



POŠTA SLOVENIJE, d.o.o.

POŠTA<sup>®</sup> CA

Slomškovo trg 10, 2500 Maribor

Tel.: +386 (0)2 449 2346

<http://postarca.posta.si/>

[info.postarca@posta.si](mailto:info.postarca@posta.si)

**E-KLJUČ**

# POLITIKA POŠTA<sup>®</sup> CA

## ZA KVALIFICIRANA DIGITALNA POTRDILA ZA FIZIČNE OSEBE

### Javni del notranjih pravil delovanja

**POŠTA<sup>®</sup> CA** - kvalificirana digitalna potrdila z dvema paroma ključev za fizične osebe in z obvezno uporabo pametne kartice

**(Napredno kvalificirano digitalno potrdilo)**

**[PolicyIdentifier OID 1.3.6.1.4.1.15284.1.1.1.2.1.0]**

**POŠTA<sup>®</sup> CA** - kvalificirana digitalna potrdila z enim parom ključev za fizične osebe in z obvezno uporabo pametne kartice

**(Standardno kvalificirano digitalno potrdilo z obvezno uporabo pametne kartice)**

**[PolicyIdentifier OID 1.3.6.1.4.1.15284.1.1.1.2.2.0]**

**POŠTA<sup>®</sup> CA** - kvalificirana digitalna potrdila z enim parom ključev za fizične osebe

**(Standardno kvalificirano digitalno potrdilo)**

**[PolicyIdentifier OID 1.3.6.1.4.1.15284. 1.1.2.2.2.0]**



## Stanje dokumenta

Izdaje politike POŠTA <sup>®</sup> CA za kvalificirana digitalna potrdila za fizične osebe	
Oznaka izdaje	Opis izdaje
Verzija 1	Politika POŠTA <sup>®</sup> CA za kvalificirana digitalna potrdila za fizične osebe <b>OID 1.3.6.1.4.1.15284.1.1.1.2.1.0;</b> <b>OID 1.3.6.1.4.1.15284.1.1.1.2.2.0;</b> <b>OID 1.3.6.1.4.1.15284. 1.1.2.2.2.0</b> Datum izdaje: 16.4.2003



<b>PREGLED</b>	<b>VSEBINE</b>
<b>1 PREDSTAVITEV .....</b>	<b>4</b>
1.1 PREGLED .....	4
1.2 IDENTIFIKACIJSKI PODATKI .....	7
1.3 SUBJEKTI IN NAMEN UPORABE .....	8
1.4 KONTAKTNE OSEBE .....	10
<b>2 SPLOŠNA DOLOČILA .....</b>	<b>11</b>
2.1 OBVEZNOSTI .....	11
2.2 ODGOVORNOST .....	12
2.3 FINANČNA ODGOVORNOST .....	13
2.4 INTERPRETACIJA IN USKLAJENOST .....	14
2.5 CENIK .....	14
2.6 OBJAVE INFORMACIJ IN JAVNI IMENIK .....	14
2.7 PREVERJANJE SKLADNOSTI .....	15
2.8 VAROVANJE PODATKOV .....	15
<b>3 PREVERJANJE ISTOVETNOSTI .....</b>	<b>16</b>
3.1 PRVA REGISTRACIJA .....	16
3.2 PREVERJANJE ISTOVETNOSTI OB RUTINSKI MENJAVI KLJUČEV .....	17
3.3 PREVERJANJE ISTOVETNOSTI ZA PONOVO IZDAJO KLJUČEV PO PREKLICU POTRDILA .....	18
3.4 PREVERJANJE ISTOVETNOSTI OB ZAHTEVI ZA PREKLIC POTRDILA .....	18
<b>4 POGOJI ZA DELOVANJE .....</b>	<b>19</b>
4.1 VLOGA ZA IZDAJO POTRDILA .....	19
4.2 IZDAJA POTRDIL .....	19
4.3 PREVZEM POTRDILA .....	19
4.4 PREKLIC POTRDILA .....	20
4.5 POSTOPKI VARNOSTNIH PREGLEDOV SISTEMA .....	23
4.6 ARHIVIRANJE PODATKOV .....	24
4.7 OBNOVA POTRDILA .....	25
4.8 OKREVALNI NAČRT .....	25
4.9 PRENEHANJE DELOVANJA OVERITELJA .....	25
4.10 DODATNI POGOJI DELOVANJA .....	26
<b>5 VARNOSTNI NADZOR PROSTOROV, OPREME, POSTOPKOV IN OSEBJA .....</b>	<b>27</b>
5.1 FIZIČNI NADZOR .....	27
5.2 NOTRANJA ORGANIZACIJA IN NADZOR OSEBJA .....	28
5.3 NADZOR OSEBJA .....	30
<b>6 TEHNIČNE VARNOSTNE ZAHTEVE .....</b>	<b>32</b>
6.1 TVORJENJE IN NAMESTITEV PARA KLJUČEV .....	32
6.2 ZAŠČITA ZASEBNEGA KLJUČA .....	33
6.3 OSTALI VIDIKI UPRAVLJANJA ŠIFRIRNIH KLJUČEV .....	35
6.4 AKTIVACIJSKI PODATKI .....	35
6.5 VARNOSTNE ZAHTEVE ZA RAČUNALNIKE .....	36
6.6 TEHNIČNI NADZOR RAZVOJA OVERITELJA .....	36
6.7 VARNOSTNE KONTROLE RAČUNALNIŠKE MREŽE .....	36
6.8 TEHNIČNE KONTROLE MODULOV ZA ŠIFRIRANJE .....	36
<b>7 PROFIL POTRDIL IN LIST PREKLICANIH POTRDIL .....</b>	<b>38</b>
7.1 PROFIL POTRDIL .....	38
7.2 PROFIL REGISTRA PREKLICANIH DIGITALNIH POTRDIL .....	39
<b>8 POSTOPKI Z DOKUMENTACIJO .....</b>	<b>41</b>
8.1 POSTOPKI SPREMINJANJA VSEBINE DOKUMENTACIJE .....	41
8.2 OBJAVLJANJE DOKUMENTACIJE .....	41
8.3 ODOBRAVANJE DOKUMENTA .....	41

# 1 PREDSTAVITEV

## 1.1 Pregled

V okviru POŠTE SLOVENIJE d.o.o., Maribor (v nadaljevanju: **organizacija**) deluje overitelj, Certifikatska agencija Pošte Slovenije, krajše POŠTA<sup>®</sup> CA (v nadaljevanju **overitelj**). POŠTA<sup>®</sup> CA izdaja različne vrste overjenih digitalnih potrdil (digitalna potrdila ter kvalificirana digitalna potrdila) različnim končnim uporabnikom (fizičnim osebam, pravnim osebam in fizičnim osebam, registriranim za opravljanje dejavnosti,...) v skladu z 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) in evropskimi direktivami. Varen elektronski podpis, overjen s kvalificiranim potrdilom, je v skladu s 15. členom Zakona o elektronskem poslovanju in elektronskem podpisu glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu.

Overitelj objavlja:

- pravila delovanja, opredeljena v izjavi o politiki delovanja (angl. Policy Disclosure Statement – v nadaljevanju: overiteljev PDS-dokument),
- splošna pravila poslovanja - politike za posamezne vrste kvalificiranih digitalnih potrdil, ki urejajo delovanje overitelja, imenovane tudi javni del notranjih pravil overitelja (angl. Certificate Practice Statement – v nadaljevanju: politika).

PDS-dokument je pripravljen v skladu s priporočili “ETSI TS 101 456 V1.2.1 (2002-04), Annex B: Model PKI disclosure statement“ in ga je mogoče pridobiti na spletni strani overitelja: <http://postarca.posta.si/dokumenti>.

Politika opisuje tehnične lastnosti in stopnjo varnosti overiteljeve infrastrukture ter postopke, ki jih overitelj uporablja za upravljanje infrastrukture in upravljanje kvalificiranih digitalnih potrdil. Politika vsebuje vse bistvene določbe, ki vplivajo na odnos med overiteljem in imetniki kvalificiranih digitalnih 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 2527). Politika vsebuje tudi poglavje RFC 2527, ki ne zavezujejo overitelja s komentarjem “*ni predpisano*”, ki označuje, da je bilo poglavje izključeno iz dokumenta po tehtni presoji overitelja. Na ta način se skuša zagotoviti primerljivost s politikami drugih overiteljev v Sloveniji in svetu.

