Politika AC NLB

Javni del notranjih pravil
za kvalificirana digitalna potrdila za strežnike

/2. izdaja z dne 30.4.2004/

CP_{NAME}: AC NLB-5

CP_{OID}: 3.6.1.4.1.7597.1.4.5

ljubljanska banka

Nova Ljubljanska banka d.d., Ljubljana

KAZALO

KRONOLOGIJA SPREMEMB

Izdaja	Datum	Opis
1.	31.7.2003	Prva izdaja
2.	30.4.2004	Popravki skladni z zahtevami ZEPEP

1. UVOD

AC NLB je overitelj digitalnih potrdil pri Novi Ljubljanski banki d.d.. Ta politika, ki predstavlja nedeljivo celoto javnega dela notranjih pravil overitelja AC NLB glede izdaje digitalnih potrdil za zaposlene, ureja namen, delovanje in metodologijo upravljanja z digitalnimi potrdili ter varnostne zahteve, ki jih morajo izpolnjevati overitelj AC NLB ter imetniki digitalnih potrdil.

AC NLB je overitelj, ki izdaja in upravlja s kvalificiranimi poslovnimi potrdili za overjanje varnega elektronskega podpisa. Veljavna digitalna potrdila pri tem ostanejo v veljavi do konca preteka veljavnosti in po stari politiki delovanja. Pod novo identifikacijsko številko (CP_{OID}) in datumom veljavnosti AC NLB predhodno objavi novo politiko AC NLB.

AC NLB izdaja potrdila v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 57/2000 in 30/2001) in njegovimi podzakonskimi predpisi, katerih pravna pravila so v celoti harmonizirana z direktivo Evropskega parlamenta in Sveta Evropske unije z dne 13. decembra 1999 o skupnem okviru Skupnosti za elektronske podpise.

Kvalificirana digitalna potrdila, ki jih izdaja overitelj na NLB, so namenjena:

- za upravljanje s podatki NLB,
- za dostop in izmenjavo podatkov, s katerimi upravlja NLB,
- za varno elektronsko komuniciranje med imetniki kvalificiranih digitalnih potrdil overitelja AC NLB in
- za storitve oz. aplikacije, za katere se zahteva uporaba digitalnih potrdil overitelja AC NLB.

Vse določbe te politike glede ravnanja AC NLB so ustrezno prenesene in podrobneje opredeljene v določbah notranje politike (*OP75106*), ki predstavlja zaupni del notranjih pravil in jo sestavljajo dokumenti zaupne narave, ki definirajo infrastrukturo, določila glede osebja AC NLB (pristojnosti, naloge, pooblastila in zahtevani pogoji posameznih članov osebja), fizično varovanje (dostop do prostorov, ravnanje s strojno in programsko opremo), programsko varovanje (varnostne nastavitve strežnikov, varnostne kopije...) in notranji nadzor (kontrola fizičnih dostopov, pooblastil,...) ter so v skladu tehničnimi zahtevami ETSI TS 101 456 (Policy requirements for certification authorities issuing qualified certificates) in ETSI TS 101 862 (Qualified certificate profile).

Overitelj AC NLB se lahko povezuje z drugimi overitelji in se z njimi priznava.
AC NLB se povezuje in se priznava z overitelji potrdil vpisanih v Register overiteljev v Republiki Sloveniji. AC NLB v ta namen sklene pogodbo o medsebojnem priznavanju.

2. SPLOŠNE DOLOČBE

NAMEN IN UPORABA POTRDIL

AC NLB upravlja (izdaja in overja, preklicuje, podaljšuje, hrani in objavlja) s kvalificiranimi digitalnimi potrdili.

Potrdila so namenjena za uporabo v specifičnih aplikacijah in za namene, ki jih potrdi AC NLB, in sicer za:

- šifriranje podatkov in sporočil v elektronski obliki,
- digitalno podpisovanje podatkov in sporočil v elektronski obliki ter overjanje identitete podpisnika,
- varno brisanje podatkov v elektronski obliki.

AC NLB izdaja:

- spletna kvalificirana digitalna potrdila za fizične osebe,
- spletna kvalificirana digitalna potrdila za zaposlene pravnih oseb in zasebnikov,
- spletna kvalificirana digitalna potrdila za strežnike,
- druga potrdila za lastno uporabo.

