Certifikatska Agencija NLB d.d.

AC NLB

Politika AC NLB

Javni del notranjih pravil delovanja

2. izdaja z dne 27.6.2017

Vsebovane politike AC NLB

Kvalificirana potrdila za fizične osebe

AC NLB - Kvalificirana potrdila
CPOID: 1.3.6.1.4.1.7597.1.5.11

Država (C)	SI
Organizacija (O)	NLB d.d.
Organizacijska enota (OU)	ACNLB
Organizacijska enota (OU)	Fizicne osebe
Splošno ime (CN)	ime in priimek imetnika potrdila
Serijska številka(serialNumber)	davčna številka fizične osebe
Ime (givenName, GN)	Ime
Priimek (surname, SN)	Priimek

Kvalificirana potrdila za zaposlene pri pravni osebi

AC NLB - Kvalificirana potrdila
CPOID: 1.3.6.1.4.1.7597.1.5.12

Država (C)	SI
Organizacija (O)	Registrirano ime pravne osebe
Organizacijska identiteta (OI)	VATSI-DŠ pravne osebe
Organizacijska enota (OU)	ACNLB
Organizacijska enota (OU)	Pravne osebe
Splošno ime (CN)	ime in priimek imetnika potrdila
Serijska številka (serialNumber)	davčna številka pravne osebe in fizične osebe
Ime (givenName, GN)	Ime
Priimek (surname, SN)	Priimek

Kvalificirana potrdila za fizične osebe za oddaljen podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa

AC NLB - Kvalificirana potrdila
CPOID: 1.3.6.1.4.1.7597.1.5.13

Država (C)	SI
Organizacija (O) *	Registrirano ime pravne osebe
Organizacijska identiteta (OI)*	VATSI-DŠ pravne osebe
Organizacijska enota (OU)	ACNLB
Organizacijska enota (OU)	PVO Fizicne ali PVO Pravne
Splošno ime (CN)	ime in priimek imetnika potrdila
Serijska številka(serialNumber)	davčna številka fizične osebe ali davčna številka pravne osebe in fizične osebe

* Polje je prisotno v potrdilih za zaposlene pri pravni osebi

Kvalificirana potrdila za fizične osebe za oddaljen podpis

AC NLB - Kvalificirana potrdila
CPOID: 1.3.6.1.4.1.7597.1.5.14

Država (C)	SI
Organizacija (O) *	Registrirano ime pravne osebe
Organizacijska identiteta (OI)*	VATSI-DŠ pravne osebe
Organizacijska enota (OU)	ACNLB
Organizacijska enota (OU)	PVO Fizicne ali PVO Pravne
Splošno ime (CN)	ime in priimek imetnika potrdila
Serijska številka(serialNumber)	davčna številka fizične osebe ali davčna številka pravne osebe in fizične osebe

* Polje je prisotno v potrdilih za zaposlene pri pravni osebi

Kvalificirana potrdila za pravne osebe za elektronski žig

AC NLB - Kvalificirana potrdila
CPOID: 1.3.6.1.4.1.7597.1.5.15

Država (C)	SI

Organizacija (O)	Registrirano ime pravne osebe
Organizacijska identiteta (OI)	VATSI-DŠ pravne osebe
Organizacijska enota (OU)	ACNLB
Organizacijska enota (OU)	Elektronski zig
Splošno ime (CN)	Naziv pravne osebe
Serijska številka(serialNumber)	davčna številka pravne osebe

Kvalificirana potrdila za pravne osebe za elektronski žig na napravi za ustvarjanje kvalificiranega elektronskega žiga

AC NLB - Kvalificirana potrdila
CPOID: 1.3.6.1.4.1.7597.1.5.16

Država (C)	SI
Organizacija (O)	Registrirano ime pravne osebe
Organizacijska identiteta (OI)	VATSI-DŠ pravne osebe
Organizacijska enota (OU)	ACNLB
Organizacijska enota (OU)	Elektronski zig
Splošno ime (CN)	Naziv pravne osebe
Serijska številka(serialNumber)	davčna številka pravne osebe

Potrdila za ostale namene, ki morajo vsebovati enolično identifikacijsko oznako, ki omogočajo jasno prepoznavo potrdila

AC NLB - Potrdila
CPOID: 1.3.6.1.4.1.7597.2 (glede na uporabo)

Država (C)	SI
Organizacija (O)	NLB d.d.
Organizacijska enota (OU)	ACNLB
Organizacijska enota (OU)	Naziv organizacije
Splošno ime (CN)	ime in priimek imetnika potrdila
Serijska številka(serialNumber)	enolični identifikator

KAZALO

1 Uvod

1.1 Pregled

AC NLB je ponudnik storitev zaupanja pri Novi Ljubljanski banki d.d., Ljubljana (v nadaljevanju NLB d.d.). Ta politika, ki predstavlja nedeljivo celoto javnega dela notranjih pravil ponudnika storitev zaupanja AC NLB, ureja namen, delovanje in metodologijo upravljanja kvalificiranih potrdil za elektronske podpise, kvalificiranih potrdil za elektronske žige in nekvalificiranih potrdil ter varnostne zahteve, ki jih morajo izpolnjevati ponudnik storitev zaupanja AC NLB ter imetniki potrdil.

Veljavna potrdila pri tem ostanejo v veljavi do izteka njihove veljavnosti po stari politiki delovanja (CP_{OID}: 1.3.6.1.4.1.7597.1.4.1, CP_{OID}: 1.3.6.1.4.1.7597.1.4.2). Pod novo identifikacijsko številko (CP_{OID}) in datumom veljavnosti AC NLB predhodno objavi novo politiko AC NLB.

AC NLB izdaja potrdila v skladu z UREDBO (EU) št. 910/2014 EVROPSKEGA PARLAMENTA IN SVETA o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (v nadaljevanju uredba eIDAS) in drugo vsakokrat veljavno zakonodajo, kot je navedena v točki 9.14.

Vse določbe te politike glede ravnanja AC NLB so ustrezno prenesene in podrobneje opredeljene v določbah notranje politike (OP75105 verzija 01.00.00), 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 s tehničnimi zahtevami ETSI TS 319 401, ETSI TS 319 411-1 in ETSI TS 319 411-2.

Ponudnik storitev zaupanja AC NLB uporablja lastno infrastrukturo za upravljanje potrdil v okviru katere deluje več izdajateljev. Korenski izdajatelj ACNLB RootCA, ki ima samo-podpisano potrdilo in izdaja potrdila podrejenim izdajateljem, ter podrejeni izdajatelji, ki izdajajo potrdila končnim uporabnikom.

Ponudnik storitev zaupanja AC NLB se lahko povezuje z drugimi ponudniki storitev in se z njimi priznava. AC NLB v ta namen lahko sklene pogodbo o medsebojnem priznavanju.

1.1.1 Potrdila ponudnika storitev AC NLB

AC NLB izvaja upravljanje potrdil v skladu z Uredbo eIDAS in ZEPEP in drugo vsakokrat veljavno zakonodajo, kot je navedena v točki 9.14., kar zagotavlja zahtevan nivo zaupanja v identiteto imetnikov za Kvalificirana potrdila in vse vrste potrdil, ki jih izdaja ponudnik storitev AC NLB.

AC NLB izdaja:

- Kvalificirana potrdila za elektronski podpis za fizične osebe.
- Kvalificirana potrdila za elektronski podpis za fizične osebe, zaposlene pri pravnih osebi.
- Kvalificirana potrdila za elektronski žig za pravne osebe
- Nekvalificirana (normalizirana) potrdila.

Kvalificirana potrdila za elektronski podpis, ki jih izdaja ponudnik storitev AC NLB, so namenjena za ustvarjanje naprednega elektronskega podpisa in kvalificiranega elektronskega podpisa ter druge namene glede na komercialni tip potrdila.

Kvalificirana potrdila za elektronski žig, ki jih izdaja ponudnik storitev AC NLB, so namenjena za ustvarjanje naprednega elektronskega žiga in kvalificiranega elektronskega žiga ter druge namene glede na komercialni tip potrdila.

Nekvalificirana (normalizirana) potrdila so namenjena uporabi v zaprtem sistemu.

1.2 Naziv dokumenta in identifikacijske oznake potrdil

Pričujoči dokument predstavlja pravila delovanja ponudnika storitev AC NLB. Polni naslov dokumenta je Politika AC NLB, javni del notranjih pravil delovanja. V nadaljevanju Politika AC NLB.

