BANKA SLOVENIJE
EVROSISTEM

Politika overitelja digitalnih potrdil na Banki Slovenije

NOVEMBER, 2023

BANKA SLOVENIJE

EVROSISTEM

Politika overitelja digitalnih potrdil na Banki Slovenije

Za digitalna potrdila za končne uporabnike

Javni del notranjih pravil delovanja

Tip	*Politika (POL)*
Oznaka akta	*POL_15-BS_PP_VOD_03*
Verzija akta	*2*
Skrbnik akta	*Upravljanje tveganj*
Področje (označite področja)	☑ pravice, obveznosti in odgovornosti zaposlenih
	☐ organizacija dela
Organ, ki je akt izdal	*Guverner*

BANKA SLOVENIJE
EVROSISTEM

Politika overitelja digitalnih potrdil na Banki Slovenije

Kazalo

BANKA SLOVENIJE
EVROSISTEM

BANKA SLOVENIJE
EVROSISTEM

BANKA SLOVENIJE
EVROSISTEM

BANKA SLOVENIJE

EVROSISTEM

Na podlagi prvega odstavka 40. člena zakona o Banki Slovenije (Uradni list RS št. 72/06 – uradno prečiščeno besedilo, 59/11 in 55/17) izdajam

Politika overitelja digitalnih potrdil na Banki Slovenije

1 Uvod

V Banki Slovenije (v nadaljevanju: BS) je vzpostavljen delujoč overitelj digitalnih potrdil (v nadaljevanju: overitelj), ki izdaja digitalna potrdila v skladu z organizacijskim okvirom Evropskega sistema centralnih bank za medsebojno priznavanje overiteljev digitalnih potrdil (ESCB Certificate Acceptance Framework – CAF) ter drugimi veljavnimi predpisi in priporočili.

Overitelj izdaja digitalna potrdila izključno zaposlenim v BS in osebam, ki delajo za BS in imajo pogodbeni odnos z BS. Potrdila izdana po tej politiki so izdana na strojnem šifrirnem modulu pametne kartice uporabnika. Izjema so digitalna potrdila za katera je zagotovljena funkcionalnost varnostne kopije zasebnega ključa.

Ta dokument je politika overitelja (angl. Certificate Policy – CP, v nadaljevanju: politika) in predstavlja javni del notranjih pravil delovanja overitelja.

Z vidika standarda X.509 V3 predstavlja politika overitelja nabor pravil, ki določa primernost uporabe digitalnih potrdil med uporabniki, sistemi in aplikacijami, za katere veljajo neke skupne varnostne zahteve.

Politika opisuje tehnične lastnosti in stopnjo varnosti overiteljeve infrastrukture ter postopke, ki jih overitelj uporablja za upravljanje infrastrukture in upravljanje življenjskega cikla izdanih digitalnih potrdil. Politika vsebuje vse bistvene določbe, ki vplivajo na odnos med overiteljem, imetniki digitalnih potrdil, ki jih izdaja overitelj in tretjimi osebami, ki se zanašajo na ta potrdila.

Struktura politike je bila oblikovana po priporočilih referenčnega dokumenta RFC 3647 z naslovom "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" (dokument potrjen novembra 2003), ki ga je pripravila PKIX delovna skupina v IETF (Internet Engineering Task Force). Z namenom zagotavljanja enotne strukture in ugotavljanja medsebojne primerljivosti s politikami drugih overiteljev v Sloveniji in v svetu, so bila v politiko vključena vsa poglavja iz RFC 3647. Poglavja, kjer po tehtni presoji overitelja ni definiranih posebnih pravil, so označena s komentarjem "*ni predpisano*".

Implementacija pravil politike je natančneje določena v splošnih postopkih delovanja overitelja (angl. Certificate Practice Statement - CPS, v nadaljevanju: splošni postopki delovanja overitelja), ki je opisan v dokumentu "Splošni postopki delovanja overitelja na Banki Slovenije" (OID dokumenta: 1.3.6.1.4.1.27213.2.2.1.2.1.2).

Politika je namenjena vsem osebam in organizacijam, ki uporabljajo ali se zanašajo na digitalna potrdila overitelja. Na podlagi politike lahko slednji preverijo stopnjo zaupanja v digitalna potrdila, ki jih izdaja overitelj.

BANKA SLOVENIJE
EVROSISTEM

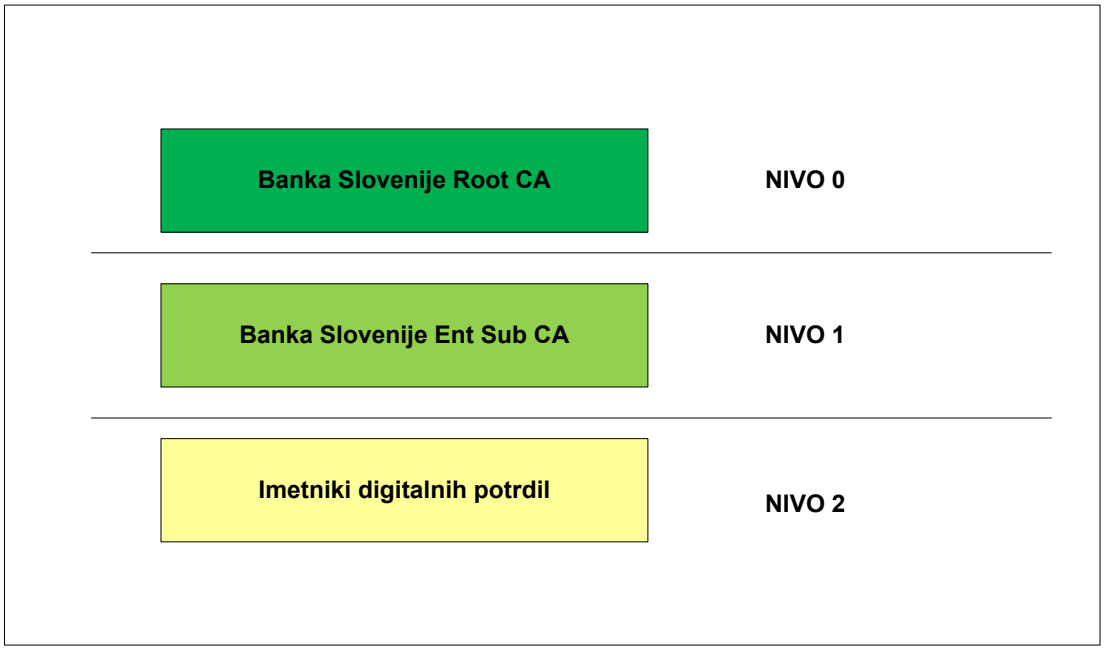
Politika ima po pravilih BS za določanje stopnje zaupnosti status javnega dokumenta in je javno objavljena na spletnih straneh overitelja.

Za informacije, ki niso navedene v tem dokumentu in so v skladu z internim pravilnikom BS na voljo osebam, ki imajo pooblastila za dostop, lahko zainteresirani kontaktirajo osebe navedene v poglavju 1.3.1.

1.1 Predstavitev infrastrukture overitelja

Infrastruktura overitelja je v upravljanju oddelka Informacijska tehnologija v BS (v nadaljevanju: oddelek IT).

Overiteljevo infrastrukturo sestavljata dva hierarhično urejena izdajateljska strežnika, kot prikazuje slika 1:



Slika 1: Overiteljeva infrastruktura Banke Slovenije

Najvišji v hierarhiji je izdajatelj "**Banka Slovenije Root CA**", ki je namenjen za izdajanje digitalnih potrdil sistemov podrejenih izdajateljev digitalnih potrdil.

Podrejeni izdajatelj "**Banka Slovenije Ent Sub CA**" izdaja digitalna potrdila končnim uporabnikom.

BANKA SLOVENIJE
EVROSISTEM

1.2 Naslov dokumenta in identifikacijske oznake izdanih digitalnih potrdil

Polni naslov tega dokumenta je "POLITIKA OVERITELJA NA BANKI SLOVENIJE ZA DIGITALNA POTRDILA ZA KONČNE UPORABNIKE "

Identifikacijska oznaka dokumenta (OID) je: **1.3.6.1.4.1.27213.2.2.1.1.1.2**

Politika velja za digitalna potrdila, ki so označena z identifikacijskimi oznakami politik v tabeli 1:

Tabela 1: Identifikacijske oznake digitalnih potrdil

Identifikacijski podatki	Opis
BS Signature Politika izdajatelja (Issuance OID): **1.3.6.1.4.1.27213.2.1.1.1.1.2**	Digitalno potrdilo z enim parom ključev in obvezno uporabo pametne kartice za kreiranje in hrambo para ključev ter digitalnega potrdila. Pametna kartica je skladna z EAL 4+ ali višjim nivojem. Pripadajoči par ključev se tvori in hrani neposredno na šifrirnem modulu pametne kartice, ki je hkrati tudi identifikacijska kartica BS. Digitalno potrdilo je namenjeno elektronskemu podpisovanju in preverjanju elektronskega podpisa. Doba veljavnosti digitalnega potrdila je 5 let.
BS Encryption Politika izdajatelja (Issuance OID): **1.3.6.1.4.1.27213.2.1.1.1.2.2**	Digitalno potrdilo z enim parom ključev in obvezno uporabo pametne kartice za hrambo para ključev ter digitalnega potrdila. Pametna kartica je skladna z EAL 4+ ali višjim nivojem. Pripadajoči par ključev se tvori na strojnem šifrirnem modulu overitelja in se v okviru postopka izdelave digitalnega potrdila shrani na šifrirni modul pametne kartice, ki je hkrati tudi identifikacijska kartica BS. Varnostna kopija para ključev se varno hrani v okviru storitve arhiva zasebnih ključev za šifriranje. Digitalno potrdilo je namenjeno šifriranju in dešifriranju elektronskih vsebin. Doba veljavnosti digitalnega potrdila je 5 let.

BANKA SLOVENIJE
EVROSISTEM

Identifikacijski podatki	Opis
BS Authentication Politika izdajatelja (Issuance OID): **1.3.6.1.4.1.27213.2.1.1.1.3.2**	Digitalno potrdilo z enim parom ključev in obvezno uporabo pametne kartice za kreiranje in hrambo para ključev ter digitalnega potrdila. Pametna kartica je skladna z EAL 4+ ali višjim nivojem. Pripadajoči par ključev se tvori in hrani neposredno na šifrirnem modulu pametne kartice, ki je hkrati tudi identifikacijska kartica BS. Digitalno potrdilo je namenjeno prijavi v sisteme. Doba veljavnosti digitalnega potrdila je 5 let.

1.3 Subjekti

Poglavje definira subjekte, ki nastopajo v tem dokumentu.

1.3.1 Organizacija v okviru katere deluje overitelj

Overitelj deluje v BS in v skladu z veljavnimi predpisi in priporočili izdaja digitalna potrdila.

Kontaktni podatki overitelja so:

Naslov:	Banka Slovenije Overitelj digitalnih potrdil Slovenska c. 35 1505 Ljubljana
Telefon:	01 4719 140
Fax:	01 2515 516
Elektronska pošta:	PKI@bsi.si
Spletna stran:	http://ca.bsi.si/pki
Center za podporo uporabnikom in preklice potrdil:	01 4719 111 helpdesk@bsi.si

Ostale naloge overitelja so:

- Določanje in objavljanje politike in splošnih postopkov delovanja overitelja;
- Določanje obrazcev za zahtevke v storitvah overitelja;
- Vodenje evidenc z zvezi z digitalnimi potrdili;
- Zagotavljanje delovanja centra za podporo in pomoč uporabnikom;
- Obveščanje uporabnikov;
- Izvajanje ostalih storitev skladno s politiko.

1.3.2 Organ potrjevanja politike

Politike overitelja potrjuje guverner. Splošne postopke delovanja overitelja potrjuje direktor oddelka Informacijska tehnologija.

1.3.3 Izdajatelji digitalnih potrdil

Izdajatelji digitalnih potrdil (angl. CA – Certification Authority) so sistemi, ki izdajajo digitalna potrdila in so določeni v skladu s splošnimi postopki delovanja overitelja.

Izdajatelji, ki delujejo znotraj overitelja na BS so:

Banka Slovenije Root CA, ki je vrhovni izdajatelj digitalnih potrdil overitelja. Digitalna potrdila izdaja za sebe in podrejene izdajatelje digitalnih potrdil overitelja, ter redno objavlja register preklicanih digitalnih potrdil, ki jih je izdal. Izdajatelj je delujoč le v času, ko izvaja naloge, za katere je bil vzpostavljen.

Imetniki digitalnih potrdil izdajatelja **Banka Slovenije Root CA** so lahko samo podrejeni izdajatelji znotraj BS.

