Certifikatska agencija POŠTA®CA

Izjava o politiki delovanja

(angl. Policy Disclosure Statement – PDS)

Pošta Slovenije

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

PREGLED VSEBINE

1 IDENTITETA OVERITELJA IN KONTAKTNE INFORMACIJE

V okviru POŠTE SLOVENIJE d.o.o., Maribor, Slovenija, deluje ponudnik kvalificiranih storitev zaupanja, Certifikatska agencija Pošte Slovenije, krajše overitelj POŠTA®CA. Overitelj POŠTA®CA izdaja različne vrste overjenih digitalnih potrdil.

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

2 KATEGORIJE DIGITALNIH POTRDIL, OVERJANJE IDENTITETE SUBJEKTOV IN NAMENI UPORABE

Overitelj izdaja naslednje kategorije kvalificiranih potrdil za zaposlene pri pravnih osebah:

- **Napredna kvalificirana potrdila -** kvalificirana potrdila z dvema paroma ključev za fizične osebe zaposlene pri pravnih osebah, z obvezno uporabo QSCD naprave. To potrdilo se lahko uporablja za kvalificirani elektronski podpis, šifriranje in avtentikacijo.
- **Kvalificirana potrdila z obvezno uporabo QSCD naprave -** kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah. Obvezna je uporaba QSCD naprave. To potrdilo se lahko uporablja za kvalificirani elektronski podpis, šifriranje in avtentikacijo.
- **Kvalificirana potrdila -** kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah. To potrdilo se lahko uporablja za napredni elektronski podpis, šifriranje in avtentikacijo.
- **Kvalificirana potrdila, izdana na QSCD napravi** - kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah. Potrdilo je izdano na QSCD napravi. To potrdilo se lahko uporablja za kvalificirani elektronski podpis, šifriranje in avtentikacijo.
- **Kvalificirana potrdila, izdana na oddaljeni QSCD napravi** - kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah, izdana na oddaljeni QSCD napravi. To potrdilo se lahko uporablja za kvalificirani elektronski podpis.
- **Kvalificirana potrdila s splošnim nazivom z obvezno uporabo QSCD naprave** - kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah, z dodatnim splošnim nazivom v polju commonName in z obvezno uporabo QSCD naprave. To potrdilo se lahko uporablja za kvalificirani elektronski podpis, šifriranje in avtentikacijo. ***OPOMBA:*** *Od objave politike verzije 1.3 se ne izdajajo več. Vsa izdana potrdila ostanejo v uporabi do izteka veljavnosti.*
- **Kvalificirana potrdila s splošnim nazivom** - kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah, z dodatnim splošnim nazivom v polju commonName. To potrdilo se lahko uporablja za napredni elektronski podpis, šifriranje in avtentikacijo.

OPOMBA: *Od objave politike verzije 1.3 se ne izdajajo več. Vsa izdana potrdila ostanejo v uporabi do izteka veljavnosti.*

- **Kvalificirana potrdila s splošnim nazivom, izdana na QSCD napravi** - kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah, z dodatnim splošnim nazivom v polju commonName, izdana na QSCD napravi. To potrdilo se lahko uporablja za kvalificirani elektronski podpis, šifriranje in avtentikacijo.
  OPOMBA: *Od objave politike verzije 1.3 se ne izdajajo več. Vsa izdana potrdila ostanejo v uporabi do izteka veljavnosti.*

Overitelj izdaja naslednje kategorije kvalificiranih potrdil za fizične osebe:

- **Napredna kvalificirana potrdila -** kvalificirana potrdila z dvema paroma ključev za fizične osebe in obvezno uporabo QSCD naprave. To potrdilo se lahko uporablja za kvalificirani elektronski podpis, šifriranje in avtentikacijo.
- **Kvalificirana potrdila z obvezno uporabo QSCD naprave -** kvalificirana potrdila z enim parom ključev za fizične osebe in obvezno uporabo QSCD naprave. To potrdilo se lahko uporablja za kvalificirani elektronski podpis, šifriranje in avtentikacijo.
- **Kvalificirana potrdila -** kvalificirana potrdila z enim parom ključev za fizične osebe. To potrdilo se lahko uporablja za napredni elektronski podpis, šifriranje in avtentikacijo.
- **Kvalificirana potrdila, izdana na QSCD napravi -** kvalificirana potrdila z enim parom ključev za fizične osebe, izdana na QSCD napravi. To potrdilo se lahko uporablja za kvalificirani elektronski podpis, šifriranje in avtentikacijo.
- **Kvalificirana potrdila, izdana na oddaljeni QSCD napravi -** kvalificirana potrdila z enim parom ključev za fizične osebe, izdana na oddaljeni QSCD napravi. To potrdilo se lahko uporablja za kvalificirani elektronski podpis.
- **Kvalificirana potrdila, izdana na profesionalni kartici v sistemu kartice zdravstvenega zavarovanja -** kvalificirana potrdila z enim parom ključev izdana na profesionalni kartici v sistemu kartice zdravstvenega zavarovanja. To potrdilo se lahko uporablja za kvalificirani elektronski podpis, šifriranje in avtentikacijo.