Pričujoči dokument opisuje javni del notranjih pravil overitelja (politika overitelja), ki se nanaša na kvalificirana digitalna potrdila za fizične osebe. Opis pravil delovanja je namenjen vsem, ki potrebujejo informacije za oceno zaupanja v kvalificirana digitalna potrdila, ki jih izdaja overitelj. Za dodatne informacije, ki niso podane v politiki, se lahko zainteresirani obrnejo na kontaktne osebe, navedene v poglavju 1.4.

Overitelj izdaja naslednje vrste kvalificiranih digitalnih potrdil za fizične osebe:

- kvalificirano digitalno potrdilo z dvema paroma ključev in obvezno uporabo pametne kartice, skladne s FIPS140-1 level 2, EAL4 ali višjim nivojem – **Napredno kvalificirano digitalno potrdilo**;

- kvalificirano digitalno potrdilo z enim parom ključev in obvezno uporabo pametne kartice, skladne s FIPS140-1 level 2, EAL4 ali višjim nivojem – **Standardno kvalificirano digitalno potrdilo z obvezno uporabo pametne kartice;**
- kvalificirano digitalno potrdilo z enim parom ključev – **Standardno kvalificirano digitalno potrdilo.**

Najdaljša časovna veljavnost posameznega potrdila je lahko pet (5) let. [glej 6.3.2].

### 1.1.1 Osnovne definicije

<b>Izraz</b>	<b>Definicija</b>
<b>Elektronski podpis</b>	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.
<b>Varen elektronski podpis</b>	Je elektronski podpis, ki izpolnjuje naslednje zahteve: <ul style="list-style-type: none"><li>da je povezan izključno s podpisnikom;</li><li>da je iz njega mogoče zanesljivo ugotoviti podpisnika;</li><li>da je ustvarjen s sredstvi za varno elektronsko poslovanje, ki so izključno pod podpisnikovim nadzorom;</li><li>da je povezan s podatki, na katere se nanaša, tako, da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi.</li></ul>
<b>Informacijski sistem</b>	Je sistem za oblikovanje, pošiljanje, prejemanje, shranjevanje in druge obdelave podatkov v elektronski obliki.
<b>Digitalno potrdilo</b>	Je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto.
<b>Kvalificirano digitalno potrdilo</b>	Je potrdilo, ki izpolnjuje zahteve iz 28. člena Zakona o elektronskem poslovanju in elektronskem podpisu in ga izda overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena tega zakona.
<b>Oprema za elektronsko podpisovanje</b>	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.
<b>Overitelj</b>	Je fizična ali pravna oseba, ki izdaja digitalna potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskim podpisovanjem.
<b>Podatki za elektronsko podpisovanje</b>	So edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa.
<b>Podatki za preverjanje elektronskega podpisa</b>	So edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa.
<b>Podpisnik</b>	Je oseba, ki ustvari elektronski podpis.
<b>Sredstvo za elektronsko podpisovanje</b>	Je sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena Zakona o elektronskem poslovanju in elektronskem podpisu.
<b>Sredstvo za preverjanje</b>	Je nastavljena programska ali strojna oprema, ki se uporablja



<b>elektronskega podpisa</b>	za preverjanje elektronskega podpisa.
<b>Sredstvo za varno elektronsko podpisovanje</b>	Je nastavljena programska ali strojna oprema, ki se uporablja za elektronsko podpisovanje.
<b>Imetnik potrdila (angl. Subject)</b>	Fizična oseba, navedena v digitalnem potrdilu v polju »subject« kot lastnik zasebnega ključa, ki ustreza javnemu ključu, navedenem v digitalnem potrdilu.
<b>Prosiliec</b>	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.

## 1.1.2 Okrajšave

Kratica	Pomen
<b>ARL</b>	angl. Authority Revocation List – register preklicanih potrdil, ki jih uporabljajodrugih overitelji
<b>CA</b>	angl. Certification Authority – overitelj
<b>CN</b>	angl. Common Name – X.500 domače ime imetnika digitalnega potrdila
<b>CRL</b>	angl. Certificate Revocation List – register preklicanih digitalnih potrdil
<b>CSP</b>	angl. Certification Service Provider – ponudnik storitve overjanja in upravljanja digitalnih potrdil
<b>CPS</b>	angl. Certificate Practice Statement – javni del notranjih pravil overitelja, politika
<b>PDS</b>	angl. Policy Disclosure Statement – Izjava o politiki delovanja, pravila delovanja
<b>DN</b>	angl. Distinguished Name – X.500 razločevalno ime
<b>EAL</b>	angl. Evaluation Assurance Level – standard označevanja varnostnih nivojev v računalniških sistemih
<b>FIPS</b>	angl. United State Federal Information Processing Standards – oznaka standarda s področja informacijskega procesiranja
<b>LRA</b>	angl. Local Registration Authority – lokalna registracijska pisarna, ki izvaja funkcijo registrske pisarne overitelja
<b>PKCS</b>	angl. Public Key Cryptographic Standars – šifrirni standardi na področju javnih ključev
<b>PKIX-CMP</b>	angl. Public Key Infrastructure (based on) X.509 Certificate Management Protocols – protokol za izmenjavo ključev in upravljanje certifikatov
<b>RA</b>	angl. Registration Authority – registracijska pisarna overitelja
<b>SCEP</b>	angl. Simple Certificate Enrollment Protocol – protokol, ki avtomatizira prevzem digitalnih potrdil. Uporablja se predvsem v CISCO-usmerjevalnikih.
<b>SSCD</b>	angl. Secure Signature Creation Device – naprava za varno oblikovanje podpisa (pametna kartica)
<b>ZEPEP</b>	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 57/2000 in 30/2001)

## 1.1.3 Pomen izrazov

Posamezni izrazi imajo v nadaljevanju tega dokumenta naslednji pomen:

- **Overitelj** je Certifikatska agencija Pošte Slovenije, krajše POŠTA<sup>®</sup> CA, ki deluje v skladu z 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 evropskimi direktivami in je registrirana za opravljanje dejavnosti. POŠTA<sup>®</sup> CA izdaja



kvalificirana digitalna potrdila za fizične osebe. Overitelj izdaja tudi kvalificirana digitalna potrdila za pravne osebe in druge vrste digitalnih potrdil.

- **Vloge** so obrazci overitelja za pridobitev ali preklic potrdila, povrnitev zgodovine dešifrirnih ključev naprednega kvalificiranega digitalnega potrdila ali obnovo standardnega kvalificiranega 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, sezname, 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.
- **Standardno kvalificirano digitalno potrdilo** vsebuje eno digitalno potrdilo X.509, izdano za digitalni ID z enim parom ključev.
- **Napredno kvalificirano digitalno 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).

## 1.2 Identifikacijski podatki

Overitelja v okviru Pošte Slovenije predstavljajo naslednji identifikacijski podatki:

Pošta Slovenije, d.o.o.  
POŠTA<sup>®</sup> CA  
Slomškov trg 10, 2500 Maribor  
Telefon: 02 449 2346  
Fax: 02 449 2255  
URL: <http://postarca.posta.si/>  
E-mail: [info.postarca@posta.si](mailto:info.postarca@posta.si)

Enolično ime: **OU=POSTArCA,O=POSTA,C=SI**

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

Ob pričetku svojega delovanja je overitelj tvoril lastno potrdilo namenjeno podpisovanju potrdil drugih imetnikov, podpisovanju registra preklicanih potrdil ter preverjanju podpisa overitelja. Potrdilo overitelja vsebuje:

Serial Number	Serijska številka	1044616010 (0x3E43934A)
Issuer	Overitelj potrdila	OU=POSTArCA,O=POSTA,C=SI



Subject	Imetnik potrdila	OU=POSTArCA,O=POSTA,C=SI
Validity: Not Before	Veljavnost potrdila od	7. FEB. 10.36.58 2003 GMT
Validity: Not After	Veljavnost potrdila do	7. FEB. 11.06.58 2023 GMT
RSA Public Key	Dolžina RSA ključa	2048 bit
Signature Algorithm	Algoritem	sha1 WithRSAEncryption
Key identifier	Identifikator ključa	<b>3F:BD:CD:8E:DF:BE:D1:6B:65:44:3F:60:EC:EA:42:2E:30:70:1F:68</b>
SHA-1 hash:	SHA-1 odtis potrdila	<b>B1EA C3E5 B824 76E9 D50B 1EC6 7D2C C11E 12E0 B491</b>
MD5 hash:	MD5 odtis potrdila	<b>2C6F 17A3 9562 0120 65D2 076E FCB8 3F6D</b>

