BANKA SLOVENIJE
EVROSISTEM

Splošni postopki delovanja overitelja na Banki Slovenije

APRIL, 2025

BANKA SLOVENIJE

EVROSISTEM

Splošni postopki delovanja overitelja na Banki Slovenije

Tip	*PST*
Oznaka akta	*POSTOPEK-8*
Verzija akta	*4*
Skrbnik akta	*Informacijska tehnologija (3000)*
Področje	*Organizacija dela*

BANKA SLOVENIJE
EVROSISTEM

Splošni postopki delovanja overitelja na Banki Slovenije

Kazalo

BANKA SLOVENIJE
EVROSISTEM

BANKA SLOVENIJE
EVROSISTEM

BANKA SLOVENIJE
EVROSISTEM

BANKA SLOVENIJE
EVROSISTEM

Splošni postopki delovanja overitelja 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. Hkrati so izdana digitalna potrdila za elektronski podpis skladna Uredbo-910/2014-EN-e-IDAS-EUR-Lex o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu.

Splošni postopki delovanja overitelja na BS (angl. Certificate Practice Statement – CPS, v nadaljevanju: splošni postopki delovanja overitelja) določajo postopke, ki jih overitelj izvaja za upravljanje celotnega življenjskega cikla digitalnih potrdil od posredovanja zahtevka, izdaje potrdila, pa vse do preteka veljavnosti ali preklica digitalnega potrdila. Akt opisuje tudi postopke, ki jih overitelj izvaja za upravljanje svoje računalniške infrastrukture.

Splošni postopki delovanja overitelja izpolnjujejo zahteve vseh politik overitelja, ki se na ta dokument sklicujejo.

Splošni postopki delovanja overitelja so javno dostopni.

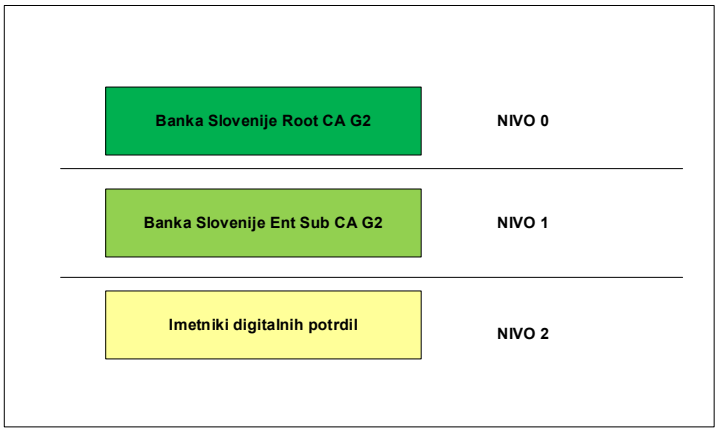
Struktura splošnih postopkov delovanja overitelja je bila oblikovana po priporočilih referenčnega dokumenta RFC 3647 z naslovom "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*" (dokument potrjen novembra 2003), ki ga je pripravila PKIX delovna skupina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

1.1 Predstavitev

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:

BANKA SLOVENIJE
EVROSISTEM



Slika 1: Overiteljeva infrastruktura Banke Slovenije

Najvišji v hierarhiji je izdajatelj "**Banka Slovenije Root CA G2**", ki je namenjen izdajanju digitalnih potrdil sistemov podrejenih izdajateljev digitalnih potrdil.

Podrejeni izdajatelj "**Banka Slovenije Ent Sub CA G2**" izdaja digitalna potrdila končnim uporabnikom in digitalna potrdila sistemov, ki delujejo v sklopu infrastrukture overitelja za upravljanje digitalnih potrdil in upravljanje identifikacijskih kartic BS.

1.2 Naslov akta in oznake

Naslov tega dokumenta je "SPLOŠNI POSTOPKI DELOVANJA OVERITELJA NA BANKI SLOVENIJE"

Mednarodna identifikacijska oznaka dokumenta (OID) v skladu s standardom ITU-T X.660 je: **1.3.6.1.4.1.27213.2.2.1.2.1.3**

Splošni postopki delovanja overitelja ustrezajo zahtevam za digitalna potrdila overitelja izdanimi pod naslednjimi politikami:

Ime digitalnega potrdila	Identifikacijski podatki politike (Issuance OID)	Ime politike
Paket digitalnih potrdil izdanih na identifikacijski kartici BS.	1.3.6.1.4.1.27213.2.1.1.1.1.3 1.3.6.1.4.1.27213.2.1.1.1.2.3 1.3.6.1.4.1.27213.2.1.1.1.3.3	Pravilnik overitelja digitalnih potrdil na Banki Slovenije (OID 1.3.6.1.4.1.27213.2.2.1.1.1.3)
Digitalna potrdila potrebna za delovanje infrastrukture overitelja	1.3.6.1.4.1.27213.2.1.1.10.1.2 1.3.6.1.4.1.27213.2.1.1.8.1.2 1.3.6.1.4.1.27213.2.1.1.8.1.2 1.3.6.1.4.1.27213.2.1.1.9.1.2 1.3.6.1.4.1.27213.2.1.1.1.3.2	Izdana digitalna potrdila so navedena v točki 7.1.

1.3 Subjekti

Opisi subjektov, vezanih na digitalna potrdila overitelja, so podani v posamezni politiki, pod katero so bila digitalna potrdila izdana.

BANKA SLOVENIJE
EVROSISTEM

1.3.1 Organizacija v okviru katere deluje overitelj

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

1.3.2 Organ potrjevanja politike

Podano v posamezni politiki, pod katero so bila digitalna potrdila izdana.

1.3.3 Izdajatelji digitalnih potrdil

Izdajatelji so programska oprema Microsoft CA services, ki tečejo na strežnikih z operacijskim sistemom Windows.

Zasebni ključi overitelja so zavarovani s strojnim šifrirnim modulom. S šifrirnimi ključi na strojnem modulu se upravlja preko programske opreme proizvajalca. Dostop imajo HSM Administrator uporabniki in Cryptographic User uporabniki, kot so določeni v dokumentu "CA Key Generation Ceremony in Banka Slovenije". Za uporabo zasebnega ključa izdajatelja Banka Slovenije Root CA G2 je vzpostavljeno načelo večkratne odobritve, zato se morata prijaviti dva od štirih Administrator operaterjev oziroma dva od treh Cryptographic user uporabnikov na particiji ključa. Enako velja za uporabo zasebnega ključa izdajatelja Banka Slovenije Ent SUB CA G2. Vsi dostopi so nadzorovani po načelu štirih oči.

1.3.4 Prijavna služba overitelja

Prijavno službo sestavljajo:

- Oddelek OK, ki izvrši prvo overitev istovetnosti prosilcev digitalnih potrdil in zahtevek za prvo izdajo potrdila posreduje na Helpdesk v oddelku IT;
- Helpdesk v oddelku IT, ki sprejema zahtevke prosilcev za upravljanje digitalnih potrdil in overja istovetnost imetnikov digitalnih potrdil v postopkih obnove, preklica ali suspenza potrdila;
- varnostna služba na recepciji BS, ki deluje v okviru oddelka UH in overja istovetnost prosilcev ob prevzemu identifikacijske kartice BS, na kateri so shranjena digitalna potrdila.

Prijavna služba v okviru izvajanja svojih nalog uporablja naslednje aplikacije:

- Sistem za upravljanje identifikacijskih kartic BS

  Uporabniki se prijavijo z naprednim digitalnim potrdilom overitelja. Sistem omogoča upravljanje življenjskega cikla identifikacijskih kartic BS, kar vključuje personalizacijo kartice ob prvi uporabi in upravljanje digitalnih potrdil shranjenih na kartici.

- Interne evidence o zaposlenih in pogodbenih izvajalcih BS
  - Imenik zaposlenih na intranetu

    Uporabniki se prijavijo z naprednim digitalnim potrdilom overitelja. Imenik omogoča vpogled v naslednje identifikacijske podatke: ime, priimek, fotografija.

  - Šifrant zaposlenih v bazi Oracle

Uporabniki se prijavijo z naprednim digitalnim potrdilom overitelja. Imenik omogoča vpogled v naslednje identifikacijske podatke: ime, priimek, matična številka v BS.

1.3.5 Arhiv zasebnih ključev

Arhiv zasebnih šifrirnih ključev se nahaja na strojnem varnostnem modulu, skladnem s FIPS 140-2 level 3. Skrbnika kopije zasebnih šifrirnih ključev (ang. Key Recovery Officer) se v sistem za upravljanje identifikacijskih kartic BS prijavita z digitalnim potrdilom, shranjenim na identifikacijski kartici BS.

Zahteve za dostop do arhiva zasebnih ključev so podane v politiki, pod katero so bila potrdila izdana.

1.3.5.1 Uporabniki digitalnih potrdil

Podano v posamezni politiki, pod katero so bila digitalna potrdila izdana.

1.3.5.2 Imetniki digitalnih potrdil

Podano v posamezni politiki, pod katero so bila digitalna potrdila izdana.

1.3.5.3 Tretje osebe

Podano v posamezni politiki, pod katero so bila digitalna potrdila izdana.

1.4 Namen uporabe digitalnih potrdil

Podano v posamezni politiki, pod katero so bila digitalna potrdila izdana.

1.4.1 Pravilna uporaba digitalnih potrdil in ključev

Podano v posamezni politiki, pod katero so bila digitalna potrdila izdana.

1.4.2 Nepravilna uporaba digitalnih potrdil in ključev

Podano v posamezni politiki, pod katero so bila digitalna potrdila izdana.

1.5 Urejanje politike overitelja

Dokumenti o splošnih postopkih delovanja overitelja morajo biti pregledani najmanj enkrat letno.

1.5.1 Kontaktne osebe

V skladu s Pravilnikom overitelja digitalnih potrdil na Banki Slovenije je odgovorna kontaktna oseba za upravljanje politike overitelja vodja informacijske varnosti, ki mu osebje overitelja posreduje sporočila v zvezi s tem, naslovljena na splošni kontaktni naslov objavljen v politiki overitelja.

Odgovorna kontaktna oseba za upravljanje splošnih postopkov delovanja overitelja je Pomočnica direktorja oddelka informacijska tehnologija.

1.5.2 Postopki spreminjanja vsebine dokumentacije

Odgovorna kontaktna oseba za upravljanje politike overitelja v skladu najmanj z zahtevano pogostnostjo pregledovanja dokumenta, določenega s politiko overitelja preveri spremembo zakonodaje in spremembo zahtev za medsebojno priznavanje izdajateljev digitalnih potrdil v okviru Evropskega sistema centralnih bank (ESCB), spremembo tehnoloških ali spremembo poslovnih zahtev. Na podlagi zaznanih sprememb predlaga potrebne dopolnitve politike in splošnih postopkov delovanja overitelja. Dopolnitve predstavi odgovorni kontaktni osebi za upravljanje splošnih postopkov delovanja overitelja.