Identifikacijske oznake potrdil ponudnika storitev AC NLB:

AC NLB - Kvalificirana potrdila za fizične osebe

Opis:	Kvalificirana potrdila za fizične osebe
Vrsta:	Kvalificirano potrdilo za elektronski podpis
Namen uporabe	Napreden elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	Do pet (5) let
Identifikacijska Oznaka:	1.3.6.1.4.1.7597.1.5.11, 0.4.0.194112.1.0

AC NLB - Kvalificirana potrdila za zaposlene pri pravni osebi

Opis:	Kvalificirana potrdila za zaposlene pri pravni osebi
Vrsta:	Kvalificirano potrdilo za elektronski podpis
Namen uporabe	Napreden elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	Do pet (5) let
Identifikacijska Oznaka:	1.3.6.1.4.1.7597.1.5.12, 0.4.0.194112.1.0

AC NLB - Kvalificirana potrdila za fizične osebe za oddaljen podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa

Opis:	Kvalificirana potrdila za fizične osebe za uporabo na napravi, ki ustreza skladnosti s FIPS 140-2 level 3 in QSCD
Vrsta:	Kvalificirano potrdilo za elektronski podpis
Namen uporabe	Kvalificiran elektronski podpis
Rok veljavnosti:	Do pet (5) let
Identifikacijska Oznaka:	1.3.6.1.4.1.7597.1.5.13, 0.4.0.194112.1.2

AC NLB - Kvalificirana potrdila za fizične osebe za oddaljen podpis

Opis:	Kvalificirana potrdila za fizične osebe
Vrsta:	Kvalificirano potrdilo za elektronski podpis
Namen uporabe	Napreden elektronski podpis
Rok veljavnosti:	Do pet (5) let
Identifikacijska Oznaka:	1.3.6.1.4.1.7597.1.5.14, 0.4.0.194112.1.0

AC NLB - Kvalificirana potrdila za pravne osebe za elektronski žig

Opis:	Kvalificirana potrdila za pravne osebe
Vrsta:	Kvalificirano potrdilo za elektronski žig
Namen uporabe	Napreden elektronski žig in avtentikacija
Rok veljavnosti:	Do pet (5) let
Identifikacijska Oznaka:	1.3.6.1.4.1.7597.1.5.15, 0.4.0.194112.1.1

AC NLB - Kvalificirana potrdila za pravne osebe za elektronski žig na napravi za ustvarjanje kvalificiranega elektronskega žiga

Opis:	Kvalificirana potrdila za pravne osebe za elektronski žig za uporabo na napravi, ki ustreza skladnosti s FIPS 140-2 level 3 in QSCD
Vrsta:	Kvalificirano potrdilo za elektronski žig
Namen uporabe	Kvalificiran elektronski žig za avtentikacijo
Rok veljavnosti:	Do pet (5) let
Identifikacijska Oznaka:	1.3.6.1.4.1.7597.1.5.16, 0.4.0.194112.1.3

AC NLB - Potrdila za druge namene

Opis:	Namenska potrdila za ostale namene v zaprtem sistemu
Vrsta:	Potrdilo za elektronski podpis
Namen uporabe	Napreden elektronski podpis, šifriranje in avtentikacija
Rok veljavnosti:	Do pet (5) let
Identifikacijska Oznaka:	1.3.6.1.4.1.7597.2.(glede na uporabo)

Druga potrdila potrebna za delovanje infrastrukture AC NLB

AC NLB - Potrdila za OCSP

Opis:	Potrdila za storitev OCSP v okviru AC NLB.
Namen uporabe	Napreden elektronski podpis odgovora storitve OCSP
Rok veljavnosti:	Do tri (3) let-a
Identifikacijska Oznaka:	1.3.6.1.4.1.7597.3.1

1.3 Udeleženci infrastrukture javnih ključev

1.3.1 Ponudniki storitev

- Ponudnik storitev AC NLB uporablja isto infrastrukturo za izdajo vseh vrst potrdil končnim uporabnikom.
- Ponudnik storitev deluje kot glavna certifikatska agencija (angl. CA - Certification Authority), ki je v postopku tvorjenja šifrirnih ključev sebi podpisala potrdilo (angl. self-signed certificate).
- Ponudnik storitev je dolžan izvajati ukrepe in postopke, ki zagotavljajo upravljanje potrdil v skladu s predpisi, ki veljajo na območju RS in notranjimi pravili ponudnika storitev.
- Ponudnika storitev v okviru NLB d.d. predstavljajo naslednji identifikacijski podatki:

Naslov:	NLB d.d. AC NLB Trg republike 2 1000 Ljubljana
Telefon:	(+386) 01 477 20 60
Fax:	(+386) 01 476 47 99
Spletna stran:	https://www.nlb.si/ac-nlb
E-mail:	acnlb@nlb.si
Pomoč uporabnikom:	(+386) 01 477 20 00
Enolično ime:	AC NLB

Potrdilo ponudnika storitev AC NLB vsebuje:

Serial Number	Serijska številka	3EC3 868E
Issuer	Ponudnik storitev	O=ACNLB,c=SI
Subject	Imetnik	O=ACNLB,c=SI
Validity: Not Before	Veljavnost od:	15.05.2003 13:52:45 GMT
Validity: Not After	Veljavnost do:	15.05.2023 14:22:45 GMT
RSA Public Key	Dolžina RSA ključa	2048 bit
Signature Algorithm	Algoritem	sha1WithRSAEncryption
Key Identifier	Identifikator ključa	CCBBBB86D66FF8BEB4472277B3B6ADD70159964D
SHA-256 hash:	SHA-256 odtis Potrdila	894CE6DDB012CB3F736954668DE63F436080E95F17B7A81BD924EB21BEE9E440
SHA-1 hash	SHA-1 odtis potrdila	0456F23D1E9C43AECB0D807F1C0647551A05F456

Potrdilo korenskega izdajatelja ACNLB RootCA vsebuje:

Serial Number	Serijska številka	EE61ADE000000000593E4965
Issuer	Ponudnik storitev	CN=ACNLB RootCA OID.2.5.4.97=VATSI-91132550 O=NLB d.d. C=SI
Subject	Imetnik	CN=ACNLB RootCA OID.2.5.4.97=VATSI-91132550 O=NLB d.d. C=SI
Validity: Not Before	Veljavnost od:	Jun 12 07:30:03 2017 GMT
Validity: Not After	Veljavnost do:	Jun 12 08:00:03 2037 GMT
RSA Public Key	Dolžina RSA ključa	3072 bit
Signature Algorithm	Algoritem	sha256WithRSAEncryption
Key Identifier	Identifikator ključa	4A79C15E3281C687
SHA-256 hash:	SHA-256 odtis Potrdila	32974009D1662C1426DBCC121468F1FFC8E7081C52C5B7050BEC0A9686ABCCFF
SHA-1 hash	SHA-1 odtis potrdila	EE6A664759F2B0A8F0F18E6A594FDD02207D30D0

Potrdilo izdajatelja ACNLB SubCA vsebuje:

Serial Number	Serijska številka	07C94F3D00000000593E49A0
Issuer	Ponudnik storitev	CN=ACNLB RootCA OID.2.5.4.97=VATSI-91132550 O=NLB d.d. C=SI
Subject	Imetnik	CN=ACNLB SubCA OID.2.5.4.97=VATSI-91132550 O=NLB d.d. C=SI
Validity: Not Before	Veljavnost od:	Jun 12 11:22:42 2017 GMT
Validity: Not After	Veljavnost do:	Apr 12 11:52:42 2036 GMT
RSA Public Key	Dolžina RSA ključa	3072 bit
Signature Algorithm	Algoritem	sha256WithRSAEncryption
Key Identifier	Identifikator ključa	454FBC6BEA4AEA8B
SHA-256 hash:	SHA-256 odtis Potrdila	A008209DA8EEA5D669AA9E48382AF0528087F5830B0919CAA99507C57ECA1A51
SHA-1 hash	SHA-1 odtis potrdila	EC9DA485FBBC92412BA524737F592F4B4D342D7B

Opomba: OID.2.5.4.97 predstavlja polje organizationIdentifier (OI)

1.3.2 Registracijska pisarna ponudnika storitev

Registracijska pisarna (angl. RA-Registration Authority), ki deluje na sedežu ponudnika storitev in organizacijskih enotah NLB d.d. Poleg overjanja identitete prosilcev je edina pooblaščena za odobravanje in posredovanje vlog sistemu (informacijskemu sistemu ponudnika storitev) za izdajo potrdil.