Spletna kvalificirana digitalna potrdila se lahko uporabljajo za:

- varno spletno komuniciranje po protokolih SSL (angl.: Secure Sockets Layer) in TLS (angl.: Transport Layer Security),
- varno pošiljanje elektronske pošte po protokolu S/MIME (angl.: Secure Multipurpose Internet Mail Extensions),
- storitve oz. aplikacije, za katere se zahteva uporaba spletnih kvalificiranih digitalnih potrdil overitelja na NLB.

Glede preklica kvalificiranih digitalnih potrdil za strežnike ima nadrejeni enake pravice kot ostali imetniki kvalificiranih digitalnih potrdil za strežnike – IT skrbniki strežnikov.

3. INFRASTRUKTURA AC NLB

OSNOVNI PODATKI O AC NLB

Naslov AC NLB:

AC NLB
Nova Ljubljanska banka d.d.
Šmartinska cesta 132
SI - 1520 LJUBLJANA
Slovenija
Tel.: (+386) 01 477 20 60
Fax: (+386) 01 476 47 99
E-pošta: acnlb@nlb.si

Osnovne informacije o AC NLB so na voljo na spletnem strežniku NLB z naslovom: http://www.nlb.si/acnlb

Identiteta:

c=si,o=ACNLB
CP_{NAME} - AC NLB-5
CP_{OID} - 1.3.6.1.4.1.7597.1.4.5

Infrastrukturo AC NLB sestavljajo:

- notranji in zunanji prostori AC NLB,
- strojna in programska oprema, ki jo AC NLB uporablja za upravljanje s potrdili ali opravljanje drugih storitev v zvezi z elektronskim podpisovanjem,
- osebje AC NLB,
- metode in postopki pri upravljanju s potrdili in drugih storitev v zvezi z elektronskim

podpisovanjem.

LASTNO POTRDILO OVERITELJA

AC NLB je oblikovala svoje lastno potrdilo, ki je namenjeno podpisovanju veljavnosti potrdil za druge uporabnike ter preverjanju podpisa oz. veljavnosti.

Potrdilo AC NLB vsebuje naslednje podatke:

Serijska številka	3EC3 868E
Overitelj potrdila	AC NLB Šmartinska cesta 132 SI - 1520 LJUBLJANA Slovenija
Imetnik potrdila	AC NLB Šmartinska cesta 132 SI - 1520 Ljubljana Slovenija
Veljavnost potrdila	20 let
Dolžina ključa	2048 bitov
Prstni odtis (SHA1)	0456 F23D 1E9C 43AE CB0D 807F 1C06 4755 1A05 F456
Prstni odtis (MD5)	BA926442 161FCBA1 16481AF6 405C5987

ŠIFRIRNI ALGORITMI, FORMATI PODATKOV IN PROTOKOLI

AC NLB uporablja:

- za podpisovanje potrdil algoritem SHA-1 z RSA s parom ključev dolžine 2048 bitov,
- za šifriranje podatkov algoritme Triple DES, CAST-128 in RC2, (standardi FIPS PUB 186-2, ANSI X9.30 (1), IEEE P1363 in ISO/IEC 14888-3),
- zgostitvene algoritme SHA-1 (FIPS PUB 180-1 in ANSI X9.30(2)) in MD5 (RFC 1321),
- način uporabe algoritma RSA za upravljanje s ključi RSA (RFC 1421 in RFC 1423(PEM) in PKCS#1),
- format potrdil ustreza priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997 ter X.509 ver. 3 (v3),
- registri preklicanih potrdil ustrezajo priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997, vključno z verzijo 2 (v2),
- oblika RSA enoličnih razločevalnih imen ter format javnega ključa ustrezajo priporočilu RFC 1422 in 1423 (PEM) in PKCS#1,
- protokol LDAP ustreza priporočilu RFC 1777 in RFC 2559,
- hranjenje zasebnega ključa ustreza priporočiloma PKCS#5 in PKCS#8,
- komunikacija med programsko opremo na strani imetnika in infrastrukturo NLB CA poteka po protokolu SEP (angl.: Secure Exchange Protocol), ki temelji na standardu GULS (angl.: Generic Upper Layers Security), ki ustreza priporočilom ITU-T za X.830, X.831, X.832 in ISO/IEC 11586-1, 11586-2 in 11586-3 ali protokolu PKIX-CMP, ki temelji na priporočilu RFC 2510.

Celoten nabor algoritmov, formatov podatkov in protokolov je na razpolago pri AC NLB.