Odgovorna kontaktna oseba za upravljanje splošnih postopkov delovanja overitelja na podlagi spremenjenih zahtev politike pripravi predloge potrebnih sprememb splošnih postopkov overitelja in jih predstavi vodstvu oddelka IT

Oddelek IT preveri potrebe po morebitnih spremembah infrastrukture, da bo le ta omogočala izvrševanje spremenjene politike overitelja in splošnih postopkov delovanja overitelja. V primeru potrebnih sprememb oddelek IT odgovorno kontaktno osebo za upravljanje politike overitelja obvesti o roku do katerega bo zagotovil potrebne infrastrukturne spremembe.

Po implementaciji potrebnih infrastrukturnih sprememb oddelek IT o izvedbi obvesti odgovorno kontaktno osebo za upravljanje politike overitelja.

Odgovorna kontaktna oseba za upravljanje splošnih postopkov delovanja overitelja predlagane spremembe splošnih postopkov posreduje odgovorni osebi za upravljanje politike overitelja, da potrdi skladnost z zahtevami politike overitelja.

1.5.3 Oseba za ugotavljanje skladnosti CPS s politiko

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

1.5.4 Objavljanje dokumentacije

Vse spremembe, vključno s kopijo tega dokumenta, bodo ob nastopu veljavnosti popravkov objavljene na internetnih straneh overitelja na BS, kjer so dostopne preko naslova http://ca.bsi.si/PKI.

1.6 Pomen izrazov in kratic

Pomen izrazov je podan v politiki overitelja, pod katero so bila digitalna potrdila izdana.

Spodnja tabela podaja pomen v dokumentu uporabljenih kratic specifičnih za BS.

1.6.1.1.1 Kratica	1.6.1.1.2 Pomen
Oddelek IT	Oddelek Informacijska tehnologija v BS
Oddelek OK	Oddelek Organizacija in kadri v BS
Oddelek UH	Oddelek Uprava hiše v BS

2 Objave informacij in javni imeniki

Spletne strani, na katerih overitelj javno objavlja informacije, gostujejo na spletnem portalu, ki ga upravlja BS (http://www.bsi.si).

BANKA SLOVENIJE
EVROSISTEM

Seznam javno objavljenih informacij in imenikov je podan v politiki overitelja, pod katero so bila digitalna potrdila izdana.

2.1 Pogostnost objav

Vsi podatki o pogostnosti in časih objave so podani v politiki overitelja, pod katero so bila digitalna potrdila izdana.

2.2 Dostop do objavljenih informacij

Javno objavljeni podatki so prosto dostopni vsem obiskovalcem spletnih strani overitelja.

BS vse podatke objavljene na svojem spletnem portalu s sistemom dostopnih pravic varuje pred nepooblaščenim spreminjanjem ali uničenjem.

Vsako objavo na spletnem portalu BS mora predhodno odobriti pooblaščeno osebje BS.

Objave na spletnem portalu BS izvaja osebje BS, ki je s sistemom dostopnih pravic pooblaščeno za objave na spletnem portalu. Za objavo se mora na delovno postajo prijaviti z digitalnim potrdilom shranjenim na identifikacijski kartici BS. Dostop do zasebnega ključa povezanega z digitalnim potrdilom je zavarovan s PIN kodo.

3 Preverjanje istovetnosti

3.1 Določanje imen

3.1.1 Vrste imen

Oblika imen je v skladu s politiko overitelja, pod katero so bila digitalna potrdila izdana.

Podatki o imetniku izhajajo iz kadrovske evidence BS, v katero so vneseni na podlagi podatkov iz uradnega osebnega dokumenta prosilca in so posredovani v zahtevku za pridobitev digitalnega potrdila.

3.1.2 Potreba po smiselnosti imen

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

3.1.3 Anonimnost imetnikov in uporaba psevdonimov

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

3.1.4 Pravila za interpretacijo različnih oblik imen

Pravila za interpretacijo različnih imen so opredeljena v politiki overitelja, pod katero so bila digitalna potrdila izdana.

3.1.5 Edinstvenost imen

Podatki razločevalnega imena v polju »subject« potrdila morajo biti edinstveni za vsako izdano digitalno potrdilo.

Edinstvenost je zagotovljena z vključevanjem serijske številke imetnika potrdila v razločevalno ime o imetniku. Serijska številka je 12 mestni niz števk oblikovan po naslednji nomenklaturi:

Znak v serijski številki	Pomen	Vrednost
1-2	Tip potrdila	00-99
3	Tip uporabnika 1=zaposleni 2=pogodbeniki 3=štipendisti 4=praktikanti 5=študentski servis 6=nagrajenci 7=štipendisti v tujini	0-9
4-9	ID uporabnika (naključno šestmestno število)	000000 – 999999
10-11	Rezervirano	00-99 (zaenkrat 00)
12	Kontrola	0-9

V kadrovskih evidencah BS se s kontrolnimi mehanizmi preverja, da ne prihaja do ponavljanja serijske številke.

3.1.6 Postopek reševanja imenskih sporov

Postopek reševanja imenskih sporov je opredeljen s politiko overitelja, pod katero so bila digitalna potrdila izdana.

3.1.7 Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk

Opredeljeno s politiko overitelja, pod katero so bila digitalna potrdila izdana.

3.2 Preverjanje istovetnosti ob prvi registraciji

Prijavna služba overitelja za vse prejete zahtevke za pridobitev digitalnega potrdila preveri istovetnost podatkov v zahtevku s podatki v identifikacijskem dokumentu prosilca.

3.2.1 Metoda za dokazovanje posesti zasebnega ključa

Metode dokazovanja posesti zasebnega ključa so opisane v politiki overitelja, pod katero so bila digitalna potrdila izdana.

Za dokazovanje posesti zasebnega ključa in kontrolo povezave med zasebnim in javnim ključem, vsebovanim v zahtevku za izdajo digitalnega potrdila, se uporablja PKCS#10 oblika zahtevka v skladu z RSA PKCS#10 Certificate Request Syntax Standard.

3.2.2 Preverjanje identitete pravne osebe

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

3.2.3 Preverjanje istovetnosti fizične osebe

Ob prevzemu identifikacijske kartice BS, na kateri so shranjeni pari ključev in izdana digitalna potrdila, mora prosilec ob fizični prisotnosti izkazati svojo identiteto s predložitvijo uradnega osebnega dokumenta. Prosilec ob tem pisno potrdi prevzem identifikacijske kartice.

V postopku preverjanja, ki ga izvede osebje prijavne službe na recepciji BS se poleg preverjanja identitete in veljavnosti uradnega osebnega dokumenta preveri, da se podatki iz zahtevka za izdajo digitalnega potrdila ujemajo s podatki z osebnega dokumenta. Osebje prijavne službe ob tem pisno potrdi, da je izvedlo preverjanje podatkov.

3.2.4 Podatki o prosilcih, ki se ne preverjajo

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

3.2.5 Preverjanje pooblastil v zahtevkih prosilcev

Prijavna služba overitelja preveri, da so zahtevki za pridobitev digitalnega potrdila BS ustrezno odobreni:

- zahtevke za zaposlene v BS lahko odobri pooblaščena oseba v oddelku OK;
- zahtevke za zunanje pogodbene izvajalce odobrijo odgovorne osebe oddelkov v BS, ki so predlagatelji za sklenitev pogodbenega odnosa BS s prosilcem za pridobitev digitalnega potrdila.

Pristnost pooblastil prijavna služba preverja na podlagi dokumentov "Sklep o pooblastilih pri podpisovanju za Banko Slovenije" in "Pravilnik o organizaciji Banke Slovenije".

Redna menjava digitalnih potrdil se izvede na osnovi podpisanega pisnega zahtevka imetnika.

3.2.6 Merila za medsebojno povezovanje

Minimalni kriteriji, ki jim mora ustrezati zunanji overitelj, da bi se medsebojno povezal z overiteljem, je:

- zunanji overitelj je eden od javno priznanih overiteljev kvalificiranih digitalnih potrdil v Republiki Sloveniji oz. v okviru EU;
- ustreznost zunanjega overitelja je po merilih okvira za medsebojno priznavanje (ESCB Certificate Acceptance Framework – CAF) potrdil Odbor za informacijsko tehnologijo (Information Technology Commitee - ITC), ki deluje v okviru ESCB.

3.3 Preverjanje istovetnosti ob zahtevi za menjavo ključev

Ob rutinski menjavi ključev ali menjavi ključev zaradi preklica obstoječega para ključev mora prosilec ob fizični prisotnosti prijavni službi na Helpdesk predložiti obstoječo identifikacijsko kartico BS.

BANKA SLOVENIJE
EVROSISTEM

Zaposleni v prijavni službi na Helpdesk preveri naslednje identifikacijske podatke:
- ime in priimek;
- matično številka zaposlenega;
- sliko.

Če prosilec ne razpolaga z identifikacijsko kartico BS, je postopek enak kot pri prvi registraciji.

3.4 Preverjanje istovetnosti ob zahtevi za preklic potrdila

Preverjanje istovetnosti ob preklicu digitalnega potrdila se v primeru fizične prisotnosti imetnika izvede na enak način kot ob izdaji digitalnega potrdila.

Preklice, posredovane po elektronski pošti, podpisane z imetnikovim digitalnim potrdilom za elektronski podpis, ki ga izda overitelj, se dodatno ne overja.

V pisnih zahtevkih odgovornih oseb oddelka BS, v katerem je zaposlen imetnik ali oddelka, ki je predlagal sklenitev pogodbe z imetnikom, se pristnost pooblastil preverja na podlagi dokumenta "Sklep o pooblastilih pri podpisovanju za Banko Slovenije" in "Pravilnik o organizaciji Banke Slovenije".

4 Upravljanje z digitalnimi potrdili

4.1 Zahtevki za pridobitev potrdila

Obrazec zahtevka za pridobitev digitalnega potrdila je objavljen na spletni strani overitelja na naslovih za objavo, opredeljenih v poglavju 2.

4.1.1 Kdo lahko zaprosi za izdajo digitalnega potrdila

Opredeljeno s politiko, po kateri se digitalno potrdilo izdaja.

4.1.2 Izpolnitev zahtevka za izdajo digitalnega potrdila in odgovornosti prosilca

Zahtevek za pridobitev digitalnega potrdila za zaposlene v BS izpolni oddelek OK.

Zahtevek za pridobitev digitalnega potrdila za prosilce, ki delajo za BS in imajo pogodbeni odnos z BS, izpolnijo odgovorne osebe oddelkov, ki so predlagatelji za sklenitev pogodbe s prosilcem za pridobitev digitalnega potrdila.