1.3.3 Naročniki in imetniki potrdil

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

Imetnik potrdila je fizična oseba, navedena v potrdilu v polju »subject« kot lastnik zasebnega ključa, ki ustreza javnemu ključu, navedenemu v potrdilu. Potrdilo je vedno izdano določeni fizični osebi.

V primeru, ko je naročnik pravna oseba, je imetnik fizična oseba zaposlena ali povezana s pravno osebo, ki uporablja potrdilo v svojem imenu. V polju "subject" je vpisano imetnikovo ime in priimek ter naziv organizacije.

S podpisom vloge se imetnik zavezuje k doslednem spoštovanju in upoštevanju javnega dela notranjih pravil ponudnika storitev.

Naročniki in imetniki potrdil morajo 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. Glej tudi 9.6.3.

1.3.4 Tretja oseba

Tretja oseba je vsak subjekt, ki se zanaša na verodostojnost potrdila, ne glede na to ali je imetnik potrdila.

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 (CRL ali OCSP).

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

1.3.5 Ostali udeleženci

Ni relevantno.

1.4 Namen uporabe potrdil

1.4.1 Dovoljena uporaba potrdil

Potrdila, ki jih izdaja ponudnik storitev AC NLB je dovoljeno uporabljati v skladu z določili za posamezen tip potrdila navedenimi v poglavju 1.2 Naziv dokumenta in identifikacijske oznake potrdil.

Kvalificirana potrdila za elektronski podpis, ki jih izdaja ponudnik storitev AC NLB, so namenjena za ustvarjanje naprednega elektronskega podpisa in kvalificiranega elektronskega podpisa ter druge namene glede na komercialni tip potrdila (glej 1.2).

Kvalificirana potrdila za elektronski žig, ki jih izdaja ponudnik storitev AC NLB, so namenjena za ustvarjanje naprednega elektronskega žiga in kvalificiranega elektronskega žiga ter druge namene glede na komercialni tip potrdila (glej 1.2).

Potrdila za ostale namene, ki jih izdaja ponudnik storitev AC NLB, so normalizirana (nekvalificirana) potrdila in so namenjena uporabi v zaprtem sistemu.

Potrdila za OCSP se uporabljajo samo za podpis odgovora storitve OCSP za izdajatelje, ki delujejo v okviru ponudnika storitev zaupanja AC NLB.

1.4.2 Nedovoljena uporaba potrdil

Uporaba potrdil je dovoljena samo za namene, ki so opisani v poglavju 1.4.1. Za vse ostale namene pa uporaba potrdil ni dovoljena.

1.5 Upravljanje s pravili delovanja

1.5.1 Organizacija, ki upravlja s pričujočim dokumentom

Pričujoči dokument (Politika AC NLB) in ponudnika storitev AC NLB kot celoto upravlja NLB d.d., Ljubljana.

1.5.2 Kontaktni podatki

1.5.2.1 Kontaktne osebe – organizacija ponudnika storitev

Kontaktna oseba, odgovorna za organizacijo ponudnika storitev, je dosegljiva na naslovu, opredeljenem v poglavju 1.3.1

1.5.2.2 Kontaktne osebe – dokumentacija ponudnika storitev

Kontaktna oseba, odgovorna za organizacijo ponudnika storitev, je dosegljiva na naslovu, opredeljenem v poglavju 1.3.1

1.5.3 Odgovorni organ za odobritev pravil delovanja ponudnika storitev (Politika AC NLB)

Pravila delovanja ponudnika storitev AC NLB potrjuje pristojni organ v NLB d.d. – Upravni odbor AC NLB.

1.5.4 Postopek odobritve pravil delovanja ponudnika storitev

Politiko AC NLB pred objavo in potrditvijo (glej 1.5.3) pregleda in po potrebi uskladi Upravni odbor AC NLB. V okviru pregleda se preveri skladnost vsebine Politike AC NLB z Uredbo eIDAS, ZEPEP in drugo vsakokrat veljavno zakonodajo.

1.6 Pojmi in kratice

1.6.1 Osnovne definicije

Elektronski podpis	Je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika.
Digitalni podpis	Je niz podatkov, ki je dodan ali kriptografska transformacija podatkov, ki omogoča prejemniku preveriti pristnost podatkov in identifikacijo podpisnika ter ščiti pred ponarejanjem.
Informacijski sistem	Je sistem za oblikovanje, pošiljanje, prejemanje, shranjevanje in druge obdelave podatkov v elektronski obliki.

Potrdilo (digitalno potrdilo)	Je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto. Pojem Potrdilo (ali potrdilo) se v tem dokumentu uporablja za X.509 digitalna potrdila kot jih opredeljuje RFC 5280 oziroma ISO/IEC 9594-8/Recommendation ITU-T X.509.
Normalizirano potrdilo	Normalizirana potrdila, zagotavljajo enak nivo varnosti, oziroma zaupanja, kot kvalificirana in so namenjena uporabi za vse ostale namene.
Potrdilo za elektronski podpis	Pomeni elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega podpisa s fizično osebo in potrjuje vsaj ime ali psevdonim te osebe.
Kvalificirano potrdilo za elektronski podpis	Pomeni potrdilo za elektronske podpise, ki ga izda kvalificirani ponudnik storitev zaupanja.
Potrdilo za elektronski žig	Pomeni elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega žiga s pravno osebo in potrjuje ime te osebe.
Kvalificirano potrdilo za elektronski žig	Pomeni potrdilo za elektronski žig, ki ga izda kvalificirani ponudnik storitev zaupanja.
Oprema za elektronsko podpisovanje	Je strojna ali programska oprema ali njuna specifična sestavina, ki jo ponudnik storitev uporablja za storitve v zvezi z elektronskim podpisovanjem oz. se uporablja za oblikovanje ali preverjanje elektronskih podpisov.
Naprava za ustvarjanje elektronskega podpisa	Pomeni konfigurirano programsko ali strojno opremo, ki se uporablja za ustvarjanje elektronskega podpisa.
Naprava za ustvarjanje kvalificiranega elektronskega podpisa	Pomeni napravo za ustvarjanje elektronskega podpisa, ki izpolnjuje zahteve Uredbe eIDAS Priloga II, ali naprave za varno ustvarjanje podpisa, katerih skladnost je bila ugotovljena v skladu z Direktivo 1999/93/ES.
Naprava za ustvarjanje elektronskega žiga	Pomeni konfigurirano programsko ali strojno opremo, ki se uporablja za ustvarjanje elektronskega podpisa.
Naprava za ustvarjanje kvalificiranega elektronskega žiga	Pomeni napravo za ustvarjanje elektronskega podpisa, ki izpolnjuje zahteve Uredbe eIDAS Priloga II, ali naprave za varno ustvarjanje podpisa, katerih skladnost je bila ugotovljena v skladu z Direktivo 1999/93/ES.
Ponudnik storitev zaupanja (ali Ponudnik storitev**)**	Pomeni fizično ali pravno osebo, ki zagotavlja eno ali več storitev zaupanja, kot ponudnik

	kvalificiranih ali nekvalificiranih storitev zaupanja. V tem dokumentu predstavlja ponudnika storitev zaupanja fizično ali pravno osebeoki izdaja potrdila ali opravlja druge storitve v zvezi s potrdili ali elektronskim podpisovanjem.
Ponudnik kvalificiranih storitev zaupanja	Pomeni ponudnika storitev zaupanja, ki zagotavlja eno ali več kvalificiranih storitev zaupanja in mu nadzorni organ dodeli kvalificirani status.
Kvalificirana storitev zaupanja	Pomeni storitev zaupanja, ki izpolnjuje zadevne zahteve iz Uredbe eIDAS.
Podatki za elektronsko podpisovanje	So edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa.
Podatki za preverjanje elektronskega podpisa	So edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa.
Podpisnik	Je oseba, ki ustvari elektronski podpis.
Napredni elektronski podpis	Pomeni elektronski podpis, ki izpolnjuje zahteve iz člena 26 po Uredbi eIDAS.
Kvalificirani elektronski podpis	Pomeni napredni elektronski podpis, ki se ustvari z napravo za ustvarjanje Kvalificiranega elektronskega podpisa in temelji na Kvalificiranem potrdilu za elektronske podpise.
Ponudnik storitev	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem potrdil ali elektronskimi podpisi. Angl.:Certification Authority (CA).
Izdajatelj potrdil (izdajatelj)	Izdajatelj potrdil (CA), ki deluje v okviru ponudnika storitev zaupanja.
Korenski izdajatelj	V infrastrukturi javnih predstavlja ključev korenski izdajatelj osnovno izhodiščno točko zaupanja pri preverjanju veljavnosti potrdil znotraj verige zaupanja. Angl: Root Certification Authotity

