



**Ponudnik storitev zaupanja Rekono.TSP
Pravila delovanja za AC NLB
(Certification Practice Statement)**

| | |
|--------------------|----------------|
| Verzija: | 1.1.1 |
| Datum izdaje: | 21. Junij 2023 |
| Datum uveljavitve: | 28. Junij 2023 |

Vsebovane politike AC NLB

Kvalificirana potrdila za fizične osebe

AC NLB - Kvalificirana potrdila
CPOID: 1.3.6.1.4.1.7597.1.5.11

| | |
|---------------------------------|----------------------------------|
| Država (C) | SI |
| Organizacija (O) | NLB d.d. |
| Organizacijska enota (OU) | ACNLB |
| Organizacijska enota (OU) | Fizicne osebe |
| Splošno ime (CN) | Ime in priimek imetnika potrdila |
| Serijska številka(serialNumber) | Davčna številka fizične osebe |
| Ime (givenName, GN) | Ime |
| Priimek (surname, SN) | Priimek |

Kvalificirana potrdila za zaposlene pri pravni osebi

AC NLB - Kvalificirana potrdila
CPOID: 1.3.6.1.4.1.7597.1.5.12

| | |
|----------------------------------|---|
| Država (C) | SI |
| Organizacija (O) | Registrirano ime pravne osebe |
| Organizacijska identiteta (OI) | VATSI-DŠ pravne osebe |
| Organizacijska enota (OU) | ACNLB |
| Organizacijska enota (OU) | Pravne osebe |
| Splošno ime (CN) | ime in priimek imetnika potrdila |
| Serijska številka (serialNumber) | davčna številka pravne osebe in fizične osebe |
| Ime (givenName, GN) | Ime |
| Priimek (surname, SN) | Priimek |

Kvalificirana potrdila za fizične osebe za oddaljen podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa

AC NLB - Kvalificirana potrdila
CPOID: 1.3.6.1.4.1.7597.1.5.13

| | |
|---------------------------------|---|
| Država (C) | SI |
| Organizacija (O) * | Registrirano ime pravne osebe |
| Organizacijska identiteta (OI)* | VATSI-DŠ pravne osebe |
| Organizacijska enota (OU) | ACNLB |
| Organizacijska enota (OU) | PVO Fizicne ali PVO Pravne |
| Splošno ime (CN) | ime in priimek imetnika potrdila |
| Serijska številka(serialNumber) | davčna številka fizične osebe ali davčna številka pravne osebe in fizične osebe |

* Polje je prisotno v potrdilih za zaposlene pri pravni osebi

Kvalificirana potrdila za fizične osebe za oddaljen podpis

AC NLB - Kvalificirana potrdila
CPOID: 1.3.6.1.4.1.7597.1.5.14

| | |
|---------------------------------|---|
| Država (C) | SI |
| Organizacija (O) * | Registrirano ime pravne osebe |
| Organizacijska identiteta (OI)* | VATSI-DŠ pravne osebe |
| Organizacijska enota (OU) | ACNLB |
| Organizacijska enota (OU) | PVO Fizicne ali PVO Pravne |
| Splošno ime (CN) | ime in priimek imetnika potrdila |
| Serijska številka(serialNumber) | davčna številka fizične osebe ali davčna številka pravne osebe in fizične osebe |

* Polje je prisotno v potrdilih za zaposlene pri pravni osebi

Kvalificirana potrdila za pravne osebe za elektronski žig

AC NLB - Kvalificirana potrdila
CPOID: 1.3.6.1.4.1.7597.1.5.15

| | |
|------------|----|
| Država (C) | SI |
|------------|----|

Rekono.TSP Pravila delovanja za AC NLB

| | |
|---------------------------------|-------------------------------|
| Organizacija (O) | Registrirano ime pravne osebe |
| Organizacijska identiteta (OI) | VATSI-DŠ pravne osebe |
| Organizacijska enota (OU) | ACNLB |
| Organizacijska enota (OU) | Elektronski žig |
| Splošno ime (CN) | Naziv pravne osebe |
| Serijska številka(serialNumber) | davčna številka pravne osebe |

Kvalificirana potrdila za pravne osebe za elektronski žig na napravi za ustvarjanje kvalificiranega elektronskega žiga

AC NLB - Kvalificirana potrdila

CPOID: 1.3.6.1.4.1.7597.1.5.16

| | |
|---------------------------------|-------------------------------|
| Država (C) | SI |
| Organizacija (O) | Registrirano ime pravne osebe |
| Organizacijska identiteta (OI) | VATSI-DŠ pravne osebe |
| Organizacijska enota (OU) | ACNLB |
| Organizacijska enota (OU) | Elektronski žig |
| Splošno ime (CN) | Naziv pravne osebe |
| Serijska številka(serialNumber) | davčna številka pravne osebe |

Potrdila za ostale namene, ki morajo vsebovati enolično identifikacijsko oznako, ki omogočajo jasno prepoznavo potrdila

AC NLB - Potrdila

CPOID: 1.3.6.1.4.1.7597.2 (glede na uporabo)

| | |
|---------------------------------|----------------------------------|
| Država (C) | SI |
| Organizacija (O) | NLB d.d. |
| Organizacijska enota (OU) | ACNLB |
| Organizacijska enota (OU) | Naziv organizacije |
| Splošno ime (CN) | ime in priimek imetnika potrdila |
| Serijska številka(serialNumber) | enolični identifikator |

Rekono.TSP Pravila delovanja za AC NLB

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

Izvorni 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 |
|-------|------------|--|
| 1.0 | 03.04.2023 | Prva izdaja dokumenta Rekono.TSP Pravila delovanja za AC NLB. |
| 1.1 | 19.04.2023 | Uskladitev datuma uveljavitve in datuma prenehanja izdaje potrdil imetnikom s strani AC NLB. |
| 1.1.1 | 21.06.2023 | Uredniški popravki |