Kvalificirana digitalna potrdila pod točko 1 iz poglavja 1.1 se izdajajo pod oznako **POŠTA<sup>®</sup> CA** – kvalificirana digitalna potrdila z dvema paroma ključev za fizične osebe in obvezno uporabo pametne kartice ali **Napredna kvalificirana digitalna potrdila**  
**PolicyIdentifier OID: 1.3.6.1.4.1.15284.1.1.1.2.1.0**

Kvalificirana digitalna potrdila pod točko 2 iz poglavja 1.1 se izdajajo pod oznako **POŠTA<sup>®</sup> CA** – kvalificirana digitalna potrdila z enim parom ključev za fizične osebe in obvezno uporabo pametne kartice ali **Standardna kvalificirana digitalna potrdila z obvezno uporabo pametne kartice**  
**PolicyIdentifier OID: 1.3.6.1.4.1.15284.1.1.1.2.2.0**

Kvalificirana digitalna potrdila pod točko 3 iz poglavja 1.1 se izdajajo pod oznako **POŠTA<sup>®</sup> CA** – kvalificirana digitalna potrdila z enim parom ključev za fizične osebe ali **Standardna kvalificirana digitalna potrdila**  
**PolicyIdentifier OID: 1.3.6.1.4.1.15284. 1.1.2.2.2.0**

## 1.3 Subjekti in namen uporabe

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

### 1.3.1 Overitelj

POŠTA<sup>®</sup> CA, overitelj kvalificiranih digitalnih 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 šifirnih ključev sebi podpisala digitalno potrdilo (angl. self-signed certificate).

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

### 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 pooblaščenca za odobravanje in posredovanje vlog sistemu (informacijskemu sistemu overitelja) za izdajo potrdil.

- Lokalna registracijska pisarna (angl. LRA-Local Registration Authority), ki deluje v okviru overitelja na oddaljenih lokacijah Pošte Slovenije. Pooblaščen je za overjanje identitete prosilcev in posredovanje vlog v center overitelja.
- Lokalni overitelj identitete, ki deluje na oddaljenih lokacijah in ima z overiteljem POŠTA<sup>®</sup> CA sklenjeno pogodbo o opravljanju storitve overjanja identitete. Pooblaščen je za overjanje identitete prosilcev in posredovanje vlog v center overitelja.

### **1.3.3 Uporabniki kvalificiranih digitalnih potrdil**

#### **1.3.3.1 Imetniki potrdil**

Overitelj izdaja kvalificirana digitalna potrdila prosilcem. Prosilec je fizična oseba, ki podpiše vlogo za izdajo kvalificiranega digitalnega potrdila. S podpisom vloge se prosilec zavezuje k doslednem spoštovanju in upoštevanju javnega dela notranjih pravil overitelja. Kvalificirano digitalno potrdilo (v nadaljevanju potrdilo) izda overitelj prosilcu, ki s tem postane imetnik kvalificiranega 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 potrdila zagotoviti, da bodo takšni dokumenti znova ustrezno podpisani z uporabo novega veljavnega podpisa.

Overitelj v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 57/2000 in 30/2001) izdaja potrdila le prosilcem. Prosilec in imetnik potrdila je vedno ena in ista fizična oseba, ki lastnoročno uporablja potrdilo.

Prosilec je dolžan:

- dati overitelju točne in popolne podatke o svoji identiteti 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.

#### **1.3.3.2 Tretje osebe (angl. Relying Parties)**

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

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

### **1.3.4 Namen uporabe**

Overitelj izdaja kvalificirana digitalna potrdila fizičnim osebam za njihovo osebno uporabo. Potrdila se lahko uporabljajo za:

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



### **1.3.4.1 POŠTA<sup>®</sup> CA - kvalificirana digitalna potrdila z dvema paroma ključev in z obvezno uporabo pametne kartice (napredna kvalificirana digitalna potrdila)**

POŠTA<sup>®</sup> CA - kvalificirana digitalna potrdila z dvema paroma ključev in z obvezno uporabo pametne kartice za fizične osebe, se lahko uporabljajo za varen elektronski podpis, za šifriranje in kontrolo dostopa.

### **1.3.4.2 POŠTA<sup>®</sup> CA - kvalificirana digitalna potrdila z enim parom ključev in z obvezno uporabo pametne kartice (standardna kvalificirana digitalna potrdila z obvezno uporabo pametne kartice)**

POŠTA<sup>®</sup> CA - kvalificirana digitalna potrdila z enim parom ključev in z obvezno uporabo pametne kartice za fizične osebe, se lahko uporabljajo za varen elektronski podpis, za šifriranje in kontrolo dostopa.

### **1.3.4.3 POŠTA<sup>®</sup> CA - kvalificirana digitalna potrdila z enim parom ključev (standardna kvalificirana digitalna potrdila)**

POŠTA<sup>®</sup> CA - kvalificirana digitalna potrdila z enim parom ključev za fizične osebe, se lahko uporabljajo za elektronski podpis, za šifriranje in kontrolo dostopa.

## **1.4 Kontaktne osebe**

### **1.4.1 Kontaktne osebe - organizacija overitelja**

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

POŠTA SLOVENIJE, d.o.o.  
POŠTA<sup>®</sup> CA - *Operativni vodja*  
Slomškovo trg 10, 2500 Maribor  
Tel: 02 449 2346  
Telefaks: 02 449 2255  
[Operativa.postarca@posta.si](mailto:Operativa.postarca@posta.si)

### **1.4.2 Kontaktne osebe – dokumentacija overitelja**

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

POŠTA SLOVENIJE, d.o.o.  
POŠTA<sup>®</sup> CA – *Projektni vodja*  
Slomškovo trg 10, 2500 Maribor  
Tel: 02 449 2346  
Telefaks: 02 449 2255  
[Dokumentacija.postarca@posta.si](mailto:Dokumentacija.postarca@posta.si)

## **2 SPLOŠNA DOLOČILA**

### **2.1 Obveznosti**

#### **2.1.1 Obveznosti overitelja potrdil**

Overitelj mora zagotoviti:

- izvajanje vseh postopkov v skladu z navedbami v dokumentu Politika POŠTA<sup>®</sup> CA – Kvalificirana digitalna potrdila za fizične osebe, (Javni del notranjih pravil overitelja) 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;
- razvoj in vzpostavitev postopkov za sprejem vlog;
- preverjanje istovetnosti prosilcev, ki zahtevajo izdajo potrdila;
- odobritev ali zavrnitev vloge;
- podpis in izdajo potrdila prosilcem;
- objavo potrdila v javnem imeniku;
- uvedbo postopka za preklic potrdila na zahtevo imetnika potrdila ali po svoji presoji;
- preklic potrdila in objavo preklica v registru preklicanih potrdil;
- priporočila minimalnih sistemskih zahtev za uporabo potrdil. Na računalniških sistemih, ki ne ustrezajo minimalnim zahtevam, overitelj ni dolžan zagotavljati delovanja potrdil;
- preverjanje istovetnosti imetnikov potrdil, ki zahtevajo obnovo potrdila ali povrnitev zgodovine šifrirnih ključev ter vzpostavitev ustreznih postopkov.

#### **2.1.2 Obveznosti registracijske pisarne overitelja (angl. RA - Registration Authority)**

Registracijska pisarna overitelja je dolžna:

- preveriti identiteto prosilca in točnost podatkov, danih v postopku prijave;
- preveriti vloge za preklic ter jih posredovati centru overitelja;
- preveriti identiteto prosilca in točnost danih podatkov v postopku obnove potrdila.

#### **2.1.3 Obveznosti imetnikov potrdil**

Imetnik potrdila je dolžan:

- varovati osebno geslo in zasebne dele ključev. Imetnik potrdila osebne 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 nepooblaščen osebe uporabile imetnikovo kvalificirano digitalno potrdilo;
- digitalno podpisovati le dokumente, katerih zahteva po veljavnosti ni daljša od roka veljavnosti potrdila;
- zagotoviti uporabo potrdil le v obdobju veljavnosti potrdila;
- zagotoviti uporabo potrdil samo za namene, ki jih je odobril overitelj;
- takoj zahtevati preklic 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 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.

V primeru neupoštevanja obveznosti imetnik potrdila nosi popolno odgovornost za vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker so tretje nepooblaščen osebe uporabile imetnikovo potrdilo.

#### **2.1.4 Obveznosti tretjih oseb**

Tretje osebe, ki se zanašajo na potrdila overitelja, so dolžne:

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

#### **2.1.5 Obveznosti javnega imenika**

Overitelj ima javno dostopen imenik, kjer so shranjena overjena digitalna potrdila in register preklicanih potrdil.

## **2.2 Odgovornost**

### **2.2.1 Odgovornost 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 odgovarja za vse obveznosti, ki so navedene v točki 2.1.1 Obveznosti overitelja potrdil, v zvezi z vsakim izdanim potrdilom.

