1.4.2. Nedovoljena uporaba digitalnih potrdil

Skladno z 1.4.1.

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 ponudnika storitev zaupanja Rekono.TSP

Naslov: 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 pravil delovanja ponudnika storitev

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

1.6. Pojmi in kratice

Glej Rekono.TSP Pravila delovanja, poglavje 1.6.

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 http://pki.rekono.si/cps/
-----------------------	--

Informacije o izdanih potrdilih in potrdila so shranjena na internih strežnikih in niso javno dostopne.

Glej tudi dokument Politika POŠTA®CA 2.1.

2.2. Objave informacij o digitalnih potrdilih

Javni imenik LDAP overitelja POŠTA®CA vsebuje naslednje informacije:

- javne informacije o imetnikih digitalnih potrdil;
- veljavna digitalna potrdila, ki jih je izdal overitelj;
- veljavne registre preklicanih potrdil;

Glej tudi Rekono.TSP Pravila delovanja, poglavje 2.2 in Politika POŠTA®CA, poglavje 2.2.

2.3. Čas in pogostost objav

Glej Rekono.TSP Pravila delovanja, poglavje 2.3.

2.4. Dostop do podatkov v repozitoriju

Informacije na javnih spletnih straneh so dostopne za branje brez omejitev.

Informacije v javnem imeniku LDAP so dostopne:

- za branje brez omejitev dostopa: registri preklicanih potrdil in digitalna potrdila overitelja POŠTA®CA;
- za branje avtoriziranim uporabnikom na osnovi avtentikacije: javne informacije o imetnikih digitalnih potrdil, digitalna potrdila imetnikov;

Glej Rekono.TSP Pravila delovanja, poglavje 2.4 in glej tudi dokument Politika POŠTA®CA, poglavje 2.

3. PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI

3.1. Določanje imen

Se ne izvaja. Glej tudi Politika POŠTA®CA, poglavje 3.1.

3.2. Prva registracija

Se ne izvaja. Glej tudi Politika POŠTA®CA, poglavje 3.2.

3.3. Preverjanje istovetnosti pri obnovi digitalnega potrdila

Se ne izvaja. Glej tudi Politika POŠTA®CA, poglavje 3.3.

3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila

Uporabnik, ki želi preklicati potrdilo, se lahko identificira po enakem postopku kot pri registraciji ali s skrivnim geslom, izbranim v postopku registracije.

Glej tudi Politika POŠTA®CA, poglavje 3.4.

4. UPRAVLJANJE Z DIGITALNIMI POTRDILI

4.1. Vloga za izdajo digitalnega potrdila

Se ne izvaja. Glej tudi Politika POŠTA®CA, poglavje 4.1.

4.2. Obdelava vloge za izdajo digitalnega potrdila

Se ne izvaja. Glej tudi Politika POŠTA®CA, poglavje 4.2.

4.3. Izdaja digitalnega potrdila

Se ne izvaja. Glej tudi Politika POŠTA®CA, poglavje 4.3.

4.4. Prezem digitalnega potrdila

Se ne izvaja. Glej tudi Politika POŠTA®CA, poglavje 4.4.

4.5. Uporaba ključev in digitalnih potrdil

Glej tudi Politika POŠTA®CA, poglavje 4.5.

4.6. Obnova digitalnih potrdil brez spremembe ključev

Se ne izvaja. Glej tudi Politika POŠTA®CA, poglavje 4.6.

4.7. Obnova digitalnih potrdil

Se ne izvaja. Glej tudi Politika POŠTA®CA, poglavje 4.7.

4.8. Sprememba digitalnega potrdila

Se ne izvaja. Glej tudi Politika POŠTA®CA, poglavje 4.7.

4.9. Začasna ukinitve veljavnosti in preklic digitalnega potrdila

Glej tudi Politika POŠTA®CA, poglavje 4.9.