Kazalo

| | | |
|--------|---|----|
| 1 | Uvod | 8 |
| 1.1 | Pregled | 8 |
| 1.1.1 | Potrdila ponudnika storitev AC NLB | 8 |
| 1.2 | Naziv dokumenta in identifikacijske oznake potrdil | 9 |
| 1.3 | Udeleženci infrastrukture javnih ključev | 10 |
| 1.3.1 | Ponudniki storitev | 10 |
| 1.3.2 | Registracijska pisarna ponudnika storitev | 11 |
| 1.3.3 | Naročniki in imetniki potrdil | 11 |
| 1.3.4 | Tretja oseba | 12 |
| 1.3.5 | Ostali udeleženci | 12 |
| 1.4 | Namen uporabe potrdil | 12 |
| 1.4.1 | Dovoljena uporaba potrdil | 12 |
| 1.4.2 | Nedovoljena uporaba potrdil | 12 |
| 1.5 | Upravljanje s pravili delovanja | 13 |
| 1.5.1 | Organizacija, ki upravlja s pričujočim dokumentom | 13 |
| 1.5.2 | Kontaktne podatki | 13 |
| 1.5.3 | Oseba, ki ugotavlja ustreznost Politike | 13 |
| 1.5.4 | Postopek odobritve pravil delovanja ponudnika storitev | 13 |
| 1.6 | Pojmi in kratice | 13 |
| 2 | Odgovornost za objave in repozitorij | 14 |
| 2.1 | Repozitorij | 14 |
| 2.2 | Objave informacij o potrdilih | 14 |
| 2.3 | Čas in pogostost objav | 14 |
| 2.4 | Dostop do podatkov v repozitoriju | 14 |
| 3 | PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI | 14 |
| 3.1 | Določanje imen | 14 |
| 3.2 | Prva registracija | 14 |
| 3.3 | Preverjanje istovetnosti pri obnovi potrdila | 14 |
| 3.4 | Preverjanje istovetnosti ob zahtevi za preklic potrdila | 14 |
| 4 | Upravljanje s potrdili | 14 |
| 4.1 | Vloga za izdajo potrdila za fizične osebe in za pravne osebe za zaposlene | 14 |
| 4.2 | Obdelava vloge za izdajo potrdila | 15 |
| 4.3 | Izdaja potrdila | 15 |
| 4.4 | Prezem potrdila | 15 |
| 4.5 | Uporaba ključev in potrdil | 15 |
| 4.6 | Obnova potrdil brez spremembe ključev | 15 |
| 4.7 | Obnova potrdil | 15 |
| 4.8 | Sprememba potrdila | 15 |
| 4.9 | Začasna ukinitve veljavnosti in preklic potrdila | 15 |
| 4.9.1 | Okoliščine preklica | 15 |
| 4.9.2 | Kdo lahko zahteva preklic | 16 |
| 4.9.3 | Postopki za preklic | 16 |
| 4.9.4 | Čas za posredovanje vloge za preklic | 16 |
| 4.9.5 | Čas od vloge za preklic do preklica | 16 |
| 4.9.6 | Obveza preverjanja registra preklicanih potrdil | 16 |
| 4.9.7 | Pogostost objav registrov preklicanih potrdil | 16 |
| 4.9.8 | Dovoljene zakasnitve sprotnega preverjanja statusa digitalnih potrdil | 16 |
| 4.9.9 | Storitev sprotnega preverjanja statusa potrdil | 16 |
| 4.9.10 | Obveza sprotnega preverjanja statusa preklicanih potrdil | 16 |
| 4.9.11 | Ostale oblike objavljanja preklicanih potrdil | 17 |
| 4.9.12 | Posebne zahteve glede zlorabe ključa | 17 |
| 4.9.13 | Okoliščine za začasno razveljavitev veljavnosti potrdila | 17 |
| 4.10 | Storitev objavljanja statusa potrdil | 17 |
| 4.10.1 | Tehnične lastnosti storitve | 17 |
| 4.10.2 | Razpoložljivost storitve dostopa do registra preklicanih potrdil | 17 |

