Certifikatska agencija POŠTA®CA

Politika POŠTA®CA za kvalificirana in normalizirana potrdila

Javni del notranjih pravil delovanja

Verzija 1.1

Datum izdaje 30.06.2016

POŠTA SLOVENIJE

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

Stanje dokumenta

Izdaje Politike POŠTA®CA	
	Opis izdaje
	Politika POŠTA®CA za kvalificirana in normalizirana potrdila, verzija 1.1 Datum izdaje: 30.06.2016 Verzija vsebuje sledeče politike potrdil overitelja POŠTA®CA:
	Kvalificirana potrdila za fizične osebe:
	POŠTA®CA - Napredna kvalificirana potrdila CP OID: 1.3.6.1.4.1.15284.1.1.1.2.1.2
	POŠTA®CA - Kvalificirana potrdila z obvezno uporabo QSCD naprave CP OID: 1.3.6.1.4.1.15284.1.1.1.2.2.3
	POŠTA®CA - Kvalificirana potrdila CP OID 1.3.6.1.4.1.15284.1.1.2.2.2.2
	POŠTA®CA - Kvalificirana potrdila, izdana na QSCD napravi CP OID: 1.3.6.1.4.1.15284.1.1.3.2.2.2
	POŠTA®CA - Kvalificirana potrdila, izdana na oddaljeni QSCD napravi CP OID: 1.3.6.1.4.1.15284.1.1.5.2.2.1
	POŠTA®CA - Kvalificirana potrdila, izdana na profesionalni kartici v sistemu kartice zdravstvenega zavarovanja CP OID: 1.3.6.1.4.1.15284.1.1.4.2.2.2
	Kvalificirana potrdila za zaposlene pri pravnih osebah:
	POŠTA®CA - Napredna kvalificirana potrdila CP OID: 1.3.6.1.4.1.15284.1.1.1.1.1.3
	POŠTA®CA - Kvalificirana potrdila z obvezno uporabo QSCD naprave CP OID: 1.3.6.1.4.1.15284.1.1.1.1.2.4
	POŠTA®CA - Kvalificirana potrdila CP OID: 1.3.6.1.4.1.15284.1.1.2.1.2.3
	POŠTA®CA - Kvalificirana potrdila, izdana na QSCD napravi CP OID: 1.3.6.1.4.1.15284.1.1.3.1.2.2
	POŠTA®CA - Kvalificirana potrdila, izdana na oddaljeni QSCD napravi CP OID: 1.3.6.1.4.1.15284.1.1.5.1.2.1
	POŠTA®CA - Kvalificirana potrdila s splošnim nazivom, izdana na pametni

	kartici CP OID: 1.3.6.1.4.1.15284.1.1.3.4.2.1
	POŠTA®CA - Kvalificirana potrdila s splošnim nazivom CP OID: 1.3.6.1.4.1.15284.1.1.2.4.2.1
	POŠTA®CA - Kvalificirana potrdila s splošnim nazivom z obvezno uporabo QSCD naprave CP OID: 1.3.6.1.4.1.15284.1.1.1.4.2.1
	Normalizirana potrdila:
	POŠTA®CA – Normalizirana potrdila za spletne strežnike CP OID: 1.3.6.1.4.1.15284.1.2.1.1.2
	POŠTA®CA - Normalizirana potrdila za pravne osebe z obvezno uporabo QSCD naprave CP OID: 1.3.6.1.4.1.15284.1.3.1.3.2.1
	POŠTA®CA - Normalizirana potrdila za pravne osebe CP OID: 1.3.6.1.4.1.15284.1.3.2.3.2.1
	POŠTA®CA - Normalizirana potrdila za pravne osebe, izdana na QSCD napravi CP OID: 1.3.6.1.4.1.15284.1.3.3.3.2.1
	Verzija nadomešča sledeče politike POŠTA®CA: Politika POŠTA®CA za kvalificirana in normalizirana digitalna potrdila - Verzija 1, Pričetek veljavnosti: 20.8.2012.

PREGLED VSEBINE

1 UVOD 6

1.1 PREGLED 6
1.2 NAZIV DOKUMENTA IN IDENTIFIKACIJSKE OZNAKE POTRDIL 8
1.3 UDELEŽENCI INFRASTRUKTURE JAVNIH KLJUČEV 14
1.4 NAMEN UPORABE POTRDIL 16
1.5 UPRAVLJANJE S PRAVILI DELOVANJA 17
1.6 POJMI IN KRATICE 18

2 ODGOVORNOST ZA OBJAVE IN REPOZITORIJ 22

2.1 REPOZITORIJ 22
2.2 OBJAVE INFORMACIJ O DIGITALNIH POTRDILIH 22
2.3 ČAS IN POGOSTOST OBJAV 23
2.4 DOSTOP DO PODATKOV V REPOZITORIJU 23

3 PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI 23

3.1 DOLOČANJE IMEN 23
3.2 PRVA REGISTRACIJA 26
3.3 PREVERJANJE ISTOVETNOSTI PRI OBNOVI POTRDILA 27
3.4 PREVERJANJE ISTOVETNOSTI OB ZAHTEVI ZA PREKLIC POTRDILA 27

4 UPRAVLJANJE S POTRDILI 27

4.1 VLOGA ZA IZDAJO POTRDILA 27
4.2 OBDELAVA VLOGE ZA IZDAJO POTRDILA 29
4.3 IZDAJA POTRDILA 29
4.4 PREVZEM POTRDILA 30
4.5 UPORABA KLJUČEV IN POTRDIL 31
4.6 OBNOVA DIGITALNIH POTRDIL BREZ SPREMEMBE KLJUČEV 31
4.7 OBNOVA POTRDIL 32
4.8 SPREMEMBA POTRDILA 33
4.9 ZAČASNA UKINITEV VELJAVNOSTI IN PREKLIC POTRDILA 34
4.10 STORITVE OBJAVLJANJA STATUSA POTRDIL 37
4.11 TRAJANJE NAROČNIŠKEGA RAZMERJA 37
4.12 VARNOSTNO KOPIRANJE IN ODKRIVANJE ZASEBNEGA KLJUČA 37
4.13 DODATNE MOŽNOSTI 38

5 FIZIČNO VAROVANJE, ORGANIZACIJSKI VARNOSTNI UKREPI IN ZAHTEVE ZA OSEBJE 39

5.1 FIZIČNO VAROVANJE 39
5.2 ORGANIZACIJSKI VARNOSTNI UKREP 40
5.3 ZAHTEVE ZA OSEBJE OVERITELJA 43
5.4 POSTOPKI ZBIRANJA IN UPRAVLJANJA REVIZIJSKIH SLEDI 44
5.5 ARHIVIRANJE PODATKOV 45
5.6 OBNOVA DIGITALNEGA POTRDILA OVERITELJA 46
5.7 POSTOPKI V PRIMERU OGROŽANJA ZASEBNEGA KLJUČA IN OKREVALNI NAČRT 46
5.8 PRENEHANJE DELOVANJA OVERITELJA 47

6 TEHNIČNE VARNOSTNE ZAHTEVE 47

6.1 TVORJENJE IN NAMESTITEV PARA KLJUČEV 47
6.2 ZAŠČITA ZASEBNIH KLJUČEV IN TEHNIČNE KONTROLE KRIPTOGRAFSKIH MODULOV 49
6.3 OSTALI VIDIKI UPRAVLJANJA S PARI KLJUČEV 50
6.4 AKTIVACIJSKI PODATKI 51
6.5 VARNOSTNE ZAHTEVE ZA RAČUNALNIKE 52
6.6 TEHNIČNI NADZOR ŽIVLJENJSKEGA CIKLA OVERITELJA 52

6.7 VARNOSTNE KONTROLE NA RAVNI RAČUNALNIŠKEGA OMREŽJA ... 53
6.8 ČASOVNO ŽIGOSANJE ... 53

7 PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL ... 53

7.1 PROFIL DIGITALNIH POTRDIL ... 53
7.2 PROFIL REGISTRA PREKLICANIH DIGITALNIH POTRDIL ... 57
7.3 PROFIL OCSP ... 57

8 PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA ... 58

8.1 POGOSTOST ALI OKOLIŠČINE IZVAJANJA NADZORNIH PREGLEDOV ... 58
8.2 POGOJI ZA IZVAJALCA NADZORA ... 58
8.3 RELACIJA MED IZVAJALCEM NADZORA IN OVERITELJEM ... 58
8.4 PODROČJA NADZORA ... 58
8.5 POSTOPKI PO OPRAVLJENEM NADZORNEM PREGLEDU ... 58
8.6 PREJEMNIKI IN OBJAVA UGOTOVITEV ... 58

9 OSTALE POSLOVNE IN PRAVNE ZADEVE ... 58

9.1 CENIK ... 58
9.2 FINANČNA ODGOVORNOST ... 59
9.3 ZAUPNOST POSLOVNIH INFORMACIJ ... 59
9.4 VAROVANJE OSEBNIH PODATKOV ... 60
9.5 ZAŠČITA INTELEKTUALNE LASTNINE ... 60
9.6 ODGOVORNOSTI IN JAMSTVA ... 61
9.7 ZANIKANJE ODGOVORNOSTI OVERITELJA ... 63
9.8 OMEJITVE ODGOVORNOSTI OVERITELJA ... 63
9.9 PORAVNAVA ŠKODE ... 64
9.10 ZAČETEK IN PRENEHANJE VELJAVNOSTI ... 64
9.11 OBVESTILA IN KOMUNICIRANJE Z UDELEŽENCI ... 65
9.12 SPREMINJANJE DOKUMENTA ... 65
9.13 REŠEVANJE SPOROV ... 65
9.14 VELJAVNA ZAKONODAJA ... 65
9.15 SKLADNOST S PRAVNIMI AKTI ... 66
9.16 SPLOŠNE DOLOČBE ... 66
9.17 OSTALE DOLOČBE ... 67

1 UVOD

1.1 Pregled

V okviru POŠTE SLOVENIJE d.o.o., Maribor (v nadaljevanju: ***organizacija***) deluje overitelj, Certifikatska agencija Pošte Slovenije, krajše overitelj POŠTA®CA. Overitelj POŠTA®CA izdaja različne vrste overjenih digitalnih potrdil (kvalificirana potrdila in normalizirana potrdila) različnim končnim uporabnikom v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/2004-UPB-1, 61/2006-ZEPT, v nadaljevanju ZEPEP), Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000, 2/2001, 86/2006), 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 objavlja:

- pravila delovanja, opredeljena v izjavi o politiki delovanja (angl. PKI Disclosure Statement – v nadaljevanju: overiteljev PDS-dokument);
- splošna pravila poslovanja, ki urejajo delovanje overitelja, imenovana tudi javni del notranjih pravil overitelja (angl. Certification Practice Statement – v nadaljevanju: politika);
- komercialni opis produktov - po potrebi, v primeru da imajo potrdila v okviru komercialnega produkta dodatne lastnosti, ki niso opredeljene v politiki.

Overiteljev PDS-dokument je pripravljen v skladu s priporočili " ETSI EN 319 411, Annex A:Model PKI disclosure statement" in ga je mogoče pridobiti na spletni strani overitelja: http://postarca.posta.si.

Politika opisuje tehnične lastnosti, stopnjo varnosti overiteljeve infrastrukture in postopke, ki jih overitelj POŠTA®CA uporablja za upravljanje infrastrukture in upravljanje vseh vrst potrdil. Politika vsebuje vse bistvene določbe, ki vplivajo na odnos med overiteljem in imetniki kvalificiranih in normaliziranih potrdil overitelja ter tretjimi osebami, ki se na ta potrdila upravičeno zanašajo.

Politika je oblikovana v skladu s priporočilom "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" (RFC 3647). Politika vsebuje tudi poglavja RFC 3647, ki ne zavezujejo overitelja s komentarjem "*ni predpisano*", ki označuje, da je bilo poglavje izključeno iz dokumenta po tehtni presoji overitelja. Na ta način je zagotovljena primerljivost s politikami drugih overiteljev v Sloveniji in svetu.

Pričujoči dokument opisuje javni del notranjih pravil overitelja (politika overitelja). Opis pravil delovanja je namenjen vsem, ki potrebujejo informacije za oceno zaupanja v potrdila, ki jih izdaja overitelj. Politika opredeljuje postopke upravljanja in lastnosti potrdil, ki opredeljujejo nivo zaupanja v potrdila, namen uporabe in enolično identiteto imetnika, ter jih overitelj POŠTA®CA zagotavlja za vse vrste potrdil. Posamezna potrdila imajo lahko v okviru posameznega komercialnega produkta dodatne lastnosti (npr. dodatno polje v razločevalnem polju, ali dodatno razširitveno polje X.509). Dodatne lastnosti v nobenem primeru ne zamenjujejo osnovnih lastnosti potrdil, ki opredeljujejo zaupanje v potrdilo, enoličnost imetnika potrdila ali namen uporabe. Za dodatne informacije, ki niso podane v politiki, se lahko zainteresirani obrnejo na kontaktne osebe, navedene v poglavju 1.4.

1.1.1 Digitalna potrdila overitelja POŠTA® CA

Overitelj POŠTA®CA izvaja upravljanje kvalificiranih in normaliziranih potrdila v skladu z veljavno zakonodajo, kar zagotavlja zahtevan nivo zaupanja v identiteto imetnikov za kvalificirana potrdila in vse vrste potrdil, ki jih izdaja overitelj POŠTA®CA. Posamezne vrste potrdil se razlikujejo glede na namen uporabe (kvalificirana in normalizirana potrdila), naročnika (pravne osebe, fizične osebe), tehnične lastnosti (napredna potrdila, standardna potrdila) in glede na kriptografski modul uporabljen za kreiranje in uporabo kriptografskih ključev. V nadaljevanju poglavja je opis posameznih lastnosti potrdil, ki jih izdaja overitelj POŠTA®CA.

Digitalna potrdila, ki jih izdaja overitelj POŠTA®CA se razlikujejo glede na sledeče lastnosti:

- **Namen uporabe - kvalificirana potrdila in normalizirana potrdila** – overitelj POŠTA®CA izvaja upravljanje vseh potrdil (kvalificiranih in normaliziranih) v skladu z veljavno zakonodajo (glej 9.14), kar zagotavlja enak nivo zaupanja v identiteto imetnikov kvalificiranih in normaliziranih potrdil. Razlika med kvalificiranimi in normaliziranimi potrdili overitelja POŠTA®CA je v namenu uporabe. Kvalificirana potrdila lahko imetniki uporabljajo za kvalificiran elektronski podpis in napredni elektronski ter ostale dovoljene namene (glej poglavje 1.4.1), normalizirana potrdila pa se lahko uporablja za napredni elektronski žig, za preverjanje istovetnosti strežnikov in naprav v okviru komunikacijskih protokolov (npr. SSL, TLS).
- **Naročnik digitalnega potrdila** - je lahko pravna oseba (pravna oseba ali fizična oseba, registrirana za opravljanje dejavnosti), ali fizična oseba. Razlika med kategorijama naročnikov je v registracijskem postopku, in sicer:
    - **Pravne osebe –** overitelj POŠTA®CA preveri identiteto pravne osebe in identiteto zakonitega zastopnika ali osebe, ki jo zakoniti zastopnik pooblasti za oddajo vloge (glej poglavje 3.2.2 Preverjanje istovetnosti organizacije).
    - **Fizične osebe** – overitelj POŠTA®CA preveri identiteto fizične osebe, ki je hkrati naročnik in imetnik digitalnega potrdila (glej poglavje 3.2.3 Preverjanje istovetnosti za fizične osebe).
    - **Fizične osebe zaposlene pri pravni osebi -** overitelj POŠTA®CA preveri identiteto pravne osebe in identiteto zakonitega zastopnika ali osebe, ki jo zakoniti zastopnik pooblasti za oddajo vloge (glej poglavje 3.2.2 Preverjanje istovetnosti organizacije). Imetniki digitalnih potrdil so fizične osebe zaposlene pri pravni osebi. Identiteto imetnikov preveri zakoniti zastopnik.
- **Tehnične lastnosti digitalnega potrdila** – overitelj POŠTA®CA izdaja napredna digitalna potrdila in standardna digitalna potrdila s sledečimi lastnostmi:
    - **Napredna potrdila** – vsebujejo dva para kriptografskih ključev in dve digitalni potrdili. Par ključev in digitalno potrdilo se uporablja za napredni elektronski podpis (zasebni ključ za podpisovanje in javni ključ vsebovan v digitalnem potrdilu za overjanje podpisa) in par ključev in digitalno potrdilo za šifriranje (zasebni ključ za dešifriranje in javni ključ vsebovan v digitalnem potrdilu za šifriranje). Par ključev za elektronski podpis se vedno kreira v kriptografskem modulu na strani uporabnika. Zasebni ključ za podpisovanje se nikoli ne dostavi overitelju in se nikoli ne hrani na strani overitelja. Par ključev za šifriranje se kreira v kriptografskem modulu na strani overitelja in se hrani v overiteljevi bazi v šifrirani obliki. Hramba

ključev na strani overitelja omogoča varno povrnitev zgodovine dešifrirnih ključev, kadar uporabnik ne more dostopati do dešifrirnega ključa zaradi izgube ključa, uničenja ključa, pozabljenega gesla, ali drugih razlogov. Napredna digitalna potrdila so primerna za napredni elektronski podpis, preverjanje istovetnosti imetnika, ter šifriranje podatkov.

- **(Standardna) potrdila** – vsebujejo en par kriptografskih ključev in eno digitalno potrdilo. Par ključev se vedno kreira v kriptografskem modulu na strani uporabnika, se nikoli ne dostavi overitelju in se nikoli ne hrani na strani overitelja. Standardna digitalna potrdila so primerna za napredni elektronski podpis in preverjanje istovetnosti imetnika. Standardna potrdila niso primerna za šifriranje podatkov, ker uporabnik v primeru, da ne more več dostopati do zasebnega ključa (zaradi izgube ključa, uničenja ključa, pozabljenega gesla, ali drugih razlogov), trajno izgubi dostop do šifriranih podatkov.