### **2.2.2 Odgovornost overitelja za registracijske pisarne (angl. RA - Registration Authority) in za podizvajalce**

Overitelj odgovarja za obveznosti registracijske pisarne overitelja, navedene v točki 2.1.2.

Overitelj je odgovoren za delo podizvajalcev, če je nanje prenesel izvajanje posameznih dejavnosti ali postopkov.

### **2.2.3 Odgovornost overitelja do imetnikov potrdila**

Overitelj odgovarja imetnikom 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 s potrdili tako, kot je določeno v tem dokumentu.

#### 2.2.4 Odgovornost overitelja do tretjih oseb

Overitelj odgovarja za škodo tretjim osebam, ki se upravičeno zanašajo na potrdila, ki ga je izdal:

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

#### 2.2.5 Omejitev overiteljeve odgovornosti

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

- če je bilo potrdilo izdano zaradi napake, neverodostojnih podatkov ali drugih nepravilnosti na strani imetnika potrdila;
- če je potekla veljavnost potrdila;
- kadar je potrdilo uporabljeno po preklicu in objavi v registru preklicanih potrdil;
- če je 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 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.

### 2.3 Finančna odgovornost

Overitelj ima ustrezno zavarovano svojo odgovornost po Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 57/2000 in 30/2001) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001). Zavarovalna vsota, za katero ima overitelj zavarovano škodno odgovornost, znaša 50.000.000,00 SIT.

Overitelj jamči za vrednost posameznega pravnega posla glede na vrsto potrdila do višine, navedene v tabeli:

1.000.000,00 SIT	Kvalificirano digitalno potrdilo z dvema paroma ključev za fizične osebe, z obvezno uporabo pametne kartice, skladne z nivojem FIPS140-1 level 2, EAL4 ali višjim nivojem ( <b>Napredno kvalificirano digitalno potrdilo</b> )
200.000,00 SIT	Kvalificirano digitalno potrdilo z enim parom ključev za fizične osebe, z obvezno uporabo pametne kartice, skladne z nivojem



	FIPS140-1 level 2, EAL4 ali višjim nivojem ( <b>Standardno kvalificirano digitalno potrdilo z obvezno uporabo pametne kartice</b> )
50.000,00 SIT	Kvalificirano digitalno potrdilo z enim parom ključev za fizične osebe ( <b>Standardno kvalificirano digitalno potrdilo</b> )

## 2.4 Interpretacija in usklajenost

Overitelj deluje v skladu z:

- Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 57/2000, 30/2001);
- Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000, 2/2001);
- drugimi veljavnimi predpisi na območju Republike Slovenije.

Oblika in vsebina javne politike overitelja je usklajena z:

- RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates.

## 2.5 Cenik

Overitelj določi cenik svojih storitev ter ga objavi na spletu ter v vsaki registracijski pisarni. Cenik je objavljen na spletni strani <http://postarca.posta.si/cenik.html>.

## 2.6 Objave informacij in javni imenik

Overitelj vzdržuje javni imenik X.500/LDAP, ldap://postarca.posta.si, ki vsebuje naslednje informacije:

- javne informacije o imetnikih potrdil;
- veljavna potrdila, ki jih je izdal overitelj;
- veljaven register preklicanih potrdil.

Javni dokumenti overitelja so objavljeni na spletni strani <http://postarca.posta.si>. Na spletnih straneh so objavljene naslednje informacije:

- POŠTA<sup>®</sup> CA - Izjava o politiki delovanja (PDS);
- Politika overitelja POŠTA<sup>®</sup> CA – Kvalificirana digitalna potrdila za fizične osebe; Javni del notranjih pravil overitelja;
- ceniki;
- vloge za pridobitev, preklic in obnovo potrdil;
- ostale informacije, vezane na delovanje overitelja.

Potrdila so objavljena takoj po izdaji.

Preklicana potrdila so objavljena v registru preklicanih potrdil, ki se objavi v javnem imeniku takoj po preklicu.

## **2.7 Preverjanje skladnosti**

Preverjanje skladnosti z zakonodajo izvaja pristojna inšpekcijska služba.

Overitelj izvaja redne notranje preglede delovanja.

## **2.8 Varovanje podatkov**

Vsi podatki, pridobljeni, ustvarjeni ali posredovani, so zaupni in bodo varovani enako kot poslovne skrivnosti overitelja 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 (Ur.l. RS, št. 59/1999, 57/2001 (59/2001 - popr.)) in na njegovi podlagi izdanimi predpisi. Izjema so 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. Overitelj varuje podatke v skladu z določili 5. in 6. poglavja te politike.

## 3 PREVERJANJE ISTOVETNOSTI

### 3.1 Prva registracija

#### 3.1.1 Vrste imen

Razločevalna imena (angl. DN – Distinguished Name) POŠTA<sup>®</sup> CA v poljih »issuer« in »subject« potrdila X.509 so oblikovana v skladu s standardom X.501.

POŠTA<sup>®</sup> CA »subject« atribut oziroma »issuer« atribut v potrdilih je:

<b>Država (C) =</b>	SI
<b>Organizacija (O) =</b>	POSTA
<b>Organizacijska enota (OU) =</b>	POSTArCA

Razločevalno ime (angl. DN) imetnikov potrdil v imeniku in polju »subject« v potrdilu je:

<b>Država (C) =</b>	SI
<b>Organizacija (O) =</b>	POSTA
<b>Organizacijska enota (OU) =</b>	POSTArCA
<b>Organizacijska enota (OU) =</b>	personal
<b>Ime (CN) =</b>	ime in priimek imetnika potrdila
<b>Serijska številka (serialNumber) =</b>	serijska številka

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

<b>Država (C) =</b>	SI
<b>Organizacija (O) =</b>	POSTA
<b>Organizacijska enota (OU) =</b>	POSTArCA:CertificateRevocationList

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

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

#### 3.1.2 Potreba po smiselnosti imen

X.500 relativno ime (RDN) imetnika potrdila sestavljata X.500 domače ime (CN), ki vsebuje ime in priimek imetnika, ter X.500 serijska številka (serialNumber). Overitelj določi serijsko številko v skladu s svojimi notranjimi pravili. Serijska številka je določena tako, da neposredno ne vsebuje osebnih podatkov.

#### 3.1.3 Pravila za interpretacijo različnih oblik imen

Imena 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:

Znak	Pretvorba
Č	C
č	C
Š	S
š	S
Ž	Z
ž	Z

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

### 3.1.4 Edinstvenost imen

Overitelj dodeli vsakemu imetniku potrdila edinstveno razločevalno ime (DN), ki je objavljeno v polju »subject« potrdila.

### 3.1.5 Postopek reševanja imenskih sporov

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 potrdila ali preklicati izdana potrdila udeležencev spora.

### 3.1.6 Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk

Glej točko 3.1.5.

### 3.1.7 Metoda za dokazovanje posesti zasebnega ključa

Dokaz o posesti zasebnega ključa je zagotovljen z uporabo protokolov PKIX-CMP oziroma PKCS#10 v postopku prevzema potrdila. Dokaz o posesti pametne kartice (SSCD) je podpisana prevzemnica imetnika potrdila.

### 3.1.8 Preverjanje istovetnosti pravne osebe

Ni predpisano.

### 3.1.9 Preverjanje istovetnosti fizične osebe

Istovetnost fizične osebe se preverja v registracijski pisarni ob fizični prisotnosti osebe na osnovi uradnega identifikacijskega dokumenta:

- osebne izkaznice ali
- potnega lista

## 3.2 Preverjanje istovetnosti ob rutinski menjavi ključev

Zamenjava ključev se vrši po protokolu PKIX-CMP za napredna kvalificirana digitalna potrdila. Lastniki standardnih kvalificiranih digitalnih potrdil se morajo ponovno identificirati po točki 3.1.9.



### **3.3 Preverjanje istovetnosti za ponovno izdajo ključev po preklicu potrdila**

V skladu s točko 3.1.9.

### **3.4 Preverjanje istovetnosti ob zahtevi za preklic potrdila**

Imetnik potrdila, 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 POGOJI ZA DELOVANJE**

### **4.1 Vloga za izdajo potrdila**

Za izdajo potrdila mora prosilec:

- izpolniti predpisano vlogo za izdajo potrdila in jo osebno oddati v registracijski pisarni overitelja;
- izpolniti identifikacijske zahteve [točke 3.1.8];
- izpolniti morebitne finančne obveznosti [točka 2.5].