Rekono.TSP Pravila delovanja za AC NLB

| | | |
|--------|---|----|
| 4.10.3 | Dodatne možnosti..... | 17 |
| 4.11 | Trajanje naročniškega razmerja..... | 17 |
| 4.12 | Varnostno kopiranje in odkrivanje zasebnega ključa..... | 17 |
| 5 | Fizično varovanje, organizacijski varnostni ukrepi in zahteve za osebe | 18 |
| 6 | Tehnične varnostne zahteve | 18 |
| 6.1 | Tvorjenje in namestitvev para ključev..... | 18 |
| 6.2 | Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov..... | 18 |
| 6.3 | Ostali vidiki upravljanja s pari ključev..... | 18 |
| 6.4 | Aktivacijski podatki..... | 18 |
| 6.5 | Varnostne zahteve za računalnike..... | 18 |
| 6.6 | Tehnični nadzor življenjskega cikla ponudnika storitev..... | 18 |
| 6.7 | Časovno žigosanje..... | 18 |
| 7 | Profil potrdil in registrov preklicanih potrdil | 18 |
| 8 | Preverjanje skladnosti in ostale oblike nadzora | 18 |
| 9 | Ostale poslovne in pravne zadeve | 19 |
| 9.1 | Cenik..... | 19 |
| 9.1.1 | Cena izdaje in upravljanja potrdil..... | 19 |
| 9.1.2 | Cena dostopa do potrdil v javnem imeniku..... | 19 |
| 9.1.3 | Cena dostopa do registra preklicanih potrdil..... | 19 |
| 9.1.4 | Cena ostalih storitev..... | 19 |
| 9.1.5 | Pravica vračila..... | 19 |
| 9.2 | Finančna odgovornost..... | 19 |
| 9.2.1 | Zavarovanje odgovornosti..... | 19 |
| 9.2.2 | Druge oblike zavarovanja..... | 19 |
| 9.2.3 | Zavarovanja ali jamstvo za druge uporabnike..... | 19 |
| 9.3 | Zaupnost poslovnih informacij..... | 19 |
| 9.3.1 | Obseg zaupnih poslovnih informacij..... | 19 |
| 9.3.2 | Informacije izven obsega zaupnih poslovnih informacij..... | 20 |
| 9.3.3 | Odgovornost za zagotavljanje zaupnosti poslovnih informacij..... | 20 |
| 9.4 | Varovanje osebnih podatkov..... | 20 |
| 9.4.1 | Načrt zagotavljanja varovanja osebnih podatkov..... | 20 |
| 9.4.2 | Obseg varovanih osebnih podatkov..... | 20 |
| 9.4.3 | Nevarovani osebni podatki..... | 20 |
| 9.4.4 | Odgovornost glede varovanja osebnih podatkov..... | 20 |
| 9.4.5 | Privolitev posameznika za uporabo osebnih podatkov..... | 20 |
| 9.4.6 | Posredovanje osebnih podatkov v sodnih in upravnih postopkih..... | 20 |
| 9.4.7 | Druge okoliščine posredovanja osebnih podatkov..... | 20 |
| 9.5 | Zaščita intelektualne lastnine..... | 20 |
| 9.6 | Odgovornosti in jamstva..... | 21 |
| 9.6.1 | Odgovornosti in jamstva ponudnika storitev..... | 21 |
| 9.6.2 | Odgovornost in jamstva prijavnne službe..... | 21 |
| 9.6.3 | Obveznosti in odgovornost imetnika..... | 21 |
| 9.6.4 | Obveznosti in odgovornost tretjih oseb..... | 22 |
| 9.6.5 | Obveznosti in odgovornosti drugih subjektov..... | 22 |
| 9.7 | Zanikanje odgovornosti ponudnika storitev..... | 22 |
| 9.8 | Omejitve odgovornosti ponudnika storitev..... | 23 |
| 9.9 | Poravnava škode..... | 23 |
| 9.10 | Začetek in prenehanje veljavnosti..... | 23 |
| 9.10.1 | Začetek veljavnosti..... | 23 |
| 9.10.2 | Prenehanje veljavnosti..... | 23 |
| 9.10.3 | Učinek in posledice prenehanja veljavnosti..... | 23 |
| 9.11 | Komuniciranje med subjekti..... | 23 |
| 9.12 | Spreminjanje dokumenta..... | 24 |
| 9.12.1 | Postopek uveljavitve sprememb..... | 24 |
| 9.12.2 | Postopek obveščanja..... | 24 |
| 9.12.3 | Spremembe, ki zahtevajo novo identifikacijsko oznako politike..... | 24 |
| 9.13 | Postopek v primeru sporov..... | 24 |
| 9.14 | Veljavna zakonodaja..... | 24 |
| 9.15 | Skladnost z veljavno zakonodajo..... | 24 |

Rekono.TSP Pravila delovanja za AC NLB

| | | |
|--------|---|----|
| 9.16 | Splošne določbe | 25 |
| 9.16.1 | Ostali obvezujoči dokumenti | 25 |
| 9.16.2 | Prenos pravic in obveznosti | 25 |
| 9.16.3 | Spremembe okoliščin delovanja | 25 |
| 9.16.4 | Uveljavljanje (povračila stroškov v primeru sporov in izjeme) | 25 |
| 9.16.5 | Višja sila | 25 |
| 9.17 | Ostale določbe | 25 |

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 izdajateljcev potrdil AC NLB.

AC NLB kvalificirani ponudnik storitve zaupanja je bil ustanovljen pri Novi Ljubljanski banki d.d., Ljubljana (v nadaljevanju NLB d.d.). AC NLB je izdajal potrdila v skladu z UREDBO (EU) št. 910/2014 EVROPSKEGA PARLAMENTA IN SVETA o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (v nadaljevanju Uredba eIDAS) od datuma vpisa (29.06.2017) na zanesljivi seznam ponudnikov kvalificiranih storitev zaupanja.

Ponudnik storitev zaupanja AC NLB je z dnem prenehanja izdajanja potrdil (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 AC NLB do konca poteka veljavnosti vseh potrdil, ki jih je izdal AC NLB, izvajal preklic potrdil in objavo statusa potrdil. To bo omogočilo nemoteno uporabo potrdil izdanih s strani AC NLB do konca obdobja njihove veljavnosti.

Do konca prenehanja izdaje potrdil AC NLB je bila v veljavi in se je v celoti uporabljala Politika AC NLB, javni del notranjih pravil delovanja (3. izdaja, 31.01.2018). V nadaljevanju Politika AC NLB.

Vsa potrdila AC NLB so bila izdana po Politiki AC NLB, ki ostane v veljavi kot referenca za potrebe ocene postopkov ponudnika storitev AC NLB do datuma prenehanja izdaje potrdil.

Politika AC NLB se preneha uporabljati z datum uveljavitve pričujočih Rekono.TSP Pravil delovanja za AC NLB (28.06.2023). Politika AC NLB postane priloga pričujočih Rekono.TSP Pravil delovanja za AC NLB.

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

Dokument Rekono.TSP Pravila delovanja za AC NLB 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 AC NLB 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 AC NLB 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].

1.1.1 Potrdila ponudnika storitev AC NLB

AC NLB potrdila so izdana v skladu z Uredbo eIDAS in ZEPEP in drugo vsakokrat veljavno zakonodajo, kot je navedena v točki 9.14., kar zagotavlja zahtevan nivo zaupanja v identiteto imetnikov za kvalificirana potrdila in druge vrste potrdil izdanih s strani ponudnika storitev AC NLB.

Potrdila AC NLB izdana po Politiki AC NLB:

- Kvalificirana potrdila za elektronski podpis za fizične osebe
- Kvalificirana potrdila za elektronski podpis za fizične osebe, zaposlene pri pravnih osebi
- Kvalificirana potrdila za elektronski žig za pravne osebe
- Nekvalificirana (normalizirana) potrdila

Kvalificirana potrdila za elektronski podpis izdana po Politiki AC NLB, so namenjena za ustvarjanje naprednega elektronskega podpisa in kvalificiranega elektronskega podpisa ter druge namene glede na komercialni tip potrdila.

Kvalificirana potrdila za elektronski žig izdana po Politiki AC NLB, so namenjena za ustvarjanje naprednega elektronskega žiga in kvalificiranega elektronskega žiga ter druge namene glede na komercialni tip potrdila.