- **Kriptografski modul –** je lahko strojni kriptografski modul (npr. pametna kartica, ali strojni varnostni modul – HSM) ali programski kriptografski modul v okviru aplikacije na strani uporabnika (npr. interni "Netscape Security Services PKCS#11" modul, ali "Microsoft Enhanced Cryptographic Provider v1.0"). Strojni kriptografski moduli zagotavljajo višji nivo varnosti zasebnega ključa kot programski moduli. Za kvalificiran elektronski podpis je zahtevana uporaba kriptografskega modula, ki izpolnjuje zahteve za naprave za ustvarjanje kvalificiranega elektronskega podpisa v skladu z Uredbo eIDAS, priloga II, ali Direktive 1999/93/ES, priloga III.

1.2 Naziv dokumenta in identifikacijske oznake potrdil

Naziv pričujočega dokumenta je Politika POŠTA®CA za kvalificirana in normalizirana potrdila. Skrajšan naziv dokumenta je Politika POŠTA®CA.

Politika POŠTA®CA velja za potrdila, ki so označena z identifikacijskimi oznakami politik (angl. Policy Object Identifiers) navedenimi v spodnji tabeli. Poleg navedenih identifikacijskih oznak lahko posamezno potrdilo vsebuje dodatno identifikacijsko oznako komercialnega produkta. Identifikacijske oznake komercialnega produkta so navedene v opisu posameznega komercialnega produkta.

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 kvalificiran elektronski podpis
Namen uporabe:	kvalificiran elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	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)

2. POŠTA®CA – Kvalificirana potrdila 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 *commonName*. Obvezna je uporaba QSCD naprave.
Vrsta:	kvalificirano potrdilo za kvalificiran elektronski podpis
Namen uporabe:	kvalificiran elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	Pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.1.1.1.2.3 qcp-natural-qscd (0.4.0.194112.1.2)

3. POŠTA ® CA – Kvalificirana potrdila

Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah, z dodatnim splošnim nazivom v polju *commonName*.
Vrsta:	kvalificirano potrdilo za elektronski podpis
Namen uporabe:	napreden elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	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)

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

Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah, z dodatnim splošnim nazivom v polju *commonName*. Potrdilo je izdano na QSCD napravi.
Vrsta:	kvalificirano potrdilo za kvalificiran elektronski podpis
Namen uporabe:	kvalificiran elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	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)

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 kvalificiran elektronski podpis
Namen uporabe:	kvalificiran elektronski podpis
Rok veljavnosti:	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)

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 obvezno uporabo QSCD naprave
Vrsta:	kvalificirano potrdilo za kvalificiran elektronski podpis
Namen uporabe:	kvalificiran elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	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)

7. POŠTA ® CA – Kvalificirana potrdila s splošnim nazivom

Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah
Vrsta:	kvalificirano potrdilo za elektronski podpis
Namen uporabe:	napreden elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	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)

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

Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe zaposlene pri pravnih osebah, izdana na QSCD napravi
Vrsta:	kvalificirano potrdilo za kvalificiran elektronski podpis
Namen uporabe:	kvalificiran elektronski podpis, šifriranje in avtentikacija

Rok veljavnosti:	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)

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 kvalificiran elektronski podpis
Namen uporabe:	kvalificiran elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	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)

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 kvalificiran elektronski podpis
Namen uporabe:	kvalificiran elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	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)

11. POŠTA®CA – Kvalificirana potrdila

Opis:	kvalificirana potrdila z enim parom ključev za fizične osebe
Vrsta:	kvalificirano potrdilo za elektronski podpis
Namen uporabe:	Napreden elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	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)

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 kvalificiran elektronski podpis
Namen uporabe:	kvalificiran elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	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)

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 kvalificiran elektronski podpis
Namen uporabe:	kvalificiran elektronski podpis
Rok veljavnosti:	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)

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 kvalificiran elektronski podpis
Namen uporabe:	kvalificiran elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	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)

Normalizirana potrdila

15. POŠTA®CA – Normalizirana potrdila za spletne strežnike

Opis:	normalizirano potrdilo za spletne strežnike z enim parom ključev
Vrsta:	normalizirano digitalno potrdilo

Namen uporabe:	overjanje identitete spletnih strežnikov in VPN naprav
Rok veljavnosti:	Tri (3) leta
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.2.1.1.2

16. POŠTA®CA – Normalizirana potrdila za pravne osebe z obvezno uporabo QSCD naprave

Opis:	normalizirano potrdilo za pravne osebe z obvezno uporabo QSCD
Vrsta:	normalizirano digitalno potrdilo
Namen uporabe:	napreden elektronski žig
Rok veljavnosti:	Pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.3.1.3.2.1

17. POŠTA®CA – Normalizirana potrdila za pravne osebe

Opis:	normalizirano potrdilo za pravne osebe
Vrsta:	normalizirano digitalno potrdilo
Namen uporabe:	napreden elektronski žig
Rok veljavnosti:	Pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.3.2.3.2.1

18. POŠTA®CA – Normalizirana potrdila za pravne osebe, izdana na QSCD napravi

Opis:	normalizirano potrdilo za pravne osebe, izdano na QSCD napravi
Vrsta:	normalizirano digitalno potrdilo
Namen uporabe:	napreden elektronski žig
Rok veljavnosti:	Pet (5) let
Identifikacijska oznaka:	1.3.6.1.4.1.15284.1.3.3.3.2.1

1.3 Udeleženci infrastrukture javnih ključev

V tem poglavju so opredeljeni subjekti v overiteljevih postopkih in namen uporabe overiteljevih kvalificiranih potrdil.

1.3.1 Overitelj

POŠTA®CA, overitelj kvalificiranih potrdil, uporablja isto infrastrukturo za izdajo vseh vrst digitalnih potrdil končnim uporabnikom. Overitelj deluje kot glavna certifikatska agencija (angl. CA - Certification Authority), ki je v postopku tvorjenja šifrirnih ključev sebi podpisala potrdilo (angl. self-signed certificate).

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

Overitelja v okviru Pošte Slovenije predstavljajo naslednji identifikacijski podatki:

Naslov:	Pošta Slovenije, d.o.o. POŠTA®CA Slomškov trg 10 2500 Maribor
Telefon:	02 449 2858
Fax:	02 449 2807
Spletna stran:	http://postarca.posta.si/
E-mail	info.postarca@posta.si
Pomoč uporabnikom:	080 44 40
Enolično ime	OU=POSTArCA,O=POSTA,C=SI

Družba je vpisana pri Okrožnem sodišču v Mariboru, štev. 1/09400/00.

Ob pričetku svojega produkcijskega delovanja je overitelj ustvaril lastno potrdilo namenjeno podpisovanju potrdil drugih imetnikov, podpisovanju registra preklicanih potrdil ter preverjanju podpisa overitelja. Digitalno potrdilo overitelja POŠTA®CA vsebuje:

Naziv polja		**Vrednost v digitalnem potrdilu overitelja POŠTA®CA**
Serial Number	Serijska številka	1044616010 (0x3E43934A)
Issuer	Overitelj	OU=POSTArCA,O=POSTA,C=SI
Subject	Imetnik	OU=POSTArCA,O=POSTA,C=SI
Validity: Not Before	Veljavnost od	7. FEB. 10:36:58 2003 GMT
Validity: Not After	Veljavnost do	7. FEB. 11:06:58 2023 GMT
RSA Public Key	Dolžina RSA ključa	2048 bit

Signature Algorithm	Algoritem	sha1WithRSAEncryption
Key identifier	Identifikator ključa	**3F:BD:CD:8E:DF:BE:D1:6B:65:44:3F:60:EC:EA:42:2E:30:70:1F:68**
SHA-1 hash:	SHA-1 odtis digitalnega potrdila	**B1EA C3E5 B824 76E9 D50B 1EC6 7D2C C11E 12E0 B491**
MD5 hash:	MD5 odtis digitalnega potrdila	**2C6F 17A3 9562 0120 65D2 076E FCB8 3F6D**

1.3.2 Registracijska pisarna overitelja

Overitelj uporablja naslednje organizacijske modele registracijske pisarne:

- Registracijska pisarna (angl. RA-Registration Authority), ki deluje na sedežu overitelja (v nadaljevanju center overitelja). Poleg overjanja identitete prosilcev je edina pooblaščena za odobravanje in posredovanje vlog sistemu (informacijskemu sistemu overitelja) za izdajo digitalnih potrdil.
- Lokalna registracijska pisarna (angl. LRA-Local Registration Authority), ki deluje v okviru overitelja na oddaljenih lokacijah Pošte Slovenije. Pooblaščena je za overjanje identitete prosilcev in posredovanje vlog v center overitelja.
- Lokalni overitelj identitete, ki deluje na oddaljenih lokacijah in ima z overiteljem POŠTA®CA sklenjeno pogodbo o opravljanju storitve overjanja identitete. Pooblaščen je za overjanje identitete prosilcev in posredovanje vlog v center overitelja.

1.3.3 Naročniki in imetniki digitalnih potrdil

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

Imetnik kvalificirnaega 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 pooblaščena 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, ki zahteva izdajo standardnega normalizirano digitalnega potrdila za spletne strežnike, 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).

Prosilec je fizična oseba, ki zahteva izdajo potrdila v svojem imenu (samostojna fizična oseba) ali v imenu organizacije (zakoniti zastopnik pravne osebe ali z njene strani pooblaščena oseba). O prosilcu govorimo le v obdobju med oddajo vloge za izdajo digitalnega potrdila in prevzemom digitalnega potrdila.

S podpisom vloge se prosilec zavezuje k doslednemu spoštovanju in upoštevanju javnega dela notranjih pravil overitelja. Digitalno potrdilo izda overitelj prosilcu, ki s tem postane imetnik digitalnega potrdila (v nadaljevanju imetnik potrdila). Imetnik potrdila se zavezuje digitalno podpisovati le dokumente, katerih zahteva po veljavnosti ni daljša od roka veljavnosti potrdila. V primeru, da je zahteva po veljavnosti dokumentov daljša od roka veljavnosti potrdila, je imetnik potrdila zavezan pred potekom veljavnosti digitalnega potrdila zagotoviti, da bodo takšni dokumenti znova ustrezno podpisani z uporabo novega veljavnega podpisa (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).

Overitelj POŠTA®CA v skladu z veljavno zakonodajo izdaja kvalificirana potrdila le prosilcem. Prosilec in imetnik potrdila je vedno ena in ista fizična oseba, ki osebno uporablja kvalificirano potrdilo.

Prosilec je dolžan:

- dati overitelju točne in popolne identifikacijske podatke in ostale informacije, vsebovane v potrdilu;
- pred podpisom vloge skrbno prebrati overiteljevo politiko oz. javni del notranjih pravil overitelja in spremljati vsa obvestila overitelja ter ravnati v skladu z njimi;
- vestno izpolnjevati vse v politiki navedene obveznosti.

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

Ni relevantno.

1.4 Namen uporabe potrdil

1.4.1 Dovoljena uporaba potrdil

Potrdila, ki jih izdaja 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[1];
- podpisovanje dokumentov v elektronski obliki;
- izkazovanje istovetnosti imetnika;
- storitve, kjer se zahteva uporaba kvalificiranega digitalnega potrdila overitelja POŠTA ®CA;

[1] Opozorilo: Standardna digitalna potrdila niso primerna za šifriranje podatkov, ker uporabnik v primeru, da ne more več dostopati do zasebnega ključa (zaradi izgube ključa, uničenja ključa, pozabljenega gesla, ali drugih razlogov) trajno izgubi dostop do šifriranih podatkov.

1.4.2 Nedovoljena uporaba digitalnih potrdil

Skladno z 1.4.1.

1.5 Upravljanje s pravili delovanja

1.5.1 Organ, ki upravlja s pričujočim dokumentom

Pričujoči dokument (Politika POŠTA®CA) in overitelja POŠTA®CA kot celoto, upravlja POŠTA SLOVENIJE d.o.o., Maribor.

1.5.2 Kontaktni podatki

1.5.2.1 Kontaktne osebe - organizacija overitelja

Kontaktna oseba, odgovorna za organizacijo overitelja, je dosegljiva na naslednjem naslovu:

Naslov:	POŠTA SLOVENIJE, d.o.o. POŠTA®CA - *Operativni vodja* Slomškov trg 10 2500 Maribor
Telefon:	02 449 2858
Fax:	02 449 2807
E-mail	operativa.postarca@posta.si

1.5.2.2 Kontaktne osebe – dokumentacija overitelja

Kontaktna oseba, odgovorna za dokumentacijo overitelja, je dosegljiva na naslednjem naslovu:

Naslov:	POŠTA SLOVENIJE, d.o.o. POŠTA®CA - *Projektni vodja* Slomškov trg 10 2500 Maribor
Telefon:	02 449 2858
Fax:	02 449 2807
E-mail	dokumentacija.postarca@posta.si

1.5.3 Odgovorni organ za odobritev pravil delovanja overitelja (Politiko POŠTA®CA)

Pravila delovanja overitelja potrjuje upravni svet overitelja.

1.5.4 Postopek odobritve pravil delovanja overitelja

Postopek odobritve in preverjanje skladnosti delovanja overitelja s Politiko POŠTA®CA izvaja upravni svet overitelja. V okviru postopka odobritve se izvede:

- preverjanje skladnosti dokumenta Politika POŠTA®CA z zahtevami ZEPEP;

- preverjanje infrastrukture ter vzpostavljene postopke glede na določila Politike POŠTA®CA in priporočila dobre prakse

1.6 Pojmi in kratice

1.6.1 Osnovne definicije

Izraz	Definicija
Elektronski podpis	Je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika.
Napreden elektronski podpis	Je elektronski podpis, ki izpolnjuje naslednje zahteve: • enolično je povezan s podpisnikom;; • z njim je mogoče identificirati podpisnika; • ustvari se na podlagi podatkov za ustvarjanje elektronskega podpisa, ki jih podpisnik z visoko stopnjo zaupanja lahko uporablja izključno pod svojim nadzorom; • s podatki, ki so na ta način podpisani, je povezan tako, da je opazna vsaka naknadna sprememba podatkov.
Informacijski sistem	Je sistem za oblikovanje, pošiljanje, prejemanje, shranjevanje in druge obdelave podatkov v elektronski obliki.
Potrdilo (ali digitalno potrdilo)	Je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto.
Kvalificirano potrdilo	„kvalificirano potrdilo“ pomeni potrdilo, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Uredbe eIDAS;.
Normalizirano potrdilo	Normalizirana digitalna potrdila, zagotavljajo enak nivo varnosti, oziroma zaupanja, kot kvalificirana in so namenjena uporabi za vse ostale namene.
Oprema za elektronsko podpisovanje	Je strojna ali programska oprema ali njuna specifična sestavina, ki jo overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem oz. se uporablja za oblikovanje ali preverjanje elektronskih podpisov.
Overitelj	Je fizična ali pravna oseba, ki izdaja digitalna potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskim podpisovanjem.
Podatki za elektronsko podpisovanje	So edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa.
Podatki za preverjanje elektronskega podpisa	So edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa.
Podpisnik	Je oseba, ki ustvari elektronski podpis.
Naprava za	Pomeni konfigurirano programsko ali strojno opremo, ki se

ustvarjanje elektronskega podpisa	uporablja za ustvarjanje elektronskega podpisa
Naprava za ustvarjanje kvalificiranega elektronskega podpisa	Pomeni napravo za ustvarjanje elektronskega podpisa, ki izpolnjuje zahteve Uredbe eIDAS, priloga II.
Naprava za ustvarjanje elektronskega žiga	Pomeni konfigurirano programsko ali strojno opremo, ki se uporablja za ustvarjanje elektronskega žiga;
QSCD naprava	Glej opis QSCD v poglavju 1.6.2.
Oddaljena QSCD naprava	Glej opis QSCD v poglavju 1.6.2.
Sredstvo za preverjanje elektronskega podpisa	Je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa.
Imetnik potrdila (angl. Subject)	Je lahko: • fizična oseba, navedena v digitalnem potrdilu v polju »subject« kot lastnik zasebnega ključa, ki ustreza javnemu ključu, navedenem v digitalnem potrdilu; ali • fizična oseba zaposlena pri pravni osebi, navedena v digitalnem potrdilu v polju »subject« kot lastnik zasebnega ključa, ki ustreza javnemu ključu, navedenem v digitalnem potrdilu, ali fizična oseba pooblaščena za uporabo digitalnega potrdila za splošne nazive, ali fizična oseba pooblaščena za uporabo digitalnega potrdila za informacijske sisteme.
Naročnik potrdila (ang. Subscriber)	Pravna ali fizična oseba, registrirana za opravljanje dejavnosti, ki zahteva izdajo digitalnega potrdila v imenu enega ali več imetnikov. Naročnik je hkrati imetnik, kadar podpiše vlogo za izdajo digitalnega potrdila v svojem imenu.
Prosilec	Fizična oseba, ki zahteva izdajo digitalnega potrdila v svojem imenu. O prosilcu govorimo le v obdobju, med oddajo vloge za izdajo digitalnega potrdila in prevzemom digitalnega potrdila.
Uradni identifikacijski dokument	Dokument, s katerim prosilec dokazuje svojo istovetnost: osebna izkaznica, potni list ali vozniško dovoljenje.