### **4.2 Izdaja potrdil**

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. Prosilec lahko prevzame potrdilo na podlagi referenčne številke in avtorizacijske kode.

Overitelj posreduje inicializacijske podatke prosilcu najkasneje v desetih dneh. Veljavnost inicializacijskih podatkov je 60 dni.

Overitelj pošlje prosilcu obvestilo o odobritvi izdaje potrdila, referenčno številko in navodila za prevzem potrdila po elektronski pošti ali s priporočeno pošiljko. Avtorizacijsko kodo prejme prosilec z ločeno priporočeno pošiljko.

Referenčno številko in avtorizacijsko kodo mora prosilec do prevzema potrdila ustrezno varovati [točka 2.1.3].

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 s priporočeno pošiljko.

### **4.3 Prevzem potrdila**

Postopek prevzema je odvisen od vrste potrdila:

- Napredna kvalificirana digitalna potrdila se prevzemajo po protokolu PKIX-CMP z ustrezno aplikacijo, v skladu z navodili za prevzem naprednega kvalificiranega digitalnega potrdila, ki se nahajajo na spletni strani: <http://postarca.posta.si>.
- Za standardna kvalificirana digitalna potrdila se uporabi eden od podprtih spletnih brskalnikov (objavljenih na spletni strani overitelja), v skladu z navodili za prevzem standardnega kvalificiranega digitalnega potrdila, ki se nahajajo na spletni strani: <http://postarca.posta.si>.

Prosilec prejme navodila za prevzem potrdila ob oddaji vloge za izdajo potrdila. Navodila so v elektronski in tiskani 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 potrdila je potrebno uporabiti zadnjo različico objavljenih navodil.

Po prevzemu se javni ključ, vsebovan v potrdilu, objavi v javnem imeniku. S prevzemom potrdila prosilec prevzema tudi vse obveze iz točke 2.1.3. Posebna pozornost je potrebna pri arhiviranju zasebnega ključa imetnika in njegovemu varovanju.

Prosilec lahko prevzame potrdilo samo z ustreznimi prevzemnimi podatki - referenčno številko in avtorizacijsko kodo [točka 4.2]. Veljavnost prevzemnih podatkov je enkratna in časovno omejena [točka 4.2]. V primeru preteka njihove veljavnosti pred prevzemom je treba ponoviti postopek, opisan v točki 4.1.

## **4.4 Preklic potrdila**

### **4.4.1 Okoliščine preklica**

Overitelj lahko prekliče potrdilo iz naslednjih razlogov:

- dejansko ali domnevno ogrožanje zasebnih ključev;
- spremembe podatkov v potrdilu, ki zahtevajo izdajo novega;
- neizpolnjevanje obveznosti iz točke 2.1.3;
- v primeru smrti imetnika potrdila;
- na zahtevo imetnika potrdila.

Imetnik potrdila je dolžan overitelju nemudoma prijaviti vsako domnevno ali dejansko ogrožanje zasebnega ključa. Pooblaščen osebje overitelja preveri okoliščine, ki so privedle do preklica potrdila in se odloči za izdajo novega potrdila ali druge ukrepe. Če do izdaje novega potrdila ne pride, bo imetnik potrdila o tem obveščen po elektronski pošti ali s priporočeno pošiljko.

### **4.4.2 Kdo lahko zahteva preklic**

Preklic potrdila lahko zahteva:

- imetnik potrdila, kateremu je bilo potrdilo izdano;
- zaposleni pri overitelju v primeru:
  - ko overitelj izve, da je imetnik potrdila umrl ali so se spremenile okoliščine, ki bistveno vplivajo na veljavnost potrdila,
  - če je podatek v potrdilu napačen ali je bilo 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 potrdila,
  - če so bili podatki za elektronsko podpisovanje ali informacijski sistem imetnika potrdila ogroženi na način, ki vpliva na zanesljivost oblikovanja elektronskega podpisa;
- pristojno sodišče, sodnik za prekrške ali upravni organ;
- dedič ali zakoniti zastopnik;
- tretja oseba, če potrdilo vsebuje podatke o tretji osebi.

### **4.4.3 Postopki za preklic**

#### **4.4.3.1 Preklic zaradi spremembe podatkov v potrdilu**

1) Zahteva za preklic se lahko poda na enega izmed naslednjih načinov:

- Imetnik potrdila pošlje vlogo za preklic po elektronski pošti na kontaktni naslov overitelja. Upoštevane bodo samo digitalno podpisane vloge z veljavnimi potrdili, ki jih je izdal overitelj.
  - Imetnik potrdila osebno odda vlogo za preklic v registracijski pisarni overitelja.
  - Po telefonu na dežurno številko za preklic. Imetnik 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 preklic v center overitelja.
  - 3) Overitelj preveri digitalni podpis in preklične potrdilo.
  - 4) Postopek izdaje novega potrdila je enak postopku izdaje prvega potrdila [točke 4.1, 4.2 in 4.3].

#### **4.4.3.2 Preklic zaradi ogrožanja zasebnega ključa**

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

#### **4.4.3.3 Preklic zaradi neizpolnjevanja obveznosti imetnika**

V primeru, da imetnik potrdila ne izpolnjuje svojih obveznosti, lahko overitelj preklične potrdilo. Overitelj obvesti imetnika potrdila o preklicu po elektronski pošti ali s priporočeno pošiljko.

#### **4.4.4 Čas od oddaje vloge za preklic do preklica potrdila**

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

#### **4.4.5 Okoliščine suspenza**

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

#### **4.4.6 Kdo lahko zahteva suspenz**

Enako kot preklic [točka 4.4.2].

#### **4.4.7 Postopki za suspenz**

- 1) Zahteva za suspenz potrdila se lahko poda na enega izmed naslednjih načinov:
  - Imetnik potrdila pošlje vlogo za suspenz po elektronski pošti na kontaktni naslov overitelja. Upoštevane bodo samo digitalno podpisane vloge z veljavnimi potrdili, ki jih je izdal overitelj.
  - Imetnik potrdila osebno odda vlogo za suspenz 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 potrdila.
  - Overitelj se odloči za suspenz po lastni presoji.
- 2) Po uspešno izvedenem postopku preverjanja istovetnosti imetnika potrdila v registracijski pisarni, osebje registracijske pisarne posreduje vlogo za suspenz v center overitelja.
- 3) Overitelj preveri digitalni podpis na vlogi in izvede suspenz potrdila.
- 4) Overitelj obvesti imetnika potrdila o suspenzu po elektronski pošti ali s priporočeno pošiljko.

##### **4.4.7.1 Postopki za preklic suspenza**

- 1) Zahteva za preklic suspenz se lahko poda na enega izmed naslednjih načinov:
  - Imetnik potrdila osebno odda vlogo za preklic suspenza 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 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 preveri digitalni podpis na vlogi in izvede preklic suspenz potrdila.
- 4) Overitelj obvesti imetnika potrdila o preklicu suspenz po elektronski pošti ali s priporočeno pošiljko.

#### **4.4.8 Omejitve obdobja suspnez**

Ni omejitev.

#### **4.4.9 Pogostost objav registra preklicanih digitalnih potrdil (angl. CRL)**

Veljavnost overiteljevega registra preklicanih digitalnih potrdil je 4 ure. Nov register se objavi pred potekom veljavnosti starega.

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

#### **4.4.10 Preverjanje registra preklicanih digitalnih potrdil**

Pred uporabo javnega ključa je treba preveriti register preklicanih digitalnih potrdil. Za preverjanje veljavnosti potrdil je merodajen samo najnovejši objavljeni register preklicanih digitalnih potrdil v javnem imeniku overitelja. Register preklicanih digitalnih potrdil podpiše overitelj z istim zasebnim ključem kot podpisuje potrdila.

#### **4.4.11 Sprotno preverjanje statusa potrdil**

Ni na voljo.

#### **4.4.12 Zahteve za sprotno preverjanje statusa potrdil**

Ni predpisano.

#### **4.4.13 Drugi repozitoriji registra preklicanih digitalnih potrdil**

Možna je objava registra preklicanih digitalnih potrdil v drugih javnih imenikih, vendar lahko pride do zakasnitev glede na register preklicanih potrdil v javnem imeniku.

### **4.5 Postopki varnostnih pregledov sistema**

Ob vseh dogodkih bo zabeležen čas in datum nastanka dogodka.

#### **4.5.1 Vrste beleženih dogodkov**

Zapisane bodo naslednje vrste dogodkov:

- dogodki v zvezi z imetnikovimi ključi in s potrdili - izdaja, prevzem, preklic, zadržanje;
- 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 kadrovske spremembami overitelja;
- dogodki, povezani z uničevanjem za to predvidenih podatkov.