Zahtevek za redno menjavo digitalnih potrdil izpolni prosilec.

Izpolnjeni in podpisani zahtevki se posredujejo prijavni službi na Helpdesk.

4.2 Obravnava vloge za izdajo potrdila

4.2.1 Preverjanje istovetnosti podatkov o prosilcu

Zahtevke za izdajo digitalnih potrdil, izdanih na identifikacijski kartici BS, obravnava prijavna služba overitelja na Helpdesk v oddelku IT. Obravnava poteka po naslednjem postopku:

- prijavna služba preveri, da se podatki na zahtevku ujemajo s podatki o prosilcu v kadrovski evidenci BS oziroma v evidencah pogodbenih izvajalcev BS. Preverijo se naslednji identifikacijski podatki: ime, priimek, matična številka v BS, enolični identifikator[1];
- če imetnik še nima kartice ali potrebuje novo, prijavna služba sproži postopek tiskanja identifikacijskih podatkov prosilca na identifikacijsko kartico BS;
- prijavna služba preveri, ali zahtevek vključuje seznanitev in sprejem izjave o pogojih uporabe digitalnih potrdil, ki jo bodoči imetnik podpiše ob prevzemu identifikacijske kartice, opisanem v točki 4.4. Izjava mora vključevati vse identifikacijske podatke o prosilcu, ki bodo zapisani v digitalnem potrdilu (ime in priimek, organizacija, naslov elektronske pošte in serijska številka imetnika);
- prijavna služba preko sistema za upravljanje identifikacijskih kartic sproži avtomatiziran postopek za: generiranje para ključev za posamezno digitalno potrdilo in njihovo varno hranjenje na identifikacijski kartici BS, pripravo in posredovanje zahtevka izdajatelju digitalnih potrdil, tvorjenje osebnega gesla za dostop do zasebnih ključev na identifikacijski kartici BS (PIN koda identifikacijske kartice), tvorjenje kode za odklepanje identifikacijske kartice BS (PUK koda identifikacijske kartice), izdajo digitalnega potrdila in vpis potrdila na identifikacijsko kartico;
- prijavna služba identifikacijsko kartico bodočega imetnika posreduje prijavni službi v oddelku UH, aktivacijske podatke za kartico pa hranijo na Helpdesku, kjer jih bodoči imetnik tudi prevzame.
- prijavna služba varno shrani vso dokumentacijo, ki jo je prejela z zahtevkom za izdajo digitalnega potrdila.

4.2.2 Odobritev ali zavrnitev vloge

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.2.3 Čas za obdelavo vloge za izdajo digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.3 Izdaja potrdila

4.3.1 Aktivnosti izdajatelja ob izdaji digitalnega potrdila

Postopek za paket digitalnih potrdil, izdanih na identifikacijski kartici:

- pooblaščena oseba prijavne pisarne se prijavi na sistem za upravljanje identifikacijskih kartic BS;
- pooblaščena oseba prijavne pisarne na podlagi imena, priimka in matične številke v BS v sistemu poišče prosilca za pridobitev digitalnega potrdila;
- pooblaščena oseba prijavne pisarne v sistemu odobri izdajo paketa digitalnih potrdil prosilcu;
- sistem za upravljanje identifikacijskih kartic BS za vsako digitalno potrdilo sproži generiranje para ključev;

[1] Davčna številka in EMŠO (za državljane Republike Slovenije), ali primerljivi enolični nacionalni identifikator (za tujce).

- sistem za upravljanje identifikacijskih kartic BS za vsako digitalno potrdilo pripravi PKCS#10 zahtevek in ga posreduje izdajatelju.

Po tem, ko je osebje prijavne pisarne na identifikacijski kartici prosilca kreiralo par ključev, programska oprema za upravljanje identifikacijskih kartic tvori zahtevek v obliki PKCS#10 in ga pošlje izdajatelju.

Izdajatelj po prejemu izvede naslednje aktivnosti:
- preveri identiteto sistema za upravljanje identifikacijskih kartic BS;
- preveri veljavnost PKCS#10 zahtevka;
- izda digitalno potrdilo za prejeti PKCS#10 zahtevek;
- digitalno potrdilo posreduje sistemu za upravljanje identifikacijskih kartic BS.

4.3.2 Obvestilo imetniku o izdaji digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.4 Prevzem potrdila

4.4.1 Postopek prevzema digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.4.2 Objava digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.4.3 Obveščanje drugih udeležencev o izdaji digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.5 Uporaba para ključev in digitalnega potrdila

4.5.1 Uporaba para ključev in digitalnega potrdila s strani imetnika

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.5.2 Uporaba javnega ključa in digitalnih potrdil s strani tretjih oseb

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.6 Obnova potrdila brez menjave ključev

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.7 Obnova digitalnega potrdila

4.7.1 Razlogi za obnovo digitalnih potrdil

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.7.2 Kdo lahko zahteva obnovo digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.7.3 Obdelava zahtevkov za obnovo digitalnega potrdila

Prijavna služba na Helpdesk preveri, ali je zahtevek v celoti izpolnjen in podpisan s strani prosilca.

Prijavna služba na Helpdesk overi identiteto prosilca s tem da:
- se identifikacijski podatki na zahtevku ujemajo s podatki v interni evidenci o zaposlenih in pogodbenih izvajalcih BS ter podatki na identifikacijski kartici prosilca;
- preveri sliko prosilca, ki se je z identifikacijsko kartico zglasil v prijavni pisarni.

4.7.4 Obvestilo imetniku o izdaji obnovljenega digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.7.5 Postopek potrditve prevzema obnovljenega digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.7.6 Objava obnovljenega digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.7.7 Obveščanje drugih udeležencev o izdaji potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.8 Sprememba potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9 Preklic in začasna razveljavitev digitalnega potrdila

4.9.1 Razlogi preklica

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9.2 Kdo lahko zahteva preklic

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9.3 Postopek za preklic digitalnega potrdila

Standardni postopek:
Osebje overitelja prekliče digitalno potrdilo po postopku opredeljenem v politiki pod katero so bila digitalna potrdila izdana. Preverjanje istovetnosti imetnika, ki preklicuje digitalno potrdilo, se izvede po enakem postopku, kot se ob prvi registraciji uporablja za preverjanje fizičnih oseb (opisano v poglavju 3.2.3).

Izredni postopek:
Varnostnik na recepciji BS po prejemu telefonskega klica za preklic digitalnega potrdila:
- zabeleži ime in priimek imetnika digitalnega potrdila in telefonsko številko klicatelja.
- po postopku usklajenem z oddelkom IT kliče kontaktne osebe IT s klicne liste Pomoč uporabnikom.
- prvemu kontaktu, ki ga prikliče prenese zabeležene podatke za preklic digitalnega potrdila.

Kontaktna oseba IT po postopku opredeljenem v politiki overitelja izvede začasno razveljavitev digitalnega potrdila.

4.9.4 Čas za posredovanje zahtevka za preklic

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9.5 Čas od prejema zahtevka za preklic do preklica potrdila

4.9.5.1 Digitalna potrdila imetnikov

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9.5.2 Digitalna potrdila overiteljeve infrastrukture

Preklic digitalnega potrdila overitelja, s katerim podpisuje digitalna potrdila, se izvede takoj.

4.9.6 Preverjanje statusa potrdil pred uporabo

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

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

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9.8 Maksimalne zakasnitve pri objavi registra preklicanih digitalnih potrdil

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9.9 Storitev sprotnega preverjanja statusa digitalnih potrdil

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9.10 Obveza tretjih oseb po sprotnem preverjanju statusa preklicanih potrdil

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9.11 Ostale oblike objavljanja preklicanih digitalnih potrdil

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9.12 Posebne zahteve za preklic digitalnih potrdil v primeru zlorabe ključev

V primeru preklica digitalnega potrdila izdajatelja zaradi zlorabe zasebnega ključa, se na spletnem mestu overitelja objavi krajša izjava za javnost, ki jo pripravi služba BS, zadolžena za odnose z javnostjo.

4.9.13 Vzroki za začasno razveljavitev digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9.14 Kdo lahko zahteva ali prekliče začasno razveljavitev digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9.15 Postopek za začasno razveljavitev digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.9.16 Čas začasne razveljavitve digitalnega potrdila

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.10 Storitve preverjanja statusa digitalnih potrdil

4.10.1 Tehnične lastnosti storitve

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.10.2 Razpoložljivost storitve

Overitelj visoko razpoložljivost računalniške infrastrukture glede na zahteve politik pod katerimi izdaja digitalna potrdila zagotavlja s stalnim spremljanjem sistema, rednim vzdrževanjem, s podvajanjem komponent, z načrti neprekinjenega delovanja in z vzpostavitvijo rezervnega računalniškega centra. Opis mehanizmov, ki jih overitelj uporablja za zagotavljanje visoke razpoložljivosti, je podan v internih aktih BS za področje neprekinjenosti poslovanja. Dokumenti so klasificirani s stopnjo zaupnosti *zaupno* in so pooblaščenemu osebju overitelja dostopni na podlagi načela nujno potrebnih informacij za opravljanje nalog.

4.10.3 Dodatne možnosti storitve

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.11 Prekinitev naročniškega razmerja med imetnikom in overiteljem

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.12 Varnostno kopiranje in odkrivanje zasebnega ključa

4.12.1 Politika in postopki varnostnega kopiranja zasebnih ključev

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

4.12.1.1 Postopek za povrnitev zgodovine ključev

Povrnitev se izvede po naslednjem postopku:

- imetnik na prijavno službo overitelja naslovi zahtevek za povrnitev zgodovine zasebnih ključev;
- imetnik se osebno zglasi v prijavni službi in se identificira z identifikacijski kartico BS;
- osebje prijavne službe po uspešnem preverjanju istovetnosti imetnika (preveri ime, priimek, matično številko in sliko), preko programske opreme za upravljanje identifikacijskih kartic v BS izvede povrnitev zgodovine zasebnih ključev imetnika, ki poteka po naslednjem vrstnem redu:
    - program za upravljanje identifikacijskih kartic na identifikacijski kartici imetnika pripravi par RSA ključev za uvoz in javni ključ pošlje modulu za povrnitev zasebnih ključev;
    - modul za povrnitev zasebnih ključev na strojnem varnostnem modulu dešifrira zasebni ključ imetnika, generira AES simetrični ključ za varen prenos podatkov, z njim šifrira zasebni ključ imetnika, simetrični šifrirni ključ pa šifrira z javnim ključem RSA za uvoz na identifikacijsko kartico. Modul šifriran zasebni ključ imetnika in šifriran simetrični ključ posreduje programu za upravljanje identifikacijskih kartic;

- program za upravljanje identifikacijskih kartic shrani simetrični ključ in zasebni ključ uporabnika na identifikacijsko kartico imetnika in s kartice izbriše par RSA ključev za uvoz.