Pomembnejši podatki, ki jih vsebuje digitalno potrdilo izdajatelja, so:

Naziv polja	Naziv polja angl.	Vrednosti polja
Verzija	Version	V3
Serijska številka	Serial Number	64 d6 57 2e d9 79 77 84 43 84 43 ec f3 42 f1 02
Identifikator ključa	Subject Key identifier	69 c6 8b 92 01 7f ca 40 1c a4 9f c2 dc a4 85 91 27 23 dc 19
Izdajatelj potrdila	Issuer	CN = Banka Slovenije Root CA O = Banka Slovenije C = SI
Imetnik potrdila	Subject	CN = Banka Slovenije Root CA O = Banka Slovenije C = SI
Veljavnost potrdila od	Valid from	14. junij 2013 11:51:26 CET
Veljavnost potrdila do	Valid to	14. junij 2043 11:51:26 CET
Dolžina RSA ključa	Public Key	4096 bit
Algoritem podpisa	Signature algorithm	sha256RSA
SHA-1 odtis potrdila	Thumbprint:	79 7a 52 04 93 b3 e6 e9 f1 5c d5 a2 d5 15 e9 04 e1 70 4d 32

Banka Slovenije Ent Sub CA je izdajatelj digitalnih potrdil, ki je podrejen izdajatelju Banka Slovenije Root CA. Digitalna potrdila izdaja za končne imetnike digitalnih potrdil. Politika se nanaša na digitalna potrdila, ki jih izdaja izdajatelj.

Pomembnejši podatki, ki jih vsebuje digitalno potrdilo izdajatelja, so:

Naziv polja	Naziv polja angl.	Vrednosti polja
Verzija	Version	V3
Serijska številka	Serial Number	14 fc 79 86 00 00 00 00 00 02
Identifikator ključa	Subject Key identifier	6c 33 15 ad fb b6 1e 0d e8 bb 88 de ba fc 91 cc b1 8d 45 e3
Izdajatelj potrdila	Issuer	CN = Banka Slovenije Root CA O = Banka Slovenije C = SI
Imetnik potrdila	Subject	CN = Banka Slovenije Ent Sub CA O = Banka Slovenije C = SI
Veljavnost potrdila od	Valid from	14. junij 2013 13:08:20 CET
Veljavnost potrdila do	Valid to	14. junij 2028 13:18:20 CET
Dolžina RSA ključa	Public Key	2048 bit
Algoritem podpisa	Signature algorithm	sha256RSA
SHA-1 odtis potrdila	Thumbprint:	25 2a 22 bb c5 6e df 1f a0 ce 49 3a d1 ef dd e7 ce 47 80 d2

1.3.4 Prijavna služba overitelja

Prijavna služba je določena v skladu s splošnimi postopki delovanja overitelja.

Prijavna služba (angl. RA-Registration Authority) sprejema vse zahtevke v zvezi z digitalnimi potrdili, overja identiteto prosilcev za pridobitev digitalnih potrdil, preverja ustreznost podatkov v zahtevkih, zbira vse podatke potrebne za izdajo digitalnega potrdila, potrjuje zahtevke in vodi aktivni status imetnikov digitalnih potrdil.

1.3.5 Arhiv zasebnih ključev

Arhiviranje zasebnih ključev je storitev v okviru katere se varno hranijo kopije zasebnih ključev imetnikov povezanih z digitalnimi potrdili za šifriranje/dešifriranje elektronskih vsebin. Storitev zagotavlja zaupnost hranjenih zasebnih ključev. Hranjene ključe lahko na identifikacijsko kartico BS, ki se glasi na imetnika digitalnega potrdila, povrne pooblaščeno osebje prijavne pisarne overitelja. Odkrivanje zasebnih ključev se lahko izvede le po načelu večkratne odobritve.

Skrbniki kopije zasebnih ključev so posamezniki, ki sodelujejo v postopku odkritja zasebnega ključa imetnika. V postopku morata vsakokrat sodelovati skrbnik kopije zasebnih ključev in pooblaščena oseba prijavne službe overitelja.

BANKA SLOVENIJE
EVROSISTEM

1.3.6 Uporabniki digitalnih potrdil

Uporabniki digitalnih potrdil so imetniki in tretje osebe.

1.3.6.1 Imetniki digitalnih potrdil

Imetniki digitalnih potrdil so subjekti, ki so kot lastniki zasebnih ključev navedeni v digitalnih potrdilih v polju "subject" in so določeni v skladu s splošnimi postopki delovanja overitelja.

Overitelj izdaja digitalna potrdila le na podlagi zahtevka za pridobitev digitalnega potrdila. Posameznik, na katerega se nanaša zahtevek za pridobitev digitalnega potrdila, se imenuje prosilec in ima status prosilca do prevzema digitalnega potrdila, ko postane imetnik digitalnega potrdila. S podpisom zahtevka se prosilci kot bodoči imetniki zavezujejo k spoštovanju in upoštevanju javnega dela notranjih pravil overitelja.

Imetniki digitalnih potrdil overitelja lahko postanejo le zaposleni v BS ali zunanji pogodbeni izvajalci.

Pridobijo lahko paket naprednih digitalnih potrdil za posameznike, ki se hranijo na pametni Identifikacijski kartici BS. Paket vključuje:
- digitalno potrdilo za elektronski podpis, katerega pripadajoči par ključev se tvori in hrani neposredno na kriptografskem strojnem modulu identifikacijske kartice BS;
- digitalno potrdilo za šifriranje, za katerega se pripadajoči par ključev tvori na strojnem šifrirnem modulu overitelja in se v okviru postopka izdelave digitalnega potrdila shrani na strojni kriptografski modul identifikacijske kartice BS, varnostna kopija para ključev pa se varno hrani v okviru storitve za razkrivanje zasebnega ključa za šifriranje;
- digitalno potrdilo za prijavo, katerega pripadajoči par ključev se tvori in hrani neposredno na strojnem kriptografskem modulu identifikacijske kartice BS.

Bolj podrobno so odgovornosti imetnika digitalnih potrdil navedene v poglavju 9.6.3.

1.3.6.2 Tretje osebe

Tretje osebe so subjekti, ki na podlagi javnega ključa vsebovanega v digitalnem potrdilu, ki ga je izdal overitelj, preverjajo identiteto imetnika potrdila ali osebe, ki imetniku pošiljajo šifrirane elektronske vsebine.

V ta namen morajo ravnati v skladu z javnim delom notranjih pravil overitelja in preverjati namen uporabe, status ter čas veljavnosti digitalnih potrdil, ki jih je izdal overitelj. Bolj podrobno so odgovornosti tretjih oseb navedene v poglavju 9.6.4.

Tretje osebe so lahko, niso pa nujno, imetniki digitalnih potrdil overitelja ali digitalnih potrdil drugih izdajateljev.

BANKA SLOVENIJE
EVROSISTEM

1.4 Namen uporabe digitalnih potrdil

Digitalna potrdila overitelja izdana po tej politiki se lahko uporabljajo samo za potrebe izvajanja poslovnih procesov BS. V ta namen se lahko uporabljajo tudi v aplikacijah v okviru Evropskega sistema centralnih bank (ESCB - European System of Central Banks).

Digitalna potrdila izdana pod to politiko se lahko uporabljajo za prijavo v računalniške sisteme, elektronsko podpisovanje in šifriranje podatkov v elektronski obliki ter izkazovanje istovetnosti imetnikov. Vrsta uporabe je odvisna od tipa digitalnega potrdila, ki je opredeljen v polju namen uporabe (angl. key usage) in polju razširjena uporaba ključa (angl. extended key usage).

1.4.1 Pravilna uporaba digitalnih potrdil in ključev

Vsakemu digitalnemu potrdilu pripada par ključev, ki ga sestavljata zasebni in javni ključ.

Vsakemu imetniku pripadajo tri digitalna potrdila:
- za digitalno podpisovanje / overjanje podpisa
  Imetnik potrdila lahko zasebni ključ uporabi za digitalno podpisovanje podatkov v elektronski obliki. Pripadajoči javni ključ lahko tretje osebe ali imetnik uporabijo za potrjevanje verodostojnosti elektronskega podpisa.
- za šifriranje / dešifriranje
  Tretje osebe ali imetnik lahko javni ključ imetnika uporabijo za šifriranje podatkov v elektronski obliki. Imetnik lahko zasebni ključ uporabi za dešifriranje podatkov.
- za prijavo v računalniške sisteme
  Imetnik lahko par ključev uporabi za prijavo v računalniške sisteme BS ali za prijavo v računalniške sisteme organizacij, ki za prijavo dovoljujejo uporabo digitalnih potrdil overitelja.

1.4.2 Nepravilna uporaba digitalnih potrdil in ključev

Potrdila, ki jih izdaja overitelj in pripadajoči pari ključev se lahko uporabljajo le v skladu z veljavno zakonodajo in v skladu s pravili, opredeljenimi v tej politiki, izključno za namene navedene v točki 1.4.1. Za uporabo izven tega overitelj ne odgovarja.

1.5 Urejanje politike overitelja

Politika in splošni postopki delovanja overitelja se redno pregledujejo. Pogostnost obveznega pregledovanja je natančneje opredeljena v splošnih postopkih delovanja overitelja.

1.5.1 Kontaktne osebe

Odgovorna kontaktna oseba overitelja za upravljanje politike in splošnih postopkov delovanja je določena v internih pravilnikih BS in je dosegljiva na naslednjem naslovu:

Banka Slovenije Overitelj digitalnih potrdil Slovenska c. 35, 1505 Ljubljana E-mail: PKI@bsi.si

1.5.2 Postopki spreminjanja vsebine dokumentacije

Postopek rednega pregledovanja in dopolnjevanja politike overitelja je določen v splošnih postopkih delovanja overitelja.

Postopek zagotavlja veljavnost dokumenta z zakonodajo in zahtevami za medsebojno priznavanje izdajateljev digitalnih potrdil v okviru ESCB.

Postopek zagotavlja usklajenost infrastrukture in splošnih postopkov delovanja overitelja z določili politike.

1.5.3 Oseba za ugotavljanje skladnosti CPS s politiko

Skladnost CPS s politiko preverja vodja informacijske varnosti.

1.5.4 Objavljanje dokumentacije

Vse spremembe, vključno s kopijo tega dokumenta, bodo ob nastopu veljavnosti popravkov objavljene na spletnih straneh overitelja na naslovu http://ca.bsi.si/pki.

1.6 Pomen izrazov in kratic

V okviru pričujočega dokumenta imajo določeni izrazi pomen, ki je specifičen za BS. V nadaljevanju dokumenta se, v kolikor ni to posebej navedeno, izrazi nanašajo na pomen, zabeležen v tem poglavju.

CPS (angl. Certificate Practice Statement) ali splošni postopki delovanja overitelja so dokument, ki dopolnjuje politiko in natančneje definira postopke overitelja.

Digitalna identiteta, digitalni ID (angl. Digital Identity, Digital ID) je par ključev – zasebni in javni – ter digitalno potrdilo javnega ključa, ki ga izda overitelj.

Digitalno potrdilo je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto. Digitalno potrdilo vsebuje eno digitalno potrdilo X.509, s katerim overitelj jamči istovetnost digitalne identitete imetnika potrdila.

BANKA SLOVENIJE
EVROSISTEM

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 na podlagi naprednega digitalnega potrdila.

Izdajatelj je podoveriteljski sistem overitelja namenjen izdajanju digitalnih potrdil določene vrste. Overitelj uporablja dva izdajatelja:
- Banka Slovenije Root CA,
- Banka Slovenije Ent SUB CA

Identifikacijska kartica BS je sredstvo za varno elektronsko podpisovanje v obliki plastične pametne kartice z vgrajenim čipom, ki vsebuje procesor in spomin. Uporablja se za varno tvorjenje in hranjenje ključev ter varno izvajanje kriptografskih operacij z zasebnim ključem.

Imetnik potrdila (angl. Subject) je fizična oseba navedena v digitalnem potrdilu v polju »subject« kot lastnik zasebnega ključa, ki ustreza javnemu ključu, navedenem v digitalnem potrdilu.

Informacijski sistem je sistem za oblikovanje, pošiljanje, prejemanje, shranjevanje in druge obdelave podatkov v elektronski obliki.

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.

Napredno digitalno potrdilo je digitalno potrdilo katerega zasebni ključ se izdela in hrani na strojnem šifrirnem modulu na podlagi podatkov za ustvarjanje elektronskega podpisa, ki jih podpisnik z visoko stopnjo zaupanja lahko uporablja izključno pod svojim nadzorom, in je s podatki, ki so na ta način podpisani, povezan tako, da je opazna vsaka naknadna sprememba podatkov.

Objava overitelja je javna objava na spletnih straneh overitelja.

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.

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.

Osebno geslo (PIN, angl. Personal Identification Number) je skrivno geslo uporabnika za avtentikacijo ob uporabi pametne kartice.

Overitelj je fizična ali pravna oseba, ki izdaja digitalna potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskim podpisovanjem. V tem dokumentu je overitelj Certifikatska agencija Banke Slovenije oziroma krajše Banka Slovenije CA. Sestavljata ga dva izdajatelja: Banka Slovenije Root CA in Banka Slovenije Ent SUB CA. Z infrastrukturo izdajatelja upravlja oddelek Informacijska tehnologija v BS. Overitelj izdaja digitalna potrdila za podoveriteljske sisteme overitelja, digitalna potrdila za zaposlene BS in digitalna potrdila za zunanje pogodbene izvajalce.

BANKA SLOVENIJE
EVROSISTEM

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.

Prijavna služba je pristojna za zbiranje in upravljanje s podatki o imetnikih digitalnih potrdil. Prijavna služba preko programske opreme izdajatelja upravlja zahtevke za vpis, izbris oziroma spremembo podatkov o imetnikih digitalnih potrdil, kar služi kot osnova za izdajo in preklic digitalnih potrdil.