1.6.2 Okrajšave

Kratica	Pomen
ARL	Angl. Authority Revocation List – register preklicanih potrdil, ki jih uporabljajo drugi ponudniki storitev
CA	Angl. Certification Authority – ponudnik storitev
CN	Angl. Common Name – X.500 domače ime imetnika potrdila
CRL	Angl. Certificate Revocation List – register preklicanih potrdil
CSP	Angl. Certification Service Provider – ponudnik storitve overjanja in upravljanja potrdil
CPS	Angl. Certificate Practice Statement – javni del notranjih pravil ponudnika storitev, politika
PDS	Angl. Policy Disclosure Statement – Izjava o politiki delovanja, pravila delovanja
DN	Angl. Distinguished Name – X.500 razločevalno ime
EAL	Angl. Evaluation Assurance Level – standard označevanja varnostnih nivojev v računalniških sistemih
FIPS	Angl. United State Federal Information Processing Standards – oznaka standarda s področja informacijskega procesiranja
	Angl. Local Registration Authority – lokalna registracijska pisarna, ki izvaja funkcijo registrske pisarne ponudnika storitev
PKCS	Angl. Public Key Cryptographic Standars – šifrirni standardi na področju javnih ključev
RA	Angl. Registration Auhority – registracijska pisarna ponudnika storitev
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 57/2000, 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14)
eIDAS	UREDBA (EU) št. 910/2014 EVROPSKEGA PARLAMENTA IN SVETA z dne 23.06.2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES.
PGG	Programski generator enkratnih gesel (angl. Soft Token)

SGG	Strojni generator enkratnih gesel (angl. Hard Token)
QSCD	Naprava za ustvarjanje kvalificiranega elektronskega podpisa (angl. Qualified Signature Creation Device**)**
HSM	Strojni varnostni (kriptografski) modul (angl. Hardware Security Module)
OCSP	Storitev sprotnega preverjanja status potrdil. Angl.: Online Certificate Status Protocol
SPKAC	Signed Public Key and Challenge

1.6.3 Pomen izrazov

Posamezni izrazi imajo v nadaljevanju tega dokumenta naslednji pomen:

- **Organizacija** je pravna ali fizična oseba, ki je registrirana za opravljanje dejavnosti.
- **Zakoniti zastopnik organizacije** je fizična oseba, ki je pooblaščena za zastopanje organizacije v pravnem prometu. Zakoniti jamči, da so vloge pravilno izpolnjene ter da so identifikacijski podatki imetnikov potrdil resnični.
- **Pooblaščena oseba za oddajo vloge** je fizična oseba, ki jo zakoniti zastopnik organizacije pooblasti za oddajo vloge.
- **Vloge** so obrazci ponudnika storitev za upravljanje s potrdili (npr. pridobitev potrdila, preklic potrdila, …).
- **Registracijska pisarna ponudnika storitev** po pooblastilu ponudnika storitev sprejema vloge in preverja istovetnosti prosilcev in imetnikov potrdil.
- **Objava ponudnika storitev** je javna objava na spletnih straneh ponudnika storitev.
- **Obvestila ponudnika storitev** so vsa navodila, pojasnila, seznami, pogoji, posamezna obvestila, priporočila, standardi in drugi dokumenti, ki jih določi ali priporoči ponudnik storitev in jih objavi ali kako drugače posreduje imetnikom potrdil ali tretjim osebam.
- **Digitalna identiteta, digitalni ID** (angl. Digital Identity, Digital ID) je par ključev – zasebni in javni – ter potrdilo javnega ključa, ki ga izda kvalificirani ponudnik storitev zaupanja.
- **Uporabnik** je naročnik ali imetnik kvalificiranega potrdila.
- **Aktivacijski podatki so podatki potrebni za prevzem potrdila (referenčna številka in avtorizacijska** koda) ali za aktiviranje zasebnih ključev.

2 Odgovornost za objave in repozitorij

2.1 Repozitorij

Ponudnik storitev objavlja informacije o svojih storitvah na javnih spletnih straneh, ki so dosegljive na spletnem naslovu https://www.nlb.si/ac-nlb.
Informacije o izdanih potrdilih in potrdila so shranjena na internih strežnikih in niso javno dostopne.

2.2 Objave informacij o potrdilih

Na javnih spletnih straneh ponudnika storitev AC NLB, so objavljene naslednje informacije:

- AC NLB – Izjava o politiki delovanja (PDS).
- Politika ponudnika storitev AC NLB.
- Vloge za pridobitev, preklic in obnovo potrdil.
- Ostale informacije vezane na delovanje ponudnika storitev.
- Status preklicnih potrdil v obliki seznama preklicanih potrdil (CRL) ali preko protokola za sprotno preverjanje status potrdil (OCSP).

2.3 Čas in pogostost objav

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

Ostale informacije so objavljene sproti ob njihovi spremembi.

2.4 Dostop do podatkov v repozitoriju

Vse informacije na spletnih straneh so dostopne za branje ves čas brez omejitve.

3 PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI

3.1 Določanje imen

3.1.1 Vrste imen

Razločevalna imena (angl. DN – Distinguised Name) AC NLB v poljih »issuer« in »subject« potrdila X.509 so oblikovana v obliki skladni s priporočili X.501 ter usklajena z RFC 5280, ETSI EN 319 412-2 in ETSI EN 319 412-3 .
V nadaljevanju poglavja so podana polja razločevalnega imena, ki enolično določajo identiteto imetnika posamezne vrste potrdila. Razločevalno ime lahko vsebuje dodatna polja, ki pa ne zamenjujejo spodaj navedenih polj in niso potrebna za opredelitev enolične identitete imetnika potrdila.

AC NLB »subject« atribut oziroma »issuer« atribut v potrdilih je:
Država (C) = SI
Organizacija (O) = NLB d.d.
Organizacijska identiteta (OI) = VATSI-91132550
Splošno ime (commonName, CN) = ACNLB RootCA ali ACNLB SubCA

Polje »subject« v potrdilih za storitev OCSP vsebuje sleče podatke:
Država (C) = SI
Organizacija (O) = NLB d.d.
Organizacijska identiteta (OI) = VATSI-91132550
Organizacijska enota (OU) = ACNLB
Splošno ime (commonName, CN) = Naziv posamezne storitve oziroma strežnika OCSP

Kvalificirana potrdila za fizične osebe v polju »subject« v potrdilu, nosijo naslednje podatke:
Država (C) = SI
Organizacija (O) = NLB d.d.
Organizacija (OU) = ACNLB
Organizacijska enota (OU) = Fizicne osebe
Ime (CN) = ime in priimek imetnika potrdila
Serijska številka (serialNumber) = davčna številka imetnika potrdila + dodatna dvomestna številka
GivenName (GN) = Ime
Surname (SN) = Priimek

Kvalificirana potrdila za zaposlene pri pravni osebi v polju »subject« v potrdilu, nosijo naslednje podatke:
Država (C) = SI
Organizacija (O)* = Registrirano ime pravne osebe
Organizacijska identiteta (OI)* = VATSI-DŠ pravne osebe
Organizacijska enota (OU) = ACNLB
Organizacijska enota (OU) = Pravne osebe
Splošno ime (CN) = ime in priimek imetnika potrdila
Serijska številka (serialNumber) = davčna številka pravne osebe + davčna številka imetnika potrdila + dodatna dvomestna številka
Ime (givenName, GN) = Ime
Priimek (surname, SN) = Priimek
* Polje je prisotno v potrdilih za zaposlene pri pravni osebi

Kvalificirana potrdila za fizične osebe za oddaljen podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa v polju »subject« v potrdilu, nosijo naslednje podatke:
Država (C) = SI
Organizacija (O)* = Registrirano ime pravne osebe
Organizacijska identiteta (OI)* = VATSI-DŠ pravne osebe
Organizacijska enota (OU) = ACNLB
Organizacijska enota (OU) = PVO Fizicne ali PVO Pravne
Splošno ime (CN) = ime in priimek imetnika potrdila
Serijska številka (serialNumber) = davčna številka imetnika potrdila + dodana dvomestna številka ali davčna številka pravne osebe + davčna številka imetnika potrdila + dodatna dvomestna številka
Ime (givenName, GN) = Ime
Priimek (surname, SN) = Priimek
* Polje je prisotno v potrdilih za zaposlene pri pravni osebi