#### **4.5.2 Pogostost pregleda revizijskih dnevnikov**

Osebe overitelja pregleduje revizijske dnevnike enkrat tedensko. Revizija vključuje:

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

#### **4.5.3 Obdobje hranjenja revizijskih dnevnikov**

Najmanj teden dni na sistemih in trajno v arhivu.

#### **4.5.4 Zaščita revizijskih dnevnikov**

Revizijske dnevnike je treba hraniti v najvišji varnostni coni. Dostop je dovoljen samo pooblaščenim osebam, kot je to definirano v varnostni politiki POŠTE SLOVENIJE, ter v okviru njej podrejene varnostne politike overitelja. Za dnevnike na operacijskem sistemu so uporabljene zaščite, kot jih le-ta dopušča. Dnevniki programske opreme za upravljanje s ključi in potrdili so zaščiteni s tehnologijo šifrirnih javnih ključev.

#### **4.5.5 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 pooblaščenih skrbniki sistemov.

#### 4.5.6 Sistem zbiranja revizijskih podatkov

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

#### 4.5.7 Obveščanje subjekta – povzročitelja dogodka

Povzročitelja dogodka v dnevniku o tem ni treba obvestiti.

#### 4.5.8 Ocene ranljivosti

Ocena ranljivosti se izvaja v sklopu pregleda revizijskih dnevnikov.

### 4.6 Arhiviranje podatkov

Overitelj hrani naslednje podatke:

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

Overitelj hrani revizijske dnevnike trajno. Potrdila in zasebni ključi se hranijo trajno. Vloge imetnikov, korespondenca z overiteljem in pogodbe se hranijo trajno.

Arhiv se hrani na drugi lokaciji, zaščiten z enakimi varnostnimi mehanizmi, kot so vzpostavljeni v centru overitelja. Dostop je dovoljen samo pooblaščenim osebam.

## **4.7 Obnova potrdila**

Napredna kvalificirana digitalna potrdila se obnavljajo avtomatsko, ko je izpolnjen eden izmed naslednjih dveh pogojev:

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

Standardna kvalificirana digitalna potrdila se po preteku veljavnosti ponovno izdajo. Postopek je enak kot pri ponovni izdaji potrdila po preklicu [postopek, opisan v točki 4.4].

## **4.8 Okrevalni načrt**

### **4.8.1 Uničenje programske opreme, strojne opreme ali podatkov**

V primeru okvare strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ overitelja ni bil uničen, bodo storitve overitelja vzpostavljeni nazaj v najkrajšem možnem času. V primeru uničenja zasebnega ključa overitelja, bo overitelj ukrepal po postopku, opisanem v točki 4.8.3.

### **4.8.2 Preklic overiteljevega digitalnega potrdila**

Glej 4.8.3.

### **4.8.3 Ogrožanje overiteljevega zasebnega ključa**

Ob ogrožanju ključa overitelja bo overitelj po elektronski pošti obvestil:

- celotno osebje overitelja;
- vse imetnike;
- morebitne medsebojno priznane ali podrejene overitelje.

Overitelj bo izvedel naslednje postopke:

- preklical vsa potrdila;
- ukinil CRL, podpisane s ogrožanim ključem;
- objavil preklic potrdila overitelja v ustrezni ARL;
- tvoril nove ključe overitelja;
- izdal imetnikom nova potrdila.

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

## **4.9 Prenehanje delovanja overitelja**

Overitelj bo v primeru prenehanja delovanja:

- obvestil vse imetnike potrdil in javno objavil informacije vsaj 90 dni pred prenehanjem delovanja;
- preklical vsa veljavna potrdila;
- zagotovil razpoložljivost in dostopnost list preklicanih potrdil za obdobje šest (6) mesecev po preklicu vseh potrdil;
- zagotovil, da bo drug overitelj, ki izdaja kvalificirana digitalna potrdila, vodil preklicana kvalificirana potrdila v svojem registru;

- zagotovil hranjenje arhiviranih podatkov za obdobje deset (10) let po prenehanju delovanja.

#### **4.10 Dodatni pogoji delovanja**

V dodatnih pogojih delovanja so navedeni postopki, ki niso predvideni po RFC 2527 in so specifični za overitelja.

##### **4.10.1 Sprememba razločevalnega imena**

Sprememba razločevalnega imena je mogoča samo za napredna kvalificirana digitalna potrdila z uporabo protokola PKIX-CMP in poteka po naslednjem postopku:

- 1) Zahteva za spremembo razločevalnega imena se poda na enega izmed naslednjih načinov:
  - Imetnik potrdila pošlje vlogo za spremembo razločevalnega imena po elektronski pošti. Upoštevane bodo samo digitalno podpisane vloge z veljavnimi potrdili, ki jih je izdal overitelj.
  - Imetnik potrdila osebno odda vlogo za spremembo razločevalnega imena v registracijski pisarni overitelja.
- 2) Po uspešno izvedenem postopku preverjanja istovetnosti imetnika potrdila osebje registracijske pisarne posreduje vlogo za preklic v center overitelja.
- 3) Osebje overitelja preveri podpis in spremeni imetnikovo razločevalno ime.
- 4) Ob prvi naslednji prijavi v aplikacijo se avtomatsko tvorijo novi ključi in izda potrdilo z novim razločevalnim imenom.

##### **4.10.2 Povrnitev zgodovine ključev za dešifriranje**

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

Postopek za povrnitev zgodovine ključev za dešifriranje:

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

##### **4.10.3 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 digitalnih potrdil razlikujejo od namena uporabe, definirane v tem dokumentu.

## **5 VARNOSTNI NADZOR PROSTOROV, OPREME, POSTOPKOV IN OSEBJA**

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

### **5.1 Fizični nadzor**

#### **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 pooblaščen operativno osebje v skladu z zaupanimi nalogami. Vsi dostopi do prostorov overitelja se beležijo in varujejo v skladu z varnostno politiko POŠTE SLOVENIJE.

#### **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 ne sme biti 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 shranjeni v ognje varnih omarah. Magnetni mediji, hranjeni na oddaljeni lokaciji, so v prostorih, kjer so zagotovljeni vsaj enaki pogoji, 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 Notranja organizacija in nadzor osebja

### 5.2.1 Notranja 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.

Operativno osebje overitelja, njihove naloge in pravice so opisane v točki 5.2.2.

### 5.2.2 Funkcije operativnega osebja

Programska oprema (CA-aplikacija), ki jo overitelj uporablja za upravljanje šifrirnih ključev in potrdil, podpira več stopenj pravic oziroma funkcij, ki so dodeljene osebju overitelja glede na njihove naloge. Odvisno od zadolžitev ima osebje systemske 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 glavni administrator	Ne	Da	3
CA administrator	Ne	Da	4
Varnostni inženir	Ne	Ne	3
Pravni svetovalec	Ne	Ne	1

Naloge operativnega vodje so:

- koordinira operativno delo;
- skrbi za nadzor operativnega osebja;
- izvaja varnostne preglede;
- skrbi za vzpostavitev 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 systemsko strojno in programsko opremo;
- izvedeta začetno konfiguracijo ter izvajata vzdrževanje aplikativne CA-programске opreme overitelja;

- izvajata zagon in zaustavitev CA-servisov;
- ustvarita prvotni uporabniški račun CA-varnostnega oficirja;
- ustvarita uporabniški račun drugih CA-varnostnih oficirjev;
- restavrira uporabniški račun CA-varnostnega oficirja;
- restavrira uporabniški račun CA-aplikativnega administrativnega servisa;
- izdelujeta varnostne kopije, izvajata restavriranje in ponovno šifriranje baze overitelja.

Osebe v funkciji 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 podeljevanje potrdil;
- izvaja medsebojno priznavanje z drugimi overitelji;
- pregleduje in analizira varnostne beležke;
- namešča in vzdržuje pravila na požarnih zidovih;
- izdeluje poročila.

Osebe v funkciji CA-administratorja ima potrebna pooblastila, da:

- upravlja s potrdili;
- izdeluje poročila.

Osebe v funkciji varnostnega inženirja ima naslednje naloge:

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

### **5.2.3 Funkcije registracijske pisarne overitelja**

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

- sprejema in posreduje vloge prosilcev;
- vnaša podatke iz vlog prosilcev za izdajo potrdil;
- distribuira inicializacijske podatke prosilcem potrdil.