4.12.1.2 Odkrivanje kopije zasebnega ključa za dešifriranje

Odkrivanje zasebnega ključa poteka po naslednjem postopku:

- prijavna služba overitelja prejme zahtevek za odkrivanje zasebnega ključa imetnika;
- osebje prijavne službe v primeru veljavnosti in ustreznosti zahtevka kontaktira enega od skrbnikov kopije zasebnih ključev;
- osebje prijavne službe overitelja pripravi prazno kartico, na katero se bo shranil odkriti zasebni ključ;
- osebje prijavne službe v sistemu za upravljanje identifikacijskih kartic BS pripravi elektronski zahtevek za odkrivanje zasebnega ključa;

  eden od skrbnikov kopije zasebnih ključev se zglasi v prostorih prijavne pisarne overitelja na Helpdesk in verificira ustreznost odobritve zahtevka za odkrivanje zasebnega ključa;
- skrbnik kopije zasebnih ključev z vstavitvijo svoje identifikacijske kartice v sistem za upravljanje identifikacijskih kartic BS odobri zahtevek za odkrivanje zasebnega ključa;
- sistem za upravljanje identifikacijskih kartic personalizira vstavljeno prazno identifikacijsko kartico na ime imetnika zasebnega ključa;
- sistem za upravljanje kartic izvede postopke 1, 2 in 3 iz opisa povrnitve zgodovine ključev v poglavju 4.12.1.1.

4.12.2 Zaščita ključa za prenos zasebnega ključa

Ključ za prenos zasebnega ključa je zavarovan s šifriranjem. Šifrira se z javnim ključem začasnega para za uvoz zasebnega ključa, ki se tvori na identifikacijski kartici BS. Postopek je opisan v točki 2 v poglavju 4.12.1.1.

5 Fizično varovanje, organizacijski varnostni ukrepi in nadzor nad osebjem

5.1 Fizično varovanje

Povzeti so najbolj pomembni ukrepi, ki so implementirani. Natančneje so postopki in ukrepi definirani v internih aktih BS za področje fizičnega varovanja.

5.1.1 Lokacija in konstrukcija prostorov overitelja

Zgradba in prostori overitelja so fizično varovani.

Strežniška oprema overitelja je v prostorih računalniškega centra in rezervnega računalniškega centra BS, za katerega so zagotovljeni naslednji varnostni ukrepi:

- prostori so brez oken;
- fizična kontrola pristopa in posamični prehodi;
- nadzorne kamere so na vhodih in v prostorih;

- prostori so opremljeni z detektorji požara, izlitja vode in gibanja;
- vzpostavljene so tri varnostne zone prostorov. Prehodi med zonami so fizično ločeni in zavarovani z dodatno fizično kontrolo pristopa;
- ožičenje, ločeno za napajanje in komunikacije, poteka po posebnih kanalih.

5.1.2 Fizični dostop do overitelja

Vstop v zgradbo imajo le zaposleni BS in zunanji pogodbeni izvajalci. Prihodi obiskovalcev morajo biti v naprej najavljeni in odobreni. Obiskovalci so v zgradbi vedno v spremstvu zaposlenega BS.

Za vstop v zgradbo se je potrebno registrirati z identifikacijsko kartico BS.

Vstop v prostore računalniškega centra ima le pooblaščeno osebje BS. Zaposleni se mora pred vstopom registrirati z identifikacijsko kartico BS in PIN kodo.

Za prehod med zonami v računalniškem centru se mora zaposleni registrirati z identifikacijsko kartico BS. Dostopne pravice do posameznih zon so dodeljene na podlagi nujno potrebnih pravic za izvajanje nalog.

5.1.3 Napajanje in klimatske naprave

Računalniški center BS ima električno omrežje priključeno preko baterijskega vira napajanja (angl. Uninterruptuble Power Supply – UPS), ki v primeru izpada omrežja vsaj 45 minut zagotavlja avtonomnost delovanja računalniškega centra.

Ob izpadu električnega omrežja se avtomatsko vključi agregat, ki zagotavlja avtonomnost delovanja računalniškega centra.

Oprema overitelja, priključena v prostorih računalniškega centra BS, ima dva ločena napajalnika.

Prostori računalniškega centra so klimatizirani in zagotavljajo vzdrževanje temperature v skladu s specifikacijami proizvajalcev za normalno delovanje opreme. Obremenitev hlajenja je enakomerno porazdeljena na dve stalno delujoči klimatski napravi. V primeru izpada ene od naprav zmogljivost druge zagotavlja vzdrževanje ustrezne temperature.

5.1.4 Zaščita pred poplavo

Oprema in ožičenje so ustrezno zavarovani pred izlitjem vode.

5.1.5 Zaščita pred požarom

Vsi prostori v zgradbi so opremljeni z detektorji in alarmi požara. Alarmi so speljani v varnostni operativni center BS, kjer je zagotovljeno 24 urno spremljanje statusov.

Hodniki in prostori računalniškega centra so opremljeni z aparati za gašenje.

Osebje overitelja se redno usposablja za uporabo aparatov za gašenje.

5.1.6 Shranjevanje medijev

Centralna diskovna polja so podvojena. Kritični diski na posameznem diskovnem polju so konfigurirani v sistemu visoke razpoložljivosti VRAID1 in omogočajo menjavo okvarjenih diskov pri delujočem sistemu brez izpada delovanja.

Za kritične podatke se izdelujejo redne varnostne kopije na virtualne trakove, mesečno pa tudi na klasične tračne medije. Ena kopija virtualnih trakov in tračnih medijev se hrani v računalniškem centru, druga kopija pa dislocirano v rezervnem računalniškem centru. Varnostno kopiranje izvaja pooblaščeno osebje overitelja.

5.1.7 Odstranjevanje odpadkov

Prostori so opremljeni z rezalniki papirja, ki zagotavljajo varno uničevanje podatkov v papirni obliki.

Magnetni mediji se pred izločanjem uničijo na napravi za razmagnetenje.

5.1.8 Hranjenje kopij podatkov na oddaljeni lokaciji

Centralni diskovni polji sta nameščeni na različnih lokacijah (v računalniškem centru BS in rezervnem računalniškem centru BS). Med diskovnimi polji je vzpostavljena sinhrona replikacija podatkov.

Varnostne kopije se izdelujejo v dveh izvodih, ki se nahajata na različnih lokacijah.

5.2 Organizacijski varnostni ukrepi

5.2.1 Notranja organizacija overitelja in porazdelitev nalog

Overitelj ima vzpostavljene naslednje vloge:

HSM Administrator - Funkcija **administratorja strojnega varnostnega modula** (angl. HSM Administrator) je namenjena sistemski administraciji strojnega varnostnega modula. Vse administrativne aktivnosti na modulu so zavarovane z administrativnim setom pametnih kartic za strojni varnostni modul.

Za izvedbo administrativnih aktivnosti na modulu mora administrator zagotoviti hkratno prisotnost vsaj dveh od štirih HSM administratorjev. Za kritične aktivnosti, kot so nalaganje vdelanih programskih modulov (angl. Firmware) in uvažanje glavnega šifrirnega ključa (angl. Master Backup Key) je potrebna prisotnost vseh štirih administratorjev strojnih varnostnih modulov.

Administrator strojnega varnostnega modula lahko opravlja tudi druge naloge. Administrator strojnega varnostnega modula ima odobren fizični dostop do strojnega varnostnega modula.

Uporabnik particije CA - Funkcija uporabnika particije je namenjena ustvarjanju in uporabi kriptografskih ključev na particiji ter ustvarjanju in obnovi varnostnih kopij ključev na particiji. Za obnavljanje varnostnih kopij ključev morata biti prisotna dva od treh uporabnikov particije in Upravitelj ključev particije.

Za ustvarjanje in uporabo ključev na particiji morata biti hkrati prisotna vsaj dva od treh Uporabnikov particije. Za aktivacijo ključev na particiji strojnega varnostnega modula je potrebna prisotnost enega od treh uporabnikov.

Uporabnik particije - Funkcija uporabnika particije je namenjena ustvarjanju in uporabi kriptografskih ključev na particiji ter ustvarjanju in obnovi varnostnih kopij ključev na particiji. Za ustvarjanje in uporabo ključev na particiji moramo zagotoviti hkratno prisotnost vsaj dveh od dveh Uporabnikov particije.

Upravitelj ključev - Funkcija upravitelja ključev particije je namenjena ustvarjanju in obnovi varnostnih kopij kliučev na particiji. Za obnavljanje varnostnih kopij ključev na particiji morata biti prisotna vsaj še dva od treh uporabnikov particije za uporabnike particij BSHSM_ROOTCAG2 in BSHSM_ENTSUBCAG2 ter dva od dveh uporabnikov particije za particijo OCSP.

Administrator particije - Funkcija administratorja particije je namenjena inicializaciji oz. ponovni inicializaciji particije in ustvarjanju uporabnika particije. Funkcija se na strojnih varnostnih modulih CC EAL4+ uporablja le na particiji »OCSP«, ki je namenjena za ključe »Onilne Certificate Service Protocol« strežnika. Funkcija se uporablja tudi na obeh particijah strojnega varnostnega modula FIPS 140-2. Za uporabo funkcije Administratorja particije na CC EAL4+ modulih moramo zagotoviti prisotnost dveh od dveh skrbnikov gesla Administratorja particije.

Sistemski administrator izdajateljskega strežnika ima pooblastila za namestitev, konfiguriranje, vzdrževanje in zaustavitev programske opreme izdajatelja, nima pa dostopa do zasebnega ključa izdajatelja. Overitelj ima ločene sistemske administratorje za izdajateljska strežnika Banka Slovenije Root CA G2 in Banka Slovenije Ent Sub CA G2. Sistemski administrator izdajateljskega strežnika lahko opravlja tudi druge naloge. Sistemski administrator izdajateljskega strežnika nima dostopa do strojnega varnostnega modula, razen, če nima dostopa v kombinaciji z drugimi vlogami, ki jih opravlja.

Sistemski administrator strežnika za upravljanje identifikacijskih kartic BS ima pooblastila za namestitev, konfiguriranje vzdrževanje in zaustavitev strežnika, ter osnovno konfiguriranje programske opreme za upravljanje identifikacijskih kartic BS. Nima pa pravic za upravljanje dostopov in delovnih tokov v programski opremi ter upravljanje identifikacijskih BS. Sistemski administrator strežnika za upravljanje identifikacijskih kartic BS lahko opravlja tudi druge naloge. Sistemski administrator strežnika za upravljanje identifikacijskih kartic BS nima dostopa do strojnega varnostnega modula, razen, če nima dostopa v kombinaciji z drugimi vlogami, ki jih opravlja.