Kvalificirana potrdila za fizične osebe za oddaljen podpis v polju »subject« v digitalnem potrdilu, vsebujejo naslednje podatke:
Država (C) = SI
Organizacija (O) = Registrirano ime pravne osebe
Organizacijska identiteta (OI) = VATSI-DŠ pravne osebe
Organizacijska enota (OU) = ACNLB
Organizacijska enota (OU) = PVO Fizicne ali PVO Pravne
Splošno ime (CN) = ime in priimek imetnika potrdila
Serijska številka (serialNumber) = davčna številka imetnika potrdila + dodana dvomestna številka ali davčna številka pravne osebe + davčna številka imetnika potrdila + dodatna dvomestna številka
Ime (givenName, GN) = Ime
Priimek (surname, SN) = Priimek

Kvalificirana potrdila za pravne osebe za elektronski žig v polju »subject« v potrdilu, nosijo naslednje podatke:
Država (C) = SI
Organizacija (O) = Registrirano ime pravne osebe
Organizacijska identiteta (OI) = VATSI-DŠ pravne osebe
Organizacijska enota (OU) = ACNLB
Organizacijska enota (OU) = Elektronski zig
Splošno ime (CN) = ime pravne osebe
Serijska številka (serialNumber) = davčna številka pravne osebe potrdila + dodana dvomestna številka

Kvalificirana potrdila za pravne osebe za elektronski žig na napravi za ustvarjanje kvalificiranega elektronskega žiga v polju »subject« v potrdilu, nosijo naslednje podatke:
Država (C) = SI
Organizacija (O) = Registrirano ime pravne osebe
Organizacijska identiteta (OI) = VATSI-DŠ pravne osebe
Organizacija (OU) = ACNLB
Organizacijska enota (OU) = Elektronski zig

Splošno ime (CN) = ime pravne osebe
Serijska številka (serialNumber) = davčna številka pravne osebe potrdila + dodana dvomestna številka

Potrdila za ostale namene:
Država (C) = SI
Organizacija (O) = Naziv organizacije
Organizacijska enota (OU) = ACNLB
Organizacijska enota (OU) = Naziv organizacije
Organizacijska identiteta (OI) = VATSI-DŠ pravne osebe
Splošno ime (CN) = ime in priimek imetnika potrdila
Serijska številka (serialNumber) = davčna številka pravne osebe + davčna številka imetnika potrdila + dodana dvomestna številka

3.1.2 Potreba po smiselnosti imen

Relativno ime (RDN) imetnika potrdila sestavljata, splošno ime (CN), ki vsebuje ime in priimek imetnika, serijska številka (serialNumber), ime imetnika (givenName) ter priimek imetnika (surName)
Ponudnik storitev določi serijsko številko v skladu s svojimi notranjimi pravili (glej 3.1.1). Le-ta je določena tako, da enolično določi imetnika potrdila.

3.1.3 Anonimnost imetnikov in uporaba psevdonimov

Se ne uporablja.

3.1.4 Pravila za interpretacijo različnih oblik imen

Razločevalno ime potrdila (subject) je sestavljeno iz črk angleške abecede. Drugi znaki se ustrezno pretvorijo.

Pravila pretvorbe:
Ä = A, ä=a, Á=A, á=a, Ö=O, ö=o, ë=e, Ë=E, é=e, É=E, ú=u, Ú=U, ü=u, Ü=U, Š=S, š=s, Č=C, č=c, Ć=C, ć=c, Ž=Z, ž=z, Đ=D, đ=d

Znake, ki niso navedeni, pretvori ponudnik storitev po svoji presoji.

3.1.5 Edinstvenost imen

Ponudnik storitev dodeli vsakemu imetniku potrdila edinstveno ime, ki je objavljeno v polju »subject« potrdila. Glej poglavje 3.1.2.

3.1.6 Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk

Ponudnik storitev dosledno upošteva pravila poimenovanja iz točk 3.1.1 in 3.1.2.
S strani uporabnika je prepovedano zahtevati imena, ki bi kršila avtorske pravice ali pravice industrijske lastnine tretjih oseb. Ponudnik storitev ne izvaja preverjanja morebitne kršitve avtorske in industrijske lastnine. Ponudnik storitev v teh primerih ne posreduje v morebitnih sporih.
Ponudnik storitev si pridržuje pravico zavrniti izdajo potrdila ali preklicati že izdana potrdila udeležencev spora.

3.2 Prva registracija

3.2.1 Metode dokazovanja lastništva zasebnega ključa

Posedovanje zasebnega ključa se preverja z uporabo splošno priznanih standardov:

- PKCS#10 (Public Key Cryptographic Standard #10) ali

- Certificate Management Protocol (CMP) ali
- Netscape SPKI (angl. Signed Public Key and Challenge, SPKAC).

3.2.2 Preverjanje istovetnosti organizacije

Pravna oseba se identificira z dokumentom, ki so podlaga za vpis v uradne evidence ali z izpisom iz uradnih evidenc. Za organizacije registrirane v Republiki Sloveniji sta to:

- sklep o vpisu v sodni register.
- izpis iz poslovnega registra Slovenije (Ajpes).

Pravno osebo zastopa zakoniti zastopnik ali pooblaščena oseba za oddajo vloge. Zakoniti zastopnik pravne osebe se preveri, kot je navedeno v poglavju 3.2.3.

3.2.3 Preverjanje istovetnosti za fizične osebe

Istovetnost fizične osebe se preveri s strani RA osebja ob fizični prisotnosti te osebe na osnovi predloženega veljavnega osebnega dokumenta.
Istovetnost fizične osebe se lahko preverja tudi na daljavo, s pomočjo sredstev elektronske identifikacije, ki izpolnjujejo pogoje iz 1(b) alineje 24. člena eIDAS.

3.2.4 Podatki o imetnikih potrdil, ki se ne preverjajo

Ponudnik storitev ne preverja verodostojnosti naslova elektronske pošte.

3.2.5 Preverjanje pooblastil

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

3.2.6 Merila za medsebojno povezovanje

Ponudnik storitev se povezuje z drugimi ponudniki storitev po lastni presoji in le v primerih, ko drugi ponudnik storitev izdaja primerljiva potrdila in zagotavlja vsaj enak nivo zaupanja.

3.3 Preverjanje istovetnosti pri obnovi potrdila

3.3.1 Preverjanje istovetnosti pri rutinski obnovi potrdil

Rutinska obnova potrdila je izdaja novega potrdila pred potekom veljavnosti obstoječega potrdila (reizdaja). Ker je bila prva izdaja potrdila izvedena po postopkih iz poglavja 3.2, se ob rutinski obnovi potrdila preverja točnost podatkov v sistemih ponudnika storitev.

3.3.2 Preverjanje istovetnosti pri obnovi potrdila po preklicu

Izvaja se po postopkih iz poglavja 3.2.

3.4 Preverjanje istovetnosti ob zahtevi za preklic potrdila

Uporabnik se lahko identificira preko katere koli ustrezne storitve NLB d.d. po enakem postopku, kot pri registraciji ali s kodo za preklic, ki jo je prejel ob registraciji.

4 Upravljanje s potrdili

4.1 Vloga za izdajo potrdila za fizične osebe in za pravne osebe za zaposlene

Potrdilo se izda na osnovi pravilno izpolnjene in podpisane Vloge za izdajo kvalificiranega potrdila in izpolnjenih identifikacijskih zahtev navedenih v poglavju 3.2.

4.1.1 Kdo lahko zaprosi za izdajo potrdila

- Za izdajo kvalificiranega potrdila za fizične osebe lahko zaprosijo osebe, ki izpolnjujejo zahteve poglavja 3.2.3 Preverjanje istovetnosti za fizične osebe.
- Za izdajo kvalificiranega potrdila za pravne osebe za zaposlene lahko zaprosi katera koli organizacija, ki izpolnjuje zahteve poglavja 3.2.2 Preverjanje istovetnosti organizacije.
- Za izdajo kvalificiranega potrdila za pravne osebe za elektronski žig lahko zaprosi katera koli organizacija, ki izpolnjuje zahteve poglavja 3.2.2 Preverjanje istovetnosti organizacije.
- Potrdila za storitev OCSP se izdaja samo za storitve v okviru ponudnika storitev zaupanja AC NLB. Uporabljanje se izvaja v okviru internih postopkov AC NLB.

4.1.2 Postopek obdelave vloge in odgovornosti

Kvalificirana potrdila za fizične osebe in Kvalificirana potrdila za zaposlene pri pravni osebi:
AC NLB preda bodočemu imetniku potrdila 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 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 s podatki za prevzem potrdila prevzeti v šestdesetih (60) dneh od izdaje, sicer veljavnost aktivacijskih kod poteče.