Prosilec je fizična oseba, ki zahteva izdajo digitalnega potrdila v svojem imenu.

Sredstvo za elektronsko podpisovanje je sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve zakona, ki ureja elektronsko poslovanje in elektronski podpis.

Sredstvo za preverjanje je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa.

Sredstvo za varno elektronsko podpisovanje je nastavljena programska ali strojna oprema, ki se uporablja za elektronsko podpisovanje.

Varen elektronski podpis je elektronski podpis, ki izpolnjuje naslednje zahteve:
- da je povezan izključno s podpisnikom;
- da je iz njega mogoče zanesljivo ugotoviti podpisnika;
- da je ustvarjen s sredstvi za varno elektronsko poslovanje, ki so izključno pod podpisnikovim nadzorom;
- da je povezan s podatki, na katere se nanaša, tako, da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi.

Zahtevki so obrazci overitelja za pridobitev ali preklic potrdila, povrnitev zgodovine dešifrirnih ključev digitalnega potrdila ali obnovo digitalnega potrdila. Dostopni so preko spletne strani overitelja http://ca.bsi.si/PKI.

Tabela 2: Seznam kratic

Kratica	Izvirno besedilo	Pomen
CA	Certification Authority [angl.]	overitelj
CN	Common Name [angl.]	X.500 domače ime imetnika digitalnega potrdila
CRL	Certificate Revocation List [angl.]	register preklicanih digitalnih potrdil
CSP	Certification Service Provider [angl.]	ponudnik storitve overjanja in upravljanja digitalnih potrdil
DN	Distinguished Name [angl.]	X.500 razločevalno ime
EAL	Evaluation Assurance Level [angl.]	standard označevanja varnostnih nivojev v računalniških sistemih
FIPS	United State Federal Information Processing Standards [angl.]	oznaka standarda s področja informacijskega procesiranja
HSM	Hardware Security Module [ngl.]	strojni šifrirni modul za varno hranjenje šifrirnih ključev in digitalnih potrdil.
PIN	Personal Identification Number [angl.]	osebno geslo
PKCS	Public Key Cryptographic Standards [angl.]	šifrirni standardi na področju javnih ključev
PKIX-CMP	Public Key Infrastructure (based on) X.509 Certificate Management Protocols [angl.]	protokol za izmenjavo ključev in upravljanje certifikatov
RA	Registration Authority [angl.]	prijavna služba overitelja
SSCD	Secure Signature Creation Device [angl.]	naprava za varno oblikovanje podpisa (pametna kartica)

2 Objave informacij in imeniki

2.1 Objavljene informacije in imeniki

BS je v zvezi z delovanjem overitelja dolžna obveščati imetnike in tretje osebe.

Javno dostopne informacije so objavljene na spletnih straneh overitelja, na naslovu http://ca.bsi.si/PKI.

Javno dostopni morajo biti naslednji dokumenti in imeniki:
- Politika delovanja overitelja;
- Podatki o vsakokrat veljavnem javnem ključu izdajateljev Banka Slovenije Root CA in Banka Slovenije Ent Sub CA;
- Register preklicanih potrdil (profil registra in naslov objave je podrobneje opisan v poglavju 7.2). Register elektronsko podpiše izdajatelj, ki ga izda;
- Ostale javne informacije o delovanju overitelja.

Splošni postopki delovanja overitelja in imenik izdanih potrdil niso javno dostopni.

Splošni postopki delovanja overitelja so dostopni le pooblaščenemu osebju overitelja in so objavljeni na intranetnih straneh BS.

Od izdanih potrdil se objavljajo le digitalna potrdila za šifriranje, ki so objavljena v internem aktivnem imeniku Windows domene BS. Imenik je dostopen uporabnikom z veljavno domensko prijavo.

2.2 Pogostnost objav

Dokumenti o politiki in splošnih postopkih delovanja overitelja se objavijo najkasneje do konca naslednjega delovnega dne od trenutka, ko postanejo veljavni.

Register preklicanih digitalnih potrdil se objavi kot je opredeljeno v poglavjih 4.9.7 in 4.9.8. Digitalna potrdila za šifriranje se objavijo v imeniku takoj, ko so izdana.

Ostale informacije so objavljene po potrebi.

2.3 Dostop do objavljenih informacij

Vse javno objavljene informacije so brez omejitev dostopne za branje in so s sistemom dostopnih pravic zaščitene pred nepooblaščenim spreminjanjem.

3 Overjanje istovetnosti

Preden prosilec prevzame digitalno potrdilo je potrebno overiti njegovo istovetnost.

3.1 Določanje imen

Določanje imen opredeljuje identifikacijske podatke imetnika, ki so vključeni v digitalno potrdilo.

3.1.1 Vrste imen

Digitalna potrdila vsebujejo razločevalna imena (ang. DN – Distinguished name), ki enolično določajo identiteto imetnika potrdila. Vsako digitalno potrdilo, ki ga izda overitelj, vsebuje:

- Razločevalno ime o izdajatelju

Naziv polja	**Razločevalno ime**	
Izdajatelj	Ime (CN)	= Banka Slovenije Ent Sub CA
(ang. "Issuer")	Organizacija (O)	= Banka Slovenije

BANKA SLOVENIJE
EVROSISTEM

	Država (C)		= SI

- Razločevalno ime o imetniku

Naziv polja	**Razločevalno ime**		
Imetnik (ang. "Subject")	Ime (CN)		= Priimek, ime imetnika
	Serijska (SerialNumber)	številka	= serijska številka
	Organizacija (O)		= organizacija imetnika potrdila
	Država (C)		= SI

Razločevalna imena so oblikovana v skladu s standardoma RFC 5280 in X.501.

Edinstveno serijsko številko določi overitelj.

Razločevalno ime lahko vsebuje dodatna polja, ki ne zamenjujejo zgoraj navedenih polj in niso potrebna za določanje identitete imetnika potrdila.

3.1.2 Potreba po smiselnosti imen

Razločevalna imena imetnikov digitalnih potrdil morajo biti smiselna in se oblikujejo po pravilih, opredeljenih v točki 3.1.1.

3.1.3 Anonimnost imetnikov in uporaba psevdonimov

"Ni predpisano".

3.1.4 Pravila za interpretacijo različnih oblik imen

Imena so sestavljena iz črk angleške abecede.

Znaki, ki se ne uporabljajo v angleški abecedi in so navedeni v tabeli 3, se pretvorijo po pravilih iz tabele 3.

Tabela 3: Pretvorba znakov

Znak	Pretvorba
Č	C
Š	S
Ž	Z
Ć	C
Đ	D
Ä	AE
Ö	OE
Ü	UE
Á	A
É	E
Í	I
Ó	O
Ú	U

Znak	Pretvorba
À	A
È	E
Ì	I
Ò	O
Ù	U
Ê	E
Ô	O
Ő	O
Ű	U

Vsi ostali znaki se pretvorijo tako, kot je opredeljeno v dokumentih "ICAO Doc 9303" v poglavju za pretvorbo znakov (ang. transliteration).

3.1.5 Edinstvenost imen

Overitelj dodeli vsakemu imetniku potrdila edinstveno, neponovljivo razločevalno ime, ki je objavljeno v polju »subject« potrdila. Postopek zagotavljanja edinstvenosti imena je opredeljen v splošnih postopkih delovanja overitelja.

3.1.6 Postopek reševanja imenskih sporov

Overitelj s postopkom edinstvenosti imen zagotavlja, da ne prihaja do imenskih sporov.

3.1.7 Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk

"Ni predpisano".

3.2 Preverjanje istovetnosti ob prvi registraciji

Digitalno potrdilo vzpostavlja zaupanje med imetnikom potrdila in parom ključev, katerega javni ključ je vsebovan v digitalnem potrdilu. Osnova za vzpostavitev zaupanja sta preverjanje istovetnosti prosilca ob prvi registraciji za pridobitev digitalnega potrdila overitelja in dokazovanje posesti zasebnega ključa v času izdaje digitalnega potrdila.

3.2.1 Metoda za dokazovanje posesti zasebnega ključa

Digitalno potrdilo vzpostavlja zaupanje med imetnikom digitalnega potrdila in njegovim zasebnim ključem.

Pri paketu naprednih digitalnih potrdil za zaposlene BS ali zunanje pogodbene izvajalce, se pari ključev tvorijo v okviru avtomatiziranega postopka personalizacije identifikacijske kartice BS, na kateri se ključi tudi varno hranijo. Zato posebno dokazovanje posesti zasebnega ključa ni predvideno. S postopkom personalizacije identifikacijskih kartic BS upravlja prijavna služba overitelja.

Kontrola povezave med zasebnim in javnim ključem, vsebovanim v zahtevku za izdajo digitalnega potrdila in oblika zahtevka sta standardizirana in sta natančneje opredeljena v splošnih postopkih delovanja overitelja.

3.2.2 Overjanje istovetnosti pravnih oseb

Overitelj izdaja digitalna potrdila izključno zaposlenim v BS ali zunanjim pogodbenim izvajalcem.

Imetniki digitalnih potrdil overitelja, ki so zaposleni v BS in imetniki digitalnih potrdil overitelja, ki imajo kot fizične osebe pogodbeni odnos z BS, zastopajo organizacijo "Banka Slovenije". Dodatno overjanje identitete organizacije "Banka Slovenije" ni predvideno.

Imetniki digitalnih potrdil overitelja, ki so zaposleni v organizaciji, ki ima pogodbeni odnos z BS, zastopajo organizacijo v kateri so zaposleni. Istovetnost organizacije se overja na podlagi potrjene dokumentacije ali s podatki iz uradnih evidenc. Zastopa jo zakoniti zastopnik ali pooblaščena oseba. Odgovorna oseba oddelka BS, ki je predlagatelj pogodbenega razmerja BS z organizacijo, mora zagotoviti izvedbo overjanja istovetnosti organizacije in overjanja pogodbenega odnosa med organizacijo in imetnikom potrdila, kar potrjuje s podpisom zahtevka za izdajo digitalnega potrdila.

3.2.3 Overjanje istovetnosti fizične osebe

Identiteta fizične osebe se overja ob fizični prisotnosti osebe na osnovi uradnega osebnega dokumenta ali obstoječe identifikacijske kartice BS, ki je bila pridobljena po postopku preverjanja ob fizični prisotnosti osebe na osnovi uradnega osebnega dokumenta.

Preverijo se naslednji podatki:
- Ime in priimek
- EMŠO (za državljane Republike Slovenije), ali primerljivi enolični nacionalni identifikator (za tujce).

3.2.4 Podatki o prosilcih, ki se ne preverjajo

"Ni predpisano".

3.2.5 Preverjanje pooblastil v zahtevkih prosilcev

Prijavna služba overitelja preverja ustreznost pooblastil podpisnikov v zahtevkih za pridobitev digitalnih potrdil. Postopek preverjanja je natančneje opisan v splošnih postopkih delovanja overitelja.

3.2.6 Merila za medsebojno povezovanje

Overitelj se lahko povezuje ali priznava z drugimi overitelji na podlagi pogodbe o medsebojnem priznavanju.

Overitelj se po lastni presoji povezuje z drugimi overitelji, ki morajo izpolnjevati vsaj enak nivo zahtev kot jih predpiše overitelj na BS. Kriteriji za povezave z ostalimi overitelji so navedeni v splošnih postopkih delovanja overitelja.

3.3 Overjanje istovetnosti ob zahtevi za menjavo ključev

Rutinska menjava ključev in menjava zaradi preklica obstoječega para ključev se izvede na podlagi zahtevka posredovanega prijavni službi overitelja.

Identiteta prosilcev se preverja ob fizični prisotnosti na osnovi obstoječe identifikacijske kartice BS. V kolikor prosilec ne razpolaga z identifikacijsko kartico BS je postopek enak kot pri prvi registraciji.

Vsi ostali postopki so enaki kot pri prvi registraciji.

3.4 Overjanje istovetnosti ob zahtevi za preklic potrdila

Zahtevo za preklic digitalnega potrdila lahko prijavni službi overitelja posreduje:
- imetnik osebno ali s posredovanjem pisne zahteve za preklic.
- odgovorna oseba oddelka imetnika potrdila, ki posreduje pisno zahtevo za preklic.

Istovetnost predlagatelja za preklic digitalnega potrdila overi prijavna služba overitelja. Postopek overjanja je natančneje opisan v splošnih postopkih delovanja overitelja.

4 Upravljanje z digitalnimi potrdili

V tem delu so opredeljene zahteve za upravljanje z digitalnimi potrdili v vseh fazah njihovega življenjskega cikla.

4.1 Zahtevki za pridobitev potrdila

Overitelj izdaja digitalna potrdila le na podlagi pisnega zahtevka.

4.1.1 Kdo lahko zaprosi za izdajo digitalnega potrdila

Za zaposlene v BS lahko zahtevek za izdelavo identifikacijske kartice BS posreduje oddelek Organizacija in kadri.

Za zunanje pogodbene izvajalce lahko zahtevek za izdelavo identifikacijske kartice BS posreduje odgovorna oseba oddelka BS, ki je predlagatelj za sklenitev pogodbenega odnosa s prosilcem za pridobitev digitalnega potrdila.