4.9.1. Okoliščine preklica

Overitelj lahko prekliče digitalno potrdilo iz naslednjih razlogov:

- dejansko ali domnevno ogrožanje zasebnih ključev;
- spremembe podatkov v digitalnem potrdilu, ki zahtevajo izdajo novega;
- spremembe podatkov v digitalnem potrdilu, ki vplivajo na veljavnost potrdila;

- spremembe statusa plačilnih storitev PSD2 pri nacionalnem pristojnem organu (NCA), ki so navedene v razširitvenem polju potrdila;
- neizpolnjevanje obveznosti iz točke 9.6.3;
- v primeru smrti imetnika potrdila;
- na zahtevo imetnika potrdila;
- osebje overitelja v primeru:
 - ko overitelj izve, da je imetnik potrdila umrl ali so se spremenile okoliščine, ki bistveno vplivajo na veljavnost digitalnega potrdila;
 - če je podatek v digitalnem potrdilu napačen ali je bilo digitalno potrdilo izdano na podlagi napačnih podatkov;
 - če overitelj preneha z delovanjem ali mu je delovanje prepovedano in njegove dejavnosti ni prevzel drug overitelj;
 - če so bili podatki za preverjanje elektronskega podpisa ali informacijski sistem overitelja ogroženi na način, ki vpliva na zanesljivost digitalnega potrdila;
 - če so bili podatki za elektronsko podpisovanje ali informacijski sistem imetnika potrdila ogroženi na način, ki vpliva na zanesljivost oblikovanja elektronskega podpisa;
 - če naročnik potrdila ne izpolnjuje svojih obveznosti iz točke 9.6.3.

Imetnik potrdila je dolžan overitelju nemudoma prijaviti vsako domnevno ali dejansko ogrožanje zasebnega ključa.

Glej tudi Politika POŠTA®CA, poglavje 4.9.1.

4.9.2. Kdo lahko zahteva preklic

Preklic digitalnega potrdila lahko zahteva:

- imetnik potrdila, kateremu je bilo digitalno potrdilo izdano;
- pooblaščen osebja, odgovorna za digitalna potrdila izdana pravni osebi;
- osebje overitelja;
- pristojno sodišče, pristojni prekrškovni organ ali upravni organ;
- dedič ali zakoniti zastopnik;
- tretja oseba, če digitalno potrdilo vsebuje podatke o tretji osebi;
- PSD2 nacionalni pristojni organ (NCA) lahko zahteva preklic PSD2 potrdil za ponudnike plačilnih storitev, za katere je izdal odobritve.

Glej tudi Politika POŠTA®CA, poglavje 4.9.2.

4.9.3. Postopki za preklic

- 1) Zahteva za preklic se lahko poda na enega izmed naslednjih načinov:
 - Imetnik potrdila osebno odda vlogo za preklic v registracijski pisarni overitelja.
 - Po telefonu na številko za preklic. Uporabnik se mora identificirati z geslom, ki ga je vpisal na vlogo za izdajo digitalnega potrdila.
 - Nacionalni pristojni organ (NCA) lahko poda zahtevo za preklic PSD2 potrdil po elektronski pošti na kontaktni naslov overitelja, naveden v poglavju 1.3.1.
- 2) Po uspešno izvedenem postopku preverjanja istovetnosti zahtevka za preklic osebje registracijske pisarne sproži postopek preklica. V primeru, da overitelj ne more potrditi istovetnosti zahtevka za preklic v 24 urah od prejema zahtevka, preklica ne izvede.
- 3) Overitelj izvede preklic digitalnega potrdila.
- 4) Overitelj obvesti imetnika potrdila o preklicu po elektronski pošti ali pisno po pošti.

Glej tudi Politika POŠTA®CA, poglavje 4.9.3.

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.

Glej tudi Politika POŠTA®CA, poglavje 4.9.4.

4.9.5. Čas od vloge za preklic do preklica

V vseh primerih bo preklicano potrdilo objavljeno na seznamu preklicanih potrdil najkasneje v 24 urah od trenutka, ko overitelj prejme veljaven zahtevek za preklic.

Glej tudi Politika POŠTA®CA, poglavje 4.9.5.

4.9.6. Obveza preverjanja registra preklicanih potrdil

Glej Politika POŠTA®CA, poglavje 4.9.6.

4.9.7. Pogostost objav registrov preklicanih potrdil

Ponudnik storitev zaupanja Rekono.TSP posodobi seznam preklicanih potrdil najkasneje v roku 60 minut, ko izvede preklic digitalnega potrdila, ali vsaj enkrat vsakih 24 ur.