Nekvalificirana (normalizirana) potrdila izdana po Politiki AC NLB, so namenjena uporabi v zaprtem sistemu.

1.2 Naziv dokumenta in identifikacijske oznake potrdil

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

| | |
|-----------------------|---|
| Naziv dokumenta, sl: | Rekono.TSP Pravila delovanja za AC NLB |
| Naziv dokumenta, en.: | Certification Practice Statement of the Rekono.TSP for AC NLB |
| Verzija: | 1.1 |
| Datum izdaje: | 19. April 2023 |
| Datum uveljavitve: | 28. Junij 2023 |

Identifikacijske oznake potrdil ponudnika storitev AC NLB:

AC NLB - Kvalificirana potrdila za fizične osebe

| | |
|--------------------------|--|
| Opis: | Kvalificirana potrdila za fizične osebe |
| Vrsta: | Kvalificirano potrdilo za elektronski podpis |
| Namen uporabe: | Napreden elektronski podpis, šifriranje in avtentikacija |
| Rok veljavnosti: | Do pet (5) let |
| Identifikacijska oznaka: | 1.3.6.1.4.1.7597.1.5.11, 0.4.0.194112.1.0 |

AC NLB - Kvalificirana potrdila za zaposlene pri pravnih osebah

| | |
|--------------------------|--|
| Opis: | Kvalificirana potrdila za zaposlene pri pravnih osebah |
| Vrsta: | Kvalificirano potrdilo za elektronski podpis |
| Namen uporabe: | Napreden elektronski podpis, šifriranje in avtentikacija |
| Rok veljavnosti: | Do pet (5) let |
| Identifikacijska oznaka: | 1.3.6.1.4.1.7597.1.5.12, 0.4.0.194112.1.0 |

AC NLB - Kvalificirana potrdila za fizične osebe za oddaljen podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa

| | |
|--------------------------|---|
| Opis: | Kvalificirana potrdila za fizične osebe za uporabo na napravi, ki ustreza skladnosti s FIPS 140-2 level 3 in QSCD |
| Vrsta: | Kvalificirano potrdilo za elektronski podpis |
| Namen uporabe: | Kvalificiran elektronski podpis |
| Rok veljavnosti: | Do pet (5) let |
| Identifikacijska oznaka: | 1.3.6.1.4.1.7597.1.5.13, 0.4.0.194112.1.2 |

AC NLB - Kvalificirana potrdila za fizične osebe za oddaljen podpis

Opis: Kvalificirana potrdila za fizične osebe
Vrsta: Kvalificirano potrdilo za elektronski podpis
Namen uporabe: Napreden elektronski podpis
Rok veljavnosti: Do pet (5) let
Identifikacijska: 1.3.6.1.4.1.7597.1.5.14, 0.4.0.194112.1.0
Oznaka:

AC NLB - Kvalificirana potrdila za pravne osebe za elektronski žig

Opis: Kvalificirana potrdila za pravne osebe
Vrsta: Kvalificirano potrdilo za elektronski žig
Namen uporabe: Napreden elektronski žig in avtentikacija
Rok veljavnosti: Do pet (5) let
Identifikacijska: 1.3.6.1.4.1.7597.1.5.15, 0.4.0.194112.1.1
Oznaka:

AC NLB - Kvalificirana potrdila za pravne osebe za elektronski žig na napravi za ustvarjanje kvalificiranega elektronskega žiga

Opis: Kvalificirana potrdila za pravne osebe za elektronski žig za uporabo na napravi, ki ustreza skladnosti s FIPS 140-2 level 3 in QSCD
Vrsta: Kvalificirano potrdilo za elektronski žig
Namen uporabe: Kvalificiran elektronski žig za avtentikacijo
Rok veljavnosti: Do pet (5) let
Identifikacijska: 1.3.6.1.4.1.7597.1.5.16, 0.4.0.194112.1.3
Oznaka:

AC NLB - Potrdila za druge namene

Opis: Namenska potrdila za ostale namene v zaprtem sistemu
Vrsta: Potrdilo za elektronski podpis
Namen uporabe: Napreden elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti: Do pet (5) let
Identifikacijska: 1.3.6.1.4.1.7597.2.(glede na uporabo)
Oznaka:

Druga potrdila potrebna za delovanje infrastrukture AC NLB

AC NLB - Potrdila za OCSP

Opis: Potrdila za storitev OCSP v okviru AC NLB.
Namen uporabe: Napreden elektronski podpis odgovora storitve OCSP
Rok veljavnosti: Do tri (3) let-a
Identifikacijska: 1.3.6.1.4.1.7597.3.1
Oznaka:

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 AC NLB je vzpostavljeno več izdajateljev. Korenski izdajatelj ACNLB RootCA, ki ima samopodpisano potrdilo in je izdal potrdila podrejenemu izdajatelju, ter podrejeni izdajatelj za upravljanje potrdil končnih uporabnikov.

| Potrdilo korenkega izdajatelja ACNLB RootCA vsebuje: | | |
|--|-------------------|--|
| Serial Number | Serijska številka | EE61ADE00000000593E4965 |
| Issuer | Ponudnik storitev | CN=ACNLB RootCA OID.2.5.4.97=VATSI-91132550 O=NLB d.d. |