IMENIK

Vsa potrdila temeljijo na standardu X.509v3 in so shranjena na strežniku CSMAX500, ki ni javno dostopen.

Potrdila se nahajajo v podstrukturi:

ou=strezniki, o=NLB, o=ACNLB, c=SI

REGISTER PREKLICANIH POTRDIL

Prevzem CRL je mogoč na naslovu acldap.nlb.si (193.201.214.60) preko LDAP protokola verzija 2 in verzije 3 na standardnem portu 389.

Na strežniku so objavljeni seznami preklicanih certifikatov (CRL) dveh CA strežnikov:

- prvi CA strežnik ima objavljene certifikate na poddrevesu katerega naslov je **c=si@o=NLB@o=CA** (o=CA,o=NLB,c=si)
- drugi CA strežnik ima objavljene certifikate na poddrevesu katerega naslov je **c=si@o=ACNLB** (o=ACNLB,c=si)

Vsi CRL seznami imajo določeno ime, ki se začne na CRLXXX, kjer XXX pomeni zaporedno številko preklicanega seznama. Tako je na primer polno ime crl seznama 219: cn=CRL219,o=ACNLB,c=si

Korenska digitalna potrdila obeh CA strežnikov sta objavljena na:
https://elba.nlb.si/images/content/_doc/ACNLB.cer
https://elba.nlb.si/images/content/_doc/CANLB.cer

Primer dostopa do CRL seznamov na običajnem LDAP odjemalcu:

1) ime ldap strežnika: acldap.nlb.si
2) tcp vhod ldap strežnika: 389
3) vstopna točka LDAP drevesa
    a. za prvi CA strežnik: o=CA,o=NLB,c=si
    b. za drugi CA strežnik o=ACNLB,c=si
4) verzija LDAP dostopa: 2 ali 3
5) način povezave na LDAP strežnik: anonymous bind
6) »searchlevel«: subtree ali onelevel
7) filter: »cn=CRL*«

Register preklicanih potrdil se osvežuje se vsake štiri (4) ure oz. z vsakim preklicem potrdila.

Register preklicanih potrdil vsebuje enolično interno serijsko številko preklicanega potrdila in čas ter datum preklica.

MOREBITNO PRENEHANJE DELOVANJA AC NLB

Če AC NLB preneha z delovanjem, prekliče vsa potrdila, ki jih je do tedaj izdal, vodenje njegovega registra preklicanih potrdil pa preda drugemu overitelju ali pristojnemu ministrstvu.

VARNOSTNE ZAHTEVE IN ZANESLJIVOST

AC NLB načrtuje in izvaja vse varnostne ukrepe v skladu s standardomoma ISO/IEC 17799:2000, BS 7799-1:2000 Information technology. Code of practice for information security management in FIPS 140-1 level 3 ter tehničnimi zahtevami ETSI TS 101 456 - Policy requirements for certification authorities issuing qualified certificates.

Oprema AC NLB je postavljena v posebnih, ločenih prostorih in je zavarovana z večnivojskim sistemom fizičnega in protivlomnega tehničnega varovanja. Prav tako je zavarovana in zaščitena s protipožarnim sistemom, s sistemom proti izlitju vode, sistemom za prezračevanje in večnivojskim sistemom neprekinjenega napajanja.

AC NLB shranjuje rezervne in distribucijske medije tako, da je v največji meri preprečena izguba, vdor ali nepooblaščena uporaba ali spreminjanje shranjenih informacij. Tako za obnovitev podatkov kot za

arhiviranje pomembnih informacij so zagotovljene rezervne kopije, ki so shranjene na drugem mestu, kot je shranjena programska oprema za upravljanje s potrdili, za zagotovitev ponovnega delovanja v primerih, ko bi bili uničeni podatki na osnovni lokaciji.

Podroben opis infrastrukture AC NLB, operativno delovanje, postopki upravljanja z infrastrukturo ter nadzor nad varnostno politiko njegovega delovanja je določen z njegovo interno politiko.

OSEBJE

AC NLB zaposluje zanesljivo in strokovno usposobljeno osebje, ki preverjeno ni bilo kaznovano za kakršnokoli kaznivo dejanje. Vse osebje se redno usposablja in pridobiva dodatna znanja s svojega strokovnega področja.