1.6.2 Okrajšave

Kratica	Pomen
ARL	angl. Authority Revocation List – register preklicanih potrdil, ki jih uporabljajo drugi overitelji
CA	angl. Certification Authority – overitelj

CN	angl. Common Name – X.500 domače ime imetnika digitalnega potrdila
CRL	angl. Certificate Revocation List – register preklicanih digitalnih potrdil
CSP	angl. Certification Service Provider – ponudnik storitve overjanja in upravljanja digitalnih potrdil
CPS	angl. Certificate Practice Statement – javni del notranjih pravil overitelja, politika
PDS	angl. Policy Disclosure Statement – Izjava o politiki delovanja, pravila delovanja
DN	angl. Distinguished Name – X.500 razločevalno ime
EAL	angl. Evaluation Assurance Level – standard označevanja varnostnih nivojev v računalniških sistemih
FIPS	angl. United State Federal Information Processing Standards – oznaka standarda s področja informacijskega procesiranja
HSM	Strojni varnostni modul (angl. Hardware Security module)
LRA	angl. Local Registration Authority – lokalna registracijska pisarna, ki izvaja funkcijo registrske pisarne overitelja
PKCS	angl. Public Key Cryptographic Standars – šifrirni standardi na področju javnih ključev
PKIX-CMP	angl. Public Key Infrastructure (based on) X.509 Certificate Management Protocols – protokol za izmenjavo ključev in upravljanje certifikatov
RA	angl. Registration Auhority – registracijska pisarna overitelja
QSCD	angl. Qualified Signature Creation Device – naprava za ustvarjanje kvalificiranega ali naprednega elektronskega podpisa in kvalificiranega ali naprednega elektronskega žiga skladna z zahtevami Uredbe eIDAS, priloga II. V dokumentu se uporablja izraz "QSCD naprava" v primeru kadar se naprava nahaja pri uporabniku in izraz "oddaljena QCSD naprava" kadar se naprava nahaja pri ponudniku storitve oddaljenega elektronskega podpisa.
SCEP	angl. Simple Certificate Enrollment Protocol – protokol, ki avtomatizira prevzem digitalnih potrdil. Uporablja se predvsem v CISCO-usmerjevalnikih.
SPKAC	Oblika zahtevka z izdajo potrdila, ki jo uporabljajo Mozilla kompatibilni brskalniki. Oblika je ekvivalent PKCS#10.
SSCD	angl. Secure Signature Creation Device – naprava za varno oblikovanje podpisa (npr. pametna kartica ali naprava za oddaljen elektronski podpis) skladna z zahtevami Direktive 1999/93/ES, priloga III.
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 57/2000 in 30/2001)
ZZZS	Zavod za zdravstveno zavarovanje Slovenije, ali kratko Zavod
ZVOP	Zakon o varstvu osebnih podatkov
KZZ	Kartica zdravstvenega zavarovanja
KDP	Kvalificirano digitalno potrdilo
NDP	Normalizirano digitalno potrdilo
PK	Profesionalna kartica zdravstvenega zavarovanja
PK-KDP	Kvalificirano digitalno potrdilo izdano na PK
OID	angl. Object Identifier - identifikacijska oznaka
2FA	Način avtentikacije pri katerem se uporabljata dva različna faktorja. Npr. "nekaj kar vem" in "nekaj kar imam".

1.6.3 Pomen izrazov

Posamezni izrazi imajo v nadaljevanju tega dokumenta naslednji pomen:

- **Overitelj** POŠTA®CA je Certifikatska agencija Pošte Slovenije, krajše POŠTA®CA, ki deluje v skladu z vsakokrat veljavnim Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 57/2000 in 30/2001), Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001) ter vsakokrat veljavnimi evropskimi direktivami in je registrirana za opravljanje dejavnosti. POŠTA®CA izdaja kvalificirana potrdila za fizične osebe.
- **Organizacija** je pravna ali fizična oseba, ki je registrirana za opravljanje dejavnosti.
- **Zakoniti zastopnik organizacije** je fizična oseba, ki je pooblaščena za zastopanje organizacije v pravnem prometu. Zakoniti zastopnik jamči, da so vloge pravilno izpolnjene ter da so identifikacijski podatki imetnikov potrdil resnični.
- **Pooblaščena oseba za oddajo vloge** je fizična oseba, ki jo zakoniti zastopnik organizacije pooblasti za oddajo vloge.
- **Vloge** so obrazci overitelja za upravljanje z digitalnimi potrdili (npr. pridobitev digitalnega potrdila, preklic digitalnega potrdila, …). Dostopni so prek spletnih strani overitelja http://postarca.posta.si in pri pooblaščenih osebah na prijavnih službah.
- **Registracijska pisarna overitelja** po pooblastilu overitelja sprejema vloge in preverja istovetnosti prosilcev in imetnikov potrdil.
- **Objava overitelja** je javna objava na spletnih straneh overitelja http://postarca.posta.si.
- **Obvestila overitelja** so vsa navodila, pojasnila, seznami, pogoji, posamezna obvestila, priporočila, standardi in drugi dokumenti, ki jih določi ali priporoči overitelj in jih objavi ali kako drugače posreduje imetnikom digitalnih potrdil ali tretjim osebam.
- **Digitalna identiteta, digitalni ID** (angl. Digital Identity, Digital ID) je par ključev – zasebni in javni – ter digitalno potrdilo javnega ključa, ki ga izda overitelj.
- **Kvalificirano potrdilo** vsebuje eno digitalno potrdilo X.509, izdano za digitalni ID z enim parom ključev.
- **Napredno kvalificirano potrdilo** vsebuje dve digitalni potrdili X.509, izdani za digitalni ID z dvema paroma ključev:
    - par ključev za elektronski podpis (zasebni ključ za podpisovanje in javni ključ za overjanje podpisa),
    - par ključev za šifriranje (zasebni ključ za dešifriranje in javni ključ za šifriranje).
- **Uporabnik** je naročnik ali imetnik kvalificiranega potrdila.
- **Digitalno potrdilo (ali krajše potrdilo)** je normalizirano potrdilo ali kvalificirano potrdilo.
- **Osebno geslo** (PIN, angl. Personal Identification Number) je skrivno geslo uporabnika za avtentikacijo ob uporabi pametne kartice.
- **Koda za odklepanje pametne kartice** (PUK, Personal Unblocking Key) je skrivno geslo za odklepanje pametne kartice, če se zaklene zaradi večkratnega zaporednega vnosa napačnega osebnega gesla.

- **Aktivacijski podatki** so podatki potrebni za prevzem digitalnega potrdila (referenčna številka in avtorizacijska koda), ali aktiviranje zasebnih ključev (osebno geslo za zaščito zasebnega ključa, osebni geslo pametne kartice, ali koda za odklepanje pametne kartice).
- **Pametna kartica** je sredstvo za elektronsko podpisovanje v obliki plastične kartice z vgrajenim čipom, ki vsebuje procesor in spomin. Uporablja se za varno tvorjenje in hranjenje kriptografskih ključev ter varno izvajanje kriptografskih operacij z zasebnim ključem.
- **Izvajalec personalizacije KZZ** je organizacija, ki izvaja grafično in električno personalizacijo pametnih kartic.
- **Kartica zdravstvenega zavarovanja (KZZ)** je pametna kartica, ki jo izda Zavod za zdravstveno zavarovanje Slovenije osebam, ki imajo urejeno obvezno zdravstveno zavarovanje.
- **Profesionalna kartica zdravstvenega zavarovanja (PK)** je pametna kartica, ki jo izda Zavod za zdravstveno zavarovanje Slovenije zdravstvenim delavcem.
- **Strojni varnostni modul** je sredstvo za elektronsko podpisovanje v okviru sistema za oddaljeni podpis ali sistema overitelja za izdajo potrdil**.**
- **Zavod** - Zavod za zdravstveno zavarovanje Slovenije.

2 ODGOVORNOST ZA OBJAVE IN REPOZITORIJ

2.1 Repozitorij

Overitelj objavlja informacije o digitalnih potrdilih in svojih storitvah v javnem imeniku LDAP in na javnih spletnih straneh.

Imenik LDAP je dosegljiv na naslovu: ldap://postarca.posta.si

Javne spletne strani so dosegljive na spletnem naslovu: http://postarca.posta.si

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;
- veljaven register preklicanih potrdil.

Na javnih spletnih straneh overitelja POŠTA®CA so objavljene naslednje informacije:

- POŠTA®CA - Izjava o politiki delovanja (PDS);
- Politika overitelja POŠTA®CA;
- ceniki;
- vloge za pridobitev, preklic in obnovo potrdil;
- namenska programska oprema za prevzem digitalnih potrdil na zunanje kriptografske naprave z navodili za uporabo;

- ostale informacije, vezane na delovanje overitelja.

2.3 Čas in pogostost objav

Overitelj objavi digitalna potrdila v imeniku LDAP takoj po izdaji.

Overitelj uvrsti preklicano digitalno potrdilo v register preklicanih potrdil takoj po opravljenem preklicu. Objava registra preklicanih potrdil se izvaja, kot je navedeno v poglavju 4.9.7.

Ostale informacije so objavljene sproti ob njihovi spremembi, ali ko postanejo dostopne overitelju.

2.4 Dostop do podatkov v repozitoriju

Vse informacije v repozitorijih so dostopne za branje brez omejitev. Repozitoriji imajo vzpostavljene ustrezne tehnične kontrole za zaščito pred nepooblaščenimi spremembami.

3 PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI

3.1 Določanje imen

3.1.1 Vrste imen

Razločevalna imena (angl. DN – Distinguished Name) POŠTA®CA v poljih »issuer« in »subject« digitalnega potrdila X.509 so oblikovana v skladu s standardom X.501. V nadaljevanju poglavja so podana polja razločevalnega imena, ki enolično določajo identiteto imetnika posamezne vrste digitalnega potrdila. Razločevalno ime lahko vsebuje dodatna polja, ki pa ne zamenjujejo spodaj navedenih polj in niso potrebna za opredelitev enolične identitete imetnika potrdila.

POŠTA®CA »subject« atribut oziroma »issuer« atribut v digitalnih potrdilih je:

Država (C) =	SI
Organizacija (O) =	POSTA
Organizacijska enota (OU) =	POSTArCA

V kvalificiranih potrdilih za fizične osebe zaposlene pri pravnih osebah vsebuje razločevalno ime v imeniku in polju »subject«, vsebovanem v digitalnem potrdilu, naslednje podatke:

Država (C) =	SI
Organizacija (O) =	registrirano ime pravne osebe
organizationIdentifier =	davčna številka pravne osebe zapisana v obliki: VATSI-"davčna številka" . Npr: VATSI-27290328
Organizacijska enota (OU) =	naziv organizacijske enote pri pravni osebi (neobvezen podatek)
Splošno ime (CN) =	ime in priimek fizične osebe ali splošni naziv osebe v povezavi s pravno osebo

Serijska številka (serialNumber) =	serijska številka
Ime (givenName) =	ime fizične osebe
Priimek (sn)=	priimek fizične osebe

V kvalificiranih potrdilih za fizične osebe vsebuje razločevalno ime v imeniku in polju »subject« v digitalnem potrdilu naslednje podatke:

Država (C) =	SI
Organizacijska enota (OU) =	POSTArCA
Organizacijska enota (OU) =	personal
Splošno ime (CN) =	ime in priimek imetnika potrdila
Ime (givenName) =	ime fizične osebe
Priimek (sn)=	priimek fizične osebe
Serijska številka (serialNumber) =	serijska številka

V normaliziranih potrdilih za pravne osebe vsebuje razločevalno ime v imeniku in polju »subject« v potrdilu naslednje podatke:

Država (C) =	SI
Organizacija (O) =	registrirano ime pravne osebe
organizationIdentifier =	davčna številka pravne osebe zapisana v obliki: VATSI-"davčna številka" . Npr: VATSI-27290328
Splošno ime (CN) =	splošni naziv, ki predstavlja pravno osebo ali storitev pravne osebe
Serijska številka (serialNumber) =	serijska številka

V normaliziranih potrdilih za spletne strežnike vsebuje razločevalno ime v imeniku in polju »subject« v digitalnem potrdilu naslednje podatke:

Država (C) =	SI
Organizacija (O) =	registrirano ime pravne osebe
organizationIdentifier =	davčna številka pravne osebe zapisana v obliki: VATSI-"davčna številka" . Npr: VATSI-27290328
Ime (CN) =	polno domensko ime (angl. Fully Qualified Domain Name, FQDN) strežnika
Serijska številka (serialNumber) =	serijska številka

Kombiniran register preklicanih digitalnih potrdil se objavlja v »certificateRevocationList« atributu POSTArCA objekta v imeniku:

Država (C) =	SI
Organizacija (O) =	POSTA
Organizacijska enota (OU) =	POSTArCA:CertificateRevocationList

Delni registri preklicanih potrdil so poimenovani v imeniku po naslednjem pravilu:

Država (C) =	SI
Organizacija (O) =	POSTA
Organizacijska enota (OU) =	POSTArCA
Ime (CN) =	CRLn (n = zaporedna številka registra)

3.1.2 Potreba po smiselnosti imen

X.500 relativno ime (RDN) imetnika potrdila sestavljata X.500 splošno ime (CN), ki vsebuje ime in priimek imetnika v skladu ~~z~~s pravili za interpretacijo kot je navedeno v poglavju 0, ter X.500 serijska številka (SerialNumber). Ime in priimek fizične osebe zapisana v poljih "givenName" in "sn", sta zapisana v obliki UTF8String. Overitelj določi serijsko številko v skladu s svojimi notranjimi pravili. Serijska številka je določena tako, da neposredno ne vsebuje osebnih podatkov.

3.1.3 Anonimnost imetnikov in uporaba psevdonimov

Se ne uporablja.

3.1.4 Pravila za interpretacijo različnih oblik imen

Imena polju splošno ime (CN) se interpretirajo v skladu z definicijami v točkah 3.1.1. in 3.1.2.

Imena so sestavljena iz črk angleške abecede. Drugi znaki se ustrezno pretvorijo po pravilih iz naslednje tabele:

Č = C	Ü = UE	Í = I	Ì = I	Ő = O
Š = S	Ć = C	Ó = O	Ò = O	Ű = U
Ž = Z	Đ = D	Ú = U	Ù = U	Ø = Oe
Ä = AE	Á = A	À = A	Ê = E	ß = Ss
Ö = OE	É = E	È = E	Ô = O	Ñ = N
Ŕ = Rz				

V primeru novih nepredvidenih znakov si overitelj pridržuje pravico poiskati ustrezno kombinacijo črk iz angleške abecede.

3.1.5 Edinstvenost imen

Overitelj dodeli vsakemu imetniku potrdila edinstveno razločevalno ime, ki je objavljeno v polju »subject« digitalnega potrdila. Glej tudi poglavje 3.1.2.

3.1.6 Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk

Overitelj dosledno upošteva pravila poimenovanja iz točk 3.1.1. in 3.1.2. Prosilcem je prepovedano zahtevati imena, ki bi kršila avtorske pravice ali pravice industrijske lastnine tretjih oseb, čeprav

overitelj tega ne bo preverjal, niti ne bo posredoval v takšnih sporih. Overitelj si pridržuje pravico zavrniti izdajo digitalnega potrdila ali preklicati izdana digitalna potrdila udeležencev spora.

3.2 Prva registracija

3.2.1 Metode dokazovanja lastništva zasebnega ključa

Dokaz o posesti zasebnega ključa je zagotovljen na sledeče načine:

- za napredna potrdila - z uporabo protokola PKIX-CMP;
- za standardna potrdila - zahtevek za izdajo digitalnega potrdila v obliki PKCS#10 v skladu z RSA PKCS#10 Certification Request Syntax Standard;
- digitalna potrdila izdana na QSCD napravi - kriptografski pari ključev in digitalno potrdilo se generirajo v okviru postopka personalizacije kartic, zato dokazovanje lastništva zasebnega ključa s strani imetnika ni potrebno. V okviru postopka generiranja ključa in izdaje potrdila se za kontrolo povezave med zasebnim in javnim ključem vsebovanim v zahtevku za izdajo digitalnega potrdila uporablja PKCS#10 oblika zahtevka v skladu z RSA PKCS#10 Certification Request Syntax Standard.

3.2.2 Preverjanje istovetnosti organizacije

Pravna oseba se identificira z uradno potrjeno dokumentacijo ali s podatki iz uradnih evidenc:

- s sklepom vpisa organizacije v Sodni register;
- izpisom iz Poslovnega registra Slovenije (Ajpes).

Zastopa jo zakoniti zastopnik ali pooblaščena oseba za oddajo vloge.

Istovetnost zakonitega zastopnika ali pooblaščene osebe za oddajo vloge se preverja v registracijski pisarni ob fizični prisotnosti osebe na osnovi uradnega identifikacijskega dokumenta.

3.2.3 Preverjanje istovetnosti za fizične osebe

Istovetnost fizične osebe se v skladu z veljavno zakonodajo preverja bodisi v registracijski pisarni ob fizični prisotnosti osebe na osnovi uradnega identifikacijskega dokumenta, bodisi se ugotavlja na podlagi veljavnega kvalificiranega potrdila, ki ga je izdal eden od registriranih overiteljev v Republiki Sloveniji in vsebuje vse podatke, potrebne za enolično identifikacijo imetnika potrdila.

Zakoniti zastopnik pravne osebe s svojim podpisom jamči za istovetnost bodočih imetnikov kvalificiranih potrdil za fizične osebe zaposlene pri pravni osebi. Preverjanje istovetnosti organizacije se izvaja kot je opisano v poglavju 3.2.2.

3.2.4 Podatki o imetnikih potrdil, ki se ne preverjajo

Overitelj ne preverja verodostojnosti naslova elektronske pošte.

3.2.5 Preverjanje pooblastil

Preverjanje pooblastil se izvaja v primeru da vlogo za digitalna potrdila za pravne osebe ne odda zakoniti zastopnik organizacije. Pooblastilo je vsebovano na obrazcu vloge in se preverja v okviru registracijskega postopka.

3.2.6 Merila za medsebojno povezovanje

Overitelj se lahko povezuje z drugimi overitelji na horizontalni ravni na podlagi pogodbe o medsebojnem priznavanju ali na podlagi pogodbenega razmerja s podrejenim overiteljem.

Overitelj se povezuje z drugimi overitelji po lastni presoji in le v primerih, ko drugi overitelj izdaja primerljiva digitalna potrdila in zagotavlja vsaj enak nivo zaupanja.

Overitelj lahko overja in objavlja javni del notranjih pravil overitelja podrejenih overiteljev v primeru, da se nameni uporabe kvalificiranih digitalnih potrdil razlikujejo od namena uporabe, definirane v tem dokumentu.

3.3 Preverjanje istovetnosti pri obnovi potrdila

3.3.1 Preverjanje istovetnosti pri rutinski obnovi potrdil

Rutinska obnova digitalnega potrdila je izdaja novega potrdila pred potekom veljavnosti obstoječega digitalnega potrdila.