Rekono.TSP Pravila delovanja za AC NLB

| | | |
|----------------------|------------------------|--|
| Subject | Imetnik | C=SI CN=ACNLB RootCA OID.2.5.4.97=VATSI-91132550 O=NLB d.d. C=SI |
| Validity: Not Before | Veljavnost od: | Jun 12 07:30:03 2017 GMT |
| Validity: Not After | Veljavnost do: | Jun 12 08:00:03 2037 GMT |
| RSA Public Key | Dolžina RSA ključa | 3072 bit |
| Signature Algorithm | Algoritem | sha256WithRSAEncryption |
| Key Identifier | Identifikator ključa | 4A79C15E3281C687 |
| SHA-256 hash: | SHA-256 odtis Potrdila | 32974009D1662C1426DBCC121468F1FFC8E7081C52C5B7050 BEC0A9686ABCCFF |
| SHA-1 hash | SHA-1 odtis potrdila | EE6A664759F2B0A8F0F18E6A594FDD02207D30D0 |

| Potrdilo izdajatelja ACNLB SubCA vsebuje: | | |
|---|------------------------|--|
| Serial Number | Serijska številka | 07C94F3D00000000593E49A0 |
| Issuer | Ponudnik storitev | CN=ACNLB RootCA OID.2.5.4.97=VATSI-91132550 O=NLB d.d. C=SI |
| Subject | Imetnik | CN=ACNLB SubCA OID.2.5.4.97=VATSI-91132550 O=NLB d.d. C=SI |
| Validity: Not Before | Veljavnost od: | Jun 12 11:22:42 2017 GMT |
| Validity: Not After | Veljavnost do: | Apr 12 11:52:42 2036 GMT |
| RSA Public Key | Dolžina RSA ključa | 3072 bit |
| Signature Algorithm | Algoritem | sha256WithRSAEncryption |
| Key Identifier | Identifikator ključa | 454FBC6BEA4AEA8B |
| SHA-256 hash: | SHA-256 odtis Potrdila | A008209DA8EEA5D669AA9E48382AF0528087F5830B0919CAA 99507C57ECA1A51 |
| SHA-1 hash | SHA-1 odtis potrdila | EC9DA485FBBC92412BA524737F592F4B4D342D7B |

Opomba: OID.2.5.4.97 predstavlja polje organizationIdentifier (OI).

1.3.2 Registracijska pisarna ponudnika storitev

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

1.3.3 Naročniki in imetniki potrdil

Naročnik potrdila je pravna ali fizična oseba, registrirana za opravljanje dejavnosti, ki je zahtevala izdajo potrdila v imenu enega ali več imetnikov, ali samostojna fizična oseba. Naročnik je hkrati imetnik, kadar podpiše zahtevek v svojem imenu.

Imetnik potrdila je fizična oseba, navedena v potrdilu v polju »subject« kot lastnik zasebnega ključa, ki ustreza javnemu ključu, navedenemu v potrdilu.

V primeru, ko je naročnik pravna oseba, je imetnik fizična oseba zaposlena ali povezana s pravno osebo, ki

uporablja potrdilo v svojem imenu. V polju "subject" so vpisani podatki imetnika ter naziv organizacije.

S podpisom vloge se imetnik zavezuje k doslednemu spoštovanju in upoštevanju pravil delovanja ponudnika storitev.

Naročniki in imetniki potrdil morajo izpolnjevati vse zahteve iz Politike AC NLB po kateri je bilo potrdilo izdano in veljavnih predpisov. Imetnik potrdila se zavezuje, da bo uporabljal svoj par ključev le v obdobju veljavnosti svojega potrdila. Glej tudi 9.6.3.

Glej tudi dokument Politika AC NLB, poglavje 1.3.3.

1.3.4 Tretja oseba

Tretja oseba je vsak subjekt, ki se zanaša na verodostojnost potrdila, ne glede na to ali je imetnik potrdila.

Ob prvi uporabi potrdil AC NLB mora tretja oseba, ki se zanaša na potrdilo, prebrati in upoštevati Politiko AC NLB.

Tretja oseba mora vedno v času uporabe potrdila preveriti, če potrdilo ni v registru preklicanih potrdil (CRL ali OCSP).

Če potrdilo vsebuje podatke o tretji osebi, je ta dolžna zahtevati preklic potrdila, če izve, da je bil zasebni ključ ogrožen, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

Glej tudi dokument Politika AC NLB, poglavje 1.3.4.

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 potrdil

1.4.1 Dovoljena uporaba potrdil

Potrdila AC NLB je dovoljeno uporabljati v skladu z določili za posamezen tip potrdila navedenimi v poglavju 1.2 Naziv dokumenta in identifikacijske oznake potrdil.

Kvalificirana potrdila za elektronski podpis AC NLB, so namenjena za ustvarjanje naprednega elektronskega podpisa in kvalificiranega elektronskega podpisa ter druge namene glede na komercialni tip potrdila (glej 1.2).

Kvalificirana potrdila za elektronski žig AC NLB, so namenjena za ustvarjanje naprednega elektronskega žiga in kvalificiranega elektronskega žiga ter druge namene glede na komercialni tip potrdila (glej 1.2).

Potrdila za ostale namene, izdana s strani AC NLB, so normalizirana (nekvalificirana) potrdila in so namenjena uporabi v zaprtem sistemu.

Potrdila za OCSP se uporabljajo samo za podpis odgovora storitve OCSP za izdajatelje AC NLB.

Glej tudi dokument Politika AC NLB, poglavje 1.4.1.

1.4.2 Nedovoljena uporaba potrdil

Uporaba potrdil je dovoljena samo za namene, ki so opisani v poglavju 1.4.1. Za vse ostale namene pa uporaba potrdil ni dovoljena.

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

1.5.2.1 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>

1.5.2.2 Kontaktni podatki AC NLB

Ponudnika storitev AC NLB, ki je deloval v okviru NLB d.d. predstavljajo naslednji identifikacijski podatki:

Naslov: NLB d.d.
AC NLB
Trg republike 2
1000 Ljubljana
Telefon: (+386) 01 477 20 60
Fax: (+386) 01 476 47 99
Spletna stran: <https://www.nlb.si/ac-nlb>
E-mail: acnlb@nlb.si
Pomoč uporabnikom: (+386) 01 477 20 00
Enolično ime: AC NLB

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.

Glej tudi dokument Politika AC NLB, poglavje 1.5.4.

1.6 Pojmi in kratice

Glej Rekono.TSP Pravila delovanja, poglavje 1.6 in Politika AC NLB, poglavje 1.6.

2 Odgovornost za objave in repozitorij

2.1 Repozitorij

Ponudnik storitev Rekono.TSP objavlja informacije o svojih storitvah na javnih spletnih straneh, ki so dosegljive na spletnem naslovu <https://www.nlb.si/ac-nlb>.

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

Glej tudi dokument Politika AC NLB, poglavje 2.1.