Operativne delovne vloge so načrtovane tako, da v največji možni meri preprečujejo možnosti zlorab in so razdeljene med posamezne, med seboj nezdružljive organizacijske skupine, ki pokrivajo naslednja vsebinska področja:

- upravljanje z informacijskim sistemom,
- upravljanje s kvalificiranimi potrdili,
- varovanje in kontrola,
- pravno-administrativno.

Vloga	Osnovne naloge	Število oseb
Glavni uporabnik (Master User)	Skrbi za centralno infrastrukturo AC NLB	3
Varnostni nadzornik (Security officer)	Kreira politiko overitelja in upravlja z varnostno občutljivimi zadevami	3
Sistemski administrator	Ima najvišje dostopne privilegije do operacijskega okolja in ostalih operacijskih sistemskih resursov	4
Skrbnik mrežne infrastrukture	Skrbi za povezave AC NLB v računalniško omrežje NLB in Internetno omrežje	2
Administrator AC NLB	Skrbi za dnevne obdelave, obnavljanje certifikatov in spremembe v zvezi z uporabniki	2
Administrator imenika AC NLB	Dodaja uporabnike v imeniku	2
Pregledovalec certifikatov	Skrbi za tekoče, usklajeno in zaključeno delovanje overitelja AC NLB	2
Pravnik	Svetuje osebju AC NLB s področja pravnih vidikov overiteljstva	1

Za vsako vlogo je v interni politiki AC NLB natančno določeno, s katero sme oz. ne sme biti združljiva. Za nekatere je potrebna prisotnost vsaj dveh za to pooblaščenih oseb. V primeru nepredvidene odsotnosti določenih zaposlenih, njihove vloge prevzamejo drugi zaposleni, če to po interni politiki ni nezdružljivo.

NADZOR

Neodvisni nadzor v smislu opravljanje funkcije notranje revizije AC NLB opravlja Center notranje revizije v NLB (CNR). CNR v primeru odkritih pomanjkljivosti odredi ustrezne ukrepe za odpravo teh pomanjkljivosti, ki jih je AC NLB dolžan izvesti, ter nadzoruje izvedbo odrejenih ukrepov.

ODGOVORNOST

AC NLB ne prevzema nobene odgovornosti za podatke, ki jih imetnik potrdila elektronsko šifrira ali podpisuje in sicer tudi v primeru, da je imetnik ali tretja oseba spoštoval vse veljavne predpise, vsa določila te politike in drugih pravil AC NLB oziroma upošteval vsa njegova navodila.

Zavarovanje odgovornosti overitelja na NLB

NLB ima glede delovanja overitelja AC NLB ustrezno zavarovano svojo odgovornost. Podrobnejše informacije so objavljene na spletnih straneh.

4. UPRAVLJANJE POTRDIL

OSNOVNA PRAVILA ZA UPRAVLJANJE S POTRDILI

Izdajanje in osnovne lastnosti potrdila:

- izdaja se uporabnikom znotraj NLB na osnovi podpisane vloge ,
- AC NLB je odgovoren samo za upravljanje z izdanimi potrdili ter za hranjenje in objavljanje potrdil v javno dostopnem imeniku po protokolu LDAP,
- AC NLB ne odgovarja za dogodke, do katerih bi prišlo zaradi napačne uporabe potrdil, kot npr.:
    - uporabe potrdil za namene, ki niso predvideni v tej politiki,
    - nepravilnega ali pomanjkljivega varovanje gesel ali zasebnih ključev, izdajanje zaupnih podatkov ali ključev tretjim osebam,
    - kakršnekoli zlorabe oz. vdora v informacijsko-komunikacijski sistem imetnika potrdila in s tem do podatkov s strani tretje osebe,
    - nedelovanja ali slabega delovanja informacijsko-komunikacijske infrastrukture imetnika potrdila ali tretjih oseb,
    - nepreverjanja podatkov in veljavnosti potrdil v registru preklicanih potrdil,
    - zaradi uporabe potrdil na nestandardni način ali na nelicenčni programski opremi.
- AC NLB ni odgovoren za vsebino podatkov, ki se šifrirajo ali podpisujejo z njegovimi potrdili ali za obnašanje imetnikov pri uporabi le-teh;
- infrastruktura AC NLB ustreza najvišjim stopnjam varovanja in zaščite potrdil in ključev; veljavnost izdanih potrdil je zagotovljena le, če imetnik upošteva in deluje v skladu s priporočili in standardi, ki jih predlaga AC NLB.