Preverjanje istovetnosti pri rutinski obnovi digitalnih potrdil se izvaja glede na tehnično lastnost digitalnega potrdila na sledeče načine:

- napredna potrdila – identifikacija se izvede na nivoju PKIX-CMP protokola z veljavnim obstoječim digitalnim potrdilom. Po preteku veljavnosti digitalnega potrdila obnova z uporabo protokola PKIX-CMP ni več možna in se mora imetnik identificirati kot je določeno v poglavju 3.2.
- standardna potrdila – identifikacija imetnika se izvede kot je določeno v poglavju 3.2.

3.3.2 Preverjanje istovetnosti pri obnovi potrdila po preklicu

Po preklicu digitalnih potrdil se izvaja preverjanje istovetnosti kot ob prvi registraciji (glej poglavje 3.2).

3.4 Preverjanje istovetnosti ob zahtevi za preklic potrdila

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

4 UPRAVLJANJE S POTRDILI

4.1 Vloga za izdajo potrdila

Za izdajo digitalnega potrdila mora prosilec:

- izpolniti predpisano vlogo za izdajo digitalnega potrdila in jo osebno oddati v registracijski pisarni overitelja,

  ali

  izpolniti elektronsko vlogo za izdajo digitalnega potrdila na spletni strani http://postarca.posta.si in opraviti osebno identifikacijo v registracijski pisarni, razen če je svojo istovetnost ob oddaji elektronske vloge izkazal s kvalificiranim potrdilom, ki izpolnjuje zahteve, navedene v poglavju 3.2.3;

- izpolniti identifikacijske zahteve navedene v poglavju 3.2;
- izpolniti morebitne finančne obveznosti navedene v poglavju 9.1.

4.1.1 Kdo lahko zaprosi za izdajo potrdila

Za izdajo kvalificiranega potrdila za fizične osebe lahko zaprosijo osebe, ki izpolnjujejo zahteve poglavja 3.2.3 Preverjanje istovetnosti za fizične osebe.

Za izdajo kvalificiranega potrdila za fizične osebe zaposlene pri pravni osebi lahko zaprosi katera koli organizacija, ki izpolnjuje zahteve poglavja 3.2.2 Preverjanje istovetnosti organizacije in 3.2.3 Preverjanje istovetnosti za fizične osebe.

Za izdajo normaliziranega potrdila lahko zaprosi katera koli organizacija, ki izpolnjuje zahteve poglavja 3.2.2 Preverjanje istovetnosti organizacije.

Za pridobitev kvalificiranega potrdila izdanega na profesionalni kartici zdravstvenega zavarovanja lahko zaprosijo fizične osebe, ki so upravičene do PK na podlagi Pravilnika o KZZ.

4.1.2 Postopek obdelave vloge in odgovornosti

4.1.2.1 Postopek obdelave vloge in odgovornosti za potrdila, ki jih imetniki prevzamejo osebno

Izpolnjene vloge se preverijo in odobrijo v registracijskih pisarnah overitelja ter na varen način posredujejo v center overitelja, kjer se izvede rezervacija razločevalnega imena in tvorjenje inicializacijskih podatkov - referenčne številke in avtorizacijske kode. Uporabnik lahko prevzame digitalno potrdilo na podlagi referenčne številke in avtorizacijske kode.

Overitelj pošlje uporabniku obvestilo o odobritvi izdaje digitalnega potrdila, referenčno številko, avtorizacijsko kodo in spletni naslov, na katerem so navodila za prevzem digitalnega potrdila, na način, ki ga je uporabnik izbral na vlogi za izdajo digitalnega potrdila. Glej tudi poglavje 6.4.2.

Referenčno številko in avtorizacijsko kodo mora uporabnik do prevzema digitalnega potrdila ustrezno varovati [glej poglavje 9.6.3].

4.1.2.2 Postopek obdelave vloge in odgovornosti za potrdila izdana na QSCD napravi

Izpolnjene vloge se preverijo in odobrijo v registracijskih pisarnah overitelja ter na varen način posredujejo v center overitelja, kjer se izvede rezervacija razločevalnega imena.

V primeru, ko se uporablja QSCD naprava se izvede tvorjenje ključev na pametni kartici, tvorjenje osebnega gesla imetnika za dostop do zasebnih ključev na pametni kartici (PIN koda pametne kartice), tvorjenje kode za odklepanje pametne kartice (PUK kode) ter izdaja potrdila in vpis potrdila na pametno kartico. Overitelj pošlje pametno kartico in osebno geslo uporabniku najkasneje v desetih (10) dneh od prejema zahtevka za izdajo potrdila. Pametna kartica in osebno geslo sta poslana uporabniku z ločenima priporočenima pošiljkama. Koda za odklepanje pametne kartice (PUK koda) je poslana uporabniku skupaj z osebnim geslom.

V primeru, ko se uporablja oddaljena QSCD naprava se izvede tvorjenje osebnega aktivacijskega gesla imetnika za prvi dostop do sistema za oddaljen elektronski podpis. Overitelj pošlje osebno aktivacijski geslo uporabniku najkasneje v desetih (10) dneh od prejema zahtevka za izdajo potrdila.

Overitelj si pridržuje pravico zavrniti vloge za izdajo potrdila brez obrazložitve. O morebitni zavrnitvi vloge za izdajo potrdila po uspešni oddaji vloge [točka 4.1] bo prosilec obveščen po elektronski pošti ali pisno po pošti.

4.2 Obdelava vloge za izdajo potrdila

4.2.1 Postopki identifikacije in avtentikacije

Osebje registracijske pisarne overitelja izvede identifikacijo organizacije v skladu s poglavjem 3.2.2 Preverjanje istovetnosti organizacije, ter fizičnih oseb v skladu s poglavjem 3.2.3 Preverjanje istovetnosti za fizične osebe.

4.2.2 Odobritev ali zavrnitev izdaje potrdila

Overitelj si pridržuje pravico zavrniti vloge za izdajo digitalnega potrdila brez obrazložitve. Ob morebitni zavrnitvi vloge za izdajo digitalnega potrdila po uspešni oddaji vloge [poglavje 4.1], v primeru nepravilnih ali pomanjkljivih podatkov, ali v primeru neizpolnjevanja obveznosti, bo uporabnik obveščen po elektronski pošti ali pisno po pošti.

4.2.3 Čas za obdelavo vloge za izdajo potrdila

Overitelj posreduje inicializacijske podatke uporabniku najkasneje v desetih (10) dneh od odobritve zahtevka. Veljavnost inicializacijskih podatkov je šestdeset (60) dni. Po tem roku inicializacijski podatki niso več uporabni.

4.3 Izdaja potrdila

4.3.1 Postopki overitelja ob izdaji potrdila

Aplikacija overitelja izda potrdila na osnovi prejetega zahteva, ki ga tvori imetnik ali aplikacija sistema za personalizacijo pametnih kartic ali sistema za oddaljeni elektronski podpis. Vsak prejeti zahtevek se na strani aplikacije overitelja obdela na sledeči način:

- preveri veljavnost inicializacijskih podatkov (referenčne številke in avtorizacijske kode), vsebovanih v zahtevku za izdajo potrdila;
- preveri, v skladu s poglavjem 3.2.1 Metode dokazovanja lastništva zasebnega ključa, da ima subjekt, ki je tvoril zahtevek dostop do zasebnega ključa povezanega z javnim ključem, vsebovanim v zahtevku;
- preveri veljavnost zahtevka, ter skladnost s tehnično specifikacijo oblike zahtevka (PKIX-CMP ali PKCS#10);
- izda digitalno potrdilo, če so izpolnjeni vsi zgoraj navedeni pogoji, ter ga kot odgovor na zahtevek posreduje imetniku oziroma sistemu, ji je poslal zahtevek (sistem za personalizacijo pametnih kartic ali sistem za oddaljeni elektronski podpis)
- objavi digitalno potrdilo v javnem imeniku LDAP;

4.3.2 Obvestilo imetniku o izdaji potrdila

Imetniki, ki prevzamejo digitalno potrdilo osebno ali preko sistema za oddaljen elektronski podpis, so obveščeni o uspešni ali neuspešni izdaji digitalnega potrdila v okviru aplikacije, s katero

prevzemajo digitalno potrdilo. Za potrdila, izdana na pametni kartici, je izdaja in vročitev pametne kartice hkrati tudi potrdilo o izdaji digitalnega potrdila.

4.4 Prevzem potrdila

4.4.1 Postopek prevzema potrdila

Postopek prevzema je odvisen od vrste digitalnega potrdila:

- Napredna kvalificirana potrdila se prevzemajo po protokolu PKIX-CMP z ustrezno aplikacijo, v skladu z navodili za prevzem naprednega kvalificiranega potrdila, ki se nahajajo na spletni strani: http://postarca.posta.si.
- Kvalificirana potrdila se prevzamejo z uporabo spletnega brskalnika (seznam podprtih brskalnikov je objavljenih na spletni strani overitelja), v skladu z navodili za prevzem standardnega kvalificiranega potrdila, ki se nahajajo na spletni strani: http://postarca.posta.si.
- Kvalificirana potrdila izdana na QSCD napravi se ob prvem prevzemu vpišejo na pametno kartico pri overitelju. Ob ponovnem prevzemu na isto kartico se uporabi namenska programska oprema, v skladu z navodili z uporabo [točka 2.2].
- Kvalificirana potrdila izdana na oddaljeni QSCD napravi se ob prevzemu potrdila shranijo na sistemu za oddaljen elektronski podpis. Navodila so objavljena na spletni strani overitelja [točka 2.2].
- Kvalificirana potrdila z obvezno uporabo QSCD naprave se prevzamejo z uporabo namenske programske opreme, v skladu z navodili za uporabo. Programska oprema in navodila so objavljeni na spletni strani overitelja [točka 2.2]. Prevzem z uporabo spletnega brskalnika je za ta tip digitalnega potrdila onemogočen.
- Kvalificiranega potrdila izdanega na profesionalni kartici zdravstvenega zavarovanja prevzame izvajalec personalizacije KZZ. Izvajalec personalizacije KZZ:
    - generira par asimetričnih ključev [točka 6.1.1];
    - generira zahtevek za izdajo digitalnega potrdila v obliki PKCS#10;
    - posreduje PKCS#10 zahtevek skupaj z aktivacijskimi kodami overiteljevemu sistemu za overjanje in upravljanje digitalnih potrdil, ki zahtevek preveri, ter overi in izda digitalno potrdilo.

Prosilec prejme spletni naslov, na katerem se nahajajo navodila za prevzem digitalnega potrdila skupaj s prevzemnimi podatki. Navodila so v elektronski obliki. Zadnja verzija navodil se vedno nahaja na spletni strani overitelja. Navodila so podvržena spremembam, novostim in izboljšavam na PKI-področju, zato niso del tega dokumenta. Za uspešen prevzem digitalnega potrdila je potrebno uporabiti zadnjo različico objavljenih navodil.

Uporabnik lahko prevzame digitalno potrdilo samo z ustreznimi aktivacijskimi podatki - referenčno številko in avtorizacijsko kodo. Veljavnost podatkov za prevzem digitalnih potrdil je enkratna in časovno omejena [točka 4.2.3]. V primeru preteka njihove veljavnosti pred prevzemom je treba ponoviti postopek, opisan v točki 4.1.

4.4.2 Postopek potrditve prevzema potrdila

Ob prevzemu digitalnega potrdila je imetnik dolžan preveriti istovetnost digitalnega potrdila in vsebino digitalnega potrdila. Če imetnik osem (8) dni od prevzema digitalnega potrdila overitelja ne obvesti o morebitnih napakah velja, da je imetnik potrdil točnost podatkov v digitalnem potrdilu in da prevzema tudi vse obveznosti in jamstva pričujoče politike.

Prevzem potrdil, ki jih imetniki prevzamejo osebno z uporabo namenske aplikacije, ali spletnega brskalnika, se zabeleži v aplikaciji na strani overitelja. Dodatno potrjevanje s strani imetnika ni potrebno.

Imetniki potrdil izdanih na karticah potrdijo prevzem digitalnega potrdila s prevzemom poštne pošiljke, s katero mu je poslana pametna kartica.

4.4.3 Objava potrdila

Digitalna potrdila javnih ključev za šifriranje se po izdaji objavijo v javnem imeniku LDAP (glej poglavje 2.2). Digitalna potrdila javnih ključev za preverjanje podpisa praviloma niso objavljena.

Digitalna potrdila se po preklicu ali preteku veljavnosti ne brišejo iz imenika.

4.4.4 Obveščanje drugih udeležencev o izdaji potrdila

Ni predvideno.

4.5 Uporaba ključev in potrdil

4.5.1 Uporaba ključev in potrdil s strani imetnikov

Imetniki lahko uporabljajo ključe in digitalna potrdila za namene označene v razširitvenem polju *keyUsage* digitalnega potrdila (glej poglavje 6.1.7) in namene opredeljene v poglavju 1.4.

Imetniki so dolžni varovati svoje zasebne ključe in pametne kartice ali drugačne nosilce zasebnih ključev ter podatke za aktivacijo zasebnih ključev v skladu s priporočili v poglavju 9.6.3, da se prepreči izguba, razkritje, sprememba ali nepooblaščena uporaba.

Zasebni ključ za podpisovanje se hrani samo pri imetniku ali na sistemu za oddaljen podpis.

4.5.2 Uporaba potrdil s strani tretjih oseb

Tretje osebe so dolžne omejiti uporabo digitalnih le na namene opredeljene v poglavju 1.4. Tretje osebe morajo poleg tega:

- upoštevati vsa določila in omejitve Politike POŠTA®CA;
- pred vsako uporabo digitalnega potrdila preveriti status digitalnega potrdila v registru preklicanih potrdil;
- obvestiti overitelja v primeru suma zlorabe ali napačne uporabe digitalnega potrdila.

4.6 Obnova digitalnih potrdil brez spremembe ključev

Se ne uporablja.

4.7 Obnova potrdil

4.7.1 Okoliščine obnove potrdil

Obnova potrdil se izvede v sledečih primeri:

- redna obnova pred ali po izteku veljavnosti obstoječega digitalnega potrdila;
- po preklicu digitalnega potrdila.

Redna obnova naprednih kvalificiranih potrdil se izvede avtomatsko, ko je izpolnjen eden izmed naslednjih dveh pogojev:

- po preteku polovice dobe veljavnosti potrdila ali
- 100 dni pred iztekom.

Redna obnova kvalificiranih potrdil se izvede pred ali po preteku veljavnosti po enakem postopku kot za izdajo prvega digitalnega potrdila.

4.7.2 Kdo lahko zahteva obnovo potrdila

Za obnovo digitalnega potrdila lahko zaprosijo isti subjekti, kot za prvo izdajo skladno s poglavjem 4.1

4.7.3 Obdelava zahtevkov za obnovo digitalnih potrdil

Tvorjenje novih parov ključev se ob obnovi naprednega potrdila izvaja samodejno po protokolu PKIX-CMP, kot je definiran v RFC Public Key Infrastructure Certificate Management Protocol (CMP). Avtomatsko tvorjenje novih parov ključev je možno samo v primeru, če je digitalno potrdilo, ki ga trenutno poseduje imetnik, veljavno. Imetniki, ki nimajo veljavnega digitalnega potrdila, morajo pridobiti novo digitalno potrdilo oziroma ponoviti postopke prve registracije.

Obnova digitalnih potrdil, prevzetih osebno s strani imetnika preko spletnega brskalnika ali sistema za oddaljen elektronski podpis, poteka po istem postopku kot prevzem prvega digitalnega potrdila.

Kvalificirana potrdila, izdana na pametni kartici, se po preteku veljavnosti ponovno izdajo na isti pametni kartici z uporabo namenske programske opreme iz točke 2.2, v kolikor je obstoječe potrdilo na kartici ob ponovnem prevzemu še veljavno. Imetniki, ki nimajo veljavnega digitalnega potrdila, izdanega na pametni kartici, morajo pridobiti novo kartico. V tem primeru je postopek izdaje in prevzema novega digitalnega potrdila je enak postopku izdaje prvega digitalnega potrdila.

Obnova digitalnih potrdil izdajateljev časovnih žigov je izvedena pod kontrolo operativnega osebja izdajatelja časovnih žigov.

4.7.4 Obvestilo imetniku o izdaji novega potrdila

Enako kot 4.3.2 Obvestilo imetniku o izdaji potrdila.

4.7.5 Postopek potrditve prevzema obnovljenega digitalnega potrdila

Enako kot 4.4.2 Postopek potrditve prevzema potrdila.

4.7.6 Objava obnovljenega potrdila

Enako kot 4.4.3 Objava potrdila.

4.7.7 Obveščanje drugih udeležencev o izdaji potrdila

Enako kot 4.4.4 Obveščanje drugih udeležencev o izdaji potrdila.

4.8 Sprememba potrdila

Sprememba digitalnega potrdila je postopek, ki omogoča uporabnikom, da v primeru spremembe enega od podatkov vsebovanih v digitalnem potrdilu zahtevajo izdajo novega digitalnega potrdila. Sprememba digitalnega potrdila vedno zahteva kreiranje novih kriptografskih ključev imetnika in se izvede po istih postopkih kot prvi prevzem.

4.8.1 Okoliščine v katerih se izvede sprememba potrdil

Sprememba digitalnega potrdila se izvede kadar se je spremenil eden od sledečih podatkov vsebovanih v digitalnem potrdilu:

- podatki vsebovani (npr. ime ali priimek fizične osebe, naziv informacijskega sistema, ...) v razločevalnem imenu digitalnega potrdila;
- alternativno ime imetnika (npr. naslov elektronske pošte, domensko ime strežnika, ...).

4.8.2 Kdo lahko zahteva spremembo potrdila

Spremembo digitalnega potrdila lahko zahtevajo isti subjekti ki~~ot~~ so podali izdajo digitalnega potrdila (prosilci) (glej poglavje 4.1.1).

4.8.3 Obdelava zahtevkov za spremembo potrdil

Sprememba razločevalnega imena je mogoča samo za napredna kvalificirana digitalna potrdila z uporabo protokola PKIX-CMP. Sprememba razločevalnega imena za druga potrdila se obravnava kot izdaja novega potrdila.