### **5.2.4 Število oseb, potrebnih za odobritev postopkov**

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

- ponovno šifriranje CA-baze podatkov;
- tvorjenje šifrnih 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 šifrnih 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 potrdil;
- medsebojno priznavanje z drugimi overitelji;
- nastavitev ali spreminjanje administrativnih pravil;
- nastavitev ali spreminjanje uporabniških pravil;
- dodajanje, brisanje ali mapiranje OID-jev s profili 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.

### **5.2.5 Preverjanja istovetnosti osebja overitelja**

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

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

Posamezno 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 potrdila in pametne kartice za prijavo v aplikacije overitelja.

## **5.3 Nadzor osebja**

### **5.3.1 Zahteve o ozadju, kvalifikacijah, izkušnjah in odobritvah**

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

### **5.3.2 Postopki za preverjanje ozadja**

Dodatna preverjanja o primernosti kandidatov (angl. security clearance checks) se izvajajo v skladu z varnostno politiko Pošte Slovenije.

### **5.3.3 Izobraževanje 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).

Osebjem 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 Dodatno izobraževanje in pogostost izobraževanja osebja**

Osebjem overitelja se udeležuje izobraževanj po potrebi, glede na nove operativne zahteve, oziroma vsaj enkrat letno za obnovo znanja.

#### **5.3.5 Pogostost in sekvenca menjave dela med pooblaščenim osebjem**

Ni predpisano.

#### **5.3.6 Sankcije za nedovoljene postopke**

Proti osebjem 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 preklicajo potrdila, izdana osebi za opravljanje funkcije.

#### **5.3.7 Zahteve za osebjem podizvajalcev**

Varnostne zahteve za osebjem podizvajalcev so enake kot za osebjem overitelja.

#### **5.3.8 Dokumentacija za osebjem**

Overitelj vzdržuje dokumentacijo na spletni strani, kot je opisano v točki 2.6. Ta dokumentacija je javno dostopna. Dodatno so osebjem overitelja na voljo interni operativni priročniki, originalna dokumentacija programske in strojne opreme ter priročniki iz sklopa izobraževanja, glede na njihovo funkcijo in plan izobraževanja.

## **6 TEHNIČNE VARNOSTNE ZAHTEVE**

Imetniki potrdil overitelja POŠTA ® CA morajo uporabljati varne informacijske sisteme, produkte in aplikacije, zaščitene pred spreminjanjem, in vzpostaviti varne tehnične in šifrirne postopke, ki jih bodo le-ti podpirali.

### **6.1 Tvorjenje in namestitvev para ključev**

#### **6.1.1 Tvorjenje para ključev**

Par ključev za podpisovanje je ustvarjen ob namestitvi CA-programске opreme. Uporabljena je zaščita, ki velja za prostore overitelja [točka 5.1.1], večkratno preverjanje istovetnosti pooblaščenih oseb [točka 6.2.2] in strojni šifrirni modul (HSM – Hardware Security Module) [točka 6.2.1].

Ustvarjanje ključev imetnikov je v domeni aplikacijskega okolja imetnika. Za napredna kvalificirana digitalna potrdila se par ključev za podpisovanje ustvari v aplikaciji oziroma na pametni kartici na strani imetnika, par ključev za šifriranje pa se ustvari v CA-aplikaciji overitelja.

#### **6.1.2 Prenos zasebnega ključa**

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

Par ključev za podpisovanje se vedno ustvari na strani imetnika. Zasebni ključ za podpisovanje se nikdar ne hrani na strojni ali programski opremi overitelja.

#### **6.1.3 Prenos javnega ključa overitelju potrdil**

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

#### **6.1.4 Dostop do overiteljevega javnega ključa**

Javni ključ overitelja v obliki potrdila je dostopen:

- v javnem imeniku v ou=POSTArCA, o=POSTA,c=SI, attribute: CAcertificate;
- na spletni strani <http://postarca.posta.si/>;
- po protokolu PKIX-CMP.

#### **6.1.5 Dolžina asimetričnih ključev**

Overitelj uporablja zasebni ključ RSA za podpisovanje dolžine 2048 bitov.

Imetniki potrdil overitelja morajo ustvariti najmanj 1024 bitov dolg zasebni ključ RSA za podpisovanje.

#### **6.1.6 Določanje parametrov javnih ključev**

Šifrirni parametri javnih ključev se ustvarijo v modulih za šifriranje v CA-programski opremi ali v imetnikovi programski opremi.

### 6.1.7 Preverjanje parametrov

Preverjanje kvalitete parametrov overiteljevega ključa za podpisovanje je bilo izvedeno v fazi ustvarjanja ključev.

### 6.1.8 Programsko/strojno ustvarjanje ključev

Ključki overitelja so ustvarjeni na strojni opremi ki ustreza varnostnemu in nivoju FIPS 140-1 level 3.

Šifrirni ključki osebja overitelja so ustvarjeni na modulih za šifrirnaje FIPS 140-1 level 2.

Strojno ali programsko ustvarjanje ključev imetnikov potrdil je v domeni imetnika potrdila in mora biti v skladu z zahtevami overitelja glede na vrsto potrdila.

### 6.1.9 Nameni ključev in potrdil (definirani v polju X.509 v3 keyUsage)

keyUsage je obvezen atribut uporabljen v vseh potrdilih.

Za podpisovanje potrdil in registrov preklicanih potrdil (CRL) se uporablja samo overiteljev zasebni ključ za podpisovanje.

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

Ostala potrdila overitelja se lahko uporabljajo v namene skladno s poljem Uporaba\*\* (angl. keyUsage) v potrdilu:

Politika	ID tip	Št. parov ključev	Uporaba**		Uporabniki
			dS	kE	
Kvalificirano potrdilo (obvezna uporaba pametne kartice, nivo EAL4)	Standarno potrdilo	1	X	X	Fizične osebe
	Napredno potrdilo	2	X	X	
Kvalificirano potrdilo	Standarno potrdilo	1	X	X	Fizične osebe

dS=angl. digitalSignature

kE=angl. keyEncipherment

## 6.2 Zaščita zasebnega ključa

### 6.2.1 Standardi za modul za šifriranje

Glej točko 6.8.

### 6.2.2 Nadzor zasebnega ključa s (n od m) pooblaščenimi osebami

Overitelj ima vzpostavljeno večkratno odobritev za operacije, navedene v točki 5.2.4.

### **6.2.3 Odkrivanje (angl. Escrow) zasebnega ključa**

Overitelj ne podpira odkrivanja zasebnega ključa za podpisovanje.

### **6.2.4 Varnostna kopija zasebnega ključa**

Overitelj hrani kopije zasebnih ključev imetnikov potrdil za dešifriranje na način in po postopkih, za napredna kvalificirana digitalna potrdila. Šifrirni ključi se hranijo v šifrirani bazi podatkov.

Overitelj izdeluje varnostne kopije baze in sistemskih datotek enkrat dnevno.

Overitelj ne hrani imetnikovih zasebnih ključev za podpisovanje.

### **6.2.5 Arhiviranje zasebnega ključa**

Overitelj arhivira kopije zasebnih ključev imetnikov potrdil za dešifriranje, kot je opisano v točki 4.6.

### **6.2.6 Zapis zasebnega ključa v modul za šifriranje**

Overiteljev zasebni ključ za podpisovanje je ustvarjen v strojnem modulu za šifriranje.

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

Imetniški zasebni ključ za podpisovanje se ustvari v modulu za šifriranje na strani imetnika potrdil.

### **6.2.7 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.

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

### **6.2.8 Postopek za deaktiviranje zasebnega ključa**

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

Imetniki potrdil morajo uporabljati PKI-aplikacije, ki deaktivirajo zasebni ključ, ko se imetnik odjavi oziroma ko poteče določen čas neaktivnosti.

### **6.2.9 Postopek za uničenje zasebnega ključa**

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

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

## **6.3 Ostali vidiki upravljanja šifrirnih ključev**

### **6.3.1 Arhiviranje javnega ključa**

Overitelj arhivira svoj javni verifikacijski šifrirni ključ in naročniške javne šifrirne ključe na način in po postopkih, kot je opisano v točki 4.6.

### **6.3.2 Obdobje veljavnosti za javne in zasebne ključe**

Veljavnost javnih in zasebnih šifrirnih 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.

Overitelj lahko kadarkoli prilagodi veljavnost posameznih uporabniških šifrirnih ključev glede na politiko in vrsto potrdila.

## **6.4 Aktivacijski podatki**

### **6.4.1 Generacija in instalacija aktivacijskih (inicializacijskih) podatkov**

Referenčne številke (angl. reference numbers) in avtorizacijske kode (angl. authorization codes) se ustvarijo v overiteljevi aplikativni programski opremi CA. Številke in kode so edinstvene ter ustvarjene po nepredvidljivem algoritmu.