Korenski overitelji posodobijo seznam preklicanih potrdil takoj, ko se izvede preklic digitalnega potrdila, ali vsaj enkrat vsakih 365 dni.

Glej tudi Politika POŠTA®CA, poglavje 4.9.7.

4.9.8. Dovoljene zakasnitve sprotnega preverjanja statusa digitalnih potrdil

Namenoma puščeno prazno.

4.9.9. Storitve 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 ukinitve veljavnosti (suspenz) digitalnega potrdila

Začasna ukinitve veljavnosti potrdil se ne uporablja.

4.9.14. Kdo lahko zahteva suspenz ali ukinitve suspenza digitalnega potrdila

Namenoma puščeno prazno.

4.9.15. Postopki za suspenz ali ukinitve suspenza digitalnega potrdila

Namenoma puščeno prazno.

4.9.16. Omejitve obdobja začasne ukinitve veljavnosti

Namenoma puščeno prazno.

4.10. Storitve objavljanja statusa digitalnih potrdil

4.10.1. Tehnične lastnosti storitve

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

Seznami preklicanih potrdil so dostopni po protokolu http. Spletni naslovi seznamov 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. Seznami preklicanih potrdil vsebujejo tudi preklicana pretečena potrdila.

Storitev OCSP je dostopna na spletnem naslovu, ki je naveden v razširitvenem polju `id-pe-authorityInfoAccess:id-ad-ocsp`, vsebovanem v vsakem izdanem digitalnem potrdilu. Storitev OCSP vsebuje tudi preklicana pretečena potrdila.

4.10.2. Razpoložljivost storitve dostopa do seznama preklicanih potrdil

Dostop do seznama preklicanih digitalnih potrdil in storitve OCSP je mogoč 24 ur 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.

Glej tudi Politika POŠTA®CA, poglavje 4.11.

4.12. Varnostno kopiranje in odkrivanje zasebnega ključa

Glej Politika POŠTA®CA, poglavje 4.12.

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

Poglavje opisuje varnostni nadzor prostorov, opreme, postopkov in osebja, ki ga izvaja ponudnik storitev za zaščito svojega delovanja.

Glej Rekono.TSP Pravila delovanja, poglavje 5.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Tvorjenje in namestitvev para ključev

Glej Politika POŠTA®CA, poglavje 6.1.

6.2. Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov

Glej Politika POŠTA®CA, poglavje 6.2.

6.3. Ostali vidiki upravljanja s pari ključev

Glej Politika POŠTA®CA, poglavje 6.3.

6.4. Aktivacijski podatki

Namenoma puščeno prazno.

6.5. Varnostne zahteve za računalnike

Glej Rekono.TSP Pravila delovanja, poglavje 6.5.

6.6. Tehnični nadzor življenjskega cikla overitelja

Glej Rekono.TSP Pravila delovanja, poglavje 6.6.

6.7. Varnostne kontrole na ravni računalniškega omrežja

Glej Rekono.TSP Pravila delovanja, poglavje 6.7.

6.8. Časovno žigosanje

Namenoma puščeno prazno.

7. PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL

Glej Politika POŠTA®CA, poglavje 7.

8. PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA

Glej Rekono.TSP Pravila delovanja, poglavje 8.

9. OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1. Cenik

9.1.1. Cena izdaje in upravljanja digitalnih potrdil

Ponudnik storitev ne izdaja potrdil naročnikom oziroma imetnikom.

9.1.2. Cena dostopa do digitalnih potrdil v javnem imeniku

Dostop do javnega imenika je brezplačen.

9.1.3. Cena dostopa do registra preklicanih potrdil

Dostop do registra preklicanih potrdil je brezplačen.

9.1.4. Cena ostalih storitev

Namenoma puščeno prazno.

9.1.5. Pravica vračila

Namenoma puščeno prazno. Glej tudi 9.1.1.

9.2. Finančna odgovornost

9.2.1. Zavarovanje odgovornosti

Namenoma puščeno prazno.

9.2.2. Druge oblike zavarovanja

Rekono d.o.o. kot ponudnik storitev zaupanja zagotavlja zadostna finančna sredstva z obveznosti prostim premoženjem za kritje morebitne škode, nadomestil, obveznost povrnitve terjatev ali obveznosti katerekoli vrste s storitvami zaupanja, ki jih izvaja.