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

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

Kvalificirana potrdila za fizične osebe za oddaljen podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa:
Vsak 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 na šifrirnem modulu ponudnika storitev, ki ima potrdila o skladnosti s FIPS 140-2 level 3 in QSCD standardi.
Ključi so najmanj 2048 - bitni RSA.

Kvalificirana potrdila za fizične osebe za oddaljen podpis:
Vsak 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 na šifrirnem modulu ponudnika storitev, skladnosti s FIPS 140-2 level 3 in QSCD.
Ključi so najmanj 2048 - bitni RSA.

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

Kvalificirana potrdila za pravne osebe za elektronski žig:
AC NLB pooblaščencu pravne osebe preda podatke za prevzem potrdila osebno v zaprti kuverti.

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

Geslo za telefonski preklic služi izključno za identifikacijo pooblaščenca pravne osebe pri morebitnem preklicu potrdila preko telefona.

Pooblaščenec pravne osebe mora po prejemu obvestila s podatki za prevzem potrdila prevzeti v šestdesetih (60) dneh od izdaje, sicer veljavnost aktivacijskih kod poteče.

Pooblaščenec pravne osebe imetnika potrdila, mora ob prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti AC NLB oziroma zahtevati preklic.

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

Kvalificirana potrdila za pravne osebe za elektronski žig na napravi za ustvarjanje kvalificiranega elektronskega žiga :
V okviru kreiranja uporabnika in odobritve izdaje potrdila v CA aplikaciji, ki ga izpelje operativno osebje ponudnika storitev, se izvedejo naslednje aktivnosti:

- Na osnovi preverjene in odobrene vloge v registracijski pisarni se kreira uporabnika v CA aplikaciji.
    - Določitev razločevalnega imena (Subject) potrdila s podatki preverjenimi v okviru postopka registracije.
    - Določitev atributov (profil) potrdilo glede na tip potrdila (Kvalificirano potrdilo za elektronski žig, Kvalificirano potrdilo za elektronski žig z uporabo QSCD).
    - Generiranje aktivacijskih kod za prevzem potrdila (referenčna številka, aktivacijska koda).
- Po izvedenem postopku kreiranja uporabnika in odobritve izdaje potrdila v CA aplikaciji se uporabniku posreduje aktivacijske kode - uporabijo se kontaktni podatki pridobljeni v okviru postopka registracije in preverjanja identitete.

Potrdilo prevzame predstavnik pravne osebe, ki ga v svojih internih postopkih pooblasti oziroma določi pravna oseba. Pri temu morata tako pravna oseba kot tudi skrbnik, ki ga določi pravna oseba, upoštevati vsa določila Politike ACNLB. V okviru postopka prevzema potrdila se izvedejo sledeče aktivnosti:

- Generiranje para kriptografskih ključev v ustreznem kriptografskem modulu glede na tip potrdila. V primeru, da je potrdil izdano za kvalificiran elektronski žig, morajo biti ključi generirani na strojnem varnostnem modulu, ki ima potrdilo skladnosti s QSCD.
- Generiranje zahtevka za izdajo potrdila. Zahtevek mora biti generiran v obliki PKCS#10. Zahtevek mora v razločevalnem imenu (Subject) vsebovati polje CN, ki mora vsebovati niz podatkov enak referenčni številki.
- Prevzem potrdila se izvede preko spletnega vmesnika CA. Pri prevzemu je potrebno vpisati referenčno številko, avtorizacijsko kodo in zahtevek generiran v prejšnjem koraku.
- Po prevzemu se mora preveriti točnost podatkov v potrdilu. V primeru napak se potrdila ne sme uporabiti. Potrdilo se mora preklicati in o napaki v potrdili obvestiti ponudnika storitev (ACNLB) na kontaktni naslov (Politika ACNLB, poglavje 1.5.2).
- Potrdilo se uvozi oziroma uporabi v okviru aplikacije imetnika.

4.2 Obdelava vloge za izdajo potrdila

4.2.1 Postopki identifikacije in avtentikacije

Prijavna služba ponudnika storitev to izvaja v skladu s poglavjem 3.2.2 za pravne osebe in skladu s poglavjem 3.2.3 za fizične osebe.

4.2.2 Odobritev ali zavrnitev izdaje potrdila

- Ponudnik storitev lahko zavrne vlogo za izdajo potrdila v primeru s strani uporabnika prejetih nepravilnih ali pomanjkljivih podatkov ali v primeru neizpolnjenih obveznosti.
- V primeru, da je ugotovljeno neskladje podatkov v registracijski pisarni v postopku preverjanja vloge, se vloga zavrne ustno.
- V primeru neskladja podatkov z zalednimi sistemi, pa je uporabnik o zavrnitvi vloge obveščen po elektronski pošti.

4.2.3 Čas za obdelavo vloge za izdajo potrdila

Najkasneje v sedmih delovnih dneh od odobritve zahtevka, uporabnik prejme aktivacijske podatke. Veljavnost le-teh je 60 dni. Po tem roku aktivacijski podatki niso več uporabni.

4.3 Izdaja potrdila

4.3.1 Postopki ponudnika storitev ob izdaji potrdila

Postopki ob izdaji kvalificiranega potrdila za fizične osebe in potrdila za zaposlene pri pravni oseb so:

Prevzem:
AC NLB preda bodočemu imetniku potrdila 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 pošti v zaprti kuverti.

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

Aplikacija ponudnika storitev ob izdaji potrdila:

- Preveri veljavnost aktivacijskih podatkov (referenčne številke in avtorizacijske kode), ki so v zahtevku za izdajo potrdila.
- V skladu s poglavjem 3.2.1, preveri metode dokazovanja lastništva zasebnega ključa, da ima subjekt, ki je tvoril zahtevek za dostop do zasebnega ključa povezanega z javnim ključem, vsebovanim v zahtevku.
- Izda potrdilo, če so izpolnjeni vsi zgoraj navedeni pogoji.

Postopki ob izdaji kvalificiranega potrdila za pravne osebe za elektronski žig so:

Osebni prevzem:

- AC NLB preda pooblaščencu pravne osebe imetnika potrdila referenčno številko, geslo za prevzem potrdila in geslo za preklic potrdila osebno v zaprti kuverti.
- Po prevzemu potrdila postaneta referenčna številka in geslo za prevzem neuporabni za prevzem drugega potrdila.

Aplikacija ponudnika storitev ob izdaji potrdila:

- Preveri veljavnost aktivacijskih podatkov (referenčne številke in avtorizacijske kode), ki so v zahtevku za izdajo potrdila.

- V skladu s poglavjem 3.2.1 preveri metode dokazovanja lastništva zasebnega ključa, da ima subjekt, ki je tvoril zahtevek za dostop do zasebnega ključa povezanega z javnim ključem, vsebovanim v zahtevku.
- Izda potrdilo, če so izpolnjeni vsi zgoraj navedeni pogoji.
- Objavi potrdilo v internem imeniku LDAP.

Postopki ob izdaji kvalificiranega potrdila za pravne osebe za elektronski žig na napravi za ustvarjanje kvalificiranega elektronskega žiga:

Osebni prevzem (ko je potrdilo izdano na pametni kartici):
AC NLB preda pooblaščencu pravne osebe imetnika potrdila osebno izroči pametno kartico in PIN za dostop do privatnega ključa na pametni kartici, v zaprti kuverti.

Postopki ob izdaji kvalificiranega potrdila za fizične osebe za oddaljen podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa:
Izdaja potrdila za fizične osebe za oddaljen podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa, se izvede s prijavo na storitev z eno od močnih avtentikacijskih metod, kjer je identiteta prijavljenega nesporna:

- S kvalificiranim potrdilom za fizične osebe.
- S kvalificiranim potrdilom za zaposlene pri pravni osebi.
- Z uporabo dvo-faktorske avtentikacije (Uporabniško ime/Geslo in enkratno geslo (strojni generator gesel ali programski generator gesel)), ki je bila dodeljena na osnovi postopka preverjanja istovetnosti, ekvivalentnega postopku, kot velja za kvalificirana potrdila (glej 3.2.3).

Kvalificirana potrdila za fizične osebe za oddaljen podpis:
Izdaja kvalificiranega potrdila za fizične osebe za oddaljen podpis, se izvede s prijavo na storitev z eno od močnih avtentikacijskih metod, kjer je identiteta prijavljenega nesporna:

- S kvalificiranim potrdilom za fizične osebe
- S kvalificiranim potrdilom za zaposlene pri pravni osebi
- Z uporabo dvofaktorske avtentikacije (Uporabniško ime/Geslo in enkratno geslo (strojni generator gesel ali programski generator gesel)), ki je bila dodeljena na osnovi postopka preverjanja istovetnosti, ekvivalentnega postopku kot velja za kvalificirana potrdila (glej 3.2.3).