Potrdilo za strežnik vsebuje oz. iz njega izhaja en par ključev za digitalno podpisovanje oziroma šifriranje:

- zasebni ključ za podpisovanje (v nadaljevanju ključ za podpisovanje) ter
- javni ključ za overjanje podpisa (v nadaljevanju ključ za overjanje podpisa).

AC NLB ne posreduje osebnih podatkov o IT skrbnikih strežnikov, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih funkcij oz. aplikacij, povezanih z potrdili ter je to odobril imetnik potrdila, ali na zahtevo pristojnega sodišča, sodnika za prekrške ali upravnega organa.

OSNOVNE LASTNOSTI SPLETNEGA POTRDILA

IT skrbnik strežnika – imetnik spletnega potrdila ima en par ključev, ki ga sestavlja zasebni in javni ključ.
Javni ključ imetnika podpiše AC NLB v postopku tvorbe potrdila. Javni ključ je objavljen kot sestavni del potrdila.
Zasebni ključ se tvori z imetnikovo programsko opremo. Zasebni ključ ima samo imetnik.

Ključi so najmanj 512 - bitni RSA.

AC NLB hrani nujno potrebne podatke o imetniku spletnega potrdila, ki so vključeni v to potrdilo. AC NLB nikoli ne hrani in tudi nima dostopa do zasebnega ključa imetnika spletnega potrdila.

Veljavnost spletnih potrdil je največ pet (5) let od prevzema.

Javno dostopni podatki iz potrdila so:

- različica,

- enolična serijska številka,
- izdajatelj
- nedvoumno razločevalno ime potrdila (DN),
- številka politike, pod katero je bilo izdano potrdilo (CP_{OID}),
- spletni naslov politike,
- rok veljavnosti potrdila,
- elektronski naslov imetnika – IT skrbnika strežnika,
- javni ključ,
- identiteta registra preklicanih potrdil,
- podatki o uporabi potrdila,
- podatki o šifrirnih algoritmih.
- drugi podatki, za katere tako določi ta politika ali veljaven predpis.

Vsak imetnik potrdila ima lahko pod istimi naštetimi podatki le eno samo potrdilo.

Imetnik potrdila je nedvoumno določen z razločevalnim imenom (DN).

Pod istimi podatki o imenu in priimku imetnika – IT skrbnika strežnika, o organizaciji, elektronskim naslovom imetnika ima imetnik lahko eno samo veljavno potrdilo.

LASTNOSTI RAZLOČEVALNEGA IMENA (DN)

Razločevalno ime vsebuje osnovne podatke o imetniku in organizaciji.

IZDAJA POTRDILA

Na podlagi pričujoče politike AC NLB izdaja spletna potrdila za strežnike v lasti NLB.
Potrdilo se izda na osnovi pravilno izpolnjene in podpisane Vloge za izdajo, preklic in obnovo digitalnega potrdila za strežnike (*OB75106*)(v nadaljevanju vloga). Vloge so dostopne na internih spletnih straneh NLB.

Pred podpisom vloge za izdajo digitalnega kvalificiranega potrdila AC NLB s to politiko in z delovanjem overitelja AC NLB natančno seznani IT skrbnika strežnika. Ob odobritvi vloge za potrdilo AC NLB opravi rezervacijo potrdila. IT skrbnik strežnika prejme:
- referenčno številko,
- geslo za prevzem potrdila in
- geslo za telefonski preklic potrdila.

Ob morebitni zavrnitvi vloge, AC NLB o tem obvesti prosilca po elektronski pošti.

AC NLB preda IT skrbniku strežnika referenčno številko, geslo za prevzem potrdila in geslo za preklic potrdila osebno v zaprti kuverti ali pa jo posreduje po dveh ločenih poteh:
- referenčno številko po elektronski pošti,
- geslo za prevzem potrdila in geslo za telefonski preklic potrdila pa po priporočeni pošti v zaprti kuverti.

Po prevzemu potrdila postaneta referenčna številka in geslo za prevzem neuporabni za prevzem drugega potrdila.

Geslo za telefonski preklic služi izključno identifikaciji imetnika pri morebitnem preklicu potrdila preko telefona.

Bodoči imetnik potrdila mora po prejemu obvestila o izdanem potrdilu, referenčne številke, gesla za prevzem in gesla za telefonski preklic potrdilo prevzeti v šestdesetih (60) dneh od izdaje, sicer AC NLB rezervacijo za potrdilo prekliče.