Obdelava zahtevkov za spremembo digitalnega potrdila se izvede po istem postopku kot zahtevek prvi zahtevek za izdajo digitalnega potrdila (glej poglavji 4.2 in 4.3).

Sprememba razločevalnega imena za napredna kvalificirana potrdila z uporabo protokola PKIX-CMP poteka po naslednjem postopku:

1) Uporabnik osebno odda vlogo za spremembo razločevalnega imena v registracijski pisarni overitelja.
2) Po uspešno izvedenem postopku preverjanja istovetnosti uporabnika potrdila osebje registracijske pisarne posreduje vlogo za preklic v center overitelja.
3) Osebje overitelja preveri podpis in spremeni uporabnikovo razločevalno ime.
4) Ob prvi naslednji prijavi v aplikacijo se avtomatsko tvorijo novi ključi in izda potrdilo z novim razločevalnim imenom.

4.8.4 Obvestilo imetniku o izdaji spremenjenega potrdila

Enako kot 4.3.2 Obvestilo imetniku o izdaji potrdila.

4.8.5 Postopek potrditve prevzema spremenjenega potrdila

Enako kot 4.4.2 Postopek potrditve prevzema potrdila.

4.8.6 Objava spremenjenega potrdila

Enako kot 4.4.3 Objava potrdila.

4.8.7 Obveščanje drugih udeležencev o izdaji spremenjenega potrdila

Enako kot 4.4.4 Obveščanje drugih udeležencev o izdaji potrdila.

4.9 Začasna ukinitev veljavnosti in preklic potrdila

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;
- 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.

4.9.2 Kdo lahko zahteva preklic

Preklic digitalnega potrdila lahko zahteva:

- imetnik potrdila, kateremu je bilo digitalno potrdilo izdano;
- pooblaščena oseba, odgovorna za digitalna potrdila izdana pravni osebi;
- osebje overitelja;
- pristojno sodišče, sodnik za prekrške ali upravni organ;
- dedič ali zakoniti zastopnik;

- tretja oseba, če digitalno potrdilo vsebuje podatke o tretji osebi.

4.9.3 Postopki za preklic

1) Zahteva za preklic se lahko poda na enega izmed naslednjih načinov:
   - Imetnik potrdila pošlje vlogo po elektronski pošti na kontaktni naslov overitelja. Upoštevane bodo samo digitalno podpisane vloge z veljavnimi digitalnimi potrdili, ki jih je izdal overitelj.
   - 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.
2) Po uspešno izvedenem postopku preverjanja istovetnosti imetnika potrdila v registracijski pisarni, osebje registracijske pisarne posreduje vlogo za preklic v center overitelja.
3) Overitelj izvede preklic digitalnega potrdila.
4) Postopek izdaje in prevzema novega digitalnega potrdila je enak postopku izdaje prvega digitalnega potrdila[točke 4.1, 4.2, 4.3].

4.9.4 Čas za posredovanje vloge za preklic

Oseba, ki je izvedela za okoliščine, ki zahtevajo preklic digitalnega potrdila, mora zahtevati preklic v najkrajšem možnem času in brez nepotrebnega odlašanja.

4.9.5 Čas od vloge za preklic do preklica

Preklic zaradi neizpolnjevanja obveznosti imetnika potrdila izvede overitelj takoj. Preklici iz drugih razlogov se izvedejo najkasneje v osmih (8) urah po prejemu vloge.

4.9.6 Obveza preverjanja registra preklicanih potrdil

Vsi subjekti, ki se zanašajo na digitalna potrdila overitelja POŠTA®CA, morajo pred uporabo javnega ključa vsebovanega v digitalnem potrdilu preveriti register preklicanih digitalnih potrdil. Za preverjanje veljavnosti digitalnih potrdil je merodajen najnovejši objavljeni register preklicanih digitalnih potrdil objavljen na spletnem naslovu navedem v razširitvenem polju vsakega digitalnega potrdila in na spletni strani overitelja (glej poglavje 2.2 Objave informacij o digitalnih potrdilih). Register preklicanih digitalnih potrdil je podpisan z istim overiteljevim zasebnim ključem, kot se uporablja za podpis digitalnih potrdil.

4.9.7 Pogostost objav registrov preklicanih potrdil

Nov register preklicanih potrdil se objavi vsakih dvanajst (12) ur. Veljavnost overiteljevega registra preklicanih digitalnih potrdil je štiriindvajset (24) ur. Nov register se objavi pred potekom veljavnosti starega.

Ob preklicu digitalnega potrdila se takoj objavi nov register preklicanih digitalnih potrdil.

4.9.8 Dovoljene zakasnitve pri objavi registrov preklicanih potrdil

Overitelj POŠTA®CA izda nove registre preklicanih potrdil vsaj eno uro pred iztekom veljavnosti starih, ter zagotavlja prenos registrov do vseh komponent repozitorija še pred iztekom veljavnosti starega registra.

4.9.9 Storitev sprotnega preverjanje statusa potrdil

Se ne uporablja.

4.9.10 Obveza sprotnega preverjanja statusa preklicanih potrdil

Ni relevantno.

4.9.11 Ostale oblike objavljanja preklicanih potrdil

Se ne uporabljajo.

4.9.12 Posebne zahteve glede zlorabe ključa

Glej 4.9.2.

4.9.13 Okoliščine za začasno ukinitev veljavnosti (suspenz) potrdila

Uporabnik lahko zahteva za določen čas (npr. daljša odsotnost) začasen suspenz digitalnega potrdila. Overitelj lahko digitalno potrdilo suspendira v času preverjanja okoliščin preklica digitalnega potrdila.

4.9.14 Kdo lahko zahteva suspenz ali ukinitev suspenza potrdila

Suspenz digitalnega potrdila lahko zahteva:

- imetnik potrdila, kateremu je bilo digitalno potrdilo izdano;
- pooblaščena oseba, odgovorna za digitalna potrdila izdana pravni osebi;
- zaposleni pri overitelju v času preverjanja okoliščin preklica digitalnega potrdila;
- pristojno sodišče, sodnik za prekrške ali upravni organ;
- dedič ali zakoniti zastopnik;
- tretja oseba, če digitalno potrdilo vsebuje podatke o tretji osebi;
- overitelj, v primeru da imetnik ne izpolnjuje finančnih obveznosti;

Ukinitev suspenza digitalnega potrdila lahko zahteva:

- imetnik potrdila, kateremu je bilo digitalno potrdilo izdano;
- pooblaščena oseba, odgovorna za digitalna potrdila izdana pravni osebi;
- zaposleni pri overitelju v primeru, ko so zahtevali suspenz in so razlogi za suspenz prenehali.

4.9.15 Postopki za suspenz ali ukinitev suspenza potrdila

1) Zahteva za suspenz ali ukinitev suspenza digitalnega potrdila se lahko poda na enega izmed naslednjih načinov:
   - Imetnik potrdila pošlje vlogo po elektronski pošti na kontaktni naslov overitelja. Upoštevane bodo samo digitalno podpisane vloge z veljavnimi digitalnimi potrdili, ki jih je izdal overitelj.
   - Imetnik potrdila osebno odda vlogo v registracijski pisarni overitelja.
   - Po telefonu na številko za preklic. Imetnik potrdila se mora identificirati z geslom, ki ga je vpisal na vlogo za izdajo digitalnega potrdila.

2) Po uspešno izvedenem postopku preverjanja istovetnosti imetnika potrdila v registracijski pisarni, osebje registracijske pisarne posreduje vlogo za suspenz v center overitelja.
3) Overitelj izvede suspenz ali ukinitev suspenza digitalnega potrdila.
4) Overitelj obvesti imetnika potrdila o suspenzu ali ukinitvi suspenza po elektronski pošti ali pisno po pošti.

4.9.16 Omejitve obdobja začasne ukinitve veljavnosti

Ni omejitev.

4.10 Storitve objavljanja statusa potrdil

4.10.1 Tehnične lastnosti storitve

Status digitalnih potrdil je objavljen z uporabo registra preklicanih potrdil v skladu z (X.509 Certificate Revocation List) in RFC5280. Register preklicanih potrdil je dostopen preko LDAP in http protokola. Točen naslov objave registra preklicanih potrdil je vsebovan v razširitvenem polju vsakega izdanega digitalnega potrdila, kot je navedeno v poglavju 7.1.2.

4.10.2 Razpoložljivost storitve dostopa do registra preklicanih potrdil

Overitelj zagotavlja razpoložljivost storitve štiriindvajset (24) ur sedem (7) dni v tednu.

4.10.3 Dodatne možnosti

Ni predvideno.

4.11 Trajanje naročniškega razmerja

Naročnik mora za sklenitev naročniškega razmerja pooblaščeni registracijski pisarni overitelja predložiti izpolnjeno in podpisano vlogo za pridobitev digitalnega potrdila. Naročniško razmerje prične teči s prevzemom digitalnega potrdila, oziroma najkasneje 5 dni po dostavi aktivacijskih podatkov. Naročniško razmerje je sklenjeno za obdobje veljavnosti digitalnega potrdila.
Razmerje med overiteljem POŠTA®CA in naročnikom preneha:

- z zadnjim dnem veljavnosti digitalnega potrdila, če ga naročnik pred tem ne podaljša;
- z dnem preklica digitalnega potrdila, če uporabnik ne zaprosi za izdajo novega digitalnega potrdila;
- s strani overitelja, če ugotovi da naročnik krši obveznosti iz politike.

4.12 Varnostno kopiranje in odkrivanje zasebnega ključa

Hranjenje zasebnih ključev pri zunanjih subjektih (ang. key escrow) ni dovoljeno. Dovoljeno je samo varnostno kopiranje zasebnih ključev (ang. key backup) in odkrivanje zasebnih dešifrirnih ključev (ang. key recovery) pri overitelju POŠTA®CA.

Overitelj POŠTA®CA zagotavlja varnostno kopiranje zasebnih dešifrirnih ključev (ang. key backup) za napredna kvalificirana potrdila v skladu s poglavjem 6.2.4 Varnostno kopiranje zasebnih ključev.

Zasebni ključi imetnikov za podpisovanje se vedno tvorijo v programski opremi pri imetniku, na pametni kartici ali na sistemu za oddaljen elektronski podpis. POŠTA®CA ne hrani varnostnih kopij

imetniških zasebnih ključev za podpisovanje. V primeru, da uporabnik izgubi zasebni ključ ali pozabi aktivacijske podatke (npr. geslo za aktiviranje podpisa na sistemu za oddaljen elektronski podpis) povrnitev uporabnikovega zasebnega ključa ni možna. Uporabnik mora zaprositi za izdajo novega potrdila.

4.12.1 Postopki povrnitve zgodovine ključev in odkrivanje kopije zasebnega ključa za dešifriranje

Povrnitev zgodovine ključev za dešifriranje je mogoča samo za napredna kvalificirana potrdila z uporabo protokola PKIX-CMP.

Povrnitev zgodovine ključev za dešifriranje se izvaja po sledečem postopku:

- Uporabnik osebno odda vlogo za povrnitev zgodovine ključev v registracijski pisarni overitelja. Po uspešno izvedenem postopku preverjanja istovetnosti imetnika potrdila osebje registracijske pisarne posreduje vlogo za povrnitev zgodovine ključev v center overitelja.
- Osebje overitelja preveri digitalni podpis in izvede povrnitev digitalnega potrdila.
- Overitelj pošlje novo referenčno številko z navodili po elektronski pošti ali pisno po pošti. Avtorizacijske kode se pošljejo pisno po pošti.
- Imetnik prevzame digitalno potrdilo po postopku, opisanem v točki 4.3.

4.12.2 Zaščita zasebnega ključa in postopek prenosa

Postopek prenosa zasebnega ključa je enak kot postopek prenosa dešifrirnega zasebnega ključa ob kreiranju novega digitalnega potrdila, torej v skladu z drugim odstavkom poglavja 6.1.2 Prenos zasebnega ključa imetniku.

4.13 Dodatne možnosti

4.13.1.1 Zahteve za medsebojno priznavanje

Overitelj se lahko povezuje z drugimi overitelji na horizontalni ravni na podlagi pogodbe o medsebojnem priznavanju ali na podlagi pogodbenega razmerja s podrejenim overiteljem.

Overitelj se povezuje z drugimi overitelji po lastni presoji in le v primerih, ko drugi overitelj izdaja primerljiva potrdila in zagotavlja vsaj enak nivo zaupanja.

Overitelj lahko overja in objavlja javni del notranjih pravil overitelja podrejenih overiteljev v primeru, da se nameni uporabe kvalificiranih potrdil razlikujejo od namena uporabe, definirane v tem dokumentu.

4.13.1.2 Odklepanje naprave za ustvarjanje podpisa

Odklepanje je mogoče le za potrdila, ki jih overitelj izdaja na QSCD napravi v obliki pametne kartice.

Uporabnik odklene pametno kartico z uporabo kode za odklepanje kartice, ki jo je prejel skupaj z osebnim geslo. Navodila za odklepanje pametnih kartic se nahajajo na spletni strani overitelja.

V primeru, da je uporabnik izgubil kodo za odklepanje pametne kartice:

1) Poda zahtevo za pridobitev kode za odklepanje pametne kartice na enega izmed naslednjih načinov:
   - Vlogo za odklepanje pametne kartice odda osebno v registracijski pisarni overitelja.
   - Po telefonu. Uporabnik potrdila se mora identificirati z geslom, ki ga je vpisal na vlogo za izdajo potrdila.
2) Po uspešno izvedenem postopku preverjanja istovetnosti imetnika potrdila v registracijski pisarni, osebje registracijske pisarne posreduje vlogo za odklepanje pametne kartice v center overitelja.
3) Osebje overitelja preveri verodostojnost vloge.
4) Overitelj pošlje uporabniku kodo za odklepanje pametne kartice s priporočeno pisemsko pošiljko v roku dveh (2) delovnih dni po prejemu zahtevka.

5 FIZIČNO VAROVANJE, ORGANIZACIJSKI VARNOSTNI UKREPI IN ZAHTEVE ZA OSEBJE

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

5.1 Fizično varovanje

5.1.1 Lokacija in konstrukcija prostorov overitelja

Dejavnosti overitelja se izvajajo v varovanih prostorih in na varni lokaciji.

5.1.2 Fizični dostop do overitelja

Dostop do posameznih delov infrastrukture overitelja ima le pooblaščeno operativno osebje v skladu z zaupanimi nalogami. Vsi dostopi do prostorov overitelja se beležijo in varujejo v skladu z notranjimi pravili overitelja.

5.1.3 Napajanje in klimatske naprave

Center overitelja je opremljen s:

- sistemom za neprekinjeno napajanje za zagotavljanje napajanja kritičnim strežnikom in mrežnim napravam;
- klimatsko napravo za kontrolo temperature in vlage.

5.1.4 Zaščita pred poplavo

V bližini prostorov overitelja ni vodne napeljave. Prostori se nahajajo na lokaciji, kjer ni možna poplava.

5.1.5 Zaščita pred ognjem

Prostori overitelja so opremljeni z detektorji temperature in dima ter gasilnim sistemom.

5.1.6 Shranjevanje medijev

Vsi magnetni mediji za arhiviranje podatkov overitelja so hranjeni v ognje varnih omarah. Magnetni mediji, hranjeni na oddaljeni lokaciji, so v prostorih, ki zagotavljajo vsaj enake pogoje, kot so v centru overitelja.

5.1.7 Odstranjevanje odpadkov

Dokumenti v papirni obliki so uničeni v varovanih prostorih overitelja. Vsebina medijev, na katerih se hranijo zaupni podatki, je pred odstranitvijo iz prostorov overitelja izbrisana v nasprotnem primeru overitelj medij fizično uniči.

5.1.8 Hranjenje na oddaljeni lokaciji

Overitelj uporablja oddaljeno lokacijo za varno hranjenje podatkov. Mediji ali strojna oprema so na oddaljeni lokaciji shranjene v varovanem območju. V prostorih na oddaljeni lokaciji je zagotovljena vsaj enaka stopnja varnosti, kot v centru overitelja.

5.2 Organizacijski varnostni ukrep

5.2.1 Organizacija overitelja

Organizacija overitelja deluje v okviru POŠTE SLOVENIJE. Sestavljena je iz naslednjih organizacijskih enot:

- upravni svet;
- operativno osebje.

Upravni svet ima funkcije nadzora delovanja operativnega osebja, revidiranja in odobravanja novih različic politike oz. javnega dela notranjih pravil overitelja (CPS). Sestavljajo ga vodja upravnega sveta (član uprave POŠTE SLOVENIJE) in štirje člani, od katerih mora biti eden operativni vodja, eden varnostni oficir in eden univerzitetni diplomirani pravnik.

Naloge upravljanja z infrastrukturo overitelja so porazdeljene med subjekte tako, da je zagotovljena ločitev med zaključenimi vsebinskimi področji upravljanja. Programska oprema (CA-aplikacija), ki jo overitelj uporablja za upravljanje šifrirnih ključev in digitalnih potrdil, podpira več stopenj pravic oziroma funkcij, ki so dodeljene osebju overitelja glede na njihove naloge.

Naloge operativnega vodje so:

- koordinira operativno delo;
- skrbi za nadzor operativnega osebja;
- izvaja varnostne preglede;
- skrbi za implementacijo novih postopkov;
- izdeluje poročila;
- pregleduje in analizira varnostne beležke;
- skrbi za strategijo delovanja;
- določa prvega varnostnega inženirja;
- skrbi za vzdrževanje varnostnih kopij.

CA prvi varnostni oficir in CA-glavni administrator imata potrebna pooblastila, da:

- konfigurirata in vzdržujeta sistemsko strojno in programsko opremo;
- izvedeta začetno konfiguracijo ter izvajata vzdrževanje aplikativne CA-programske opreme overitelja;
- izvajata zagon in zaustavitev CA-servisov;
- ustvarita prvotni uporabniški račun CA-varnostnega oficirja;
- ustvarita uporabniški račun drugih CA-varnostnih oficirjev;
- restavrirata uporabniški račun CA-varnostnega oficirja;
- restavrirata uporabniški račun CA-aplikativnega administrativnega servisa;
- izdelujeta varnostne kopije, izvajata restavriranje in ponovno šifriranje baze overitelja.