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: pooblaščenca 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 nepooblaščen oseba.

Glej tudi Politika POŠTA®CA, poglavje 9.3.1.

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.

Glej tudi Politika POŠTA®CA, poglavje 9.3.2.

9.3.3. Odgovornost za zagotavljanje zaupnosti poslovnih informacij

Glej Rekono.TSP Pravila delovanja, poglavje 9.3.3.

9.4. Varovanje osebnih podatkov

9.4.1. Načrt zagotavljanja varovanja osebnih podatkov

Glej Rekono.TSP Pravila delovanja, poglavje 9.4.1.

9.4.2. Obseg varovanih osebnih podatkov

Glej Rekono.TSP Pravila delovanja, poglavje 9.4.2.

9.4.3. Osebni podatki, ki se ne obravnavajo kot zaupni

Glej Rekono.TSP Pravila delovanja, poglavje 9.4.3.

9.4.4. Odgovornost glede varovanja osebnih podatkov

Glej Rekono.TSP Pravila delovanja, poglavje 9.4.4.

9.4.5. Privolitev posameznika za uporabo osebnih podatkov

Glej Rekono.TSP Pravila delovanja, poglavje 9.4.5.

9.4.6. Posredovanje osebnih podatkov v sodnih in upravnih postopkih

Glej Rekono.TSP Pravila delovanja, poglavje 9.4.6.

9.4.7. Druge okoliščine posredovanja osebnih podatkov

Glej Rekono.TSP Pravila delovanja, poglavje 9.4.7.

9.5. Zaščita intelektualne lastnine

Glej Rekono.TSP Pravila delovanja, poglavje 9.5.

9.6. Odgovornost in jamstva

9.6.1. Odgovornost in jamstva ponudnika storitev

Ponudnik storitev zagotavlja opravljanje storitev v zvezi z elektronskim podpisovanjem po pravilih stroke in po običajih (s skrbnostjo dobrega strokovnjaka) in temu ustrezno prevzema odgovornost.

Ponudnik storitev v splošnem jamči za:

- izvajanje vseh postopkov v skladu z navedbami v pravilih delovanja ter predpisi, ki veljajo na območju Republike Slovenije;
- izvajanje funkcij upravljanja s ključi, kot so tvorjenje para ključev overitelja, varno upravljanje ključev overitelja in distribucija javnega ključa overitelja oziroma digitalnega potrdila overitelja;
- točnost podatkov v izdanih digitalnih potrdilih;
- razvoj in vzpostavitev postopkov za sprejem vlog;
- preverjanje istovetnosti naročnikov, ki zahtevajo izdajo digitalnega potrdila;¹
- odobritev ali zavrnitev vloge;¹
- podpis in izdajo digitalnega potrdila naročnikom;¹
- objavo digitalnega potrdila v javnem imeniku;¹
- uvedbo postopka za preklic digitalnega potrdila na zahtevo naročnika ali po svoji presoji;
- preklic digitalnega potrdila in objavo preklica v registru preklicanih potrdil;
- priporočila minimalnih sistemskih zahtev za uporabo digitalnih potrdil. Na računalniških sistemih, ki ne ustrezajo minimalnim zahtevam, overitelj ni dolžan zagotavljati delovanja digitalnih potrdil;
- preverjanje istovetnosti naročnikov, ki zahtevajo obnovo digitalnega potrdila ali povrnitev zgodovine šifrirnih ključev ter vzpostavitev ustreznih postopkov.¹
- Ponudnik storitev odgovarja naročnikom potrdila:
 - za neskladnost med podatki, ki jih je dal prosilec in med podatki v digitalnem potrdilu, če so posledica nevestnega poslovanja overitelja;
 - za škodo, ki nastane zaradi tega, ker digitalno potrdilo ne izpolnjuje zahtev, opisanih v tem dokumentu;

¹ Overitelj POŠTA®CA je prenehal z izdajo potrdil. Glej tudi 1.1.

- za škodo, če ne upravlja digitalna potrdila tako, kot je določeno v tem dokumentu.