BANKA SLOVENIJE
EVROSISTEM

Overitelj na podlagi prejetega zahtevka za izdelavo identifikacijske kartice BS za bodočega imetnika kartice izdela tudi paket naprednih digitalnih potrdil.

Zahtevke za redno menjavo digitalnega potrdila lahko imetniki prijavni službi overitelja posredujejo sami.

4.1.2 Izpolnitev zahtevka za izdajo digitalnega potrdila in odgovornosti prosilca

Zahtevek za pridobitev digitalnega potrdila je dostopen na spletnih straneh overitelja. Predlagatelj izpolnjen in podpisan zahtevek posreduje prijavni službi overitelja.

Predlagatelj je v zahtevku za pridobitev digitalnega potrdila dolžan navesti resnične in pravilne podatke o prosilcu.

Prosilec ob prevzemu podpiše izjavo o pravilnosti podatkov, navedenih v digitalnem potrdilu, ter seznanitvi in strinjanju s pogoji uporabe parov ključev in digitalnih potrdil.

4.2 Obdelava zahtevka za izdajo digitalnega potrdila

4.2.1 Preverjanje istovetnosti podatkov o prosilcu

Osebje prijavne službe overitelja preveri istovetnost podatkov, ki jih je prosilec navedel v zahtevku za pridobitev digitalnega potrdila, s podatki o prosilcu, ki so vnešeni v kadrovski evidenci BS. Postopek je natančneje opisan v splošnih postopkih delovanja overitelja.

4.2.2 Odobritev ali zavrnitev zahtevka

Zahtevek za pridobitev digitalnega potrdila odobri ali zavrne osebje prijavne službe overitelja.

Zahtevek se zavrne v primeru nepravilnih ali pomanjkljivih podatkov.

O morebitni zavrnitvi zahtevka je predlagatelj obveščen pisno ali po elektronski pošti.

4.2.3 Čas za obdelavo zahtevka za izdajo digitalnega potrdila

Overitelj ne prevzema odgovornosti za zamudo v postopku obdelave zahtevka in izdelave digitalnega potrdila.

Praviloma so zahtevki obdelani in v primeru odobritve digitalna potrdila izdana v roku enega delovnega dne od prejema zahtevka.

BANKA SLOVENIJE
EVROSISTEM

4.3 Izdaja potrdila

4.3.1 Aktivnosti izdajatelja ob izdaji digitalnega potrdila

Izdajatelj, ki deluje v okviru overitelja, izda digitalno potrdilo na osnovi elektronskega zahtevka, ki ga prejme od overiteljevega sistema za upravljanje z identifikacijskimi karticami BS.

Elektronski zahtevki med sistemom za upravljanje z identifikacijskimi karticami BS in programsko opremo izdajatelja so standardizirani in se izmenjujejo po varnem protokolu.

Za vsak prejeti zahtevek izdajatelj preveri skladnost s tehnično specifikacijo oblike zahtevka in v primeru ustreznosti izda digitalno potrdilo, ki ga podpiše s svojim privatnim ključem.

Natančneje je postopek opisan v splošnih postopkih delovanja overitelja.

4.3.2 Obvestilo imetniku o izdaji digitalnega potrdila

Izdajatelj ne obvešča imetnikov o izdaji digitalnega potrdila.

Imetnika o izdaji digitalnega potrdila obvesti prijavna služba overitelja ob vročitvi identifikacijske kartice BS.

4.4 Prevzem potrdila

4.4.1 Postopek prevzema digitalnega potrdila

Prosilec postane imetnik digitalnega potrdila s prevzemom identifikacijske kartice BS.

Prosilec novo identifikacijsko kartico prevzame pri varnostni službi na recepciji BS. Preden varnostna služba prosilcu izroči identifikacijsko kartico:
- overi istovetnost prosilca v skladu z zahtevami opredeljenimi v poglavju 3.2.3.;
- prosilcu posreduje v podpis izjavo o strinjanju s pogoji uporabe, potrditvi pravilnosti podatkov o imetniku vsebovanih v digitalnem potrdilu in prevzemu identifikacijske kartice BS.

4.4.2 Objava digitalnega potrdila

Izdajatelj objavi digitalno potrdilo v internem imeniku, če je objava za to vrsto digitalnega potrdila predvidena.

4.4.3 Obveščanje drugih udeležencev o izdaji digitalnega potrdila

"Ni predpisano".

BANKA SLOVENIJE
EVROSISTEM

4.5 Uporaba para ključev in digitalnega potrdila

4.5.1 Uporaba para ključev in digitalnega potrdila s strani imetnika

Imetnik lahko par ključev in digitalno potrdilo uporablja le za namene opredeljene v poglavju 1.4. Namen uporabe je označen v poljih digitalnega potrdila namen uporabe (angl. key usage) in razširjeni namen uporabe (angl. extended key usage).

Imetniki lahko par ključev in digitalno potrdilo uporabljajo le, če so podpisali izjavo o seznanitvi in strinjanju s pogoji uporabe digitalnih potrdil.

Imetniki so zato, da preprečijo izgubo, razkritje, spremembo ali nepooblaščeno uporabo dolžni varovati identifikacijske kartice BS in kode za dostop do podatkov na kartici kot je navedeno v poglavju 9.6.3.

4.5.2 Uporaba javnega ključa in digitalnih potrdil s strani tretjih oseb

Tretje osebe se lahko zanašajo na digitalno potrdilo izdano s strani overitelja v BS le za namene opredeljene v poglavju 1.4 in 1.4.1.

Tretje osebe so pred vsako uporabo dolžne preveriti čas in status veljavnosti digitalnega potrdila, ob uporabi pa upoštevati vsa določila in omejitve politike.

4.6 Obnova potrdila brez menjave ključev

Pari ključev in digitalna potrdila imajo enako življenjsko dobo, zato se ob obnovi digitalnega potrdila vedno zahteva tudi menjava ključev.

Posledično poglavja 4.6.1 do 4.6.7 iz standarda RFC 3647 niso vključena v politiko delovanja overitelja in za njih velja vrednost "Ni predpisano".

4.7 Obnova digitalnega potrdila

4.7.1 Razlogi za obnovo digitalnih potrdil

Razlog za obnovo digitalnega potrdila je lahko:
- pretek veljavnosti obstoječega digitalnega potrdila;
- sprememba identifikacijskih podatkov navedenih v digitalnem potrdilu;
- sum zlorabe para ključev;
- sprememba oblike zapisa digitalnega potrdila.

Redna obnova digitalnih potrdil se lahko izvede v obdobju zadnjih 30 dni veljavnosti obstoječega digitalnega potrdila.

4.7.2 Kdo lahko zaprosi za obnovo digitalnega potrdila

Zahtevek za obnovo svojega digitalnega potrdila lahko posreduje imetnik potrdila.

4.7.3 Obdelava zahtevkov za obnovo digitalnega potrdila

Prijavna služba overitelja preveri, da so identifikacijski podatki imetnika še vedno veljavni. Vse morebitne spremembe identifikacijskih podatkov morajo biti zavedene tudi v novi izjavi o seznanitvi in strinjanju s pogoji uporabe digitalnih potrdil.

Ob obnovi se mora imetnik osebno zglasiti v prijavni službi overitelja in se identificirati z obstoječo identifikacijsko kartico BS.

Postopek je natančneje opisan v splošnih postopkih delovanja overitelja.

4.7.4 Obvestilo imetniku o izdaji obnovljenega digitalnega potrdila

Ker se obnova digitalnega potrdila izvede ob fizični prisotnosti imetnika potrdila, dodatno obveščanje o izdaji novega digitalnega potrdila ni predvideno.

4.7.5 Postopek potrditve prevzema obnovljenega digitalnega potrdila

Ob prevzemu obnovljenega digitalnega potrdila na obstoječo identifikacijsko kartico BS imetnik v prijavni službi podpiše izjavo o prevzemu.

4.7.6 Objava obnovljenega digitalnega potrdila

Izdajatelj objavi digitalno potrdilo v imeniku, če je objava za to vrsto digitalnega potrdila predvidena.

4.7.7 Obveščanje drugih udeležencev o izdaji potrdila

"Ni predpisano".

4.8 Sprememba potrdila

Vse spremembe v digitalnih potrdilih se izvede po postopku za obnovo digitalnega potrdila določenem v poglavju 4.7.

Poseben postopek za spremembo digitalnega potrdila ni predviden. Posledično poglavja 4.8.1 do 4.8.7 iz standarda RFC 3647 niso vključena v politiko delovanja overitelja in za njih velja vrednost "Ni predpisano".

BANKA SLOVENIJE
EVROSISTEM

4.9 Preklic in začasna razveljavitev digitalnega potrdila

Preklic digitalnega potrdila je postopek, v okviru katerega se prekliče veljavnost digitalnega potrdila, ki se objavi v javnem registru preklicanih digitalnih potrdil (ang. CRL – Certificate Revocation List).

4.9.1 Razlogi preklica

Overitelj lahko prekliče potrdilo iz naslednjih razlogov:
- dejansko ali domnevno ogrožanje zasebnih ključev;
- spremembe podatkov v potrdilu, ki zahtevajo izdajo novega;
- neskladnost z zahtevami opredeljenimi v varnostni politiki overitelja;
- imetnikovo neupoštevanje določil o pogojih uporabe digitalnih potrdil;
- prekinitev pogodbenega razmerja med imetnikom in BS ali napovedana daljša odsotnost imetnika;
- na podlagi prejete pisne zahteve za preklic digitalnega potrdila.

4.9.2 Kdo lahko zahteva preklic

Preklic potrdila lahko zahteva:
- imetnik potrdila;
- odgovorna oseba oddelka BS, v katerem je imetnik zaposlen, oziroma je predlagatelj za sklenitev pogodbenega razmerja BS z imetnikom;
- zaposleni pri overitelju v primeru:
    - ko overitelj izve, da je imetnik potrdila prekinil delovno razmerje ali pogodbeni odnos z BS 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.

4.9.3 Postopek za preklic digitalnega potrdila

Digitalno potrdilo, ki ga izda overitelj na BS, se lahko prekliče po standardnem ali po izrednem postopku.

Standardni postopek se uporablja v rednem delovnem času overitelja (vsak delavni dan od 6:30 – 17:00). V standardnem postopku se lahko zahteva za preklic overitelju pošlje na naslednje načine:
- imetnik potrdila zahteva preklic osebno na prijavni službi overitelja.

- imetnik potrdila ali odgovorna oseba oddelka BS, v katerem je imetnik zaposlen, oziroma je predlagatelj za sklenitev pogodbenega razmerja BS z imetnikom, pošlje na elektronski naslov overitelja (glej poglavje 1.3.1) zahtevek za preklic digitalnega potrdila. Sporočilo z zahtevkom mora elektronsko podpisati s svojim digitalnim potrdilom, ki ga je izdal overitelj na BS. Hkrati mora o tem telefonsko obvestiti overitelja s klicem na telefonsko številko za preklice potrdil (glej poglavje 1.3.1).

Izredni postopek se uporablja izven rednega delovnega časa overitelja (vsak delovni dan od 17:00 do 6:30, ob vikendih in ob praznikih). V izrednem postopku lahko imetnik digitalnega potrdila preklic zahteva telefonsko s klicem na telefonsko številko za preklice potrdil (glej poglavje 1.3.1). Prijavna služba overitelja v tem primeru digitalno potrdilo začasno razveljavi (po postopku kot je določen v poglavju 4.9.15).

V zahtevi za preklic mora biti obvezno naveden razlog za preklic.

Ko prijavna služba overitelja prejme zahtevo za preklic digitalnega potrdila, preveri če zahtevek vsebuje vse zahtevane podatke, overi identiteto pošiljatelja zahtevka za preklic in preveri skladnost razloga za preklic digitalnega potrdila z razlogi, ki so navedeni poglavju 4.9.1. Če ni razlogov za zavrnitev zahtevka za preklic, osebje prijavne službe overitelja izvede preklic digitalnega potrdila in sproži postopek osveževanja in objave registra preklicanih digitalnih potrdil. Če je zahtevek za preklic zavrnjen, prijavna služba overitelja o tem obvesti pošiljatelja zahtevka.

Poleg zgoraj omejenih postopkov za redni in izredni preklic lahko osebje overitelja prekliče digitalno potrdilo imetnika tudi, ko se seznani z enim od razlogov za preklic digitalnega potrdila navedenih v poglavju 4.9.1.

Osebje overitelja o preklicu digitalnega potrdila, datumu preklica in razlogih za preklic obvesti imetnika digitalnega potrdila.

Overitelj ohrani kopijo digitalne identitete, katere digitalno potrdilo je bilo preklicano. Slednje lahko na podlagi zahtevka pristojne službe izda v primerih, ko je potrebno digitalno identiteto uporabiti za dešifriranje šifriranih podatkov.

4.9.4 Čas za posredovanje zahtevka za preklic

V primeru zaznavanja okoliščin, ki zahtevajo preklic digitalnega potrdila, morajo osebe, ki lahko zahtevajo preklic digitalnega potrdila, v najkrajšem možnem času overitelju podati zahtevek za preklic digitalnega potrdila.