4.3.2 Obvestilo imetniku o izdaji potrdila

Imetniki so v okviru postopka za prevzem potrdila obveščeni o uspešni ali neuspešni izdaji potrdila.

4.4 Prevzem potrdila

4.4.1 Postopek prevzema potrdila

- Standardna kvalificirana potrdila za fizične osebe in za zaposlene pri pravni osebi se prevzemajo preko spletnega brskalnika.
- Navodila za prevzem standardnega kvalificiranega potrdila, so opisana v elektronski pošti, ki jo prejme uporabnik ob prejemu enega dela aktivacijskih podatkov.
- Uporabnik lahko prevzame potrdilo samo z ustrezno referenčno številko in aktivacijsko kodo. Ti sta enkratni in časovno omejeni (60 dni).
- Če uporabnik ne prevzame potrdilo v roku 60 dni, mora ponoviti postopek opisan v točki 4.1.
- Kvalificirana potrdila za fizične osebe za oddaljen podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa se prevzemajo preko aplikacije za varno podpisovanje elektronskih dokumentov.

4.4.2 Postopek potrditve prevzema potrdila

Kvalificirana potrdila za fizične osebe in kvalificirana potrdila za zaposlene pri pravni osebi:
Dodatno potrjevanje s strani imetnika ni potrebno.

Kvalificirana potrdila za fizične osebe za oddaljen podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa:

- V primeru kvalificiranega elektronskega podpisa imetnik potrdi prevzem potrdila z vpisom gesla, ki ga uporabi vsakič, ko dostopa do svojega potrdila in z eno od metod močne avtentikacije pri dostopu.

- V primeru naprednega elektronskega podpisa imetnik potrdi prevzem potrdila z dodatno potrditvijo istovetnosti z eno od metod močne avtentikacije, ki jo uporabi vsakič, ko dostopa do svojega potrdila.

4.4.3 Objava potrdila

Potrdila se ne objavljajo v javnem imeniku.

4.4.4 Obveščanje drugih udeležencev o izdaji potrdila

Ni predvideno.

4.5 Uporaba ključev in potrdil

4.5.1 Uporaba ključev in potrdil s strani imetnikov

V razširjenem polju keyUsage (poglavje 6.1.7), so označeni nameni, za katere lahko imetnik uporablja ključe in potrdila.

Imetniki so dolžni varovati svoje zasebne ključe, da se prepreči izguba, razkritje, sprememba ali nepooblaščena uporaba (glej poglavje 9.6.3).

4.5.2 Uporaba potrdil s strani tretjih oseb

Tretje osebe so dolžne omejiti uporabo potrdil le na namene opredeljene v poglavju 1.4.

4.6 Obnova potrdil brez spremembe ključev

Se ne uporablja. Imetniki morajo ob vsaki obnovi generirati nov par kriptografskih ključev.

4.7 Obnova potrdil

4.7.1 Okoliščine obnove potrdil

Gre za redno obnovo, obnovo po izteku veljavnosti obstoječega potrdila in obnovo po preklicu potrdila.

Redna obnova potrdil se izvede skladno s preverjanjem identitete s poglavjem 3.3.1.

4.7.2 Kdo lahko zahteva obnovo potrdila

Obnovo potrdila, lahko izvedejo isti subjekti, kot za prvo izdajo, skladno s poglavjem 4.1.

4.7.3 Obdelava zahtevkov za obnovo potrdil

Obnova kvalificiranih potrdil poteka po istem postopku kot prevzem prvega potrdila.

4.7.4 Obvestilo imetniku o izdaji novega potrdila

Glej poglavje 4.3.2.

4.7.5 Postopek potrditve prevzema obnovljenega potrdila

Glej poglavje 4.4.2.

4.7.6 Objava obnovljenega potrdila

Glej poglavje 4.4.3.

4.7.7 Obveščanje drugih udeležencev o izdaji potrdila

Glej poglavje 4.4.4.

4.8 Sprememba potrdila

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

4.8.1 Okoliščine v katerih se izvede sprememba potrdil

Sprememba potrdila se izvede, kadar se je spremenil eden od podatkov vsebovanih v potrdilu:

- Podatki vsebovani v razločevalnem imenu potrdila (ime ali priimek fizične osebe, davčna številka).
- Alternativno ime imetnika (elektronska pošta).

4.8.2 Kdo lahko zahteva spremembo potrdila

Spremembo potrdila lahko zahtevajo isti subjekti kot izdajo potrdila. Glej poglavje 4.1.1.

4.8.3 Obdelava zahtevkov za spremembo potrdila

Izvede se po istem postopku kot pri zahtevku za prvo izdajo digitalnega potrdila Glej poglavji 4.2 in 4.3.

4.8.4 Obvestilo imetniku o izdaji spremenjenega potrdila

Glej poglavje 4.3.2.

4.8.5 Postopek potrditve prevzema spremenjenega potrdila

Glej poglavje 4.4.2.

4.8.6 Objava spremenjenega potrdila

Glej poglavje 4.4.3.

4.8.7 Obveščanje drugih udeležencev o izdaji spremenjenega potrdila

Glej poglavje 4.4.4.

4.9 Začasna ukinitev veljavnosti in preklic potrdila

4.9.1 Okoliščine preklica

Ponudnik storitev prekliče potrdilo:

- Ob domnevni ali dejanski ogroženosti zasebnih ključev.
- Ob spremembi podatkov v potrdilu, ki zahtevajo izdajo novega.
- Ob neizpolnjevanju obveznosti iz točke 9.6.3.
- V primeru smrti imetnika potrdila.
- Če to zahteva imetnik potrdila.
- V primeru smrti imetnika potrdila ali spremembe okoliščin, ki bistveno vplivajo na veljavnost potrdila.
- Ob napačnem podatku v potrdilu, oziroma je bilo potrdilo izdano na podlagi napačnih podatkov.
- Ob prenehanju delovanja ponudnika storitev ali prepovedi delovanja ponudnika storitev in njegove dejavnosti ni prevzel drug ponudnik storitev.
- Ob ogroženosti informacijskega sistema ponudnika storitev ali podatkov za preverjanje podpisa, na način, ki vpliva na zanesljivost potrdila.
- Ob neizpolnjevanju obveznosti iz točke 9.6.3 s strani naročnika.

Imetnik potrdila je dolžan ponudniku storitev nemudoma prijaviti vsako domnevno ali dejansko ogrožanje zasebnega ključa ter vse podatke, ki so relevantni za morebiten preklic pooblastila.

4.9.2 Kdo lahko zahteva preklic

Preklic potrdila lahko zahteva:

- Osebje ponudnika storitev.
- Imetnik potrdila.
- Pristojno sodišče, sodnik za prekrške ali upravni organ.
- Dedič ali zakoniti zastopnik.
- Tretja oseba, če potrdilo vsebuje podatke o tretji osebi ali če obstaja nevarnost zlorabe.

4.9.3 Postopki za preklic

- Zahtevek za preklic se lahko poda:
    - osebno z oddajo vlogoe za preklic osebju ponudnika storitev,
    - po telefonu na številko za preklic z uporabo kode za preklic.
- Po uspešno izvedenem postopku preverjanja istovetnosti imetnika potrdila RA službe, se poda zahteva za preklic v center ponudnika storitev.
- Ponudnik storitev izvede preklic potrdila.

4.9.4 Čas za posredovanje vloge za preklic

V primeru okoliščin, ki zahtevajo preklic potrdila, mora imetnik zahtevo za preklic posredovati v najkrajšem možnem času.

4.9.5 Čas od vloge za preklic do preklica

Preklic zaradi neizpolnjevanja obveznosti imetnika potrdila, izvede ponudnik storitev takoj. Preklici iz drugih razlogov se izvedejo najkasneje v 60 minutah po prejemu zahtevka.

4.9.6 Obveza preverjanja registra preklicanih potrdil

- Preverjanje statusa potrdil se mora izvesti vsaj preko enega načina, to je preko najnovejše liste preklicanih potrdil CRL ali preko storitve OCSP.