Ponudnik storitev odgovarja in jamči za škodo tretjim osebam, ki se upravičeno zanašajo na digitalna potrdila, ki jih je izdal:

- če digitalno potrdilo ne vsebuje vseh podatkov ali če registracijska pisarna overitelja pri izdaji digitalnega potrdila ne preveri podatkov;
- če zasebni ključ imetnika potrdila v času izdaje potrdila ne ustreza javnemu ključu v digitalnem potrdilu;
- če ne izvede in objavi preklica digitalnega potrdila v osmih urah po prejemu vloge za preklic.

Ponudnik storitev zagotavlja stalno dostopnost svojih storitev, in sicer 24ur vse dni v letu s sledečimi izjemami:

- vnaprej napovedana vzdrževalna dela, ki jih ponudnik storitev najavi vsaj tri (3) dni pred prekinitvijo;
- prekinitve zaradi nenačrtovanih tehničnih okvar;
- prekinitve zaradi nedelovanja infrastrukture izven pristojnosti ponudnika storitev in prekinitve kot posledica višje sile ali izrednih dogodkov.

9.6.2. Odgovornost in jamstva prijavnih služb

Ponudnik storitev odgovarja za obveznosti registracijske pisarne. Ponudnik storitev je odgovoren za delo registracijskih pisarn, tudi če je prenesel izvajanje posameznih dejavnosti ali postopkov na podizvajalce.

Registracijska pisarna ponudnika storitev jamči za:

- preverjanje točnosti podatkov na vlogah;
- preverjanje identitete prosilcev;
- posredovanje vlog centru ponudnika storitev.

9.6.3. Odgovornost in jamstva imetnikov digitalnih potrdil

Imetnik potrdil je dolžan:

- varovati osebno geslo in zasebne dele ključev. Imetnik aktivacijskih podatkov in zasebnih delov ključev ne sme dati na vpogled ali v uporabo tretjim osebam, sicer nosi popolno odgovornost za vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker so tretje nepooblaščenice osebe uporabile imetnikovo kvalificirano digitalno potrdilo;
- digitalno podpisovati le dokumente, katerih zahteva po veljavnosti ni daljša od roka veljavnosti digitalnega potrdila (izjema so podpisani dokumenti, za katere je zagotovljeno ohranjanje dolgoročne veljavnosti

elektronskega podpisa na drug način, na primer dokumenti hranjeni v elektronskem arhivu, ki podpira storitev ohranjanja dolgoročne veljavnosti podpisa);

- zagotoviti uporabo digitalnih potrdil le v obdobju njihove veljavnosti;
- zagotoviti uporabo digitalnih potrdil samo za namene, ki jih je odobril overitelj;
- takoj zahtevati preklic digitalnega potrdila, če sumi, da je prišlo do zlorabe ali razkritja zasebnega ključa;
- v 48 urah obvestiti overitelja, če je prišlo do spremembe podatkov, vsebovanih v potrdilu ali podatkov na vlogi za izdajo digitalnega potrdila;
- upoštevati overiteljeva pravila delovanja in spremljati vsa obvestila overitelja ter ravnati v skladu z njimi;
- spremljati razvoj tehnologije in posodabljati ustrezno strojno ter programsko opremo, ki je v skladu z obvestili overitelja, ter upoštevati sledeča priporočila za zagotavljanje varnosti računalnika, na katerem uporablja digitalno potrdilo:
- na računalniku naj bo nameščena in redno posodabljana protivirusna zaščita;
- na računalniku naj bo nameščena požarna pregrada;
- redno nameščanje varnostnih popravkov operacijskega sistema in programske opreme;
- odjava iz sistema ali zaklepanje namizja ob odsotnosti;
- odstranitev pametne kartice iz čitalca pametnih kartic ob odsotnosti;
- v primeru ko imetnik sam generira par kriptografskih ključev, mora upoštevati zahteve v poglavju 6.1.5 v skladu z ETSI TS 119 312;²
- v roku poravnati vse finančne obveznosti do overitelja;
- digitalno potrdilo za spletne strežnike uporabljati le za SSL ali TLS protokol na strežniku, za katerega je bilo izdano.