4.9.5 Čas od prejema zahtevka za preklic do preklica potrdila

Overitelj po prejemu upravičene zahteve za preklic digitalno potrdilo prekliče čim hitreje, v vsakem primeru pa najkasneje v roku 1 ure po prejemu zahtevka.

4.9.6 Preverjanje statusa potrdil pred uporabo

Tretje osebe, ki se zanašajo na digitalna potrdila, ki jih izdaja overitelj na BS, so pred vsako uporabo javnega ključa dolžne preveriti register preklicanih potrdil overitelja. Vsakokrat je

veljaven najnovejši register preklicanih digitalnih potrdil objavljen na spletnih straneh overitelja na naslovu podanem v poglavju 7.2. Ti naslovi so navedeni tudi v polju "CRL distribution point" v vsakem digitalnem potrdilu, ki ga izda overitelj na BS. Register preklicanih digitalnih potrdil je podpisan z zasebnim ključem izdajatelja s katerim le ta podpisuje izdana digitalna potrdila.

4.9.7 Pogostost objav registra preklicanih digitalnih potrdil (angl. CRL)

Veljavnosti registrov preklicanih digitalnih potrdil izdajateljskih strežnikov overitelja so podane v tabeli 4.

Tabela 4: Obdobja veljavnosti registra preklicanih certifikatov

Izdajateljski strežnik overitelja	**Obdobje veljavnosti CRL**	**Pogostnost objav CRL**
Banka Slovenije CA Root	1 leto	Vsako leto
Banka Slovenije CA Ent SUB (celoten register)	7 dni	Vsake 4 dni
Banka Slovenije CA Ent SUB (spremembe)	1 dan	Vsak dan

Nov register se objavi pred potekom veljavnosti starega.

Ob preklicu potrdila osebje prijavne službe ročno proži objavo nove verzije registra preklicanih digitalnih potrdil.

4.9.8 Maksimalne zakasnitve pri objavi registra preklicanih digitalnih potrdil

Register preklicanih digitalnih potrdil je objavljen najkasneje v 1 uri po kreiranju novega registra.

4.9.9 Storitev sprotnega preverjanja statusa digitalnih potrdil

Sprotno preverjanje statusa digitalnih potrdil je dostopno preko protokolov HTTP in OCSP.

4.9.10 Obveza tretjih oseb po sprotnem preverjanju statusa preklicanih potrdil

Tretje osebe morajo ob uporabi potrdila vedno preveriti, ali je potrdilo, na katerega se zanašajo, preklicano.

4.9.11 Ostale oblike objavljanja preklicanih digitalnih potrdil

"Ni predpisano".

4.9.12 Posebne zahteve za preklic digitalnih potrdil v primeru zlorabe ključev

"Ni predpisano".

4.9.13 Razlogi za začasno razveljavitev digitalnega potrdila

Začasna razveljavitev digitalnega potrdila je postopek zaradi katerega postane digitalno potrdilo nedelujoče še pred potekom njegove veljavnosti. Razveljavitev mora biti vedno začasna oziroma časovno omejena. Začasna razveljavitev digitalnega potrdila imetniku potrdila onemogoča njegovo uporabo. V času začasne razveljavitve je digitalno potrdilo javno objavljeno v registru preklicanih digitalnih potrdil (CRL).

Digitalno potrdilo se lahko začasno razveljavi v naslednjih primerih:
- sum razkritja digitalnega potrdila
- ko osebje overitelja prejme zahtevo za preklic potrdila, vendar ne more preveriti pooblastila osebe, ki je podala zahtevo (npr. preklic digitalnega potrdila po izrednem postopku)

4.9.14 Kdo lahko zahteva ali prekliče začasno razveljavitev digitalnega potrdila

Začasno razveljavitev digitalnega potrdila lahko zahteva:
- imetnik digitalnega potrdila
- osebje overitelja v primeru suma razkritja digitalnega potrdila

Začasno razveljavitev digitalnega potrdila lahko prekliče prijavna služba overitelja.

4.9.15 Postopek za začasno razveljavitev digitalnega potrdila

Imetnik digitalnega potrdila v primeru suma razkritja ali drugega prepoznanega ogrožanja digitalnega potrdila prijavni službi overitelja takoj posreduje zahtevek za začasno razveljavitev digitalnega potrdila.

Prav tako se kot zahtevek za začasno razveljavitev digitalnega potrdila šteje preklic digitalnega potrdila, ki se izvede po izrednem postopku (kot je opredeljen v poglavju 4.9.3). Ker izredni postopek preklica digitalnega potrdila ne omogoča overjanja identitete pošiljatelja zahtevka, osebje prijavne službe overitelja v tem primeru digitalno potrdilo začasno razveljavi, dokler po rednem postopku ne prejme zahteve za preklic digitalnega potrdila ali zahteve za preklic razveljavitve digitalnega potrdila.

Ko prijavna služba overitelja prejme zahtevo za začasno razveljavitev digitalnega potrdila, overi identiteto pošiljatelja zahtevka in preveri skladnost vzroka za začasno razveljavitev digitalnega potrdila z vzroki, ki so navedeni poglavju 4.9.13. Če ni razlogov za zavrnitev zahtevka za začasno razveljavitev, osebje prijavne službe overitelja izvede začasno razveljavitev digitalnega potrdila in sproži postopek osveževanja in objave registra preklicanih digitalnih potrdil. Če je zahtevek za začasno razveljavitev zavrnjen, prijavna služba overitelja o tem obvesti pošiljatelja zahtevka.

Osebje prijavne službe overitelja o začasni razveljavitvi digitalnega potrdila, datum začasne razveljavitve in razlogih za razveljavitev obvesti imetnika digitalnega potrdila.

4.9.16 Čas začasne razveljavitve digitalnega potrdila

Začasno razveljavljeno digitalno potrdilo ostane razveljavljeno dokler osebje overitelja razveljavitve ne prekliče. Najdaljši dovoljeni čas, ki lahko poteče od začasne razveljavitve do preklica razveljavitve digitalnega potrdila, je 1 delovni dan.

4.10 Storitve preverjanja statusa digitalnih potrdil

4.10.1 Tehnične lastnosti storitve

Register je dostopen na naslovih, ki so navedeni v poglavjih 7.2 in 7.3. Ti naslovi so navedeni tudi v poljih "CRL distribution point" in "Authority Information Access" v vsakem digitalnem potrdilu, ki ga izda overitelj na BS.

4.10.2 Razpoložljivost storitve

Overitelj se obvezuje, da bo razpoložljivost storitve za Register preklicanih digitalnih potrdil v režimu 24 ur na dan 7 dni v tednu, na letnem nivoju vsaj 99,5%. Pri tem izračunu se nedelovanje v času preventivnih vzdrževalnih del ne upošteva. Sistem zagotavljanja visoke razpoložljivosti je natančneje opisan v splošnih postopkih delovanja overitelja.

4.10.3 Dodatne možnosti storitve

"Ni predpisano".

4.11 Prekinitev naročniškega razmerja med imetnikom in overiteljem

Naročniško razmerje med imetnikom in overiteljem prične teči s prevzemom digitalnega potrdila.

Naročniško razmerje med imetnikom in overiteljem se prekine:
- ko preteče veljavnost imetnikovega digitalnega potrdila in imetnik ne poda zahtevka za obnovitev potrdila;
- ko je potrdilo preklicano imetnik pa ne poda zahtevka za pridobitev novega potrdila, oziroma je overitelj njegov zahtevek zavrnil;

4.12 Varnostno kopiranje in odkrivanje zasebnega ključa

4.12.1 Politika in postopki varnostnega kopiranja zasebnih ključev

Uporaba storitve varnostnega kopiranja in hranjenja zasebnih ključev imetnikov pri zunanjih subjektih ni predvidena.

Zasebni ključi imetnikov, ki so namenjeni elektronskemu podpisu in prijavi, se vedno tvorijo neposredno na identifikacijski kartici BS. Zato izdelava varnostne kopije ni predvidena.

Overitelj izdeluje varnostne kopije zasebnih ključev imetnikov, ki so namenjeni šifriranju/dešifriranju elektronskih vsebin. Varnostne kopije se izdelujejo v skladu s poglavjem 6.2.4.

4.12.1.1 Postopek za povrnitev zgodovine zasebnih ključev

Povrnitev zgodovine zasebnih ključev za dešifriranje lahko zahteva le imetnik potrdil.

Povrnitev zasebnih ključev se lahko izvede le ob fizični prisotnosti imetnika na identifikacijsko kartico BS, ki se glasi na njegovo ime.

Postopek povrnitve uporablja varne mehanizme v vseh fazah prenosa zasebnega ključa iz varnostne kopije do šifrirnega modula identifikacijske kartice BS.

Postopek je natančneje opisan v splošnih postopkih delovanja overitelja.

4.12.1.2 Odkrivanje kopije zasebnega ključa za dešifriranje

Zahtevek za odkrivanje zasebnega ključa imetnika za dešifriranje lahko podasta le guverner ali druga oseba na podlagi zakona.

V postopku za odkrivanje zasebnega ključa mora sodelovati vsaj eden od dveh skrbnikov kopije zasebnih ključev in predstavnik pooblaščenega osebja prijavne službe overitelja.

Postopek je natančneje opisan v splošnih postopkih delovanja overitelja.

4.12.2 Zaščita ključa za prenos zasebnega ključa

Ključ za prenos zasebnega ključa je zavarovan tako, da se vedno prenaša v šifrirani obliki. Postopek je natančneje opisan v splošnih postopkih delovanja overitelja.

5 Fizično varovanje, organizacijski varnostni ukrepi in nadzor nad osebjem

5.1 Fizično varovanje

Zahteve za fizično varovanje opredeljujejo varnostni nadzor prostorov, v katerih deluje overitelj. Overitelj ima vzpostavljene varnostne kontrole, ki so skladne z zahtevami varnostnih politik in tehničnih standardov BS za varovana računalniška okolja. Vzpostavljene varnostne kontrole so natančneje opredeljene v splošnih postopkih delovanja overitelja. Opredeljeni so naslednji vsebinski sklopi:

- lokacija in konstrukcija prostorov overitelja;
- fizični dostop do overitelja;

- napajanje in klimatske naprave;
- zaščita pred poplavo
- zaščita pred požarom;
- shranjevanje medijev;
- odstranjevanje odpadkov;
- hranjenje kopij podatkov na oddaljeni lokaciji.

5.2 Organizacijski varnostni ukrepi

Organizacijski varnostni ukrepi zagotavljajo, da so naloge, ki jih izvaja overitelj, ustrezno porazdeljene med različne izvajalce. S tem overitelj preprečuje konflikt interesov in nenadzorovano izvajanje nalog. Vzpostavljene organizacijske varnostne kontrole so natančneje opredeljene v splošnih postopkih delovanja overitelja. Opredeljeni so naslednji vsebinski sklopi:

- notranja organizacija overitelja in porazdelitev nalog;
- Število oseb potrebnih za izvedbo nalog;
- preverjanje istovetnosti osebja overitelja;
- nezdružljive naloge.

5.3 Nadzor nad osebjem

Vzpostavljene varnostne kontrole nadzora nad osebjem so natančneje opredeljene v splošnih postopkih delovanja overitelja. Opredeljeni so naslednji vsebinski sklopi:

- kvalifikacije, izkušnje in varnostno preverjanje;
- preverjanje primernosti osebja;
- izobraževanje in usposabljanje osebja;
- pogostost dodatnega izobraževanja in usposabljanja osebja;
- kroženje med delovnimi mesti;
- sankcije za nedovoljene postopke;
- zahteve za osebje zunanjih izvajalcev;
- dostop osebja do dokumentacije.

5.4 Beleženje in upravljanje revizijskih sledi

Overitelj ima vzpostavljene mehanizme zagotavljanja pristnosti in celovitosti revizijskih sledi. Varnostne zahteve za beleženje in upravljanje revizijskih sledi so natančneje opredeljene v splošnih postopkih delovanja overitelja. Opredeljeni so naslednji vsebinski sklopi:

- vrste beleženih dogodkov;
- pogostnost pregledovanja revizijskih dnevnikov;
- obdobje hrambe revizijskih dnevnikov;
- zaščita revizijskih dnevnikov ;
- varnostne kopije revizijskih dnevnikov;
- sistem zbiranja revizijskih podatkov;
- obveščanje povzročitelja dogodka;
- ocena ranljivosti.

BANKA SLOVENIJE
EVROSISTEM

5.5 Arhiviranje podatkov

5.5.1 Vrste arhiviranih podatkov

Overitelj shrani naslednje podatke:
- revizijske sledi, opredeljene v poglavju 5.4;
- zahtevke prosilcev in njihove izjave o seznanitvi in sprejemanju pogojev uporabe digitalnih potrdil;
- zahtevke o preklicih potrdil in prijave ogrožanja ključev;
- potrdila;
- različice politik in splošnih postopkov delovanja overitelja;
- zasebne ključe za dešifriranje.

5.5.2 Čas hrambe

Korespondenca z overiteljem in pogodbe se hranijo 20 let.
Potrdila, register preklicanih potrdil in zasebni ključi se hranijo 20 let ali več.

5.5.3 Zaščita arhiva

Dostop do arhiva je zaščiten z enakovrednimi varnostnimi mehanizmi, kot so vzpostavljeni v centru overitelja.