Skrbnika aktivacijskih podatkov (angl. Crypto Custodian) sta dva. Prvi skrbnik ima dostop do kuvert, v katerih so shranjene avtentikacijske pametne kartice za strojni varnostni modul. Drugi skrbnik ima dostop do kuvert v katerih so shranjene PIN kode avtentikacijskih pametnih kartic za strojni varnostni modul. Vsak skrbnik ima imenovanega enega ali več namestnikov. Skrbnik kuvert s pametnimi karticami ne more biti tudi skrbnik kuvert s PIN kodami pametnih kartic. Skrbnika aktivacijskih podatkov in njuni namestniki ne morejo opravljati drugih nalog in nimajo dostopa do strojnega varnostnega modula.

CA Template Admin - **Upravitelj predlog za digitalna potrdila** (angl. CA template admin) ima v aktivnem imeniku dostop do predlog digitalnih potrdil, ki jih izdaja overitelj. Funkcija

upravitelja predlog je dostopna preko posebnega uporabniškega imena, ki se prijavlja z digitalnim potrdilom, shranjenim na pametni kartici. Dostop do pametne kartice ima varnostni inženir, PIN koda za dostop do zasebnega ključa na pametni kartici pa je poznana sistemskim administratorjem. Upravitelj predlog za digitalna potrdila lahko opravlja tudi druge naloge. Upravitelj predlog za digitalna potrdila nima dostopa do strojnega varnostnega modula, razen, če nima dostopa v kombinaciji z drugimi vlogami, ki jih opravlja.

Certificate Issuer - Potrjevalec zahtevkov za digitalna potrdila za programsko opremo ima pooblastila, da na izdajateljskem strežniku Banka Slovenije Ent Sub CA G2 potrjuje digitalna potrdila za programsko opremo overitelja, ki zahtevajo ročno potrditev. Potrjevalec zahtevkov za digitalna potrdila za programsko opremo lahko opravlja tudi druge naloge. Potrjevalec zahtevkov za digitalna potrdila za programsko opremo nima dostopa do strojnega varnostnega modula, razen, če nima dostopa v kombinaciji z drugimi vlogami, ki jih opravlja.

SECO - Varnostni inženir je pooblaščen za spremljanje ustreznosti predlog za izdajanje digitalnih potrdil, ustreznosti konfiguracije programske opreme izdajatelja, ustreznosti konfiguracije programske opreme za upravljanje identifikacijskih kartic BS in za spremljanje revizijskih sledi. Varnostni inženir lahko opravlja tudi druge naloge. Varnostni inženir nima dostopa do strojnega varnostnega modula, razen, če nima dostopa v kombinaciji z drugimi vlogami, ki jih opravlja.

CMS Key Recovery Officer - **Skrbnik kopije zasebnih ključev** ima v aplikaciji za upravljanje identifikacijskih kartic BS pooblastila za potrjevanje zahtevkov za odkrivanje zasebnega ključa imetnika za šifriranje na identifikacijsko kartico BS, ki ga pripravi osebje prijavne pisarne na Helpdesk. Skrbnik kopije zasebnih ključev v okviru svojih zadolžitev preveri ustreznost avtorizacije za odkrivanje zasebnega ključa imetnika za šifriranje. Skrbnik kopije zasebnih ključev lahko opravlja tudi druge naloge. Skrbnik kopije zasebnih ključev nima dostopa do strojnega varnostnega modula, razen, če nima dostopa v kombinaciji z drugimi vlogami, ki jih opravlja.

CMS Admin - Upravitelj aplikacije za upravljanje identifikacijskih kartic BS ima v aplikaciji pooblastila za upravljanje vseh nastavitev, vključno z upravljanjem dostopnih pravic in delovnih tokov, ter povrnitev konfiguracije z varnostnih kopij. Funkcija upravitelja predlog je dostopna preko posebnega uporabniškega imena, ki se prijavlja z digitalnim potrdilom shranjenim na pametni kartici. Dostop do pametne kartice ima varnostni inženir, PIN koda za dostop do zasebnega ključa na pametni kartici pa je poznana sistemskim administratorjem. Upravitelj aplikacije za upravljanje identifikacijskih kartic BS lahko opravlja tudi druge naloge. Upravitelj aplikacije za upravljanje identifikacijskih kartic BS nima dostopa do strojnega varnostnega modula, razen, če nima dostopa v kombinaciji z drugimi vlogami, ki jih opravlja.

CMS Operator - Osebje prijavne pisarne na Helpdesk ima v aplikaciji za upravljanje identifikacijskih kartic BS pooblastila za upravljanje življenjskega cikla identifikacijskih kartic in digitalnih potrdil imetnikov. Osebje prijavne pisarne v okviru svojih zadolžitev potrjuje ustreznost zahtevkov, preverja istovetnost prosilcev in uporablja sistem za upravljanje identifikacijskih kartic BS. Osebje prijavne pisarne na Helpdesk lahko opravlja tudi druge naloge. Osebje prijavne pisarne na Helpdesk nima dostopa do strojnega varnostnega modula, razen, če nima dostopa v kombinaciji z drugimi vlogami, ki jih opravlja.

Aktivnosti, ki jih zgoraj navedene vloge izvedejo v okviru namestitve in inicializacije strojnega varnostnega modula, so opisane v dokumentu " BSI - Produkcijsko okolje - HSM ceremonija " in "".

System Auditor - Revizor je pooblaščen za pregledovanje ustreznosti izvedbe sprememb konfiguracij in vsebine sistemskih sporočil.

5.2.2 Število oseb potrebnih za izvedbo nalog

Za izvajanje nalog administratorja strojnega varnostnega modula je overitelj določil štiri osebe, vsakokrat pa sta hkrati potrebni najmanj dve osebi.

Za izvajanje nalog uporabnika particije strojnega varnostnega modula za izdajatelja Banka Slovenije Root CA G2 je overitelj določil tri osebe, vsakokrat pa sta hkrati potrebni najmanj dve osebi.

Za izvajanje nalog uporabnika particije strojnega varnostnega modula za izdajatelja Banka Slovenije Ent Sub CA G2 je overitelj določil tri osebe, vsakokrat pa sta hkrati potrebni najmanj dve osebi.
Za izvajanje nalog skrbnika kopije zasebnega ključa je overitelj določil dve osebi, vsakokrat pa sta hkrati potrebni en skrbnik in en zaposleni prijavne službe.

Za izvajanje nalog upravitelja predlog za izdajanje digitalnih potrdil je overitelj določil dve osebi, vsakokrat sta hkrati potrebna upravitelj predloge in sistemski administrator.

Za izvajanje nalog upravitelja aplikacije za upravljanje identifikacijskih kartic je overitelj določil dve osebi, vsakokrat sta hkrati potrebna upravitelj aplikacije in sistemski administrator.

Za vse ostale naloge je overitelj določil najmanj dve osebi, za izvedbo nalog pa je vsakokrat dovolj le ena oseba.

5.2.3 Preverjanje istovetnosti osebja overitelja

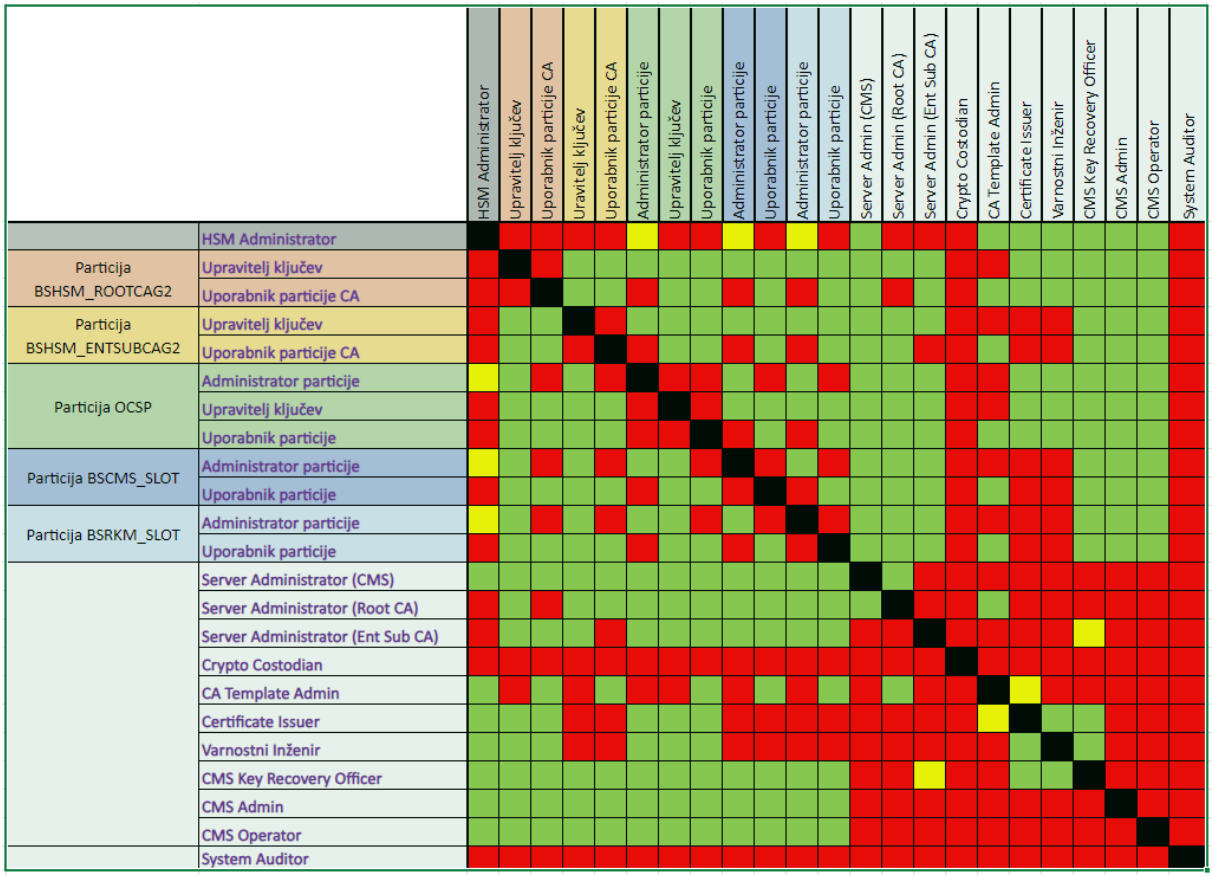
Upravitelji strojnega varnostnega modula izkazujejo identiteto z uporabo posebnih pametnih kartic za upravljanje oziroma uporabo strojnega šifrirnega modula. Kartice se generirajo v okviru vzpostavitve in prve konfiguracije strojnega šifrirnega modula oziroma ob vzpostavitvi programske opreme in tvorjenja ključa izdajatelja.