Overitelj izdaja naslednje kategorije kvalificiranih potrdil za pravne osebe:

- **Kvalificirana potrdila za pravne osebe z obvezno uporabo QSCD naprave -** kvalificirana potrdila za pravne osebe z dvema paroma ključev z obvezno uporabo QSCD naprave. To potrdilo se lahko uporablja za kvalificirani elektronski žig.
- **Kvalificirana potrdila za pravne osebe -** kvalificirana normalizirana potrdila za pravne osebe z enim parom ključev. To potrdilo se lahko uporablja za napredni elektronski žig.
- **Kvalificirana potrdila za pravne osebe, izdana na QSCD napravi -** kvalificirana potrdila za pravne osebe z enim parom ključev, izdana na QSCD napravi. To potrdilo se lahko uporablja za kvalificirani elektronski žig.
- **Kvalificirana potrdila za pravne osebe, izdana na oddaljeni QSCD napravi -** kvalificirana potrdila za pravne osebe z enim parom ključev, izdana na oddaljeni QSCD napravi. To potrdilo se lahko uporablja za kvalificirani elektronski žig.

Overitelj izdaja naslednje kategorije kvalificiranih potrdil za spletne strežnike oziroma avtentikacijo spletišč:

- **Kvalificirana potrdila za spletne strežnike -** kvalificirana potrdila za spletne strežnike z enim parom ključev. To potrdilo se lahko uporablja za overjanje identitete spletnih strežnikov.

Overitelj izdaja naslednje kategorije normaliziranih potrdil:

- **Normalizirana potrdila za spletne strežnike -** to potrdilo se lahko uporablja za overjanje identitete spletnih strežnikov in VPN naprav.
- **Normalizirana potrdila za storitev časovnega žiga -** to potrdilo se lahko uporablja za potrjevanje veljavnosti naprednega elektronskega podpisa storitve časovnega žiga.
- **Normalizirana potrdila za storitev OCSP -** to potrdilo se lahko uporablja za potrjevanje veljavnosti naprednega elektronskega podpisa storitve OCSP.

Vse kategorije digitalnih potrdil zagotavljajo dokazilo identitete uporabnika. Preverjanje istovetnosti uporabnika se izvaja na sledeči način:

- Pravna in fizična oseba, registrirana za opravljanje dejavnosti se identificira z uradno potrjeno dokumentacijo ali s podatki iz uradnih evidenc. Zastopa jo odgovorna oseba ali od nje pooblaščena druga oseba. Odgovorna oseba ali od nje pooblaščena druga oseba se identificira z veljavnim osebnim dokumentom za identifikacijo.
- Fizična oseba se identificira z veljavnim osebnim dokumentom za identifikacijo.

3 OMEJITVE ZAUPANJA V DIGITALNA POTRDILA (ANGL. RELIANCE LIMITS)

Overitelj hrani vse podatke vezane na vsebino digitalnega potrdila in preverjanje veljavnosti digitalnega potrdila, vsaj sedem let od poteka veljavnosti potrdila. Digitalna potrdila se lahko uporabljajo samo v namene določene v poglavju "Kategorije digitalnih potrdil, overjanje identitete subjektov in nameni uporabe" ter v zadnji objavljeni verziji dokumenta Politika POŠTA®CA za kvalificirana in normalizirana potrdila, Javni del notranjih pravil delovanja, objavljenem na spletnem naslovu http://postarca.posta.si/dokumenti. Overitelj POŠTA®CA ne odgovarja za potrdila, ko le-ta niso več veljavna.