5.5.4 Zahteve za časovno žigosanje zapisov

"Ni predpisano".

5.5.5 Način arhiviranja

"Ni predpisano".

5.5.6 Dostop do arhivskih podatkov

Dostop je dovoljen samo pooblaščenim osebam overitelja, opredeljenim v splošnih postopkih delovanja overitelja.

5.6 Podaljšanje veljavnosti potrdil overitelja

Izdajatelj lahko izdaja le digitalna potrdila, katerih obdobje veljavnosti ni daljše od obdobja veljavnosti digitalnega potrdila izdajatelja.

Postopki, ki jih overitelj izvede ob podaljšanju veljavnosti lastnih potrdil, so natančneje opredeljeni v splošnih postopkih delovanja overitelja.

Overitelj izvedbo postopkov podaljšanja lastnih potrdil načrtuje tako, da le ti ne ogrožajo neprekinjenosti delovanja storitev, ki so odvisne od veljavnosti digitalnih potrdil izdajatelja.

5.7 Postopki v primeru ogrožanja zasebnega ključa overitelja in okrevalni načrti

Okrevalni načrti v primeru varnostnih incidentov ali ogrožanja zasebnega ključa overitelja so natančneje opredeljeni v splošnih postopkih delovanja overitelja. Opredeljeni so naslednji vsebinski sklopi:

- postopki odzivanja na varnostne incidente in zlorabe;
- okrevalni načrti v primeru okvar ali uničenja strojne opreme, programske opreme in podatkov;
- okrevalni načrti v primeru ogrožanja zasebnega ključa overitelja;
- neprekinjenost poslovanja v primeru incidentov.

5.8 Prenehanje delovanja overitelja na BS

Overitelj bo v primeru prenehanja delovanja:

- obvestil vse imetnike potrdil in javno objavil informacije o prenehanju delovanja;
- preklical vsa veljavna potrdila;
- varno uničil zasebne ključe overitelja in varno odstranil opremo overitelja ter vodil zapise o izvedbi. Vse aktivnosti se izvedejo po principu 4 oči.
- zagotovil razpoložljivost in dostopnost list preklicanih potrdil za obdobje šest (6) mesecev po preklicu vseh potrdil;
- zagotovil, da bo drug izdajatelj digitalnih potrdil prevzel vodenje preklicanih digitalnih potrdil v svojem registru;
- zagotovil hrambo arhiviranih podatkov za obdobje 5 let po prenehanju delovanja.

6 Tehnične varnostne zahteve

6.1 Tvorjenje in namestitev para ključev

6.1.1 Tvorjenje para ključev

6.1.1.1 Pari ključev overitelja

Par ključev, ki ga izdajatelj uporablja za podpisovanje digitalnih potrdil, je bil ustvarjen po predpisanem postopku med nameščanjem programske opreme overitelja. Postopek je opredeljen in zabeležen v dokumentu "CA Key Generation Ceremony in Banka Slovenije". Par ključev se je tvoril in je shranjen na strojnem šifrirnem modulu overitelja (HSM modul), ki je v skladu s specifikacijami FIPS 140-2 Level 3 ali višje.

6.1.1.2 Pari ključev imetnikov

Način tvorjenja parov ključev imetnikov digitalnih potrdil, ki jih izdaja overitelj je odvisen od vrste digitalnega potrdila:

- pri digitalnem potrdilu za prijavo v sisteme in digitalnem potrdilu za elektronski podpis se para ključev tvorita in hranita na šifrirnem modulu identifikacijske kartice BS, ki je v skladu s specifikacijami CC EAL4+ ali višje;
- pri digitalnem potrdilu za šifriranje/dešifriranje se par ključev tvori na strojnem šifrirnem modulu sistema za upravljanje identifikacijskih kartic BS, ki je v skladu s specifikacijami FIPS 140-2 Level 3 ali višje. Po tvorjenju se ena kopija para ključev šifrira z zasebnim ključem, ki je shranjen na strojnem šifrirnem modulu overitelja v skladu s specifikacijami FIPS 140-2 Level 3 ali višje, in shrani v okviru storitev arhiviranja ključev. Druga kopija ključev se shrani na šifrirnem modulu identifikacijske kartice BS, ki je v skladu s specifikacijami CC EAL4+ ali višje;

6.1.2 Prenos zasebnega ključa do imetnika

Pri digitalnem potrdilu za prijavo in digitalnem potrdilu za elektronski podpis se zasebni ključ tvori in varno hrani na šifrirnem modulu identifikacijske kartice BS. Imetnik zasebni ključ prevzame hkrati z identifikacijsko kartico.

Pri digitalnem potrdilu za šifriranje se tako ob tvorjenju, kakor tudi ob povrnitvi zgodovine ključev ali odkrivanju zasebnega ključa, zasebni ključ med programsko opremo izdajatelja, sistemom za arhiviranje ključev, sistemom za upravljanje identifikacijskih kartic in šifrirnim modulom identifikacijske kartice BS prenaša preko standardiziranih varnih protokolov. Zato tudi v tem primeru neposreden prenos ključa do imetnika ni predviden.

6.1.3 Prenos javnega ključa imetnika k overitelju

Pri digitalnem potrdilu za šifriranje javni ključ tvori programska oprema overitelja, zato prenos ni predviden.

Pri digitalnem potrdilu za prijavo in digitalnem potrdilu za elektronski podpis se javni ključ tvori in hrani na šifrirnem modulu identifikacijske kartice BS. Med identifikacijsko kartico, programsko opremo za upravljanje identifikacijskih kartic in programsko opremo izdajatelja se javni ključ prenaša po standardiziranih varnih protokolih.

6.1.4 Dostop do overiteljeva javnega ključa

Javni ključ izdajatelja v obliki potrdila je dostopen:

- na spletni strani http://ca.bsi.si/pki,

Ker so digitalna potrdila elektronsko podpisana je s tem zagotovljena celovitost objavljenega javnega ključa.

Pristnost objavljenega javnega ključa je možno preveriti preko prstnega odtisa ključa (angl. fingerprint). Prstni odtis je objavljen na zgoraj navedeni spletni strani. Uporabniki lahko prstni odtis preverijo tudi preko telefona navedenega v točki 1.3.1.

6.1.5 Dolžina asimetričnih ključev

Izdajatelj za podpisovanje infrastrukture overitelja uporablja zasebni ključ RSA dolžine 4096 bitov, za podpisovanje ključev in digitalnih potrdil imetnikov pa uporablja zasebni ključ RSA dolžine 2048 bitov.

Imetniki uporabljajo zasebne ključe RSA dolžine najmanj 2048 bitov.

6.1.6 Parametri za generiranje javnih ključev in preverjanje parametrov

Vsi postopki v zvezi z generiranjem RSA ključev so v skladu s priporočili PKCS #1. Vsi parametri ključev se generirajo v strojnem šifrirnem modulu.

6.1.7 Namen uporabe ključev in potrdil (definirani v X.509 v3 v poljih "key usage" in "extended key usage")

V vseh digitalnih potrdilih je vsebovan atribut keyUsage, ki določa namen uporabe digitalnega potrdila. Natančneje je namen uporabe posamezne vrste digitalnega potrdila opredeljen v poglavju 1.4.

Tabela 5: Vsebina polja "KeyUsage"

Vrsta potrdila	**Key usage polje**
Šifrirni	Encryption: 1
Podpisni	Non repudiation: 1
Prijavni	Digital Signature:1

V vseh digitalnih potrdilih je vsebovan atribut Extended KeyUsage, ki dodatno določa namen uporabe digitalnega potrdila.

Tabela 6: Vsebina polja "Extended key usage"

Vrsta potrdila	**Extended Key usage polje**
Šifrirni	Any Purpose (2.5.29.37.0) Secure Email (1.3.6.1.5.5.7.3.4) Encrypting File System (1.3.6.1.4.1.311.10.3.4)
Podpisni	Document Signing (1.3.6.1.4.1.311.10.3.12) Secure Email (1.3.6.1.5.5.7.3.4) Any Purpose (2.5.29.37.0)
Prijavni	Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Client Authentication (1.3.6.1.5.5.7.3.2)

Izdajateljev zasebni ključ se uporablja za podpisovanje:
- digitalnih potrdil prosilcev;
- registrov preklicanih potrdil (CRL).

6.2 Zaščita zasebnega ključa in kriptografskih modulov

6.2.1 Standardi za modul za šifriranje

Za tvorjenje in varno hranjenje zasebnega ključa overitelja se uporablja strojni varnostni modul, ki mora ustrezati varnostnemu nivoju FIPS 140-2 Level 3.

Posledično namestitev in konfiguriranje programske opreme izdajatelja vključuje naslednje korake:

- zagon strojnega šifrirnega modula;
- tvorjenje administratorskih in operatorskih setov pametnih kartic;
- tvorjenje overiteljevega zasebnega in javnega ključa.

Osebje overitelja in imetniki potrdil uporabljajo šifrirni modul identifikacijske kartice BS, ki je v skladu s specifikacijami CC EAL4+ ali višje;

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

Overitelj ima vzpostavljeno večkratno odobritev za dostop do zasebnih ključev overitelja in operacijo odkritja zasebnega ključa imetnika. Postopek večkratne odobritve je natančneje opisan v splošnih postopkih delovanja overitelja.

6.2.3 Odkrivanje (angl. Escrow) zasebnega ključa

Ni predpisano.

6.2.4 Varnostna kopija zasebnega ključa

Varnostne kopije zasebnega ključa overitelja

Overitelj izdeluje varnostne kopije zasebnih ključev overitelja shranjenih na strojnih varnostnih modulih. Varnostne kopije so šifrirane z zasebnim ključem, shranjenim na operatorski pametni kartici za strojni modul.

Varnostne kopije zasebnih ključev imetnikov

Overitelj izdeluje varnostne kopije zasebnih ključev digitalnih potrdil imetnikov za šifriranje. Varnostne kopije so šifrirane z zasebnim ključem, shranjenim na operatorski pametni kartici za strojni modul.

6.2.5 Arhiviranje zasebnega ključa

Overitelj izvaja varno hranjenje kopije zasebnega ključa in ima vzpostavljene postopke za prepis zasebnih ključev na identifikacijsko kartico imetnika potrdila. Postopek je natančneje opisan v poglavju 4.12.1.

6.2.6 Zapis zasebnega ključa v modul za šifriranje

Izdajateljevi zasebni ključi za podpisovanje podoveriteljskih sistemov so ustvarjeni v strojnem modulu za šifriranje. Dodaten prenos in zapis v modul za šifriranje ni predviden.

Zasebni ključi imetnikov za digitalna potrdila za prijavo in elektronski podpis so tvorjeni na šifrirnem modulu identifikacijske kartice BS. Dodatne prenos in zapis v modul za šifriranje ni predviden.

Zasebni ključi imetnikov za digitalna potrdila za šifriranje in dešifriranje se tvorijo na strojnem šifrirnem modulu overitelja in se v procesu personalizacije identifikacijske kartice BS po standardiziranih varnih protokolih zapišejo v šifrirni modul identifikacijske kartice BS.

6.2.7 Hramba zasebnega ključa v strojnem modulu za šifriranje

Overiteljeve zasebne ključe se lahko aktivira in uporablja samo na strojnem šifrirnem modulu.

Imetnikovi zasebni ključi se hranijo v šifrirnem modulu identifikacijske kartice BS.

6.2.8 Postopek za aktiviranje zasebnega ključa

Izdajateljev zasebni ključ za podpisovanje se aktivira ob zagonu programske opreme izdajatelja.
Za aktiviranje je potrebna pametna kartica in PIN koda za strojni modul za šifriranje.

Zasebni ključi imetnika so hranjeni na šifrirnem modulu identifikacijske kartice BS. Dostop do ključev je zavarovan s PIN kodo.

6.2.9 Postopek za deaktiviranje zasebnega ključa

Zasebni ključ izdajatelja za podpisovanje se deaktivira z zaustavitvijo programske opreme izdajatelja.

Zasebni ključi imetnika se deaktivirajo, ko imetnik izvleče identifikacijsko kartico iz čitalnika pametnih kartic. Nekatere aplikacije samodejno deaktivirajo zasebne ključe po določenem času neaktivnosti imetnika.

6.2.10 Postopek za uničenje zasebnega ključa

Uničenje zasebnih ključev overitelja je po nadzorovanem postopku izvedeno po koncu obdobja uporabe zasebnih ključev overitelja.

Vsi zasebni ključi imetnika, shranjeni na identifkacijski kartici BS, se uničijo:
- ob prekinitvi naročniškega razmerja;
- v primeru fizičnega uničenja ali poškodovanja identifikacijske kartice BS.

Zasebni ključ imetnika za digitalno potrdilo za prijavo in digitalno potrdilo za elektronski podpis se ob vsakokratni obnovi digitalnih potrdil zbriše z identifikacijske kartice BS na kateri je bil tvorjen.

6.2.11 Stopnja varnosti strojnih modulov za šifriranje

Opisano v poglavju 6.2.1.

6.3 Ostali vidiki upravljanja ključev

6.3.1 Arhiviranje javnega ključa

Overitelj arhivira svoj javni ključ in javne ključe imetnikov na način, ki je opisan v točki 5.5.