Ostalo osebje overitelja identiteto izkazujejo z identifikacijskimi karticami BS, na kateri imajo shranjene zasebne ključe in digitalna potrdila za prijavo v sisteme in programsko opremo overitelja.

5.2.4 Nezdružljive naloge

Nezdružljive naloge so podane v spodnji tabeli. Rdeče obarvane naloge so popolnoma nezdružljive in jih iste osebe ne smejo opravljati. Rumeno obarvano naloge so načeloma obravnavane kot nezdružljive. V primeru, da jih opravljajo iste osebe, je treba vzpostaviti dodatne varnostne mehanizme, ki zagotavljajo preverjanje ustreznosti avtorizacije za izvedbo aktivnosti in ustreznost sledljivosti izvedenih aktivnosti. Naloge, ki so obarvane z zeleno, lahko opravljajo iste osebe.

BANKA SLOVENIJE
EVROSISTEM



HSM Administrator[2] – Administrativni skrbnik strojnega varnostnega modula
Upravitelj ključev[2] - Upravitelj varnostnih kopij ključev particije
Uporabnik particije CA[3] - Uporabnik ključev na particiji strojnega varnostnega modula
Administrator particije[2] – Skrbnik particije strojnega varnostnega modula
Uporabnik particije[3] - Uporabnik ključev na particiji strojnega varnostnega modula
Server Administrator[2] - Sistemski administrator izdajateljskega strežnika
Crypto Custodian - Skrbnik aktivacijskih podatkov
CA Template Admin[2] - Upravitelj predlog za digitalna potrdila
Certificate Issuer - Potrjevalec zahtevkov za digitalna potrdila za programsko opremo
SECO[1] - Varnostni inženir
CMS Key Recovery Officer[3] – Skrbnik kopije zasebnih ključev
CMS Admin[2] - Upravitelj aplikacije za upravljanje identifikacijskih kartic BS
CMS Operator[3] - Osebje prijavne pisarne
System Auditor[4] - Revizor

Povezava 4 zahtevanih trusted vlog definiranih v **ETSI EN 319 401** tč. **REQ-7.2-14X** z vlogami navedenimi v tem dokumentu:

1. Varnostni inženirji
2. Sistemski administratorji
3. Sistemski operaterji
4. Revizorji

Particija BSCMS_SLOT se uporablja za hranjenje SSL sistemskih avtentikacijskih certifikatov, ki se uporabljajo komunikacijo komponent BlueX (BlueX applications server, BlueX Crypt service, BlueX transfer service) in hranjenje šifrirnega ključa BlueX podatkovne baze.

Particija BSRKM_SLOT se uporablja za hranjenje SSL sistemskega avtentikacijsega certifikata komponente BlueX Remote Key Manager in za hranjenje uporabniških šifrirnih ključev.

5.3 Nadzor nad osebjem

5.3.1 Kvalifikacije, izkušnje in varnostno preverjanje

Overitelj v skladu s politiko zaposlovanja BS zaposluje osebje z ustreznimi kvalifikacijami in delovnimi izkušnjami.

5.3.2 Preverjanje primernosti osebja

Pred sklenitvijo delovnega razmerja oddelek OK kandidate preveri v skladu z zakonodajo.

5.3.3 Izobraževanje in usposabljanje osebja

Osebje overitelja se redno izobražuje in usposablja na področjih varovanja informacij in komunikacijskih sistemov, uporabe in novosti programske opreme overitelja ter internih postopkov za naloge, ki jih posameznik izvaja.

5.3.4 Pogostost dodatnega izobraževanja in usposabljanja osebja

Po potrebi, glede na spremembe infrastrukture in zadolžitev osebja.

5.3.5 Kroženje med delovnimi mesti

Ni predpisano.

5.3.6 Sankcije za nedovoljene postopke

V primeru kršitev BS postopa v skladu z zakonodajo.

5.3.7 Zahteve za osebje zunanjih izvajalcev

Overitelj za izvajanje svojih nalog ne najema zunanjih izvajalcev. Izjema so posegi na strojni opremi v primeru napak v delovanju. Veljajo splošne zahteve BS za dostop do informacijskega sistema BS za pogodbene zunanje izvajalce.

5.3.8 Dostop osebja do dokumentacije

Osebje ima dostop do vseh politik in splošnih pravil overitelja.

5.4 Beleženje in upravljanje revizijskih sledi

5.4.1 Vrste beleženih dogodkov

Proces beleženja dogodkov se prične ob zagonu strežnika in konča ob ugašanju.

Beležijo se naslednje vrste dogodkov:

- dogodki v zvezi z upravljanjem, arhiviranjem (angl. backup), varnostno politiko in uporabo aplikacij overitelja;

- dogodki v zvezi z imetnikovimi ključi in s potrdili - izdaja, prevzem, preklic, zadržanje;
- dogodki v zvezi s ključi overitelja;
- dogodki v zvezi s pripravo pametnih kartic za kreiranje in hrambo para ključev in digitalnega potrdila imetnika
- dogodki na operacijskih sistemih in strojni opremi;
- dogodki v zvezi z varnostno politiko, upravljanjem in s strojno opremo na mreži;
- dogodki v zvezi s fizičnim dostopom do sistemov overitelja;
- dogodki v zvezi s kadrovskimi spremembami overitelja.

5.4.2 Pogostnost pregledovanja revizijskih dnevnikov

Dogodki se posredujejo v centralni sistem za beleženje in analiziranje dogodkov, kjer so za določene dogodke nastavljeni varnostni alarmi, ki zahtevajo takojšnje posredovanje.

Ročno se podatki analizirajo po potrebi.

5.4.3 Obdobje hrambe revizijskih dnevnikov

Informacija o obdobju hrambe revizijskih dnevnikov na strežnikih overitelja in v centralnem sistemu za analiziranje in beleženje dogodkov je zaupne narave in je dostopna le pooblaščenemu osebju overitelja. Čas hrambe revizijskih sledi v arhivu je opredeljen s politiko overitelja.

5.4.4 Zaščita revizijskih dnevnikov

Na sistemih overitelja so revizijski dnevniki varovani s sistemom dostopnih pravic. Dostop do sistemskih dnevnikov je omogočen le pooblaščenemu osebju na podlagi nujno potrebnih dostopnih pravic za izvajanje nalog.

Na centralnem sistemu za beleženje in analiziranje dogodkov sistemski skrbniki strežnikov overitelja nimajo možnosti spreminjanja ali brisanja revizijskih sledi. Sledi o aktivnostih varnostnih inženirjev overitelja, ki so skrbniki centralnega sistema za beleženje dogodkov, se zapisujejo v poseben strežnik, ki je dostopen le preko sistema za upravljanje skrbniških dostopov[2], kar zagotavlja sledljivost morebitnega nepooblaščenega spreminjanja revizijskih sledi strežnikov overitelja.

5.4.5 Varnostne kopije revizijskih dnevnikov

Varnostne kopije sistemskih dnevnikov se izdelujejo hkrati z varnostnimi kopijami sistemov in podatkov po dinamiki, ki velja za ostale kritične sisteme BS.

5.4.6 Sistem zbiranja revizijskih podatkov

Revizijski podatki se zbirajo avtomatsko in ročno.

Dogodki v zvezi z delovanjem sistemov overitelja ter uporabe programske opreme izdajatelja in programske opreme za upravljanje identifikacijskih kartic se zbirajo avtomatsko.

[2] PAM – Privileged Access Management

5.4.7 Obveščanje povzročitelja dogodka

Ni predpisano.

5.4.8 Ocena ranljivosti

Ocena ranljivosti se izvaja v sklopu upravljanja ranljivosti in nameščanja varnostnih popravkov. Izvaja se skladno s politiko BS, ki opredeljuje upravljanje ranljivosti in nameščanje varnostnih popravkov.

5.5 Arhiviranje podatkov

5.5.1 Vrste arhiviranih podatkov

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

5.5.2 Čas hrambe

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

5.5.3 Zaščita arhiva

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

5.5.4 Zahteve za časovno žigosanje zapisov

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

5.5.5 Način arhiviranja

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

5.5.6 Dostop do arhivskih podatkov

Dostop je pooblaščenemu osebju dodeljen po načelu minimalno potrebnih dostopnih pravic za izvajanje nalog, opredeljenih v poglavju 5.2.1.

5.6 Podaljšanje veljavnosti potrdil overitelja

Overitelj izvede enake postopke kot pri prvem tvorjenju zasebnega ključa izdajatelja. Postopek je opisan v poglavju 6.1.1.1.

Novo izdana digitalna potrdila izdajatelja se objavijo na spletni strani overitelja.

Overitelj o menjavi digitalnega potrdila na svojih spletnih straneh obvesti vse subjekte.

5.7 Postopki v primeru ogrožanja zasebnega ključa overitelja in okrevalni načrti

5.7.1 Postopki odzivanja na varnostne incidente in zlorabe

V primeru varnostnih incidentov overitelj postopa po standardnih postopkih BS, opisanih v dokumentu "Navodilo za upravljanje z varnostnimi incidenti v BS".

5.7.2 Okrevalni načrti v primeru okvar ali uničenja strojne opreme, programske opreme in podatkov

Vsa oprema overitelja je podvojena in v primeru okvare ali uničenja omogoča nadaljevanje izvajanja operacij na nadomestni opremi.

V primeru uničenja programske opreme bo overitelj ustavil svoje sisteme vse dokler ne bo vzpostavil normalnega delovanja. Istočasno bo sprožil postopek odkrivanja vzroka napake, da se slednja ne bi ponovila.

V primeru uničenja podatkov bo overitelj ustavil delovaje sistemov dokler ne vzpostavi konsistentnega stanja podatkovnih baz. V kolikor bo potrebno si bo pomagal s povrnitvijo podatkov z zadnje varnostne kopije.

5.7.3 Okrevalni načrti v primeru ogrožanja zasebnega ključa overitelja

V primeru ogrožanja zasebnega ključa overitelja bo overitelj preklical vsa digitalna potrdila podpisana z ogroženim zasebnim ključem, generiral in objavil novo listo preklicanih potrdil, zaustavil svoje sisteme in preko svoje spletne strani o tem obvestil vse imetnike in tretje osebe.

Overitelj bo ponovno vzpostavil delovanje v čim krajšem možnem času. Pri tem bo ponovil postopek tvorjenja lastnih ključev, opisan v poglavju 6.1.1.1.

5.7.4 Neprekinjenost poslovanja v primeru naravnih nesreč

Overitelj ima podvojene produkcijske sisteme na dislocirani lokaciji v prostorih rezervnega računalniškega centra BS. V primeru naravnih nesreč, ki z uničenjem ne prizadenejo obeh lokacij, bo overitelj v skladu z načrti neprekinjenega poslovanja BS v zahtevanih časovnih rokih vzpostavil delujoče stanje sistemov.