Osebje z vlogo CA-varnostnega oficirja (Operativni vodja, CA prvi varnostni oficir in CA drugi varnostni oficir) ima potrebna pooblastila, da:

- vodi ostale CA-varnostne oficirje in uporabniške račune CA-administratorjev;
- usmerja imetnike potrdil;
- namešča in spreminja politiko delovanja CA-aplikativne programske opreme;
- skrbi za določanje in izvajanje pravil varnega delovanja sistema za izdajo digitalnih potrdil;
- izvaja medsebojno priznavanje z drugimi overitelji;
- pregleduje in analizira varnostne beležke;
- namešča in vzdržuje pravila na požarnih zidovih;
- izdeluje poročila.

Osebje z vlogo CA-administratorja ima potrebna pooblastila, da:

- upravlja z digitalnimi potrdili;
- izdeluje poročila.

Osebje z vlogo varnostnega inženirja ima naslednje naloge:

- upravlja sistem za preprečevanje in odkrivanje vdorov;
- skrbi za administracijo požarnih zidov.

Osebje registracijske pisarne overitelja (RA-, LRA-administratorji) ima na aplikativni programski opremi overitelja za vodenje registra imetnikov potrdil potrebna pooblastila in pravice, da:

- prejema in posreduje vloge uporabnikov;
- vnaša podatke iz vlog naročnikov digitalnih potrdil;
- distribuira inicializacijske podatke naročnikom digitalnih potrdil.

5.2.2 Število oseb, potrebnih za izvedbo postopkov

Za izvedbo naslednjih nalog je zahtevana odobritev dveh zaposlenih v funkciji CA-glavnega administratorja:

- ponovno šifriranje CA-baze podatkov;
- tvorjenje kriptografskih ključev overitelja;
- spreminjanje gesel CA-aplikacije;
- spreminjanje števila potrebnih odobritev za kritične operacije, ki jih izvaja CA-varnostni oficir;
- restavriranje uporabniških računov CA-varnostnih oficirjev;
- spreminjanje nastavitve zgoščevalnih algoritmov;

- spreminjanje nastavitve šifrirnih algoritmov;
- aktiviranje avtomatskega starta CA-postopkov;
- deaktiviranje večkratne avtorizacije za operacije CA-glavnega administratorja.

Za izvedbo naslednjih nalog je zahtevana odobritev dveh zaposlenih v funkciji CA-varnostnega oficirja:

- nastavitev dolžine življenjske dobe digitalnih potrdil;
- medsebojno priznavanje z drugimi overitelji;
- nastavitev ali spreminjanje administrativnih pravil;
- nastavitev ali spreminjanje uporabniških pravil;
- dodajanje, brisanje ali mapiranje OID-jev s profili digitalnih potrdil;
- dodajanje, spreminjanje ali brisanje uporabniških računov za CA-varnostnega oficirja.

Za izvedbo naslednjih nalog je zahtevana odobritev dveh zaposlenih s CA-administratorskimi pooblastili:

- povrnitev zgodovine imetnikovih ključev za dešifriranje.

5.2.3 Preverjanje istovetnosti operativnega osebja

Pred dodelitvijo nalog in potrebnih pooblastil se osebje overitelja preveri v skladu s postopki določenimi v točki 5.3.

Vsako digitalno potrdilo in uporabniški račun na sistemu ali v aplikaciji za osebje overitelja je ustvarjeno za določeno fizično osebo.

Posamezno digitalno potrdilo in uporabniški račun za osebje overitelja lahko uporablja le ena oseba. Njihova uporaba je z uporabo mehanizmov in kontrolnih postopkov CA-aplikacije in sistemske programske opreme omejena na operacije, vezane na posamezno funkcijo osebja overitelja.

Osebje registracijske pisarne overitelja uporablja digitalna potrdila in pametne kartice za prijavo v aplikacije overitelja.

5.2.4 Nezdružljivost nalog

Odvisno od zadolžitev ima osebje sistemske in aplikativne uporabniške račune, omejene na nujno potrebne pravice za opravljanje svojih nalog. Razporeditev funkcij je opisana v naslednji tabeli:

Osebje overitelja	Sistemski uporabniški račun	CA-aplikativni uporabniški račun	Min. število zaposlenih oseb
Operativni vodja	Ne	Da	1
CA prvi varnostni oficir	Da	Da	1
CA drugi varnostni oficir	Ne	Da	1
CA tretji varnostni oficir	Ne	Da	1
CA glavni administrator	Ne	Da	3
CA administrator	Ne	Da	4
Varnostni inženir	Ne	Ne	3
Pravni svetovalec	Ne	Ne	1
RA osebje	Ne	Ne	4

5.3 Zahteve za osebje overitelja

5.3.1 Kvalifikacije, izkušnje in varnostno preverjanje

Overitelj zaposluje osebje z ustreznimi kvalifikacijami, v skladu s politiko zaposlovanja Pošte Slovenije.

5.3.2 Preverjanje primernosti osebja

Preverjanja primernosti osebja (angl. security clearance checks) se izvajajo v okviru postopkov kadrovske službe Pošte Slovenije.

5.3.3 Usposabljanje osebja

Osebje overitelja se redno izobražuje na naslednjih področjih:

- varnost informacijskih in komunikacijskih sistemov;
- pridobivanja specifičnih znanj za opravljanje svojih funkcij;
- za aplikativno programsko opremo CA;
- za obvladovanje postopkov ukrepanja ob incidentih, obnove poslovanja (angl. Business Continuation) ter okrevalnega načrta (angl. Disaster Recovery).

Osebje overitelja z LRA nalogami se redno izobražuje na naslednjih področjih:

- osnove varnosti informacijskih in komunikacijskih sistemov;
- aplikacije za vodenje registra imetnikov potrdil.

5.3.4 Pogostost dodatnih usposabljanj

Osebje overitelja se udeležuje izobraževanj po potrebi, glede na nove operativne zahteve in spremembe na infrastrukturi overitelja.

5.3.5 Kroženje med delovnimi mesti

Ni predpisano.

5.3.6 Ukrepi ob kršitvah pooblastil

Proti osebju overitelja, ki ne izvaja svojih nalog po predpisanih postopkih, se uvede disciplinski postopek po pravilniku o disciplinskem postopku Pošte Slovenije. V primeru nepravilnosti ali suma nepravilnosti se osebi odvzamejo pooblastila za sisteme ter prekličejo digitalna potrdila, izdana osebi za opravljanje funkcije.

5.3.7 Zahteve za pogodbene in zunanje izvajalce

Overitelj praviloma ne angažira pogodbenih in zunanjih izvajalcev na funkcijah navedenih v poglavju 5.2.1. Izjema je osebje registracijskih pisarn. Varnostne zahteve za pogodbene in zunanje izvajalce so enake kot za osebje overitelja.

5.3.8 Dokumentacija za osebje overitelja

Overitelj vzdržuje dokumentacijo na spletni strani, kot je opisano v točki 2.6. Ta dokumentacija je javno dostopna. Dodatno so osebju overitelja na voljo interni operativni priročniki, originalna

dokumentacija programske in strojne opreme ter priročniki iz sklopa izobraževanja, glede na njihovo funkcijo in plan izobraževanja.

5.4 Postopki zbiranja in upravljanja revizijskih sledi

5.4.1 Vrste beleženih dogodkov

Zapisane bodo naslednje vrste dogodkov:

- dogodki v zvezi z uporabniškimi ključi in z digitalnimi potrdili - izdaja, prevzem, preklic, suspenz;
- dogodki v zvezi s ključi overitelja;
- dogodki v zvezi z upravljanjem, arhiviranjem (angl. backup), varnostno politiko in uporabo aplikacij in imenika overitelja;
- dogodki na operacijskih sistemih in strojni opremi;
- dogodki v zvezi z varnostno politiko, upravljanjem in s strojno opremo na mreži;
- dogodki v zvezi s fizičnim dostopom do sistemov overitelja;
- dogodki v zvezi s kadrovskimi spremembami overitelja;
- dogodki, povezani z uničevanjem za to predvidenih podatkov.

5.4.2 Pogostost pregleda revizijskih dnevnikov

Osebje overitelja pregleduje revizijske dnevnike enkrat tedensko. Revizija vključuje:

- zbiranje vseh dnevnikov od zadnjega pregleda;
- pregled zapisov v dnevniku;
- analizo in poročanje o relevantnih dogodkih - razreševanje ali eskalacija problemov.

5.4.3 Obdobje hranjenja revizijskih dnevnikov

Najmanj sedem (7) dni na sistemih in trajno v arhivu.

5.4.4 Zaščita revizijskih dnevnikov

Revizijski dnevniki se hranijo na sistemu kjer nastanejo, ter na mediju za izdelavo varnostne kopije (glej tudi poglavje 5.4.5). Za dnevnike na operacijskem sistemu so uporabljene zaščite, kot jih le-ta dopušča. Dnevniki programske opreme za upravljanje s ključi in digitalnimi potrdili so zaščiteni s tehnologijo šifrirnih javnih ključev.

5.4.5 Varnostne kopije revizijskih dnevnikov

Dnevniki se vsak dan shranjujejo na trak. Enkrat tedensko se prestavijo v varovan prostor na drugi lokaciji. Za izdelavo varnostnih kopij so zadolženi pooblaščeni skrbniki sistemov.

5.4.6 Način zbiranja revizijskih dnevnikov

Revizijski podatki se zbirajo avtomatsko in ročno, kot to prikazuje spodnja tabela:

Beleženi dogodki	**Zbiranje podatkov**	**Odgovorna oseba/sistem**
Dogodki, povezani s CA uporabniki	avtomatsko	CA-aplikacija

Dogodki, povezani s CA ključi	avtomatsko	CA-aplikacija
Dogodki, povezani s CA, RA aplikacijo	avtomatsko	CA-aplikacija
Dogodki na LRA-aplikaciji	avtomatsko	LRA-aplikacija
Dogodki na aplikaciji direktorij	avtomatsko	CA aplikacija, aplikacija direktorij
Dogodki na operacijskem sistemu	avtomatsko	operacijski sistem
Dogodki na mreži	avtomatsko	usmerjevalniki, operacijski sistem
Backup/restore CA-baze uporabnikov	avtomatsko	CA-aplikacija, operacijski sistem
Backup/restore CA-logov, konfiguracije	avtomatsko	CA-aplikacija, operacijski sistem
Backup/restore direktorija	avtomatsko	direktorij aplikacija, operacijski sistem
Fizični dostop do CA	Ročno	CA-osebje
Spremembe konfiguracije/hw na sistemu	Ročno	CA-osebje
Vzdrževalna dela na sistemu/prostoru	Ročno	CA-osebje
Kadrovske spremembe	Ročno	CA-osebje
Uničenje za to predvidenih podatkov	Ročno	CA-osebje

5.4.7 Obveščanje povzročitelja dogodka

Povzročitelja dogodka v dnevniku o tem ni treba obvestiti.

5.4.8 Ocena in odprava ranljivosti

Ocena ranljivosti se izvaja v sklopu pregleda revizijskih dnevnikov.

5.5 Arhiviranje podatkov

5.5.1 Vrste arhiviranih podatkov

Overitelj hrani naslednje podatke:

- revizijske dnevnike iz točke 4.5;
- pogodbe z uporabniki in njihove vloge;
- vloge o preklicih digitalnih potrdil in prijave ogrožanja ključev;
- digitalna potrdila, različice politik oz. javnih delov notranjih pravil overitelja;
- zasebne ključe uporabnikov za šifriranje, ki imajo Napredna kvalificirana potrdila.

5.5.2 Čas hrambe

Overitelj hrani vloge uporabnikov za izdajo in preklic digitalnih potrdil vsaj toliko časa, kot bodo hranjeni podatki, podpisani z elektronskim podpisom, na katerega se nanaša digitalno potrdilo, najmanj pa pet od izdaje potrdila. Ostali arhivirani podatki se hranijo trajno.

5.5.3 Zaščita arhiva

Varnostna kopija arhiv se hrani na drugi lokaciji, zaščiten z enakimi varnostnimi mehanizmi, kot so vzpostavljeni v centru overitelja.

5.5.4 Varnostna kopija arhiva

Ob izdelavi arhiva podatkov, ki se beležijo v okviru informacijskega sistema overitelja, se izdela varnostna kopija.

5.5.5 Zahteve za časovno žigosanje zapisov

Ni predpisano.

5.5.6 Način arhiviranja

Ni predpisano.

5.5.7 Postopek za dostop do arhivskih podatkov in njihova verifikacija

Dostop do arhiviranih podatkov je dovoljen samo pooblaščenim osebam overitelja na osnovi potrebe po vedenju, ali v skladu z veljavno zakonodajo.

5.6 Obnova digitalnega potrdila overitelja

Overitelj ob vsaki obnovi lastnega digitalnega potrdila tvori nov par ključev. Postopek je izveden nadzorovano v varnih prostorih in ob upoštevanju ostalih določil poglavja 5 FIZIČNO VAROVANJE, ORGANIZACIJSKI VARNOSTNI UKREPI IN ZAHTEVE ZA OSEBJE, ter določil poglavja 6 TEHNIČNE VARNOSTNE ZAHTEVE.

5.7 Postopki v primeru ogrožanja zasebnega ključa in okrevalni načrt

5.7.1 Postopki za odzivanje na varnostne incidente in nepravilnosti

Overitelj izvaja postopke za odzivanje na varnostne incidente in nepravilnosti v skladu z ISO / IEC 17799.

5.7.2 Uničenje programske, strojne opreme ali podatkov

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

5.7.3 Ogrožanje overiteljevega zasebnega ključa

Ob ogrožanju ključa overitelja bo overitelj pisno, ali po elektronski pošti obvestil:

- celotno osebje overitelja;
- vse uporabnike oziroma pooblaščene osebe;
- morebitne medsebojno priznane ali podrejene overitelje.

Overitelj bo izvedel naslednje postopke:

- preklical vsa digitalna potrdila;
- ukinil CRL, podpisane z ogroženim ključem;
- objavil preklic digitalnega potrdila overitelja v ustrezni ARL;
- tvoril nove ključe overitelja;

- izdal uporabnikom nova digitalna potrdila.

Postopek prevzema digitalnih potrdil se opravi po postopku navedenem v točki 4.3.

5.7.4 Okrevalni načrt v primeru naravne in druge nesreče

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

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

5.8 Prenehanje delovanja overitelja

Overitelj bo v primeru prenehanja delovanja:

- pisno, po elektronski pošti, ali preko svoje spletne strani obvestil vse naročnike in javno objavil informacije vsaj devetdeset (90) dni pred prenehanjem delovanja;
- preklical vsa veljavna digitalna potrdila;
- zagotovil razpoložljivost in dostopnost list preklicanih potrdil za obdobje šest (6) mesecev po preklicu vseh digitalnih potrdil;
- zagotovil, da bo drug overitelj, ki izdaja kvalificirana potrdila, vodil preklicana digitalna potrdila v svojem registru;
- zagotovil hranjenje arhiviranih podatkov za obdobje deset (10) let po prenehanju delovanja.

6 TEHNIČNE VARNOSTNE ZAHTEVE

6.1 Tvorjenje in namestitev para ključev

6.1.1 Tvorjenje para ključev

Overiteljev par ključev za podpisovanje je ustvarjen ob namestitvi CA-programske opreme. Uporabljena je zaščita, ki velja za prostore overitelja [poglavje 5.1], večkratno preverjanje istovetnosti pooblaščenih oseb [poglavje 6.2.2] in strojni šifrirni modul (HSM – Hardware Security Module) [poglavje 6.2.1].

Ustvarjanje ključev uporabnikov je v domeni aplikacijskega okolja uporabnika. Za vse vrste digitalnih potrdil, ki jih izdaja overitelj POŠTA®CA, se par ključev za podpisovanje ustvari v aplikaciji na strani uporabnika, na QSCD napravi ali v oddaljeni QSCD napravi. Par ključev za šifriranje za napredna kvalificirana potrdila se ustvari v CA-aplikaciji overitelja.

6.1.2 Prenos zasebnega ključa imetniku

Za napredna kvalificirana potrdila se zasebni par ključev za šifriranje prenese do uporabnika po protokolu PKIX-CMP.

Uporabniški zasebni ključi za podpisovanje se nikdar ne hranijo na strojni ali programski opremi overitelja.

V primeru osebnega prevzema preko spletnega brskalnika se zasebni ključ ustvari in hrani v programskem ali stojnem kriptografskem modulu na strani uporabnika.

V primeru potrdil izdanih na QSCD napravi, se zasebni ključ ustvari in hrani na QSCD napravi. Aktivacija zasebnega ključa za podpis je vedno pod nadzorom uporabnika.

6.1.3 Prenos imetnikovega javnega ključa overitelju

Javni ključ za podpisovanje imetniki potrdil dostavijo overitelju po protokolih PKIX-CMP,PKIX#10 ali SPKAC.

6.1.4 Dostop do overiteljevega javnega ključa

Javni ključ overitelja v obliki digitalnega potrdila je dostopen:

- v javnem imeniku v ou=POSTARCA, o=POSTA,c=SI, attribute: CAcertificate;
- na javni spletni strani overitelja (glej poglavje 2.1)
- po protokolu PKIX-CMP.

6.1.5 Dolžina asimetričnih ključev

Overitelj uporablja zasebni ključ RSA za podpisovanje dolžine 2048 bitov.

Uporabniki morajo ustvariti RSA par ključev dolžine najmanj 2048 bitov.

6.1.6 Parametri za generiranje javnih ključev in preverjanje parametrov

Vsi postopki v zvezi z RSA ključi so v skladu s PKCS#1 priporočili.

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

Namen uporabe ključev je označen v razširitvenem polju *keyUsage* vsakega izdanega digitalnega potrdila v skladu s priporočilom RFC 3280.