Imetnik potrdila mora ob prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti AC NLB oziroma zahtevati preklic.

PODALJŠANJE VELJAVNOSTI POTRDILA

AC NLB pošlje obvestilo o preteku digitalnega potrdila 15 do 60 dni pred pretekom potrdila. 5 do 50 dni pred pretekom potrdila AC NLB pošlje imetniku potrdila novo referenčno številko in geslo za prevzem ter geslo za telefonski preklic potrdila.

Po dvakratnem (2x) podaljšanju oz. petnajstih (15) letih od izdaje digitalnega potrdila mora imetnik ponovno zaprositi za izdajo potrdila.

PREKLIC POTRDILA IN OBJAVA V REGISTRU PREKLICANIH POTRDIL

Preklic potrdila lahko imetnik potrdila zahteva kadarkoli, mora pa ga zahtevati v primeru:

- spremembe razločevalnega imena (DN),
- ko imetnik potrdila zamenja ključne podatke, povezane s potrdilom (ime ali priimek, elektronski naslov, zaposlitev in podobno),
- ko se ugotovi ali sumi, da je prišlo bodisi do razkritja ključa za podpisovanje bodisi do zlorabe potrdila,
- nadomestitvi potrdila z drugim potrdilom, (npr. ob izgubi pametne kartice, izgubi gesel za dostop do podatkov na kartici in podobno).

AC NLB prekliče potrdilo brez zahteve in brez predhodnega obvestila imetniku takoj ko izve:

- da je podatek v potrdilu napačen ali je bilo potrdilo izdano na podlagi napačnih podatkov,
- da je bila infrastruktura AC NLB ogrožena na način, ki vpliva na zanesljivost potrdila,
- da bo AC NLB prenehala z delovanjem ali ji je delovanje prepovedano in njene dejavnosti ni prevzel drug overitelj,
- da je preklic odredilo pristojno sodišče, sodnik za prekrške ali upravni organ,
- da je preklic odredil pristojni inšpektor.

Preklic potrdila je mogoč 24 ur dnevno. Točna navodila za preklic potrdila AC NLB so javno objavljena na spletnih straneh.

AC NLB bo na podlagi pravilne vloge oz. postopka za preklic potrdila potrdilo preklical najkasneje v štirih (4) urah. V tem času bo preklicano potrdilo v imeniku označeno kot preklicano in dodano v register preklicanih potrdil.

Register preklicanih potrdil vsebuje:

- identifikacijsko oznako preklicanega potrdila in
- čas in datum preklica.

5. IMETNIKI POTRDIL

VARNOSTNE ZAHTEVE

Imetnik potrdila se zavezuje, da bo digitalno podpisoval le dokumente, katerih zahteva po veljavnosti ni daljša od roka veljavnosti potrdila ali pa bo, če je zahteva po veljavnosti dokumentov daljša od roka veljavnosti potrdila, imetnik potrdila pred potekom veljavnosti potrdila zagotovil, da bodo takšni dokumenti znova ustrezno podpisani z uporabo novega veljavnega potrdila.

Imetnik oziroma bodoči imetnik potrdila je dolžan:

- skrbno prebrati to politiko pred podpisom zahtevka ter spremljati vsa obvestila AC NLB in ravnati v skladu z njimi in to politiko,
- Spremljati razvoj tehnologije oziroma obvestila AC NLB in ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
- uporabljati tako programsko opremo, ki je v skladu z obvestili AC NLB (npr. z dovolj močnimi kriptografskimi moduli),
- ključ za podpisovanje in vse druge zaupne podatke ščititi s primernim geslom ali na drug način

tako, da ima dostop do njih samo imetnik,
- vse spremembe, ki so povezane s potrdilom, nemudoma sporočiti AC NLB,
- zahtevati preklic potrdila, če je bil ključ za podpisovanje ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

Imetnik potrdila mora izpolnjevati vse zahteve iz te politike in veljavnih predpisov.

Imetnik potrdila se zavezuje, da bo uporabljal svoj par ključev le v obdobju veljavnosti svojega potrdila.

PRAVICE IMETNIKA POTRDILA

Imetnik potrdila lahko kadarkoli zahteva vse informacije glede veljavnosti potrdila, glede določb te politike ter glede obvestil AC NLB.