6.3.2 Obdobje veljavnosti ključev in digitalnih potrdil

Obdobje veljavnosti digitalnih potrdil je enaka obdobju veljavnosti pripadajočih parov ključev.

Veljavnost javnega ključa izdajatelja za overjanje je 30 let.
Veljavnost zasebnega ključa izdajatelja za podpisovanje je 30 let.
Veljavnost javnega ključa podoveriteljskega sistema za overjanje je 15 let.
Veljavnost zasebnega ključa podoveriteljskega sistema za podpisovanje je 15 let.

Veljavnost imetniškega zasebnega ključa za prijavo je 5 let.
Veljavnost imetniškega javnega ključa za overjanje je 5 let.
Veljavnost imetniškega zasebnega ključa za podpisovanje je 5 let.
Veljavnost imetniškega javnega ključa za šifriranje je 5 let.
Veljavnost imetniškega zasebnega ključa za dešifriranje ni omejena.

6.4 Aktivacijski podatki

6.4.1 Tvorjenje in instalacija aktivacijskih podatkov

Aktivacijski podatki za uporabo strojnega šifrirnega modula se tvorijo ob inicializaciji modula. Aktivacijski podatki se na način, ki zagotavlja njihovo zaupnost in celovitost, dostavijo do pooblaščenega osebja overitelja, ki mora aktivacijske podatke poznati v skladu z dodeljenimi nalogami. Aktivacijski podatek je PIN koda administratorske pametne kartice za upravljanje strojnega šifrirnega modula in operaterske pametne kartice za dostop do zasebnega ključa overitelja shranjenega na strojnem šifrirnem modulu.

Aktivacijski podatki šifrirnega modula identifikacijske kartice BS se tvorijo ob inicializaciji in personalizaciji identifikacijske kartice. Aktivacijski podatki se na način, ki zagotavlja njihovo zaupnost in celovitost, dostavijo do imetnika. Postopek je natančneje opredeljen v splošnih postopkih delovanja overitelja. Aktivacijski podatek je PIN koda za dostop do zasebnih ključev

shranjenih na šifrirnem modulu identifikacijske kartice. Ob prvi uporabi identifikacijske kartice BS so imetniki dolžni PIN kodo spremeniti.

6.4.2 Zaščita aktivacijskih podatkov

Aktivacijski podatki se hranijo na način, ki varuje njihovo zaupnost in celovitost vse dokler jih ne prevzame končni prejemnik, ki je v nadaljevanju odgovoren za zagotavljanje zaupnosti, celovitosti in razpoložljivosti aktivacijskih podatkov. Postopki so natančneje opredeljeni v splošnih postopkih delovanja overitelja.

6.4.3 Drugi vidiki aktivacijskih podatkov

"Ni predpisano".

6.5 Varnostne zahteve za računalniško opremo izdajatelja

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:
- kontrola dostopa do postopkov programske opreme overitelja in dodeljenih pooblastil za opravljanje nalog;
- močna avtentikacija osebja overitelja z uporabo šifrirnih modulov za hranjenje zasebnih ključev;
- šifrirane seje med odjemalsko aplikacijo na delovni postaji osebja overitelja in strežniško programsko opremo overitelja;
- kontroliran dostop do podatkovnih baz overitelja;
- varen arhiv overitelja in varne revizijske sledi;
- revizijske sledi o vseh varnostno veljavnih dogodkov;
- vzpostavljene mehanizme povrnitve z varnostne kopije programske opreme overitelja, šifrirnih ključev overitelja ter baze podatkov overitelja;

Tehnične varnostne zahteve, specifične za posamezen izdajateljski strežnik overitelja, so natančneje podane v splošnih postopkih delovanja overitelja.

6.5.2 Stopnja varnostne zaščite računalnikov

Na vseh elementih programske opreme overitelja je v skladu z navodili proizvajalcev in dobre prakse izvedeno varnostno utrjevanje.

Natančneje so stopnje zaščite posameznega elementa opreme overitelja opredeljene v splošnih postopkih delovanja overitelja.

6.6 Varnostne kontrole življenjskega cikla overitelja

6.6.1 Nadzor razvoja sistema

BS zagotavlja, da programska oprema overitelja ustreza zahtevam varnostnih politik Informacijskega sistema Banke Slovenije.

6.6.2 Upravljanje varnosti

Overitelj ima vzpostavljene postopke za upravljanje z incidenti, problemi in spremembami, za vse komponente svoje infrastrukture. Vse spremembe se beležijo v revizijskih sledeh.

Overitelj ima vzpostavljene postopke za reden nadzor celovitosti programske opreme.

6.7 Varnostne zahteve za računalniško omrežje

Overitelj zagotavlja, da so dostopi do računalniškega omrežja overitelja omejeni zgolj na povezave, ki so potrebne za upravljanje in uporabo računalniške infrastrukture overitelja. Vpeljane varnostne kontrole so natančneje opredeljene v splošnih postopkih delovanja overitelja.

6.8 Časovno žigosanje

Vsi sistemi overitelja so časovno usklajeni z javnimi NTP strežniki.

7 Profil digitalnih potrdil, registra preklicanih potrdil in sprotnega preverjanja statusa potrdil

7.1 Profil potrdil

7.1.1 Različica potrdil

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

Signature	Overiteljev podpis
Issuer	Edinstveno razločevalno ime overitelja
Validity	Datum aktiviranja in poteka veljavnosti potrdila

BANKA SLOVENIJE
EVROSISTEM

Subject	Edinstveno razločevalno ime imetnika potrdila
SubjectPublicKeyInformation	Oznaka algoritma ključa
Version	Različica potrdila X.509
SerialNumber	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 RFC5280, ki dovoljuje tudi definiranje in dodajanje lastnih razširitvenih polj za potrebe overiteljev.

7.1.2.1 Standardna razširitvena polja

Overitlej uporablja naslednja razširitvena polja:

Naziv atributa	**Opis**
authorityKeyIdentifier*	Odtis javnega ključa overitelja s katerim je podpisano potrdilo (doda CA aplikacija)
subjectKeyIdentifier	Odtis javnega ključa imetnika (doda CA aplikacija)
KeyUsage*	Kot je opisano v poglavju 6.1.7
extKeyUsage	Kot je opisano v poglavju 6.1.7
privateKeyUsagePeriod	Kot je opisano v 6.3.2
certificatePolicies	OID oznaka vrste potrdila in URI objave pravil delovanja
cRLDistributionPoints	Naslovi, na katerih je objavljen register preklicanih potrdil
Authority Information Access	Naslovi, na katerih je dostopno digitalno potrdilo izdajatelja in preverjanje statusa digitalnih potrdil preko protokola OCSP.
subjectAlternativeName	Nadomestno ime imetnika (naslov elektronske pošte).
basicConstraints*	Doda CA aplikacija

***KRITIČNA POLJA:** Uporabniške aplikacije morajo procesirati razširitvena polja potrdila, označena kot kritična, v skladu s priporočili PKIX.

7.1.3 Identifikacijske oznake (angl. object identifiers) podprtih algoritmov

Vsi uporabljeni algoritmi in oznake se uporabljajo v skladu z veljavnimi standardi in priporočili.

7.1.4 Oblike imen

Overiteljeva potrdila vsebujejo X.501 polno razločevalno ime overitelja in imetnika potrdila v poljih »issuer name« ter »subject name«, kot je navedeno v poglavju 3.1.1

7.1.5 Omejitve imen

Kot je opredeljeno v poglavju 3.1.1.

7.1.6 Identifikacijska oznaka politike potrdila

Vsako potrdilo vsebuje eno ali več identifikacijskih oznak politike, pod katero je bilo izdano. Overitelj uporablja polje *»certificatePolicies«* za označevanje vrste potrdil. Identifikacijske oznake politike potrdil so določene v poglavju 1.2.

7.1.7 Uporaba razširitvenega polja "Policy Constraints"

"Ni predpisano".

7.1.8 Sintaksa in semantika polja "Policy qualifiers"

Overitelj uporablja polje *»certificatePolicies policy qualifiers«* za objavo spletnega naslova, kjer se nahaja dokumenta o politiki delovanja overitelja.

7.1.9 Procesiranje oznake kritičnosti razširitvenih polj potrdila

Aplikacije morajo procesirati razširitvena polja označena kot kritična v skladu z RFC5280.

7.2 Profil registra preklicanih potrdil

Vsakokrat veljaven register preklicanih digitalnih potrdil je objavljen na naslovih, navedenih v tabeli 7.

Tabela 7: Mesta objav registra preklicanih digitalnih potrdil

Izdajatelj	Preko HTTP	Preko OCSP
Banka Slovenije Root CA	http://ca.bsi.si/pki/crls/Banka Slovenije Root CA.crl	
Banka Slovenije Ent Sub CA	http://ca.bsi.si/pki/crls/Banka Slovenije Ent Sub CA.crl	http://ocsp.bsi.si

7.2.1 Različica

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

Version	V2
Signature	Overiteljev podpis
Issuer	Razločevalno ime
thisUpdate	Čas izdaje registra
nextUpdate	Čas izdaje naslednjega registra
revokedCertificate	Serijske številke preklicanih potrdil

7.2.2 Vsebina registra in razširitve

Overitelj v skladu s priporočili PKIX Part 1 uporablja naslednje X.509 Version 2 CRL in ARL-razširitve:

cRLNumber	Doda programska oprema izdajatelja
reasonCode	Razlog preklica se ne objavlja
holdInstructionCode	"Ni predpisano".
invalidityDate	Programska oprema izdajatelja, če je podatek vsebovan v zahtevku
issuingDistributionPoint	Doda programska oprema izdajatelja
certificateIssuer	"Ni predpisano".
deltaCRLIndicator	"Ni predpisano".

7.3 Sprotno preverjanje statusa potrdil

Sprotno preverjanje statusa digitalnih potrdil je dostopno na naslovu http://ocsp.bsi.si.

8 Revidiranje usklajenosti in ostali pregledi

Preverjanje skladnosti se izvaja v skladu z zahtevami BS.

Overitelj izvaja redne notranje in po potrebi zunanje preglede delovanja.

BANKA SLOVENIJE
EVROSISTEM

8.1 Pogostnost izvajanja preverjanj skladnosti

Overitelj najmanj enkrat letno izvaja notranje preverjanje skladnosti.

Overitelj po potrebi zagotovi izvedbo zunanjega preverjanja.

8.2 Identiteta in usposobljenost izvajalcev preverjanj

Preverjanja lahko izvajajo:
- notranji presojevalci za varovanje informacij v BS;
- oddelek Notranje revizije BS;
- zunanji presojevalci, revizorji ali drugi pristojni zunanji subjekti.

Overitelj zagotovi, da ima izvajalec preverjanj ustrezna znanja in izkušnje s področja varovanja informacij ali področja predmeta izvajanja pregleda.

8.3 Odnos med revizorjem in overiteljem

Osebje overitelja ne sme izvajati preverjanja lastnih nalog.

Izvajalec pregleda mora za izvedbo pridobiti ustrezno dovoljenje overitelja.

Izvajalec zunanjega pregleda je izbran na javnem razpisu ali po službeni dolžnosti. Pred izvedbo pregleda zunanji pregledovalec in BS podpišeta pogodbo, v kateri natančno opredelita predmet in obseg pregleda, ter zagotovita ustrezno varovanje zaupnosti.

8.4 Predmet preverjanja

Predmet preverjanja so:
- infrastruktura overitelja;
- postopki overitelja;
- skladnost delovanja s politiko delovanja overitelja in splošnimi postopki delovanja overitelja;
- skladnost z zakonodajo.

8.5 Korektivni ukrepi kot posledica ugotovljenih nepravilnosti

Overitelj po vsakem preverjanju pripravi natančen časovni načrt odprave morebitnih nepravilnosti.

8.6 Poročanje o preverjanjih

O rezultatih preverjanja skladnosti overitelj poroča:
- vodstvu oddelka IT;
- vodji informacijske varnosti;
- Odboru za tveganja v BS.

9 Ostale finančne in pravne zadeve

9.1 Cenik

"Ni predpisano".

Posledično so poglavja 9.1.1 do 9.1.4 opredeljena kot "Ni predpisano".

9.2 Finančna odgovornost

9.2.1 Zavarovanje odškodninske odgovornosti

Overitelj ima za tveganja, ki izhajajo iz uporabe digitalnih potrdil, ki jih izdaja overitelj, sklenjeno zavarovanje splošne odgovornosti v pogodbeno opredeljenem obsegu.
Poleg tega Banka Slovenije vzdržuje zadostne rezerve za pokrivanje morebitnih stroškov iz tega naslova.

9.2.2 Druge oblike zavarovanja

"Ni predpisano".

9.2.3 Zavarovanje imetnikov

"Ni predpisano".

9.3 Zaupnost poslovnih podatkov

9.3.1 Obseg zaupnih podatkov

Kot zaupni se štejejo naslednji podatki:
- splošni postopki delovanja overitelja;
- zasebni ključi overitelja in imetnikov;
- aktivacijski podatki za zasebne ključe overitelja in imetnikov;
- revizijske sledi;

- zahtevki za preklic digitalnih potrdil;
- zahtevki za pridobitev potrdil in pripadajoča dokazila;
- osebni podatki o imetnikih.