2.2 Objave informacij o potrdilih

Glej Rekono.TSP Pravila delovanja, poglavje 2.2.

2.3 Čas in pogostost objav

Glej Rekono.TSP Pravila delovanja, poglavje 2.3.

2.4 Dostop do podatkov v repozitoriju

Glej Rekono.TSP Pravila delovanja, poglavje 2.4.

3 PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI

3.1 Določanje imen

Se ne izvaja. Glej tudi Politika AC NLB, poglavje 3.1.

3.2 Prva registracija

Se ne izvaja. Glej tudi Politika AC NLB, poglavje 3.2.

3.3 Preverjanje istovetnosti pri obnovi potrdila

Se ne izvaja. Glej tudi Politika AC NLB, poglavje 3.3.

3.4 Preverjanje istovetnosti ob zahtevi za preklic potrdila

Uporabnik se lahko identificira preko katere koli ustrezne storitve NLB d.d. po enakem postopku, kot pri registraciji (glej Politika AC NLB, poglavje 3.2) ali s kodo za preklic, ki jo je prejel ob registraciji.

4 Upravljanje s potrdili

4.1 Vloga za izdajo potrdila za fizične osebe in za pravne osebe za zaposlene

Se ne izvaja. Glej tudi Politika AC NLB, poglavje 4.1.

4.2 Obdelava vloge za izdajo potrdila

Se ne izvaja. Glej tudi Politika AC NLB, poglavje 4.2.

4.3 Izdaja potrdila

Se ne izvaja. Glej tudi Politika AC NLB, poglavje 4.3.

4.4 Prevzem potrdila

Se ne izvaja. Glej tudi Politika AC NLB, poglavje 4.4.

4.5 Uporaba ključev in potrdil

Glej Politika AC NLB, poglavje 4.5.

4.6 Obnova potrdil brez spremembe ključev

Glej Politika AC NLB, poglavje 4.6.

4.7 Obnova potrdil

Glej Politika AC NLB, poglavje 4.7.

4.8 Sprememba potrdila

Glej Politika AC NLB, poglavje 4.8.

4.9 Začasna ukinitve veljavnosti in preklic potrdila

Glej tudi Politika AC NLB, poglavje 4.9.

4.9.1 Okoliščine preklica

Ponudnik storitev prekliče potrdilo:

- Ob domnevni ali dejanski ogroženosti zasebnih ključev.
- Ob spremembi podatkov v potrdilu, ki zahtevajo izdajo novega.
- Ob neizpolnjevanju obveznosti iz točke 9.6.3 Politike AC NLB.
- V primeru smrti imetnika potrdila.
- Če to zahteva imetnik potrdila.
- V primeru smrti imetnika potrdila ali spremembe okoliščin, ki bistveno vplivajo na veljavnost potrdila.
- Ob napačnem podatku v potrdilu, oziroma je bilo potrdilo izdano na podlagi napačnih podatkov.
- Ob prenehanju delovanja ponudnika storitev ali prepovedi delovanja ponudnika storitev in njegove dejavnosti ni prevzel drug ponudnik storitev.
- Ob ogroženosti informacijskega sistema ponudnika storitev ali podatkov za preverjanje podpisov, na način, ki vpliva na zanesljivost potrdila.
- Ob neizpolnjevanju obveznosti iz točke 9.6.3 Politike AC NLB s strani naročnika.

Imetnik potrdila je dolžan ponudniku storitev nemudoma prijaviti vsako domnevno ali dejansko ogrožanje zasebnega ključa ter vse podatke, ki so relevantni za morebiten preklic pooblastila.

4.9.2 Kdo lahko zahteva preklic

Preklic potrdila lahko zahteva:

- Osebe ponudnika storitev.
- Imetnik potrdila.
- Pristojno sodišče, sodnik za prekrške ali upravni organ.
- Dedič ali zakoniti zastopnik.
- Tretja oseba, če potrdilo vsebuje podatke o tretji osebi ali če obstaja nevarnost zlorabe.

4.9.3 Postopki za preklic

- Zahtevek za preklic se lahko poda:
 - osebno z oddajo vloge za preklic osebju ponudnika storitev,
 - po telefonu na številko za preklic z uporabo kode za preklic.
- Po uspešno izvedenem postopku preverjanja istovetnosti imetnika potrdila s strani RA službe NLB, se posreduje zahteva za preklic ponudniku storitev Rekono.TSP.
- Ponudnik storitev izvede preklic potrdila.

4.9.4 Čas za posredovanje vloge za preklic

V primeru okoliščin, ki zahtevajo preklic potrdila, mora imetnik zahtevo za preklic posredovati v najkrajšem možnem času.

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.

4.9.6 Obveza preverjanja registra preklicanih potrdil

Glej Politika AC NLB, 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 izdajatelj posodobi seznam preklicanih potrdil takoj, ko se 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 potrdil

Glej Politika AC NLB, poglavje 4.9.9.

4.9.10 Obveza sprotnega preverjanja statusa preklicanih potrdil

Glej Politika AC NLB, poglavje 4.9.10.

4.9.11 Ostale oblike objavljanja preklicanih potrdil

Glej Politika AC NLB, poglavje 4.9.11.

4.9.12 Posebne zahteve glede zlorabe ključa

Glej Politika AC NLB, poglavje 4.9.12.

4.9.13 Okoliščine za začasno razveljavitev veljavnosti potrdila

Začasna ukinitve veljavnosti potrdil se ne uporablja.

4.10 Storitev objavljanja statusa 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 registra preklicanih potrdil

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

Glej tudi Rekono.TSP Pravila delovanja, poglavje 4.10.2.

4.10.3 Dodatne možnosti

Namenoma puščeno prazno.

4.11 Trajanje naročniškega razmerja

Naročniško razmerje začne teči s prevzemom potrdila. Naročniško razmerje je sklenjeno za obdobje veljavnosti potrdila.

Naročniško razmerje preneha:

- Ob poteku veljavnosti potrdila.
- Ob preklicu potrdila.
- Če naročnik krši obveznosti Politike AC NLB, lahko ponudnik storitev prekine naročniško razmerje.