9.6.4. Odgovornost in jamstva tretjih oseb

Tretje strani, ki se zanašajo na digitalna potrdila overitelja, so dolžne:

- omejiti zaupanje v potrdilo le na namen, določen v tej politiki;
- preveriti veljavnost digitalnega potrdila;
- skrbno prebrati pričujoči dokument ter se seznaniti z odgovornostjo in omejitvami odgovornosti overitelja;
- če digitalno potrdilo vsebuje podatke o tretji osebi, je ta dolžna zahtevati preklic digitalnega potrdila, če izve, da je bil zasebni ključ ogrožen na

² Overitelj POŠTA®CA je prenehal z izdajo potrdil. Glej tudi 1.1.

način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe ali če so spremenjeni podatki, ki so navedeni v digitalnem potrdilu.

9.6.5. Odgovornost in jamstva drugih udeležencev

Namenoma puščeno prazno.

9.7. Zanikanje odgovornosti

Overitelj ne odgovarja za nobeno škodo, stroške in druge terjatve, nastale zaradi uporabe digitalnih potrdil, v naslednjih primerih:

- če je bilo digitalno potrdilo izdano zaradi napake, neverodostojnih podatkov ali drugih nepravilnosti na strani imetnika potrdila;
- če je potekla veljavnost digitalnega potrdila;
- kadar je digitalno potrdilo uporabljeno po preklicu in objavi v registru preklicanih potrdil;
- če je digitalno potrdilo ponarejeno ali kakor koli predrugačeno ali spremenjeno;
- če prosilec, imetnik potrdila ali tretja oseba ne ravna v skladu z določbami tega dokumenta, overiteljevimi pravili delovanja, ali veljavnimi zakoni in na njihovi podlagi izdanimi podzakonskimi predpisi;
- če je bil zasebni ključ ogrožen ali obstaja objektivno utemeljen sum, da je bil ogrožen;
- če je bilo digitalno potrdilo uporabljeno v drugačne namene, kot je določeno z naročniško pogodbo, overiteljevimi pravili delovanja, ali veljavnimi zakoni in na njihovi podlagi izdanimi podzakonskimi predpisi;
- če nastane škoda zaradi napake v delovanju strojne ali programske opreme prosilca, imetnika potrdila 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 brez upoštevanja ali v nasprotju z določbami teh Rekono.TSP Pravil delovanja za POŠTA®CA s strani naročnika, imetnika ali tretjih oseb, 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 uporabo digitalnih potrdil.

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 za POŠTA®CA in veljavno zakonodajo (glej 9.14).

9.10. Začetek in prenehanje veljavnosti

9.10.1. Začetek veljavnosti

Rekono.TSP Pravila delovanja za POŠTA®CA 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 za POŠTA®CA 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

Z uveljavitvijo nove verzije pravil delovanja ostanejo za vsa potrdila, izdana pred tem, v veljavi tista določila prej veljavnih pravil delovanja, ki se smiselno ne morejo nadomestiti z ustreznimi določili novih pravil delovanja.

9.11. Obvestila in komuniciranje z udeleženci

Rekono.TSP objavlja trenutno verzijo teh Rekono.TSP Pravil delovanja za POŠTA®CA 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 verzijo 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 za POŠTA®CA 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

Namenoma puščeno prazno.

9.13. Reševanje sporov

Spori med subjekti (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

Pravica uporabe digitalnih potrdil ni prenosljiva.

9.16.3. Spremembe okoliščin delovanja

Ničnost enega ali več delov teh Rekono.TSP Pravil delovanja za POŠTA®CA 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)

Zahtevki povračila stroškov v primeru sporov se obravnavajo v skladu z veljavnimi predpisi na območju Republike Slovenije.

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

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"
- [13] EN 419241-1 "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements"
- [14] ISO/IEC 9594-8/Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks".
- [15] EN 319 411-2 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates"
- [16] RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP"
- [17] Zakon o elektronski identifikaciji in storitvah zaupanja (Uradni list RS, št. 121/21 in 189/21 – ZDU-1M)
- [18] Uredba o določitvi sredstev elektronske identifikacije in uporabi centralne storitve za spletno prijavo in elektronski podpis (Uradni list RS, št. 29/22)
- [19] Rekono.TSP Pravila delovanja (<http://pki.rekono.si/cps/>)

[20] Politika POŠTA®CA (<http://postarca.posta.si>)