9.3.2 Podatki izven obsega zaupnih podatkov

"Ni predpisano".

9.3.3 Odgovornost za varovanje zaupnih podatkov

Overitelj bo zaupne podatke varoval v skladu z zahtevami BS in veljavno zakonodajo.

9.4 Varovanje osebnih podatkov

9.4.1 Načrt varovanja osebnih podatkov

Načrt varovanja je določen z navedbami v poglavjih 9.3 in 9.4.2 do 9.4.7.

9.4.2 Varovani osebni podatki

Kot zaupni so varovani vsi osebni podatki o imetniku digitalnega potrdila, ki jih overitelj pridobi ali ustvari v okviru izvajanja svojih storitev, razen osebnih podatkov, ki so navedeni v digitalnem potrdilu imetnika in v registru preklicanih digitalnih potrdil.

9.4.3 Nevarovani osebni podatki

Nevarovani osebni podatki so tisti, ki so navedeni v digitalnem potrdilu imetnika in v registru preklicanih digitalnih potrdil in so javno dostopni.

9.4.4 Odgovornost glede varovanja osebnih podatkov

Overitelj bo varovane osebne podatke varoval v skladu z veljavno zakonodajo in notranjimi akti, ki urejajo varstvo zaupnih podatkov Banke Slovenije.

Imetnik digitalnega potrdila je pred izdajo potrdila v okviru vsakokrat veljavne politike (javno objavljenega notranjega akta overitelja) seznanjen, kateri osebni podatki bodo vsebovani v potrdilu oziroma kateri drugi osebni podatki se obdelujejo v zvezi z izdajo potrdila.

Imetnik digitalnega potrdila s potrditvijo zahteve za izdajo digitalnega potrdila potrdi seznanitev s pravili glede obdelave osebnih podatkov kot izhaja iz te oziroma vsakokrat veljavne politike.

9.4.5 Pooblastilo glede uporabe osebnih podatkov

Overitelj uporablja osebne podatke le za namene, za katere je prosilec podal pooblastilo v okviru zahtevka za pridobitev digitalnega potrdila.

Pravna podlaga za obdelavo podatkov je sklenjena pogodba o zaposlitvi oziroma o izvajanju storitev, osebni podatki se obdelujejo v zvezi z izvajanjem pogodbe.

9.4.6 Posredovanje osebnih podatkov

Overitelj osebne podatke sporoča le na zahtevo imetnika digitalnega potrdila ali na pisno zahtevo druge osebe na podlagi zakona.

9.4.7 Druga določila glede varovanja osebnih podatkov

"Ni predpisano".

9.5 Zaščita intelektualne lastnine

Zasebni ključi overitelja, ključi imetnikov, javni dokumenti o delovanju overitelja in dokumentacija v zvezi z izdajanjem digitalnih potrdil so last Banke Slovenije.

9.6 Obveznosti in odgovornosti

9.6.1 Odgovornosti overitelja

Overitelj odgovarja, da:
- izvaja vse postopke v skladu z navedbami v tej politiki delovanja in v skladu z veljavno zakonodajo;
- zavaruje zasebne ključe;
- izdaja digitalna potrdila v skladu s politiko, ki velja za posamezno vrsto potrdila;
- preverja pravilnost prejetih zahtevkov, da omogočajo izdajo digitalnega potrdila v skladu z določili X.509 v3 in zahtevami programske opreme izdajatelja;
- kadar je potrebno objavi digitalna potrdila, kot je določeno v politiki in splošnih postopkih delovanja overitelja;
- pravočasno obdela in izvede zahtevke za preklic digitalnih potrdil;
- pravočasno objavlja najnovejši register preklicanih digitalnih potrdil, kot je določeno s politiko in splošnimi postopki delovanja overitelja;
- vzdržuje dostopnost registra preklicanih digitalnih potrdil, v skladu z določili te politike in splošnih postopkov delovanja overitelja;
- v primeru prenehanja delovanja o tem pravočasno obvesti imetnike digitalnih potrdil;
- za vsako izdano digitalno potrdilo vsaj 15 let hrani vso dokumentacijo v zvezi s tem potrdilom;
- so podatki za kreiranje in preverjanje elektronskih podpisov konsistentni.

9.6.2 Odgovornosti prijavne službe

Prijavna služba je odgovorna, da:
- overi identiteto prosilcev skladno z določili te politike in splošnih postopkov delovanja overitelja;
- seznani prosilca s pogoji uporabe digitalnih potrdil;
- obdela zahtevke za pridobitev digitalnega potrdila v skladu z določili te politike in splošnih postopkov delovanja overitelja;
- programski opremi izdajatelja posreduje popolne, točne, veljavne in pravočasno odobrene zahtevke za izdajo potrdila;
- varno in pravočasno shrani vso dokumentacijo, nastalo v procesu izdaje, suspenza ali preklica digitalnega potrdila;
- opravlja ostale naloge, predpisane s to politiko in splošnimi postopki delovanja overitelja.

9.6.3 Odgovornosti imetnikov digitalnih potrdil

Imetniki so pri uporabi digitalnih potrdil odgovorni, da:
- v zahtevku za pridobitev digitalnega potrdila navedejo popolne, resnične in prave podatke;
- obvestijo overitelja o spremembi podatkov, navedenih v digitalnem potrdilu;
- se seznanijo in strinjajo s pogoji uporabe digitalnih potrdil, kot so navedeni v izjavi, ki so jo podpisali in v tej politiki overitelja;
- omejijo uporabo digitalnih potrdil izključno na namen, ki je za posamezno vrsto digitalnega potrdila naveden v tej politiki;
- varujejo svoje identifikacijske kartice BS pred poškodovanjem, izgubo, razkritjem, spremembo ali neodobreno uporabo;
- za dostop do zasebnih ključev, shranjenih na identifikacijski kartici, tvorijo kvalitetno PIN kodo in varujejo njeno zaupnost;
- v primeru nastopa okoliščin, ki ogrožajo zasebni ključ, nemudoma zahtevajo preklic digitalnega potrdila;
- ne izkoriščajo in preizkušajo morebitnih varnostnih pomanjkljivosti v infrastrukturi overitelja;
- ne prenašajo svojih odgovornosti, povezanih z uporabo digitalnih potrdil, na tretje osebe;
- redno spremljajo obvestila na spletni strani overitelja.

9.6.4 Odgovornosti tretjih oseb

Tretje osebe so pri zanašanju na digitalna potrdila odgovorne, da:
- preverijo, da je bilo digitalno potrdilo uporabljeno izključno za namen uporabe, kot je za posamezno vrsto digitalnega potrdila opredeljen v tej politiki;
- ob prejemu dokumentov, ki so bili elektronsko podpisani, preverijo veljavnost digitalnih potrdil oziroma v javnem registru preklicanih digitalnih potrdil (CRL) preverijo, da niso bila digitalna potrdila preklicana;
- pravilno preverijo veljavnost elektronskega podpisa;
- preden digitalna potrdila uvrstijo med zaupanja vredna preverijo njihovo veljavnost, oziroma v javnem registru preklicanih digitalnih potrdil (CRL) preverijo, da digitalna potrdila niso bila preklicana;

- se zavedajo odgovornosti in jamstev, ki jih sprejemajo z uvrstitvijo digitalnih potrdil med zaupanja vredna;
- obveščajo overitelja o dogodkih, ki ogrožajo zasebne ključe imetnikov in bi jih lahko šteli kot razlog za preklic njihovih digitalnih potrdil.

9.7 Zanikanje odgovornosti overitelja

Overitelj ne prevzema obveznosti in ne odgovarja za škodo, stroške, nadomestila ali druge terjatve, ki bi nastale v primerih:

- ko je bilo digitalno potrdilo izdano zaradi napake ali neverodostojnih podatkov na strani imetnika potrdila;
- da je potekla veljavnost digitalnega potrdila oziroma je bilo potrdilo suspendirano ali preklicano;
- da potrdilo ni bilo uporabljeno za namene, kot so opredeljeni s to politiko;
- nepravilne uporabe ali zlorabe digitalnega potrdila ali registra preklicanih digitalnih potrdil;
- ravnanja imetnika ali tretje osebe, ki ni v skladu s to politiko ali obvestili overitelja;
- zlorabe ali vdora v računalniški sistem imetnika potrdila ali tretje osebe;
- ko je imetnik dovolil uporabo digitalnega potrdila nepooblaščenim osebam oziroma je prišlo do zlorabe imetnikovega digitalnega potrdila;
- nepravilnega delovanja računalniškega sistema imetnika ali tretje osebe;
- izpada ali nepravilnega delovanja infrastrukture, ki ni v upravljanju overitelja;
- višje sile.

9.8 Omejitve odgovornosti overitelja

Overitelj ne prevzema nobene obveznosti in odgovornosti do imetnikov in tretjih oseb, razen obveznosti in odgovornosti, ki so opredeljene s politiko in splošnimi postopki delovanja overitelja.

9.9 Povrnitev škode

Overitelj ne prevzema finančne odgovornosti in ne namerava povrniti škode za uporabo digitalnih potrdil in registra preklicanih potrdil, ki ni v skladu z določili te politike in z veljavno zakonodajo.

9.10 Začetek in prenehanje veljavnosti politike overitelja

9.10.1 Začetek veljavnosti

Začetek veljavnosti je opredeljen v končnih določbah v točki 9.17.

9.10.2 Prenehanje veljavnosti

Politika overitelja preneha veljati v primeru:
- uveljavitve nove verzije politike;
- menjave zasebnega ključa overitelja, s katerim podpisuje digitalna potrdila;
- prenehanja delovanja overitelja.

9.10.3 Posledice prenehanja veljavnosti

Ta dokument nadomešča prejšnjo objavljeno verzijo politike.

Po preteku veljavnosti politike zaradi izdaje nove verzije politike, imetniki uporabljajo digitalna potrdila do preteka njihove veljavnosti po določilih politike, pod katero so bila izdana. V primeru spremenjenih okoliščin, ki to onemogočajo, bo overitelj o tem obvestil imetnike.

9.11 Komuniciranje med subjekti

Vsa obvestila za imetnike in tretje osebe so objavljena na spletni strani overitelja na naslovu, navedenem v poglavju 2.1.

9.12 Dopolnitve politike

9.12.1 Postopek uveljavitve dopolnitev

V primeru tipografskih, uredniških ali vsebinskih sprememb, ki ne vplivajo bistveno na delovanje overitelja, bo overitelj spremembe objavljal v obliki dopolnitev k tej politiki.

Vse ostale spremembe bodo objavljene v obliki nove verzije politike overitelja.

Dopolnitve in spremembe politike se sprejemajo po enakem postopku kot politika.

9.12.2 Postopek obveščanja o dopolnitvah in spremembah

Dopolnitve bodo najkasneje 3 dni pred nastopom veljavnosti objavljene na spletnih straneh overitelja.

Nove verzije politike bodo z nastopom veljavnosti objavljene na spletnih straneh overitelja.

Vse imetnike, tretje osebe in medsebojno priznane overitelje bo overitelj o dopolnitvah in spremembah politike obveščal na svojih spletnih straneh.

9.12.3 Spremembe, ki zahtevajo novo identifikacijsko oznako politike

O tem, ali spremembe politike zahtevajo novo identifikacijsko oznako politike, odloča overitelj.

BANKA SLOVENIJE
EVROSISTEM

9.13 Urejanje sporov

Stranki bosta skušali sporazumno reševati vse morebitne spore.

V primeru da do sporazumne rešitve spora ne pride, je za reševanje sporov pristojno sodišče v Ljubljani.

9.14 Veljavna zakonodaja

Overitelj deluje v skladu s predpisi, ki veljajo na območju Republike Slovenije.

9.15 Skladnost z zakonodajo

Overitelj zagotavlja nadzor nad skladnostjo delovanja overitelja z veljavno zakonodajo z rednimi notranjimi in po potrebi zunanjimi revizijskimi pregledi.

9.16 Splošne določbe

9.16.1 Celovit dogovor

Vsi sodelujoči v celoti sprejemajo določila politike.

9.16.2 Prenos pravic in obveznosti

Imetnik digitalnega potrdila ne sme v nobenem primeru prenesti pravic in obveznosti uporabe digitalnih potrdil delno ali v celoti na tretjo stran.

9.16.3 Neodvisnost določil

V primeru, da zaradi spremenjene zakonodaje ali okoliščin postane del politike neveljaven, ostanejo ostali deli veljavni do objave spremembe politike.

9.16.4 Terjatve

"Ni predpisano".

9.16.5 Višja sila

Višja sila so izredne okoliščine, ki nastopijo po sklenitvi naročniškega razmerja in na katere udeleženci nimajo vpliva (npr. vojno stanje, požar, potres in druge elementarne nezgode).

BANKA SLOVENIJE
EVROSISTEM

V kolikor je zaradi višje sile onemogočeno izvrševanje obveznosti po tem dokumentu, se roki za izvršitev ustrezno podaljšajo.

9.17 Ostale določbe

Oblika in vsebina politike overitelja sta usklajeni z:

- RFC 3674: Internet X.509 Public Key Infrastructure Certificate Policy an Certification Practices Framework

Politika overitelja začne veljati od 15.11.2023 dalje.

V Ljubljani, 13. 11. 2023

Boštjan Vasle
GUVERNER