5.8 Prenehanje delovanja overitelja na BS

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

6 Tehnične varnostne zahteve

6.1 Tvorjenje in namestitev para ključev

6.1.1 Tvorjenje para ključev

6.1.1.1 Pari ključev overitelja

Ključi se tvorijo kot je opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

Ključi se hranijo na treh strojnih varnostnih modulih. Administrator HSM z ročnimi postopki zagotavlja konsistentnost konfiguracije in digitalnih potrdil vseh treh strojnih varnostnih modulov. Strežniki overitelja imajo v konfiguraciji navedene vse tri strojne varnostne module. V primeru izpada enega strojnega varnostnega modula izdajateljski strežniki avtomatsko uporabijo naslednji strojni varnostni modul naveden v konfiguraciji.

6.1.1.2 Pari ključev imetnikov

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

6.1.2 Prenos zasebnega ključa do imetnika

V primeru izdelave nove identifikacijske kartice izroči prijavna pisarna imetniku kartico in aktivacijske podatke za dostop do zasebnih ključev na kartici, naslednji delovni dan po tvorjenju, ob prihodu imetnika v zgradbo BS.

V primeru uporabe obstoječe identifikacijske kartice jo imetnik prevzame v prijavni pisarni takoj po tvorjenju ključev in digitalnih potrdil.

6.1.3 Prenos javnega ključa imetnika k overitelju

Javni ključi se med identifikacijsko kartico, programsko opremo za upravljanje identifikacijskih kartic in programsko opremo izdajatelja prenašajo v obliki PKCS#10 zahtevkov.

6.1.4 Dostop do overiteljeva javnega ključa

Overiteljev javni ključ se k imetnikom in tretjim osebam prenaša v obliki X.509 v3 digitalnega potrdila overitelja.

6.1.5 Dolžina asimetričnih ključev

Izdajatelj Banka Slovenije Root CA G2 in izdajatelj Banka Slovenije Ent Sub CA G2 za podpisovanje uporabljata zasebni ključ RSA dolžine 4096 bitov.

Dolžine zasebnih ključev imetnikov so opredeljene s politiko, pod katero so bila digitalna potrdila izdana.

6.1.6 Parametri za generiranje javnih ključev in preverjanje parametrov

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

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

Namen uporabe digitalnih potrdil je opredeljen s politiko overitelja pod katero so bila digitalna potrdila izdana.

Vsa digitalna potrdila vključujejo X.509 v3 polje "key usage".

Dodane omejitve so lahko podane preko polja "Extended key usage".

6.2 Zaščita zasebnega ključa in kriptografskih modulov

6.2.1 Standardi strojnih varnostnih modulov

Overitelj uporablja strojne varnostne module, ki so certificirani za ustreznost po varnostnemu nivoju CC EAL 4+ in module, ki so certificirani po varnostnem nivoju FIPS 140-2 Level 3.

V sistemu sta uporabljena dva tipa strojnih varnostnih modulov, ki se razlikujeta po certifikaciji varnostnega nivoja. Za ključe overitelja, torej “Banka Slovenije Root CA G2” in “Banka Slovenije Ent Sub CA G2”, se uporabljajo strojni varnostni moduli certificirani po varnostnem nivoju CC EAL 4+. Za hranjenje uporabniških šifrirnih ključev, ključa za šifriranje podatkovne baze sistema za upravljanje s pametnimi karticami in infrastrukturnih ključev (SSL) pa se uporabljajo strojni varnostni moduli skladni z varnostnim nivojem FIPS 140-2 level 3.

Osebje overitelja za upravljanje strojnega varnostnega modula uporablja pametne kartice, ki imajo vgrajen strojni varnostni modul, certificiran za skladnost po varnostnem nivoju Common Criteria EAL5+

Osebje overitelja uporablja identifikacijske kartice BS, ki imajo vgrajen strojni varnostni modul, ki je certificiran za skladnost s specifikacijami CC EAL4+ ali višje.

Imetniki potrdil uporabljajo šifrirne module kot so predpisani z varnostno politiko, pod katero so digitalna potrdila izdana.

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

Overitelj ima za administracijo strojnega varnostnega modula, na katerem so shranjeni zasebni ključi overitelja s katerimi podpisuje digitalna potrdila, izdan set štirih kartic z zasebnimi ključi za administratorje. Za izvajanje funkcij administracije strojnega varnostnega modula se morata vedno s pametno kartico zaporedno prijaviti vsaj dva od imenovanih administratorjev.

Overitelj ima za dostop do zasebnega ključa izdajatelja Banka Slovenije Root CA G2 izdan set treh kartic z zasebnimi ključi za uporabnike particije CA na strojnih varnostnih modulih. Za izvajanje funkcij, ki zahtevajo dostop do zasebnega ključa izdajatelja se morata vedno zaporedno prijaviti vsaj dva od imenovanih uporabnikov particije CA.

Overitelj ima za dostop do zasebnega ključa izdajatelja Banka Slovenije Ent Sub CA G2 izdan set treh kartic z zasebnimi ključi za uporabnike particije CA. Za izvajanje funkcij, ki zahtevajo dostop do zasebnega ključa izdajatelja se mora s pametno kartico prijaviti vsaj eden od imenovanih uporabnikov particij CA.

6.2.3 Odkrivanje (angl. Escrow) zasebnega ključa

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

6.2.4 Varnostna kopija zasebnega ključa

Varnostne kopije zasebnega ključa overitelja

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

Povrnitev zasebnega ključa overitelja z varnostne kopije je naloga funkcije administratorja strojnega varnostnega modula. Postopek dostopa do funkcije administratorja je opisan v poglavju 6.2.2.

Varnostne kopije zasebnih ključev imetnikov

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

6.2.5 Arhiviranje zasebnega ključa

Arhivske kopije zasebnih ključev digitalnih potrdil za šifriranje se varno hranijo v strojnih varnostnih modulih, ki so skladni s FIPS 140-2 level 3. Varnostne kopije arhivske baze se izdelujejo skupaj z varnostnimi kopijami ostalih podatkov overitelja, kar je natančneje opisano v poglavjih 5.1.6 in 5.1.8.

Postopki za povrnitev so opredeljeni s politiko overitelja, pod katero so bila digitalna potrdila izdana.

6.2.6 Zapis zasebnega ključa v strojni varnostni modul

Izdajateljevi zasebni ključi se lahko uporabljajo le na aktiviranih strojnih varnostnih modulih. Aktiviranje strojnih varnostnih modulov na katerih je dovoljeno uporabljati izdajateljeve zasebne ključe izvedejo osebe z nalogo administratorja strojnega varnostnega modula. Postopek prijave je opisan v prvem odstavku poglavja 6.2.2.

Zasebni ključi se aktivirajo v strojnem varnostnem modulu ob startu aplikacije overitelja. Odobritev prenosa ključev v strojni varnostni modul in aktiviranje izvedejo osebe z nalogo Uporabnik particije strojnega varnostnega modula. Postopek prijave je opisan v drugem odstavku poglavja 6.2.2.

Zasebni ključi imetnika za prijavo in elektronski podpis se kreirajo na strojnem varnostnem modulu identifikacijske kartice BS zato dodaten zapis na modul ni potreben.

Zapis zasebnega ključa imetnika za šifriranje in dešifriranje na strojni varnostni modul identifikacijske kartice BS se izvede po naslednjem postopku:

- prijavna služba overitelja prejme zahtevek za izdelavo identifikacijske kartice imetnika;
- osebje prijavne službe po uspešnem preverjanju istovetnosti imetnika (preveri ime, priimek, matično številko in sliko), preko programske opreme za upravljanje identifikacijskih kartic v BS izvede izdelavo para ključev imetnika za šifriranje in dešifriranje, ki poteka po naslednjem vrstnem redu:
    - program za upravljanje identifikacijskih kartic na kartici pripravi par RSA ključev za uvoz in javni ključ pošlje modulu za upravljanje digitalnih potrdil;
    - modul za upravljanje digitalnih potrdil na strojnem varnostnem modulu generira par ključev imetnika za šifriranje in dešifriranje;
    - modul za upravljanje digitalnih potrdil generira AES simetrični ključ za varen prenos podatkov, z njim šifrira zasebni ključ imetnika, simetrični šifrirni ključ pa šifrira z javnim ključem RSA za uvoz na identifikacijsko kartico. Modul šifriran zasebni ključ imetnika in šifriran simetrični ključ posreduje programu za upravljanje identifikacijskih kartic.
    - program za upravljanje identifikacijskih kartic shrani simetrični ključ in zasebni ključ uporabnika na identifikacijsko kartico imetnika in s kartice izbriše par RSA ključev za uvoz.

6.2.7 Hramba zasebnega ključa v strojnem varnostnem modulu

Specifikacije so podane v poglavju 6.2.1.

6.2.8 Postopek za aktiviranje zasebnega ključa

Aktiviranje zasebnih ključev izdajatelja je naloga funkcije uporabnika particije CA strojnega varnostnega modula. Postopek prijave je opisan v poglavju 6.2.2.

Postopek aktiviranja zasebnega ključa imetnika je opredeljen s politiko, pod katero so digitalna potrdila izdana.

6.2.9 Postopek za deaktiviranje zasebnega ključa

Zaustavitev programske opreme izdajatelja, s katero se deaktivira zasebni ključ izdajatelja za podpisovanje, je naloga funkcije sistemskega administratorja programske opreme izdajatelja.

Deaktiviranje zasebnega ključa imetnika je opredeljeno s politiko, pod katero je bilo digitalno potrdilo izdano.

6.2.10 Postopek za uničenje zasebnega ključa

Ob zaustavitvi CA storitve se uničijo vse kopije zasebnega ključa izdajatelja, ki se nahajajo v pomnilniku operacijskega sistema.

Ob prenehanju veljavnosti zasebnega ključa izdajatelja ali njegovem preklicu se zasebni ključ sistematično uniči tako, da ga ni več možno povrniti.

Uničenje zasebnih ključev imetnikov je opredeljeno s politiko, pod katero je bilo digitalno potrdilo izdano.

6.2.11 Stopnja varnosti strojnih varnostnih modulov

Opredeljeno v poglavju 6.2.1.

6.3 Ostali vidiki upravljanja ključev

6.3.1 Arhiviranje javnega ključa

Opredeljeno s politiko, pod katero je bilo digitalno potrdilo izdano.

6.3.2 Obdobje veljavnosti ključev in digitalnih potrdil

Opredeljeno s politiko, pod katero je bilo digitalno potrdilo izdano.