4.12 Varnostno kopiranje in odkrivanje zasebnega ključa

Glej Politika AC NLB, poglavje 4.12.

5 Fizično varovanje, organizacijski varnostni ukrepi in zahteve 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 AC NLB, poglavje 6.1.

6.2 Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov

Glej Politika AC NLB, poglavje 6.2.

6.3 Ostali vidiki upravljanja s pari ključev

Glej Politika AC NLB, poglavje 6.3.

6.4 Aktivacijski podatki

Glej Politika AC NLB, poglavje 6.4.

6.5 Varnostne zahteve za računalnike

Glej Rekono.TSP Pravila delovanja, poglavje 6.5.

6.6 Tehnični nadzor življenjskega cikla ponudnika storitev

Glej Rekono.TSP Pravila delovanja, poglavje 6.6.

6.7 Časovno žigosanje

Namenoma puščeno prazno.

7 Profil potrdil in registrov preklicanih potrdil

Glej Politika AC NLB, 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 potrdil

Ponudnik storitev ne izdaja potrdil naročnikom oziroma imetnikom.

9.1.2 Cena dostopa do potrdil v javnem imeniku

Dostop do javnega imenika ni možen.

9.1.3 Cena dostopa do registra preklicanih potrdil

Dostop do registra preklicanih potrdila je brezplačen.

9.1.4 Cena ostalih storitev

Stroške potrebne strojne ali programske opreme za varno shranjevanje in uporabo potrdil, krije naročnik oziroma imetnik potrdila.

9.1.5 Pravica vračila

Namenoma puščeno prazno. Glej tudi 9.1.1.

9.2 Finančna odgovornost

9.2.1 Zavarovanje odgovornosti

9.2.2 Druge oblike zavarovanja

Rekono d.o.o. ima 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 jamstvo za druge uporabnike

Ni predvideno.

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 nepooblaščenca oseba.

Glej Politika AC NLB, 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 Politika AC NLB, 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 Nevarovani osebni podatki

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 Odgovornosti in jamstva

9.6.1 Odgovornosti in jamstva ponudnika storitev

Ponudnik storitev je dolžan:

- delovati v skladu s svojimi notranjimi pravili in ostalimi veljavnimi predpisi in zakonodajo,
- delovati v skladu z mednarodnimi priporočili,
- objavljati vse pomembne dokumente, ki določajo njegovo delovanje (politike delovanja, zahteve, cenik, navodila za varno uporabo Kvalificiranih potrdil ipd.),
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti ponudnika storitev, ki kakorkoli vplivajo na imetnike potrdil in tretje osebe,
- zagotoviti delovanje prijavnih služb v skladu z določili ponudnika storitev in ostalimi veljavnimi predpisi,
- spoštovati določila glede varnega ravnanja z osebnimi, poslovnimi in zaupnimi podatki o ponudniku storitev, imetnikih potrdil ali tretjimi osebami,
- preklicati potrdilo in objaviti preklicano potrdilo v registru preklicanih potrdil, ko ugotovi, da so podani razlogi po tej politiki ali drugih veljavnih predpisih,
- izdajati potrdila v skladu s to politiko in ostalimi predpisi ter priporočili,
- zagotoviti pravilnost podatkov izdanih potrdil.
- zagotoviti, da ima imetnik potrdila v času izdaje le-tega zasebni ključ, ki pripada v potrdilu navedenemu javnemu ključu (glej podpogl. 3.2.1),
- zagotoviti pravilnost objave registra preklicanih potrdil,
- zagotoviti pravilnost delovanja sprotnega preverjanja statusa potrdil.
- zagotoviti enoličnost razločevalnih imen,
- zagotoviti primerno fizično varnost prostorov in dostopov do samih prostorov ponudnika storitev, .
- kot dober gospodar skrbeti za nemoteno delovanje in čim večjo razpoložljivost storitve,
- kot dober gospodar skrbeti za čim večjo dostopnost storitev,
- kot dober gospodar skrbeti za nemoteno delovanje vseh ostalih spremljajočih storitev,
- poskušati odpraviti nastale probleme po najboljših močeh in v najkrajšem času,
- obveščati vse ustrezne subjekte o pomembnih zadevah,
- izpolnjevati vse druge zahteve v skladu s to politiko.

Ponudnik storitev zagotavlja čim večjo dostopnost svojih storitev, in sicer 24ur/7dni/365dni, razen v naslednjih primerih

- delovanje registracijske pisarne je samo v delovnem času,
- pri načrtovanih in vnaprej napovedanih tehničnih ali servisnih posegih na infrastrukturi,
- pri nenačrtovanih tehničnih ali servisnih posegih na infrastrukturi, kot posledica nepredvidenih okvar,
- pri tehničnih ali servisnih posegih zaradi okvare infrastrukture izven pristojnosti ponudnika storitev,
- zaradi nedostopnost, kot posledico 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 Obveznosti in odgovornost imetnika

Imetnik oziroma bodoči imetnik potrdila je dolžan:

- seznaniti se s to politiko pred izdajo potrdila,

- ravnati v skladu s to politiko in ostalimi veljavnimi predpisi,
- po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti ponudnika storitev oziroma zahtevati preklic potrdila,
- če po oddaji zahtevka za pridobitev potrdila oz. drugo storitev od ponudnika storitev ne prejme obvestila po e-pošti, ki jo je navedel v zahtevku, potem se mora obrniti na pooblaščen osebe ponudnika storitev,
- spremljati vsa obvestila ponudnika storitev in ravnati v skladu z njimi,
- v skladu z obvestili ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
- vse spremembe, ki so povezane s potrdilom, nemudoma sporočiti ponudniku storitev,
- zahtevati preklic potrdila, če so bili zasebni ključi ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe,
- uporabljati potrdilo za namen določen v podpoglavju 1.4.1.

Imetnik odgovarja za:

- nastalo škodo v primeru zlorabe potrdila od prijave preklica do preklica,
- vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba imetnikovega potrdila s strani nepooblaščenih oseb,

vsako drugo škodo, ki izvira iz neupoštevanja določil te politike in drugih obvestil ponudnika storitev ter veljavnih predpisov.