Imetniki potrdil uporabljajo gesla za aktiviranje modulov za šifriranje. Vsak imetnik potrdila izbere svoje geslo. Če imetnik potrdila uporablja overiteljevo PKI-aplikacijo, mora izbrati geslo v skladu s politiko, ki jo je določil overitelj. Gesla niso shranjena v overiteljevi PKI-aplikaciji.

### **6.4.2 Zaščita aktivacijskih (inicializacijskih) podatkov**

Avtorizacijske kode se varno ustvarijo v overiteljevi aplikativni programski opremi CA in shranijo v šifrirani bazi. Avtorizacijske kode se pod nadzorom osebja overitelja tiskajo na slepe kuverte.

Referenčna številka in avtorizacijska koda se dostavita prosilcu po različnih komunikacijskih kanalih. Avtorizacijska koda se dostavi prosilcu s priporočeno pisemsko pošiljko.

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 slepi kuverti pod nadzorom osebja overitelja. Prosilci morajo skrbno varovati vse aktivacijske podatke.

### **6.4.3 Drugi vidiki aktivacijskih podatkov**

Ni predpisano.

## **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 šifrnih modulov za hranjenje šifrnih ključev osebja overitelja;
- šifrirane seje med aplikativno programsko opremo CA in naročniško PKI-aplikacijo overitelja;
- šifrirano bazo podatkov overitelja;
- varen arhiv overitelja in imetniških šifrnih ključev ter varnostnih beležk;
- varnostne beležke vseh varnostno veljavnih dogodkov;
- vzpostavljene mehanizme restavriranja sistema, šifrnih ključev overitelja ter baze podatkov overitelja.

### **6.5.2 Stopnja varnostne zaščite računalnikov**

Strežniški operacijski sistemi overitelja, ki dosegajo stopnjo varnosti EAL3 (C2).

## **6.6 Tehnični nadzor razvoja overitelja**

### **6.6.1 Nadzor razvoja sistema**

Overiteljeva CA-programska oprema je bila razvita pri proizvajalcu Entrust, po strogih merilih, in verificirana po kriterijih EAL3 in FIPS 140-1 level 2.

### **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 redni nadzor celovitosti programske opreme. Kontrola celovitosti se izvaja enkrat tedensko.

## **6.7 Varnostne kontrole računalniške mreže**

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.

## **6.8 Tehnične kontrole modulov za šifriranje**

Ustvarjanje overiteljevih šifrnih ključev za digitalni podpis ter digitalni podpis z overiteljevimi šifrnimi ključi se izvaja na strojnem modulu za šifriranje FIPS 140-1 level 3. Vse ostale šifrirne operacije overitelja se izvajajo na modulih za šifriranje s stopnjo najmanj FIPS 140-1 level 2.

Osebe overitelja uporabljajo module za šifriranje FIPS 140-1 level 2.



Imetniki storitev overitelja morajo uporabljati module za šifriranje skladno z zahtevami glede na vrsto potrdila overitelja.

## 7 PROFIL POTRDIL IN LIST PREKLICANIH POTRDIL

### 7.1 Profil potrdil

#### 7.1.1 Različica potrdil

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

<i>Signature</i>	Overiteljev podpis
<i>Issuer</i>	Edinstveno razločevalno ime overitelja
<i>Validity</i>	Datum aktiviranja in poteka veljavnosti potrdila
<i>Subject</i>	Edinstveno razločevalno ime lastnika potrdila
<i>SubjectPublicKeyInformation</i>	Oznaka algoritma ključa
<i>Version</i>	Različica potrdila X.509
<i>SerialNumber</i>	Edinstvena serijska številka

#### 7.1.2 Razširitvena polja

Razširitvena polja so namenjena uporabi dodatnih atributov v X.509 v3 potrdilih. Standardna razširitvena polja so definirana v skladu z RFC2459, ki dovoljuje tudi definiranje in dodajane lastnih razširitvenih polj za potrebe overiteljev. Dodana posebna razširitvena polja za potrebe overitelja so definirana v 7.1.2.2.

##### 7.1.2.1 Standardna razširitvena polja

<i>Naziv atributa</i>	<b>Kritičen</b>	<b>Opis</b>
<i>authorityKeyIdentifier</i>	•	Doda CA aplikacija
<i>subjectKeyIdentifier</i>		Doda CA aplikacija
<i>KeyUsage</i>	•	Kot je opisano v 6.1.9
<i>privateKeyUsagePeriod</i>		Kot je opisano v 6.3.2
<i>certificatePolicies</i>		OID oznaka vrste potrdila in URI objave pravil delovanja
<i>cRLDistributionPoints</i>		Naslovi na katerih je objavljen register preklicanih potrdil
<i>policyMappings</i>		Uporabljeno v potrdilu za medsebojno priznavanje
<i>subjectAlternativeName</i>		Elektronski poštni naslov
<i>issuerAlternativeName</i>		Se ne uporablja
<i>subjectDirectoryAttributes</i>		Se ne uporablja
<i>nameConstraints</i>	•	Uporabljeno v potrdilu za medsebojno priznavanje
<i>basicConstraint</i>	•	Uporabljeno v potrdilu za medsebojno priznavanje
<i>policyConstraints</i>	•	Uporabljeno v potrdilu za medsebojno priznavanje

##### 7.1.2.2 Posebna razširitvena polja POŠTA<sup>®</sup> CA

<i>Naziv atributa</i>	<b>Kritičen</b>	<b>OID</b>	<b>Sintaksa</b>	<b>Opis</b>
<i>Psdavcna</i>		1.3.6.1.4.1.15284.10.2.1	IA5String	Davčna številka

#### 7.1.3 Identifikacijske oznake (angl. object identifiers) podprtih algoritmov

<b>Algoritem</b>	<b>Identifikacijska oznaka</b>
dsa-with-sha1	1 3 14 3 2 27
sha1WithRSAEncryption	1 2 840 113549 1 1 5



Algoritem	Identifikacijska oznaka
dsa-with-sha1	1 3 14 3 2 27
DES-EDE3-CBC	1 2 840 113549 3 7
cast3CBC	1 2 840 113533 7 66 3
cast3MAC	1 2 840 113533 7 66 4
cast5CBC	1 2 840 113533 7 66 10
cast5MAC	1 2 840 113533 7 66 11
3DESMAC	1 2 840 113533 7 66 14

#### 7.1.4 Oblike imen

Overiteljeva potrdila vsebujejo polno razločevalno ime X.500 (DN) overitelja potrdila 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 potrdilih v skladu s priporočili PKIX Part 1.

#### 7.1.6 Identifikacijska oznaka potrdila

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

#### 7.1.7 Uporaba omejitve imen

Overitelj uporablja polje »*policyConstraints*« v medsebojnih 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 potrdila

Uporabniške aplikacije morajo procesirati razširitvena polja 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. Registri preklicanih potrdil vsebujejo naslednja osnovna polja:

<i>Version</i>	V2
<i>Signature</i>	Overiteljev podpis
<i>Issuer</i>	Razločevalno ime POŠTA <sup>®</sup> CA
<i>thisUpdate</i>	Čas izdaje registra
<i>nextUpdate</i>	Čas izdaje naslednjega registra
<i>revokedCertificate</i>	Serijske številke preklicanih 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:

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

## 8 POSTOPKI Z DOKUMENTACIJO

### 8.1 Postopki spreminjanja vsebine dokumentacije

Overitelj bo izvajal uredniške in tipografske popravke katerega koli dela tega dokumenta in skrbel za njihovo objavo, brez posebnega obvestila. Uredniške in tipografske spremembe 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 trideset (30) dni pred nastopom veljavnosti novega dokumenta. O teh spremembah bodo obveščeni Ministrstvo za informacijsko družbo, Direkcija za poslovno informacijsko središče imetniki potrdil, medsebojno priznani overitelji in druge zainteresirane osebe. Imetniki potrdil bodo obveščeni po elektronski pošti, druge zainteresirane osebe in medsebojno priznani overitelji pa bodo obveščeni s priporočeno poštno pošiljko. Te spremembe zavezujejo le tiste imetnike potrdil, ki bodo potrdila pridobili po uveljavitvi novega dokumenta.

### 8.2 Objavljanje dokumentacije

Kopija tega dokumenta je dostopna na spletnih straneh overitelja na naslovu <http://postarca.posta.si/dokumenti>. Dokument je mogoče pridobiti tudi preko elektronske pošte na naslovu [info.postarca@posta.si](mailto:info.postarca@posta.si).

### 8.3 Odobravanje dokumenta

Ta dokument je odobril upravni svet overitelja.