6.4 Aktivacijski podatki

6.4.1 Tvorjenje in instalacija aktivacijskih podatkov

Aktivacijski podatki za uporabo strojnega varnostnega modula se tvorijo ob inicializaciji modula kot je opisano v dokumentih “Banka Slovenije Produkcijsko okolje HSM Ceremonija” , “ROOT CA G2 Certificate Auhority Key Generation Ceremony Script in Banka Slovenije” in »ENT SUB CA G2 Certificate Auhority Key Generation Ceremony Script in Banka Slovenije«. Imenovani HSM administratorji, uporabniki particije CA, in upravitelji ključev v postopku inicializacije nastavijo PIN kodo pametne kartice za strojni varnostni modul.

Aktivacijske podatke šifrirnega modula identifikacijske kartice BS avtomatsko generira CMS programska oprema overitelja za upravljanje identifikacijskih kartic BS.

6.4.2 Zaščita aktivacijskih podatkov

HSM Administratorji, uporabniki particije CA in upravitelji ključev varnostnega modula so vedno v parih. Eden je skrbnik pametne kartice, drugi je skrbnik PIN kode. Skrbniki zapišejo PIN kode pametnih kartic strojnega varnostnega modula in jih shranijo v ovojnico, skozi katero se

podatki ne morejo prebrati. Pametne kartice in ovojnice se ločeno shranijo v ognjevarne omare tako, da nikdar ena oseba nima hkratnega dostopa do dveh pametnih kartic in PIN kod za kartice iz istega seta.

Osebje prijavne službe natisne aktivacijske podatke imetniških digitalnih potrdil, jih shrani v ovojnico skozi katero se podatki ne morejo prebrati in jo hrani do predaje imetniku digitalnega potrdila.

Geslo administratorja particije je sestavljeno iz dveh delov. Skrbnika gesla administratorja particije vsak svoj del gesla zapišeta in shranita v ovojnico, skozi katero se podatki ne morejo prebrati. Ovojnici se ločeno shranita v ognjevarne omare tako, da nikdar ena oseba nima hkratnega dostopa do obeh delov gesla.

6.4.3 Drugi vidiki aktivacijskih podatkov

Opredeljeno s politiko, pod katero je bilo digitalno potrdilo izdano.

6.5 Varnostne zahteve za računalniško opremo izdajatelja

6.5.1 Specifične tehnične varnostne zahteve za računalnike

Informacije, ki naj bi jih naslavljali v tem poglavju so klasificirane s stopnjo zaupnosti "*zaupno".* Opredeljene so v drugih notranjih aktih overitelja in so pooblaščenemu osebju overitelja dostopne na podlagi načela nujno potrebnih informacij za opravljanje nalog.

Specifične tehnične varnostne zahteve so opredeljene v tehničnih standardih varovanja opreme overitelja.

6.5.2 Stopnja varnostne zaščite računalnikov

Informacije, ki naj bi jih naslavljali v tem poglavju so klasificirane s stopnjo zaupnosti "*zaupno".* Opredeljene so v drugih notranjih aktih overitelja in so pooblaščenemu osebju overitelja dostopne na podlagi načela nujno potrebnih informacij za opravljanje nalog.

Strežniški sistemi overitelja so dodatno utrjeni po priporočilih proizvajalcev in dobre prakse.

Oprema ustreza zahtevam varnostnih politik in tehničnih standardov varovanja, ki veljajo za računalniško opremo BS za obdelavo podatkov primerljive stopnje zaupnosti.

6.6 Varnostne kontrole življenjskega cikla overitelja

6.6.1 Nadzor razvoja sistema

Opredeljeno s politiko overitelja, pod katero je bilo digitalno potrdilo izdano.

6.6.2 Upravljanje varnosti

Informacije, ki naj bi jih naslavljali v tem poglavju so klasificirane s stopnjo zaupnosti "*zaupno".* Opredeljene so v drugih notranjih aktih overitelja in so pooblaščenemu osebju overitelja dostopne na podlagi načela nujno potrebnih informacij za opravljanje nalog.

Overitelj ima vzpostavljene postopke za reden nadzor celovitosti programske opreme.

Vpeljane varnostne kontrole so natančneje opredeljene v tehničnih standardih opreme overitelja.

6.7 Varnostne zahteve za računalniško omrežje

Informacije, ki naj bi jih naslavljali v tem poglavju so klasificirane s stopnjo zaupnosti "*zaupno".* Opredeljene so v drugih notranjih aktih overitelja in so pooblaščenemu osebju overitelja dostopne na podlagi načela nujno potrebnih informacij za opravljanje nalog.

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 tehničnih standardih opreme overitelja.

6.8 Časovno žigosanje

Opredeljeno s politiko, pod katero je bilo digitalno potrdilo izdano.

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

7.1 Profil potrdil

Profili potrdil imetnikov so opredeljeni s politiko overitelja pod katero so bila potrdila izdana.

Za potrebe delovanja svoje programske opreme je overitelj v okviru instalacijskega postopka po različnih predlogah izdal pet digitalnih potrdil. Eno od potrdil se avtomatsko obnavlja, za ostala je v okviru izdaje zagotovljeno dvostopenjsko potrjevanje. Zahtevek za izdajo potrdila pripravi sistemski administrator opreme, potrdi pa ga potrjevalec zahtevkov za digitalna potrdila za programsko opremo.

Izdane so bile naslednje vrste potrdil:

Namen	Zasebni ključ v strojnem varnostnem modulu	Veljavnost	CA Predloga	Avtomatska obnova	OID
OCSP Response Signing	Ne	12 dni	OCSP ResponseSigning	Da	1.3.6.1.4.1.27213.2.1.1.10.1.2
Remote MWCA Certificate	Da	5 let	CMS Environment User G2	Ne	1.3.6.1.4.1.27213.2.1.1.8.1.2

Remote Key Manager Certificate	Da	5 let	CMS Environment User G2	Ne	1.3.6.1.4.1.27213.2.1.1.8.1.2
Enrollment Agent Certificate	Da	5 let	BS Enrollment Agent G2	Ne	1.3.6.1.4.1.27213.2.1.1.9.1.2
CMS User	Ne	5 let	BS CMS User	Ne	1.3.6.1.4.1.27213.2.1.1.1.3.2

7.1.1 Različica potrdil
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.1.2 Razširitvena polja
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.1.2.1 Standardna razširitvena polja
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.1.3 Identifikacijske oznake (angl. object identifiers) podprtih algoritmov
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.1.4 Oblike imen
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.1.5 Omejitve imen
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.1.6 Identifikacijska oznaka politike potrdila
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.1.7 Uporaba razširitvenega polja "Policy Constraints"
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.1.8 Sintaksa in semantika polja "Policy qualifiers"
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.1.9 Procesiranje oznake kritičnosti razširitvenih polj potrdila
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.2 Profil registra preklicanih potrdil
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.2.1 Različica
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.2.2 Vsebina registra in razširitve

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

7.3 Sprotno preverjanje statusa potrdil

Opredeljeno s politiko overitelja, pod katero je bilo digitalno potrdilo izdano.

8 Revidiranje usklajenosti in ostali pregledi

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

8.1 Pogostnost izvajanja preverjanj skladnosti

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

8.2 Identiteta in usposobljenost izvajalcev preverjanj

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

8.3 Odnos med revizorjem in overiteljem

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

8.4 Obseg preverjanj

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

8.5 Korektivni ukrepi kot posledica ugotovljenih nepravilnosti

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

8.6 Poročanje o preverjanjih

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9 Ostale finančne in pravne zadeve

9.1 Cenik

Opredeljeno s politiko overitelja, pod katero je bilo digitalno potrdilo izdano.

9.2 Finančna odgovornost

9.2.1 Zavarovanje odgovornosti

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.2.2 Druge oblike zavarovanja

Opredeljeno s politiko overitelja, pod katero je bilo digitalno potrdilo izdano.

9.2.3 Zavarovanje imetnikov

Opredeljeno s politiko overitelja, pod katero je bilo digitalno potrdilo izdano.

9.3 Zaupnost poslovnih podatkov

9.3.1 Obseg zaupnih podatkov

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.3.2 Podatki izven obsega zaupnih podatkov

Opredeljeno s politiko overitelja , pod katero je bilo digitalno potrdilo izdano.

9.3.3 Odgovornost za varovanje zaupnih podatkov

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.4 Varovanje osebnih podatkov

9.4.1 Načrt varovanja osebnih podatkov

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.4.2 Varovani osebni podatki

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.4.3 Nevarovani osebni podatki

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.4.4 Odgovornost glede varovanja osebnih podatkov

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.4.5 Pooblastilo glede uporabe osebnih podatkov

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.4.6 Posredovanje osebnih podatkov

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.4.7 Druga določila glede varovanja osebnih podatkov

Ni predpisano.

9.5 Zaščita intelektualne lastnine

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.6 Obveznosti in odgovornosti

9.6.1 Odgovornosti overitelja

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.6.2 Odgovornosti prijavne službe

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.6.3 Odgovornosti imetnikov digitalnih potrdil

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.6.4 Odgovornosti tretjih oseb

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.7 Zanikanje odgovornosti overitelja

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.8 Omejitve odgovornosti overitelja

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.9 Povrnitev škode

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

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

Splošni postopki delovanja overitelja prenehajo veljati z uveljavitvijo nove verzije ali v primeru prenehanja delovanja overitelja.

9.10.3 Posledice prenehanja veljavnosti

Obveznosti in odgovornosti overitelja opredeljene s splošnimi postopki delovanja overitelja, ki se nanašajo na revizijske preglede in varovanje zaupnosti ostanejo v veljavi tudi po objavi nove verzije, razen če niso v nasprotju z določili nove verzije splošnih postopkov delovanja overitelja.

9.11 Komuniciranje med subjekti

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.12 Dopolnitve politike

9.12.1 Postopek uveljavitve dopolnitev

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.12.2 Postopek obveščanja o dopolnitvah in spremembah

Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

BANKA SLOVENIJE
EVROSISTEM

9.12.3 Spremembe, ki zahtevajo novo identifikacijsko oznako politike
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.13 Urejanje sporov
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.14 Veljavna zakonodaja
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.15 Skladnost z zakonodajo
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.16 Splošne določbe
9.16.1 Celovit dogovor
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.16.2 Prenos pravic in obveznosti
Opredeljeno s politiko, pod katero je bilo digitalno potrdilo izdano.

9.16.3 Neodvisnost določil
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.16.4 Terjatve
Opredeljeno s politiko, pod katero je bilo digitalno potrdilo izdano.

9.16.5 Višja sila
Opredeljeno v politiki overitelja, pod katero so bila digitalna potrdila izdana.

9.17 Ostale določbe

Splošni postopki delovanja overitelja pričnejo veljati od 18. 4. 2025 dalje.

V Ljubljani, 09. 04. 2025

Jože Kranjc
DIREKTOR ODDELKA
Informacijska tehnologija