Obveznosti imetnika glede uporabe potrdil so določene v 4.5.1.

9.6.4 Obveznosti in odgovornost tretjih oseb

Tretje osebe morajo proučiti vse zahteve in okoliščine, preden se odločijo za uporabo potrdil, ki jih izda ponudnika storitev.

Tretje osebe, ki uporabljajo izdana potrdila ponudnika storitev, morajo:

- skrbno proučiti vse možnosti tveganja in odgovornosti pri uporabi potrdil in določiti politiko za način uporabe,
- za overjanje podpisa oz. druge kriptografske operacije uporabljati programsko in strojno opremo, s katero lahko na verodostojen način preverijo vse zahteve za varno uporabo potrdil,
- obvestiti ponudnika storitev, če izvedo, da so bili zasebni ključi imetnika potrdila, na katerega se zanašajo, ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, navedeni v potrdilu,
- upoštevati druge določbe iz morebitnih medsebojnih dogovorov,
- upoštevati vsa navodila oz. priporočila ponudnika storitev glede zanesljive uporabe,
- ob morebitnih napakah ali problemih takoj obvestiti ponudnika storitev,
- seznaniti se s to politiko in upoštevati vsa določila glede njihove obveznosti, odgovornosti ter omejitve glede zaupanja in uporabe potrdil,
- spremljati vsa obvestila in objave ponudnika storitev in ravnati v skladu z le-timi,
- upoštevati morebitna druga pravila, ki so izven pristojnosti ponudnika storitev in so določena drugje.

Tretje osebe nosijo vse posledice, ki bi nastale zaradi morebitnega neupoštevanja določil te politike, morebitnega dogovora z ponudnikom storitev in veljavne zakonodaje.

9.6.5 Obveznosti in odgovornosti drugih subjektov

Obveznosti in odgovornosti drugih subjektov niso predpisane.

9.7 Zanikanje odgovornosti ponudnika storitev

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

- če je bilo potrjeno izdano zaradi napake, neverodostojnih podatkov ali drugih nepravilnosti na strani imetnika potrdila,
- če je potekla veljavnost potrdila,
- kadar je potrjeno uporabljeno po preklicu in objavi v registru preklicanih potrdil,
- če je potrjeno ponarejeno ali kakor koli predrugačeno ali spremenjeno,
- če prosilec, imetnik potrdila ali tretja oseba ne ravna v skladu z določbami tega dokumenta, pravili delovanja ponudnika storitev, ali veljavnimi zakoni in na njihovi podlagi izdanimi podzakonskimi predpisi,
- če je bil zasebni ključ imetnika ogrožen ali obstaja objektivno utemeljen sum, da je bil ogrožen,
- če je bilo varovanje gesel ali zasebnih ključev imetnikov nepravilno ali pomanjkljivo ali pa je prišlo do izdajanja zaupnih podatkov ali ključev tretjim osebam in neodgovornega ravnanja imetnika,
- če je bilo potrjeno uporabljeno v drugačne namene, kot je določeno z naročniško pogodbo, pravili delovanja ponudnika storitev, ali veljavnimi zakoni in na njihovi podlagi izdanimi podzakonskimi predpisi,
- če je prišlo do zlorabe oz. vdora v informacijski sistem imetnika potrdila in s tem do podatkov o potrdilih s strani nepooblaščenih oseb,
- če nastane škoda zaradi napake v delovanju strojne ali programske opreme prosilca, imetnika potrdila ali tretje osebe.

9.8 Omejitve odgovornosti ponudnika storitev

Ponudnik storitev zanika kakršnokoli odgovornost vseh vrst, za nadomestila, škodo ali druge terjatve ali obveznosti katerekoli vrste, ki izhajajo iz škod, pogodb ali iz katerihkoli drugih razlogov v zvezi s katerokoli storitvijo povezano z izdajo, uporabo, ali zanašanjem na digitalno potrdilo, ki ga je izdal ponudnik storitev in ki presega ceno digitalnega potrdila.

9.9 Poravnava škode

Glej poglavji 9.7 in 9.8.

9.10 Začetek in prenehanje veljavnosti

9.10.1 Začetek veljavnosti

Rekono.TSP Pravila delovanja za AC NLB 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 AC NLB 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 (na primer postopek, ki določa način, po katerem je bilo to potrdilo izdano ipd.).

9.11 Komuniciranje med subjekti

Kontaktne podatke ponudnika storitev oz. izdajatelja so objavljeni na spletnih straneh in podani v podpoglavju 1.3.1.

Kontaktne podatke imetnikov so podani v zahtevkih v zvezi s potrdili.

Kontaktne podatke tretjih oseb so podani v morebitnem medsebojnem dogovoru med tretjo osebo in ponudnikom storitev.

Ponudnik storitev ostale subjekte obvešča preko obvestil objavljenih na svojih spletnih straneh.

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

Vse spremembe Rekono.TSP Pravil delovanja bodo objavljene, kot je opisano v poglavju **Error! Reference source not found.** 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 **Error! Reference source not found.**

9.12.3 Spremembe, ki zahtevajo novo identifikacijsko oznako politike

Namenoma puščeno prazno.

9.13 Postopek v primeru 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 **Error! Reference source not found.**

Ponudnik storitev deluje v skladu z:

- UREDBO (EU) št. 910/2014 EVROPSKEGA PARLAMENTA IN SVETA o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (na kratko Uredbo eIDAS).
- Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/2004 - ZEPEP).
- Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 94/2007-UPB1 -ZVOP-1).
- drugimi predpisi veljavnimi v Republiki Sloveniji.

9.15 Skladnost z veljavno zakonodajo

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

Potrdilo, ki ga ponudnik storitev izda imetniku ter morebitne pravice, povezane z uporabo potrdila, so namenjene izključno imetniku in niso prenosljive na tretje osebe.

9.16.3 Spremembe okoliščin delovanja

Ničnost enega ali več delov teh Rekono.TSP Pravil delovanja za AC NLB 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 so obravnavajo v skladu s predpisi, ki veljajo v Republiki Sloveniji.

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"
- [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 AC NLB (<https://www.nlb.si/ac-nlb>)