4 OBVEZNOSTI NAROČNIKOV IN IMETNIKOV 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 nepooblaščene 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 politike POŠTA®CA za kvalificirana in normalizirana potrdila, poglavje 6.1.5 in zahteve ETSI TS 119 312;
- v roku poravnavati vse finančne obveznosti do overitelja;
- digitalno potrdilo za spletne strežnike uporabljati le za SSL ali TLS protokol na strežniku za katerega je bilo izdano.

Pričujoči dokument vsebuje povzetek pravil delovanja overitelja POŠTA®CA. Imetniki in naročniki se morajo seznaniti tudi z dokumentom Politika POŠTA®CA za kvalificirana in normalizirana potrdila, Javni del notranjih pravil delovanja, objavljenem na spletnem naslovu http://postarca.posta.si/dokumenti.

5 OBVEZNOST TRETJIH STRANI GLEDE PREVERJANJA STATUSA POTRDIL

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

6 OMEJITVE ODGOVORNOSTI OVERITELJA

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.

7 MERODAJNA PRAVILA DELOVANJA IN OSTALI JAVNI DOKUMENTI OVERITELJA

Overitelj na svojih spletnih straneh objavlja naslednje dokumente:

- javni del notranjih pravil delovanja overitelja za posamezen tip digitalnih potrdil na naslovu http://postarca.posta.si/dokumenti;
- vloge za pridobitev, preklic in obnovo potrdil na naslovu http://postarca.posta.si/dokumenti;
- navodila za prevzem posameznih tipov digitalnih potrdil;
- seznam registracijskih pisarn;
- cenik.

Overitelj bo na spletni strani http://postarca.posta.si objavljal tudi vsa obvestila, ki so relevantna za vse uporabnike potrdil izdanih s strani overitelja.

8 VAROVANJE PODATKOV

Vsi podatki pridobljeni, ustvarjeni ali posredovani so varovani kot zaupni podatki, razen:

- digitalna potrdila in liste preklicanih potrdil ter osebne ali poslovne informacije vsebovane v njih;
- ta dokument in ostali dokumenti objavljeni na javnih spletnih straneh overitelja.

9 PRAVICA VRAČILA (ANGL. REFUND POLICY)

V primeru odstopa od zahtevka pred končanim postopkom, ali zavrnitve izdaje digitalnega potrdila, bo overitelj POŠTA®CA povrnil stroške izdaje digitalnega potrdila in postopka po veljavnem ceniku.

Prosilec fizična oseba se s podpisom vloge za pridobitev potrdila strinja, da nima pravice odstopiti od naročila potrdila, ko overitelj v celoti izpolni naročilo oziroma dobavi digitalne vsebine, saj je potrdilo izdelano glede na potrebe prosilca, podane na vlogi, in prilagojeno njegovim osebnim potrebam.

Overitelj POŠTA®CA v primeru vračila zaradi upravičene reklamacije krije le stroške izdaje digitalnega potrdila in postopka po veljavnem ceniku.

10 MERODAJNI ZAKONI, PRIPOROČILA, PRITOŽBE IN REŠEVANJE SPOROV

Overitelj deluje v skladu z:

- Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1993/93/ES (Uredba eIDAS);
- Zakonom o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/2004-UPB-1, 61/2006-ZEPT);
- drugimi veljavnimi predpisi in priporočili.

Oblika pričujočega dokumenta, POŠTA ® CA izjava o politiki delovanja, sledi " ETSI EN 319 411-1, Annex A.2 The PDS structure" priporočilom.

Oblika in vsebina javnega dela notranjih pravil delovanja overitelja je usklajena z:

- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI 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.

Vse pritožbe in spore, ki bi nastali, bo overitelj skušal reševati sporazumno. Če to ne bo mogoče, je za reševanje pristojno krajevno sodišče v Mariboru.

11 REGISTRACIJA IN AKREDITACIJA

Pošta Slovenije ima status ponudnika kvalificiranih storitev zaupanja v skladu z uredbo eIDAS za storitve izdaje kvalificiranih potrdil za elektronski podpis, elektronski žig in avtentikacijo spletišč.

Status ponudnika kvalificiranih storitev zaupanja potrdi pristojni nadzorni organ v Republiki Sloveniji z ustrezno odločbo in vpisom v zanesljivi seznam ponudnikov kvalificiranih storitev zaupanja (https://webgate.ec.europa.eu/tl-browser).

Skladnost delovanja overitelja z zahtevami uredbe eIDAS in ustreznih standardov (glej 10) preverja organ za ugotavljanje skladnosti z ustrezno akreditacijo.