Imetnik lahko kadarkoli zahteva preklic strežniškega potrdila.

6. TRETJE OSEBE

VARNOSTNE ZAHTEVE

Ob prvi uporabi potrdil AC NLB po tej politiki mora tretja oseba, ki se zanaša na potrdilo, skrbno prebrati to politiko in od tedaj redno spremljati vsa obvestila AC NLB.

Tretja oseba mora vedno v času uporabe potrdila natančno preveriti, če potrdilo ni v registru preklicanih potrdil.

Če potrdilo vsebuje podatke o tretji osebi, je ta dolžna zahtevati preklic potrdila, če izve, da je bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

PRAVICE TRETJE OSEBE

Tretja oseba se lahko do preklica potrdila zanese na takšno potrdilo.

Tretja oseba lahko kadarkoli zahteva vse informacije glede veljavnosti kateregakoli izdanega potrdila, glede določb te politike ter glede obvestil AC NLB.

7. KONČNE IN PREHODNE DOLOČBE

SPLOŠNO

Določbe glede avtorskih, sorodnih in drugih pravic:

- na ključu za podpisovanje pripadajo vse pravice imetniku potrdila;
- na potrdilu in drugih ključih ter vseh ostalih podatkih vse pravice pripadajo AC NLB.

REŠEVANJE SPOROV

Vse pritožbe imetnikov potrdil AC NLB rešuje nadzorna skupina.

Morebitne spore med imetnikom potrdila ali tretjo osebo in AC NLB rešuje stvarno pristojno sodišče v Ljubljani ob uporabi materialnega prava Republike Slovenije.

VELJAVNOST

AC NLB si pridržuje pravico do spremembe politike delovanja in nadgradnje infrastrukture brez predhodnega obveščanja imetnikov potrdil. Veljavna potrdila pri tem ostanejo v veljavi do konca preteka veljavnosti in po stari politiki delovanja. Vsa potrdila izdana po začetku veljavnosti nove politike, se obravnavajo po novi politiki delovanja.

Ta politika začne veljati z dnem, ko jo sprejme pristojni direktor.

8. TERMINOLOŠKI SLOVAR IN KRATICE

CA	Overitelj potrdil. *Angl.: Certification Authority ali Certification Agency*
CPName	Ime politike delovanja overitelja (*Angl.: Certification Policy Name*), enolično povezano z mednarodno številko politike delovanja CPOID (*Angl.: Certification Policy Object Identifier*)
CPOID	Mednarodna številka, ki enolično določa politiko delovanja (*Angl.: Certification Policy Object IDentifier*).
CRL	Certificate Revocation List – seznam preklicanih digitalnih potrdil
NLB	Nova Ljubljanska banka d.d., Trg Republike 2, 100 Ljubljana
DN	Enolično razločevalno ime (prim. definicijo Razločevalno ime). *Angl.: Distinguished Name*
Imenik potrdil	Imenik potrdil po priporočilu X.500, kjer so shranjena potrdila po priporočilu X.509 ver. 3, do katerih je možen dostop po protokolu LDAP
LDAP	Lightweight Directory Access Protocol je protokol, ki določa dostop do imenika in je specificiran po IETF (Internet Engineering Task Force) priporočilu RFC 1777
Nedvoumna identifikacija	Preverjanje istovetnosti je osebno preverjanje istovetnosti osebe s pomočjo veljavnega osebnega dokumenta ali elektronsko dokazovanje istovetnosti z veljavnim potrdilom overjenim s strani AC NLB ali s strani AC NLB priznanih overiteljev.
Overitelj potrdila	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi. *Angl.: Certification Authority (CA*).
Potrdilo	Kvalificirano potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo ter potrjuje njeno identiteto. *Angl.: Certificate*
Prijavna služba	Služba ali oseba, ki sprejema vloge za potrdila in prevzema identificiranje in preverjanje istovetnosti bodočih imetnikov v imenu overitelja potrdil. *Angl.: Registration Authority (RA)*.
Razločevalno ime	Enolično ime (prim. definicijo DN) v potrdilu, ki nedvoumno in enolično definira uporabnika v strukturi imenika.
SSL	Secure Sockets Layer

REFERENČNI DOKUMENTI

- Politika AC NLB – Zaupni del notranjih pravil AC NLB (*OP75106*)
- Vloga za izdajo, preklic in obnovo digitalnega potrdila za strežnike (*OB75106*)