Overiteljevi zasebni ključi se uporabljajo samo za podpisovanje digitalnih potrdil in registrov preklicanih potrdil. Overiteljevi javni ključi se uporabljajo samo za preverjanje veljavnosti digitalnih potrdil in registrov preklicanih potrdil. Namen ključev je v overiteljevih digitalnih potrdilih je v skladu z RFC 3280 označen v razširitvenem polju keyUsage z bitoma keyCertSign in cRLSign.

Ključi in digitalna potrdila osebja overitelja se uporabljajo samo za delo na infrastrukturi overitelja.

Namen ključev v imetniških digitalnih potrdilih je v skladu z RFC 3280 označen v razširitvenem polju *keyUsage* z biti *digitalSignature*, *nonRepudiation (contentCommitment)* in/ali *keyEncipherment*.

Namen uporabe v digitalnih potrdilih za spletne strežnike je v skladu z RFC 3280 dodatno označen v razširitvenem polju extKeyUsage z identifikacijskimi oznakami za id-kp-serverAuth (angl. TLS WWW server authentication) in id-kp-clientAuth (angl. TLS WWW client authentication)

6.2 Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov

6.2.1 Standardi za kriptografski modul

Ustvarjanje overiteljevih šifrirnih ključev za digitalni podpis ter digitalni podpis z overiteljevimi šifrirnimi ključi se izvaja na strojnem modulu za šifriranje, ki ima potrdilo o skladnosti z FIPS 140-1 level 3. Vse ostale šifrirne operacije overitelja se izvajajo na modulih za šifriranje s stopnjo najmanj FIPS 140-1 level 2.

Osebje overitelja uporablja module za šifriranje, ki ima potrdilo o skladnosti vsaj z FIPS 140-1 level 2.

Imetniki storitev overitelja morajo uporabljati module za šifriranje skladno z zahtevami glede na vrsto digitalnega potrdila. Naprave za ustvarjanje kvalificiranega elektronskega podpisa morajo imeti potrdilo skladnosti z zahtevami Direktive 1999/93/ES, priloga III ali Uredbe eIDAS, priloga II.

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

Overitelj ima implementirano večkratno odobritev za operacije, navedene v točki 5.2.2.

6.2.3 Odkrivanje (angl. Escrow) zasebnega ključa

Overitelj ne podpira odkrivanja zasebnega ključa za podpisovanje.

6.2.4 Varnostno kopiranje zasebnih ključev

Varnostna kopija overiteljevega zasebnega ključa se izdela na strojnem kriptografskem modulu in se pred izvozom iz modula in zapisom kopije na medij v modulu šifrira z močnim simetričnim šifrirnim algoritmom. Dešifrirni ključ je zaščiten s ključi porazdeljenimi na pametnih karticah strojnega kriptografskega modula.

Overitelj hrani kopije zasebnih ključev imetnikov potrdil za dešifriranje za napredna kvalificirana digitalna potrdila. Dešifrirni ključi imetnikov naprednih potrdil se hranijo v bazi podatkov v šifrirani obliki.

Overitelj izdeluje varnostne kopije baze in sistemskih datotek enkrat dnevno.

6.2.5 Arhiviranje zasebnega ključa

Glej 6.2.4 Varnostno kopiranje zasebnih ključev.

6.2.6 Prenos zasebnega ključa v kriptografski modul in iz njega

Zasebni ključ overitelja se prenese v nov strojni kriptografski modul v prisotnosti vsaj dveh pooblaščenih oseb, ki se morata identificirati s pametno kartico strojnega kriptografskega modula in geslom kartice, ter odobriti prenos, oziroma uporabo na novem strojnem kriptografskem modulu. Glej tudi poglavje 6.2.4.

Uporabniški zasebni ključi za dešifriranje, ki so ustvarjeni v overiteljevem aplikativnem programskem modulu za šifriranje CA, se prenesejo v naročnikov kriptografski modul z uporabo protokola PKIX-CMP.

Uporabniški zasebni ključ za podpisovanje se ustvari v programskem modulu za šifriranje na strani imetnika potrdil, na pametni kartici ali sistemu za oddaljen podpis.

6.2.7 Hranjenje overiteljevega zasebnega ključa v kriptografskem modulu

Overiteljevi ključi se uporabljajo v strojnem kriptografskem modulu v katerem so bili tvorjeni, oziroma na katerem je bila odobrena in omogočena uporaba kot je določeno v poglavju 6.2.6 Prenos zasebnega ključa v kriptografski modul in iz njega.

6.2.8 Postopek za aktiviranje zasebnega ključa

Overiteljev zasebni ključ za podpisovanje se aktivira ob zagonu CA-aplikacije. Za aktiviranje je potrebna pametna kartica za strojni modul za šifriranje ter geslo uporabnika v funkciji CA glavnega uporabnika.

Uporabniki morajo uporabljati ustrezno PKI-aplikacijo, ki preveri istovetnost uporabnika z geslom ter po uspešnem preverjanju istovetnosti aktivira zasebni ključ.

Za aktiviranje podpisnih ključev na QSCD napravi za oddaljen elektronski podpis je obvezna uporaba osebnega gesla za aktiviranje podpisnega ključa in predhodna močna dvo-faktorska (2FA) avtentikacija. Močna dvo-faktorska (2FA) avtentikacija mora izpolnjevati zahteve oziroma biti ekvivalentna nivoju "srednji" ali "visoki" Uredbe eIDAS.

6.2.9 Postopek za deaktiviranje zasebnega ključa

Zasebni ključ overitelja za podpisovanje se deaktivira z zaustavitvijo aplikativne programske opreme CA.

Uporabniki morajo uporabljati PKI-aplikacije, ki deaktivirajo zasebni ključ, ko se uporabniki odjavijo. Ključi za podpis na QSCD napravi za oddaljen podpis morajo biti deaktivirani takoj po izvedenem podpisu.

6.2.10 Postopek za uničenje zasebnega ključa

Ob zaustavitvi aplikativne opreme CA se uničijo vsi ključi, ki se nahajajo v sistemskem spominu.

Uporabniki morajo uporabljati PKI-aplikacije, ki uničijo ključe, ki se nahajajo v spominu, ter ključe, ki se nahajajo na disku, z operacijo brisanja.

6.2.11 Stopnja varnosti kriptografskih modulov

Glej 6.2.1 Standardi za kriptografski modul.

6.3 Ostali vidiki upravljanja s pari ključev

6.3.1 Arhiviranje javnega ključa

Overitelj arhivira svoj javni verifikacijski šifrirni ključ in imetniške javne ključe na način in po postopkih, kot je opisano v poglavju 5.5 Arhiviranje podatkov.

6.3.2 Obdobje veljavnosti ključev in potrdil

Veljavnost javnih in zasebnih kriptografskih ključev overitelja:

- overiteljev javni ključ za overjanje: 20 let;
- overiteljev zasebni ključ za podpisovanje: 20 let;
- imetniški javni ključ za overjanje: 5 let;
- imetniški zasebni ključ za podpisovanje: 5 let;
- imetniški javni ključ za šifriranje: 5 let;
- imetniški zasebni ključ za dešifriranje: ni omejitve;
- javni ključ potrdil za spletne strežnike: 3 leta

Overitelj lahko kadarkoli prilagodi veljavnost posameznih uporabniških šifrirnih ključev glede na politiko, vrsto digitalnega potrdila ali komercialno ponudbo.

6.4 Aktivacijski podatki

6.4.1 Generiranje in instalacija aktivacijskih podatkov

Referenčne številke (angl. reference numbers) in avtorizacijske kode (angl. authorization codes) se ustvarijo v overiteljevi aplikativni programski opremi CA. Referenčne številke in avtorizacijske kode so edinstvene za vsako digitalno potrdilo. Avtorizacijske kode so ustvarjene po nepredvidljivem algoritmu.

Imetniki potrdil uporabljajo osebna gesla za aktiviranje modulov za šifriranje. Osebno geslo za dostop do zasebnega ključa naj izpolnjuje minimalno sledeče kriterije:

- dolžina najmanj 9 znakov;
- vsebuje naj velike in male črke, številke ter posebne znake;
- naj ne vsebuje besed iz slovarja.

Gesla niso shranjena v overiteljevi PKI-aplikaciji.

6.4.2 Zaščita aktivacijskih podatkov

Avtorizacijske kode in referenčne številke se varno ustvarijo v overiteljevi aplikativni programski opremi CA in shranijo v bazi v šifrirani obliki.

Referenčna številka in avtorizacijska koda se dostavita naročniku po različnih komunikacijskih kanalih.

Avtorizacijska koda se dostavi s priporočeno pisemsko pošiljko ali s pomočjo storitve varnega elektronskega vročanja. V primeru, da se avtorizacijska koda dostavi s priporočeno pisemsko pošiljko, bo tiskana na slepo kuverto pod nadzorom osebja overitelja.

Referenčna številka se dostavi prek elektronske pošte ali s priporočeno pisemsko pošiljko. V primeru, da se referenčna številka dostavi s priporočeno pisemsko pošiljko, bo tiskana na slepo kuverto pod nadzorom osebja overitelja.

Uporabniki morajo do prevzema digitalnega potrdila skrbno varovati vse inicializacijske podatke.

Uporabnikom, ki opravijo prevzem na pametno kartico na podlagi identifikacije z veljavnim kvalificiranim potrdilom POŠTA®CA, kot je opisano v tretjem odstavku poglavja 4.4.1, se inicializacijski podatki ne dostavijo. Podatki se varno hranijo v informacijskem sistemu overitelja do uporabnikovega zahtevka za prevzem, ko se s pomočjo spletne storitve posredujejo programski opremi za prevzem potrdil na zunanje kriptografske naprave.

Osebna gesla (PIN pametne kartice) in kode za odklepanje pametnih kartic (PUK pametne kartice) se varno ustvarijo v overiteljevi aplikativni programski opremi. Imetniku se dostavijo s priporočeno pisemsko pošiljko ali s pomočjo storitve varnega elektronskega vročanja. V primeru, da se osebna gesla dostavijo s priporočeno pisemsko pošiljko, so tiskana na slepo kuverto pod nadzorom osebja overitelja.

Overitelj ne hrani osebnih gesel imetnikov.

Kode za odklepanje pametnih kartic se varno hranijo v šifrirani obliki v overiteljevi bazi in se lahko dostavijo imetniku na njegovo zahtevo. Kode za odklepanje pametnih kartic se dešifrirajo pod nadzorom in z odobritvijo dveh pooblaščenih oseb overitelja, ter tiskajo na slepe kuverte, ki se dostavijo imetniku s priporočeno pošiljko.

6.4.3 Drugi vidiki aktivacijskih podatkov

Gesla operativnega osebja ter gesla pametnih kartic strojnega kriptografskega modula se menjajo ob vsaki menjavi osebe, zadolžene za izvajanje funkcije.

6.5 Varnostne zahteve za računalnike

6.5.1 Specifične tehnične varnostne zahteve za računalnike

Overitelj ima na sistemski programski opremi in aplikativni programski opremi CA vzpostavljene tehnične varnostne kontrole, ki vključujejo:

- nadzor dostopa do CA-postopkov in dodeljenih pooblastil za opravljanje nalog;
- razdelitev nalog za posamezno funkcijo;
- uporabo šifrirnih modulov za hranjenje kriptografskih ključev osebja overitelja;
- šifrirane seje med aplikativno programsko opremo CA in naročniško PKI-aplikacijo overitelja;
- šifrirano bazo podatkov overitelja;
- varen arhiv overitelja in uporabniških kriptografskih ključev ter varnostnih beležk;
- varnostne beležke vseh varnostno veljavnih dogodkov;
- vzpostavljene mehanizme restavriranja sistema, šifrirnih ključev overitelja ter baze podatkov overitelja.

6.5.2 Nivo varnostne zaščite računalnikov

Strežniški operacijski sistemi overitelja so komercialni produkti dodatno varnostno okrepljeni za zagotavljanje varnega izvajanja postopkov overitelja.

6.6 Tehnični nadzor življenjskega cikla overitelja

6.6.1 Nadzor razvoja sistema

Overiteljeva CA-programska oprema je verificirana po kriterijih EAL4+.

6.6.2 Upravljanje varnosti

Overitelj ima vzpostavljene postopke za upravljanje problemov, sprememb in konfiguracij za vse komponente svoje infrastrukture.

Overitelj ima vzpostavljene postopke za reden nadzor celovitosti programske opreme. Kontrola celovitosti se izvaja enkrat tedensko.

6.6.3 Upravljanje varnosti čez življenjski cikel

Ni predpisano.

6.7 Varnostne kontrole na ravni računalniškega omrežja

Računalniško mrežo overitelja sestavlja več ločenih segmentov, na katerih se nahajajo strežniki in delovne postaje. Segmenti so med seboj ločeni s požarnim zidom. Računalniška mreža je prek požarnega zidu povezana z računalniškim omrežjem Pošte Slovenije. Varnostna pravila na požarnem zidu dovoljujejo prehod samo protokolom, potrebnim za dostop do CA-servisov, ter varnostni nadzor in upravljanje strežnikov.

6.8 Časovno žigosanje

Ni predpisano.

7 PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL

7.1 Profil digitalnih potrdil

7.1.1 Različica digitalnih potrdil

Overitelj izdaja digitalna potrdila X.509 Version 3 v skladu s priporočili PKIX. Digitalna potrdila vsebujejo naslednja osnovna polja:

Naziv atribura	**Opis**
Signature *(signature)*	Overiteljev podpis
Issuer *(issuer)*	Edinstveno razločevalno ime overitelja
Validity *(thisUpdate, nextUpdate)*	Datum aktiviranja in poteka veljavnosti digitalnega potrdila
Subject *(subject)*	Edinstveno razločevalno ime imetnika digitalnega potrdila
Subject Public Key Info *(subjectPublicKeyInfo)*	Oznaka algoritma ključa
Version *(version)*	Različica digitalnega potrdila X.509
Serial Number *(serialNumber)*	Edinstvena serijska številka

7.1.2 Razširitvena polja

Razširitvena polja so namenjena uporabi dodatnih atributov v digitalnih potrdilih X.509 v3. Standardna razširitvena polja so definirana v skladu z RFC5280, ki dovoljuje tudi definiranje in dodajane lastnih razširitvenih polj za potrebe overiteljev potrdil. Dodana posebna razširitvena polja za potrebe overitelja so definirana v poglavjih 7.1.2.2 do 7.1.2.5.

7.1.2.1 Standardna razširitvena polja

Naziv atributa	Kritičen	Opis
Authority Key Identifier (authorityKeyIdentifier)		odtis javnega ključa overitelja POŠTA®CA s katerim je podpisano potrdilo
Subject Key Identifier (subjectKeyIdentifier)		odtis imetnikovega javnega ključa
Key Usage (keyUsage)	da	Kot je opisano v 6.1.7
Private Key Usage Period (privateKeyUsagePeriod)		Kot je opisano v 6.3.2
Certificate Policies (certificatePolicies)		OID oznaka vrste digitalnega potrdila v skladu s poglavjem 1.2 in URI objave pravil delovanja. Glej tudi poglavje 7.1.2.4.
CRL Distribution Points (cRLDistributionPoints)		Naslovi na katerih je objavljen register preklicanih potrdil
Policy Mappings (policyMappings)		Uporabljeno v digitalnem potrdilu za medsebojno priznavanje
Subject Alternative Name (subjectAlternativeName)		Alternativno ime imetnika v skladu z RFC5280 (Elektronski poštni naslov, domensko ime strežnika, ...)
Issuer Alternative Name (issuerAlternativeName)		Se ne uporablja
Subject Directory Attributes (subjectDirectoryAttributes)		Se ne uporablja
Name Constraints (nameConstraints)	da	Uporabljeno v digitalnem potrdilu za medsebojno priznavanje
Basic Constraints (basicConstraint)		Doda CA aplikacija
Policy Constraints (policyConstraints)		Uporabljeno v digitalnem potrdilu za medsebojno priznavanje
Qualified Certificate Statements qCStatements		Oznaka kvalificiranega potrdila v skladu z ETSI TS 101 862. Glej tudi poglavje 7.1.2.5.
Extended Key Usage (extKeyUsage)		Razširjena uporaba, neobvezen atribut, uporabi se lahko v glede na zahteve aplikativnega okolja (glej tudi 7.1.2.2)

7.1.2.2 Posebna razširitvena polja POŠTA®CA

Naziv atributa	Kritičen	OID	Sintaksa	Opis
psdavcna		1.3.6.1.4.1.15284.10.2.1	IA5String	Davčna številka imetnika

Razširitveno polje psdavcna (OID 1.3.6.1.4.1.15284.10.2.1) vsebuje davčno številko imetnika. V primeru, da imetnik nima davčne številke izdane v Sloveniji, je v polje psdavcna vpisana 9-mestna številka, ki jo določi overitelj.

Digitalna potrdila lahko v okviru posameznega komercialnega produkta vsebujejo dodatna razširitvena polja. Dodatna razširitvena polje so po potrebi opredeljena v opisu komercialnega produkta.

7.1.2.3 Posebna razširitvena polja Zavoda

Digitalna potrdila, ki jih izdaja overitelj POŠTA®CA po pričujoči politiki, vsebujejo sledeča razširitvena polja za potrebe Zavoda:

Identifikacijska oznaka	Oblika zapisa	Ime podatka vsebovanega v razširitvenem polju
1.3.6.1.4.1.29715.1.1.1	IA5STRING	ZZZS števila
1.3.6.1.4.1.29715.1.1.2	IA5STRING	Števila izvoda KZZ/PK
1.3.6.1.4.1.29715.1.1.3	UTF8STRING	Priimek 1
1.3.6.1.4.1.29715.1.1.4	UTF8STRING	Vezaj priimek
1.3.6.1.4.1.29715.1.1.5	UTF8STRING	Priimek 2
1.3.6.1.4.1.29715.1.1.6	UTF8STRING	Ime 1
1.3.6.1.4.1.29715.1.1.7	UTF8STRING	Vezaj ime
1.3.6.1.4.1.29715.1.1.8	UTF8STRING	Ime 2
1.3.6.1.4.1.29715.1.1.9	IA5STRING	Datum rojstva
1.3.6.1.4.1.29715.1.1.10	IA5STRING	Spol
1.3.6.1.4.1.29715.1.1.11	IA5STRING	IVZ številka imetnika
1.3.6.1.4.1.29715.1.1.12	IA5STRING	EMŠO imetnika
1.3.6.1.4.1.29715.1.1.13	IA5STRING	Identifikacijska št. nosilca (OE)
1.3.6.1.4.1.29715.1.1.14	IA5STRING	Številka izdajatelja kartice
1.3.6.1.4.1.29715.1.1.15	IA5STRING	Vrsta digitalnega potrdila (PK-KDP za kvalificirana digitalna potrdila izdana na PK)

7.1.2.4 Razširitveno polje certificatePolicies

Razširitveno polje *certificatePolicies* digitalnih potrdil vsebuje identifikacijo oznako overitelja POŠTA®CA in identifikacijsko oznako politik kvalificiranih digitalnih potrdil v skladu z ETSI EN 319 411-2 V1.1.1.

Identifikacijske oznake politik digitalnih potrdil overitelja POŠTA®CA so registrirane pod korenskim OID 1.3.6.1.4.1.15284. Navedene so v poglavju 1.2.

Standardna in napredna kvalificirana potrdila izdana na QSCD napravi, z obvezno uporabo QSCD naprave ali za uporabo na oddaljeni QSCD napravi, vsebujejo ETSI EN 319 411-2 V1.1.1 identifikacijsko oznako politike qcp-natural-qscd (0.4.0.194112.1.2).

Ostala kvalificirana digitalna potrdila za elektronski podpis vsebujejo ETSI EN 319 411-2 identifikacijsko oznako politike qcp-natural (0.4.0.194112.1.0).

7.1.2.5 Razširitveno polje qCStatements

Razširitveno polje *qCStatements* (1.3.6.1.5.5.7.1.3) vsebuje oznake kvalificiranih potrdil v skladu z ETSI EN 319 412-5 .

Razširitveno polje *qCStatements* v kvalificiranih digitalnih potrdilih , izdanih na QSCD napravi, ali z obvezno uporabo pametne QSCD naprave ali za uporabo na oddaljeni QSCD napravi vsebuje oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-esign (0.4.0.1862.1.6.1)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

Razširitveno polje *qCStatements* v ostalih kvalificiranih potrdilih vsebuje oznako:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-esign (0.4.0.1862.1.6.1)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)

7.1.3 Identifikacijske oznake (angl. object identifiers) algoritmov

Algoritem	Identifikacijska oznaka
SHA-1 With RSA Encryption	1.2.840.113549.1.1.5
SHA256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1.2.840.113549.1.1

7.1.4 Oblike imen

Overiteljeva digitalna potrdila vsebujejo polno razločevalno ime overitelja in imetnika potrdila v poljih »issuer name« ter »subject name«. Razločevalna imena so v obliki X.501 »printable string«.

7.1.5 Omejitve imen

Overitelj uporablja polje »*nameConstraints*« v medsebojnih digitalnih potrdilih v skladu s priporočili PKIX Part 1.

7.1.6 Identifikacijska oznaka digitalnega potrdila

Vsako digitalno potrdilo vsebuje eno ali več identifikacijskih oznak. Overitelj uporablja polje »*certificatePolicies*« za označevanje vrste digitalnih potrdil.

7.1.7 Uporaba omejitve imen

Overitelj uporablja polje *»policyConstraints«* v medsebojnih digitalnih potrdilih (angl. cross-certificates) v skladu s priporočili PKIX Part 1.

7.1.8 Policy qualifiers

Overitelj uporablja polje *»certificatePolicies policy qualifiers«* za objavo spletnega naslova repozitorija pravil delovanja.

7.1.9 Procesiranje oznake kritičnosti razširitvenih polj digitalnega potrdila

Uporabniške aplikacije morajo procesirati razširitvena polja digitalnega potrdila, označena kot kritična, v skladu s priporočili PKIX.

7.2 Profil registra preklicanih digitalnih potrdil

7.2.1 Različica

Overitelj izdaja X.509 Version 2 CRL in ARL v skladu s priporočili PKIX Part 1. Liste preklicanih potrdil vsebujejo naslednja osnovna polja:

Naziv atributa	Opis
Version	V2
Signature	Overiteljev podpis
Issuer	Razločevalno ime POŠTA®CA
thisUpdate	Čas izdaje liste
nextUpdate	Čas izdaje naslednje liste
revokedCertificate	Serijske številke preklicanih digitalnih potrdil

7.2.2 CRL and CRL entry extensions

Overitelj uporablja X.509 Version 2 CRL in ARL-razširitve v skladu s priporočili PKIX Part 1, kot je podano v naslednji tabeli:

cRLNumber	Doda CA-aplikacija
reasonCode	Razlog preklica se ne objavlja
holdInstructionCode	Ni podprto
invalidityDate	Doda CA-aplikacija, če je podatek vsebovan v vlogi
issuingDistributionPoint	Doda CA-aplikacija
certificateIssuer	Ni podprto
deltaCRLIndicator	Ni podprto

7.3 Profil OCSP

Se ne uporablja.

8 PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA

8.1 Pogostost ali okoliščine izvajanja nadzornih pregledov

Preverjanje skladnosti z zakonodajo izvaja pristojna inšpekcijska služba.

Overitelj izvaja redne notranje preglede delovanja.

8.2 Pogoji za izvajalca nadzora

Ni predpisano. Overitelj določi izvajalca notranjih pregledov po svoji presoji.

8.3 Relacija med izvajalcem nadzora in overiteljem

Glej 8.1 in 8.2.

8.4 Področja nadzora

Pristojna inšpekcijska služba izvaja preverjanje skladno z zakonodajo.

Notranji nadzorni pregledi ugotavljajo skladnost delovanja overitelja s pričujočo politiko overitelja POŠTA®CA ter veljavno zakonodajo.

8.5 Postopki po opravljenem nadzornem pregledu

V primeru ugotovljenih nepravilnosti bo overitelj pripravil načrt za odpravo pomanjkljivosti in po izvedbi poročilo o odpravi pomanjkljivosti.

8.6 Prejemniki in objava ugotovitev

Izvajalec notranjega nadzora posreduje ugotovitve upravnemu svetu overitelja. Upravni svet se po svoji presoji odloči, ali je potrebno o ugotovitvah obvestiti imetnike in tretje osebe. Obvestilo imetnikom in tretjim stranem objavi v skladu s poglavjem 9.11.

9 OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1 Cenik

9.1.1 Cena izdaje in upravljanja digitalnih potrdil

Cena izdaje in upravljanja digitalnih potrdil je določena v ceniku objavljenem na spletni strani http://postarca.posta.si.

9.1.2 Cena dostopa do digitalnih potrdil v javnem imeniku

Dostop do javnega imenika digitalnih potrdil je brezplačen.

9.1.3 Cena dostopa do registra preklicanih potrdil

Dostop do registra preklicanih potrdil je brezplačen.

9.1.4 Cena ostalih storitev

Cena ostalih storitev overitelja je določena v ceniku objavljenem na spletni strani http://postarca.posta.si, oziroma v pogodbi o uporabi storitev overitelja POŠTA®CA.

9.1.5 Pravica vračila

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.

9.2 Finančna odgovornost

9.2.1 Zavarovanje odgovornosti

Overitelj ima zavarovano svojo odgovornost v skladu z ZEPEP in veljavno Uredbo.

Overitelj jamči za vrednost posameznega pravnega posla do višine navedene v poglavju 9.8 Omejitve odgovornosti overitelja.

9.2.2 Druge oblike zavarovanja

Ni predpisano.

9.2.3 Zavarovanje ali jamstva za končne uporabnike

Uporabniki in tretje osebe so izključno odgovorni za zagotovitev ustreznega kritja zavarovanja ali garancije glede na njihovo uporabo digitalnega potrdila.

9.3 Zaupnost poslovnih informacij

9.3.1 Obseg zaupnih poslovnih informacij

Vse podatki, ki jih zbira, ustvari, posreduje, in vzdržuje overitelj se štejejo za zaupne, razen podatkov navedenih v poglavju 9.3.2.

9.3.2 Informacije izven obsega zaupnih poslovnih informacij

Informacije, objavljene v digitalnih potrdilih, listah preklicanih potrdil, politiki overitelja in druge informacije objavljenih v javnih repozitorijih overitelja (glej poglavje 2.1), se ne štejejo za zaupne.

9.3.3 Odgovornost za zagotavljanje zaupnosti poslovnih informacij

Overitelj je odgovoren za zagotavljanje zaupnosti poslovnih informacij v skladu z veljavnimi predpisi na območju Republike Slovenije.

9.4 Varovanje osebnih podatkov

9.4.1 Načrt zagotavljanja varovanja osebnih podatkov

V skladu z navedbami v poglavju 9.3 in ostalih poglavjih 9.4.

9.4.2 Obseg varovanih osebnih podatkov

Vsi podatki, pridobljeni, ustvarjeni ali posredovani, imajo status varovanih osebnih podatkov in jih overitelj sporoča le na zahtevo imetnika potrdila in na pisno zahtevo sodišča, če je proti imetniku potrdila uveden sodni postopek, ter v drugih primerih, ki jih določa veljavni Zakon o varstvu osebnih podatkov in na njegovi podlagi izdanimi predpisi. Izjema so digitalna potrdila in register preklicanih potrdil.

Overitelj in imetnik sta dolžna zagotavljati visoko raven varnostnih ukrepov, ki bodo zagotovili minimiziranje tveganj neavtoriziranega dostopa do podatkov, spreminjanja podatkov in izgube podatkov.

9.4.3 Osebni podatki, ki se ne obravnavajo kot zaupni

Informacije, objavljene v digitalnih potrdilih, listah preklicanih potrdil, politiki overitelja in druge informacije objavljenih v javnih repozitorijih overitelja (glej poglavje 2.1), se ne štejejo za zaupne.

9.4.4 Odgovornost glede varovanja osebnih podatkov

Kot navedeno v poglavju 9.3.3.

9.4.5 Dovoljenje za uporabo osebnih podatkov

Overitelj uporablja osebne podatke samo za namene, za katere je dal imetnik soglasje v postopku registracije.

9.4.6 Posredovanje osebnih podatkov v sodnih in upravnih postopkih

Glej poglavje 9.4.2.

9.4.7 Druge okoliščine posredovanja osebnih podatkov

Ni predpisano.

9.5 Zaščita intelektualne lastnine

Ni predpisano.

9.6 Odgovornosti in jamstva

9.6.1 Odgovornosti in jamstva overitelja

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

Overitelj v splošnem jamči za:

- izvajanje vseh postopkov v skladu z navedbami v pričujoči politiki overitelja POŠTA®CA, 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;
- odobritev ali zavrnitev vloge;
- podpis in izdajo digitalnega potrdila naročnikom;
- objavo digitalnega potrdila v javnem imeniku;
- 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.

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

Overitelj odgovarja in jamči za škodo tretjim osebam, ki se upravičeno zanašajo na digitalna potrdila, ki ga 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.

Overitelj POŠTA®CA zagotavlja stalno dostopnost svojih storitev, in sicer 24ur vse dni v letu s sledečimi izjemami:

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

9.6.2 Odgovornost in jamstva prijavne službe

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

Registracijska pisarna overitelja jamči za:

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

9.6.3 Odgovornost in jamstva imetnikov digitalnih potrdil

Imetnik potrdil je dolžan:

- varovati osebno geslo in zasebne dele ključev. Imetnik potrdila osebnega gesla 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 namizna ob odsotnosti;

    - odstranitev pametne kartice iz čitalca pametnih kartic ob odsotnosti;
- v roku poravnavati vse finančne obveznosti do overitelja;
- digitalno potrdilo za spletne strežnike uporabljati le za SSL ali TLS protokol na spletnem 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 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

Ni relevantno.

9.7 Zanikanje 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.

9.8 Omejitve odgovornosti overitelja

Overitelj zanika kakršno koli odgovornost vseh vrst, za nadomestila, škodo ali druge terjatve ali obveznosti katere koli vrste, ki izhajajo iz škod, pogodb ali it kateri koli drugih razlogov v zvezi s katero koli storitvijo povezano z izdajo, uporabo, ali zanašanja na digitalno potrdilo ki ga je izdal overitelj in ki presega vrednost navedene v spodnji tabeli:

Vrednost	Vrsta digitalnega potrdila
	Kvalificirana potrdila za zaposlene pri pravnih osebah
20.800,00 EUR	POŠTA®CA – Napredna kvalificirana potrdila
4.100,00 EUR	POŠTA®CA – Kvalificirana potrdila z obvezno uporabo QSCD naprave
410,00 EUR	POŠTA®CA – Kvalificirana potrdila
10.400,00 €	POŠTA®CA – Kvalificirana potrdila, izdana na QSCD napravi
10.400,00 €	POŠTA®CA – Kvalificirana potrdila, izdana na oddaljeni QSCD napravi
	Kvalificirana potrdila za fizične osebe
4.100,00 EUR	POŠTA®CA – Napredna kvalificirana potrdila
830,00 EUR	POŠTA®CA – Kvalificirana potrdila z obvezno uporabo QSCD naprave
200,00 EUR	POŠTA®CA – Kvalificirana potrdila
2.000,00 EUR	POŠTA®CA – Kvalificirana potrdila, izdana na QSCD napravi
2.000,00 EUR	POŠTA®CA – Kvalificirana potrdila, izdana na oddaljeni QSCD napravi
2.100 EUR	POŠTA®CA – Kvalificirana potrdila izdana na profesionalni kartici v sistemu kartice zdravstvenega zavarovanja
	Normalizirana potrdila
2.000,00 EUR	POŠTA®CA – Normalizirana potrdila za spletne strežnike
8.300,00 EUR	POŠTA®CA – Normalizirana potrdila za pravne osebe z obvezno uporabo QSCD naprave
2.000,00 EUR	POŠTA®CA – Normalizirana potrdila za pravne osebe
8.300,00 EUR	POŠTA®CA – Normalizirana potrdila za pravne osebe, izdana na QSCD napravi

Glej tudi poglavje 9.7.

9.9 Poravnava škode

Glej poglavja 9.2, 9.7 in 9.8 .

9.10 Začetek in prenehanje veljavnosti

9.10.1 Začetek veljavnosti

Pričujoča Politika POŠTA®CA začne veljati naslednji dan po podpisu.

9.10.2 Prenehanje veljavnosti

Veljavnost politike Politika POŠTA®CA ni časovna omejena in velja do uveljavitve nove verzije, oziroma do prenehanja delovanja overitelja.

9.10.3 Učinek in posledice prenehanja veljavnosti

Po prenehanju veljavnosti politike Politika POŠTA®CA zaradi objave nove verzije imetniki praviloma uporabljajo obstoječa digitalna potrdila v skladu z določili politike Politika POŠTA®CA, po kateri so bila izdana. V primeru, da zaradi spremenjenih okoliščin to ne bo več mogoče, bo overitelj ob izdaji nove verzije Politike POŠTA®CA o tem preko svoje spletne strani, ali pisno, ali preko elektronske pošte obvestil imetnike .

9.11 Obvestila in komuniciranje z udeleženci

Obvestila imetnikom so objavljena na spletni strani navedeni v poglavju 2.1.

9.12 Spreminjanje dokumenta

9.12.1 Postopek uveljavitve sprememb

Overitelj bo izvajal uredniške in tipografske popravke katerega koli dela tega dokumenta in skrbel za njihovo objavo, brez posebnega obvestila. Verzije z uredniškimi in tipografskimi popravki bodo objavljene na spletnih straneh overitelja sedem (7) dni pred nastopom veljavnosti popravkov.

Vse ostale spremembe javnega dela notranjih pravil overitelja (nov dokument) bodo objavljene vsaj deset (10) dni pred nastopom veljavnosti novega dokumenta. O teh spremembah bo obveščeno pristojno ministrstvo v skladu z obstoječo zakonodajo. Imetniki potrdil, druge zainteresirane osebe in medsebojno priznani overitelji bodo o spremembah obveščeni na spletni strani overitelja.

9.12.2 Postopek obveščanja in rok za pripombe

Glej poglavje 9.12.1.

9.12.3 Spremembe, ki zahtevajo novo identifikacijsko oznako politike

Overitelj po lastni presoji odloči, ali so spremembe vsebine politike overitelja digitalnih potrdil takšne, da zahtevajo objavo nove Politike POŠTA®CA z novo identifikacijsko oznako.

9.13 Reševanje sporov

Pogodbeni stranki si bosta prizadevali vse morebitne spore rešiti sporazumno, skladno s področno zakonodajo upoštevajoč načela vestnosti in poštenja.

Če do sporazumne rešitve spora ne pride, je za vse spore pristojno sodišče v Mariboru.

9.14 Veljavna zakonodaja

Overitelj deluje v skladu z veljavnimi predpisi na območju Republike Slovenije navedenimi v poglavju 9.15. Skladnost s pravnimi akti.

9.15 Skladnost s pravnimi akti

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, Uradni list Evropske unije, L 257/73)
- Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 98/2004 – UPB-1, 61/2006-ZEPT)
- Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000, 2/2001, 86/2006);
- Zakonom o varstvu osebnih podatkov (Ur.l. RS, št. 94/2007-UPB1 -ZVOP-1);
- drugimi veljavnimi predpisi na območju Republike Slovenije.

9.16 Splošne določbe

9.16.1 Ostali obvezujoči dokumenti

Ni predpisano.

9.16.2 Prenos pravic in obveznosti

Pravica uporabe digitalnih potrdil ni prenosljiva.

9.16.3 Spremembe okoliščin delovanja

Če postane zaradi spremenjenih okoliščin delovanja ali spremembe zakonodaje del pričujočega dokumenta nepravilen ali neveljaven, ostanejo ostali deli veljavni vse dokler se ne objavi sprememba. Postopek uveljavitve spremembe je opisan v poglavju 9.12.1 Postopek uveljavitve sprememb.

9.16.4 Uveljavljanje (povračila stroškov v primeru sporov in izjeme)

Zahtevki povračila stroškov v primeru sporov so 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 dokument, ali dogovoru, se rok za izvršitev ustrezno podaljša.

9.17 Ostale določbe

Oblika in vsebina javne politike overitelja je usklajena z:

- RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.