- Preverjanje v registru preklicanih potrdil se izvaja pred uporabo javnega ključa vsebovanega v potrdilu AC NLB.
- Merodajen je najnovejši objavljeni register preklicanih potrdil, objavljen na spletnem naslovu v razširitvenem polju vsakega potrdila.
- Register preklicanih potrdil je podpisan z istim zasebnim ključem ponudnika storitev, kot se uporablja za podpis potrdil.

4.9.7 Pogostost objav registrov preklicanih potrdil

Nov register preklicanih potrdil se objavi vsaj vsakih osem ur oziroma takoj, vendar najkasneje 10 minut po preklicu potrdila. Veljavnost vsakokratnega registra ponudnika storitev preklicanih potrdil je do objave novega registra preklicanih potrdil.

4.9.8 Dovoljena zakasnitev pri objavi registrov preklicanih potrdil

Čas med prejemom preklica v skladu s točko 4.9 in javno objavo preklicanih potrdil v registru preklicanih potrdil je največ 10 minut.

4.9.9 Storitev sprotnega preverjanja statusa potrdil

Poleg preverjana statusa potrdil na listi preklicanih potrdil CRL je možno tudi sprotno preverjanje statusa potrdil preko storitve sprotnega preverjanja statusa potrdil OCSP.

Spletni naslov storitve OCSP je naveden v vsakem potrdilu v razširitvenem polju Authority Information Access (RFC 5280: id-pe-authorityInfoAccess/id-ad-ocsp).

4.9.10 Obveza sprotnega preverjanja statusa preklicanih potrdil

Tretje osebe morajo pred uporabo potrdila, na katerega se zanašajo, preveriti njegovo veljavnost. Preverjanje statusa morajo izvesti vsaj preko enega načina. To je preko najnovejše liste preklicanih potrdil CRL ali preko storitve OCSP.

4.9.11 Ostale oblike objavljanja preklicanih potrdil

Ponudnik storitev AC NLB ne objavlja ostalih oblik preklicanih potrdil.

4.9.12 Posebne zahteve glede zlorabe ključa

Glej 4.9.2.

4.9.13 Okoliščine za začasno razveljavitev veljavnosti potrdila

Ponudnik storitev uporablja začasno razveljavitev veljavnosti samo v okviru internih postopkov potrjevanja preklica.

4.10 Storitev objavljanja statusa potrdil

4.10.1 Tehnične lastnosti storitve

Status potrdil je objavljen z uporabo registra preklicanih potrdil v skladu z (X.509 Certificate Revocation List) in RFC5280. Register preklicanih potrdil je dostopen preko LDAP in http protokola.

Točen naslov objave registra preklicanih potrdil je vsebovan v razširitvenem polju vsakega izdanega potrdila, kot je navedeno v poglavju 7.1.2.

4.10.2 Razpoložljivost storitve dostopa do registra preklicanih potrdil

Razpoložljivost je 365x24x7.

4.10.3 Dodatne možnosti

Ni dodatnih možnosti.

4.11 Trajanje naročniškega razmerja

Naročniško razmerje začne teči s prevzemom potrdila. Naročniško razmerje je sklenjeno za obdobje veljavnosti potrdila.
Razmerje med ponudnikom storitev AC NLB in naročnikom preneha:

- Ob poteku veljavnosti potrdila, če ga naročnik ne podaljša.
- Ob preklicu potrdila, če imetnik ne zaprosi za izdajo novega potrdila.
- Če naročnik krši obveznosti politike, lahko ponudnik storitev prekine naročniško razmerje.

4.12 Varnostno kopiranje in odkrivanje zasebnega ključa

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

Se ne uporablja. Ponudnik storitev AC NLB ne hrani varnostnih kopij zasebnih ključev.

4.12.2 Zaščita zasebnega ključa in postopek prenosa

Se ne uporablja.

4.13 Dodatne možnosti

Niso predvidene.

5 Fizično varovanje, organizacijski varnostni ukrepi in zahteve za osebje

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

5.1 Fizično varovanje

5.1.1 Lokacija in konstrukcija prostorov ponudnika storitev

Dejavnosti ponudnika storitev se izvajajo v varovanih prostorih in na varni lokaciji.

5.1.2 Fizični dostop

Dostop do posameznih delov infrastrukture ponudnika storitev ima le pooblaščeno operativno osebje v skladu z zaupanimi nalogami. Tretje osebe lahko dostopajo le v spremstvu pooblaščenga operativnega osebja. Vsi dostopi do prostorov ponudnika storitev se beležijo in varujejo v skladu z notranjimi pravili ponudnika storitev.

5.1.3 Napajanje in klimatske naprave

Center ponudnika storitev je opremljen s:
- Sistemom za neprekinjeno napajanje za zagotavljanje napajanja strežnikom in mrežnim napravam.
- Klimatsko napravo za kontrolo temperature in vlage.

5.1.4 Zaščita pred poplavo

Izvedena je s sistemom proti izlitju vode in sistemom za prezračevanje.

5.1.5 Zaščita pred ognjem

Prostori ponudnika storitev so opremljeni s protipožarnim sistemom.

5.1.6 Shranjevanje medijev

AC NLB shranjuje 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.

5.1.7 Odstranjevanje odpadkov

Papirna dokumentacija se uniči na varen način. Vsebina medijev, na katerih se hranijo podatki, je pred odstranitvijo izbrisana, v nasprotnem primeru ponudnik storitev zagotovi fizično uničenje medija.

5.1.8 Hranjenje na oddaljeni lokaciji

V prostorih na oddaljeni lokaciji je zagotovljena vsaj enaka stopnja varnosti, kot na osnovni lokaciji.

5.2 Organizacijski varnostni ukrepi

5.2.1 Organiziranost ponudnika storitev

Ponudnik storitev deluje v okviru NLB d.d. in ga sestavlja:
- Upravni odbor ponudnika storitev AC NLB.
- Operativno osebje ponudnika storitev.

Neodvisni nadzor v smislu opravljanje funkcije notranje revizije AC NLB opravlja Center notranje revizije NLB d.d. (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.
CNR je tudi v funkciji nadzora delovanja operativnega osebja in revidiranja novih različic politike, oziroma javnega dela notranjih pravil ponudnika storitev.

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

Vloga	Osnovne naloge
Upravni odbor AC NLB:	Upravni odbor ima funkcije imenovanja in nadzora delovanja operativnega osebja, revidiranja in odobravanja novih različic politike oz. javnega dela notranjih pravil ponudnika storitev. Upravni odbor sestavljajo:

	• Vodja upravnega odbora • Operativni vodja • Varnostni nadzornik • Pravnik
Upravljalec sistema ACNLB RootCA	Konfiguracija ter izvajanje vzdrževanja aplikativne CA programske opreme ponudnika storitev na RootCA
Administrator strojnega varnostnega modula sistema ACNLB RootCA	Upravljanje strojnega kriptografskega modula (HSM) na sistemskem nivoju RootCA.
Skrbnik kriptografskega ključa ACNLB RootCA	Upravljanje s kriptografskimi ključi, shranjenimi na strojnem kriptografskem modulu (HSM) za RootCA.
CA nadzornik ACNLB RootCA	Nastavljanje politik, upravljanje z ostalimi CA administratorji.
Upravljalec sistema ACNLB SubCA	Konfiguracija ter izvajanje vzdrževanja aplikativne CA programske opreme ponudnika storitev na SubCA.
Administrator strojnega varnostnega modula sistema ACNLB SubCA	Upravljanje strojnega kriptografskega modula (HSM) na sistemskem nivoju SubCA.
Skrbnik kriptografskega ključa ACNLB SubCA	Upravljanje s kriptografskimi ključi, shranjenimi na strojnem kriptografskem modulu (HSM) za SubCA.
Sistemski administrator ACNLB RootCA in ACNLB SubCA	Konfiguriranje in vzdrževanje sistemske strojne in programske opreme.
CA nadzornik ACNLB SubCA	Nastavljanje politik, upravljanje z ostalimi CA administratorji.
CA Administrator ACNLB SubCA	Skrbi za dnevne obdelave, obnavljanje certifikatov in spremembe v zvezi z uporabniki.
Upravljalec omrežja ACNLB RootCA in ACNLB SubCA	Skrbi za povezave infrastrukture AC NLB v računalniško omrežje NLB in ostala omrežja.

5.2.2 Število oseb, potrebnih za izvedbo postopka

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 potrdili.
- Varovanje in kontrola.
- Pravno-administrativno.

Vse varnostno občutljive operacije se vršijo po principu štirih oči, kar pomeni, da sta za izvedbo postopka hkrati prisotna vsaj dva člana osebja ponudnika storitev AC NLB.

5.2.3 Preverjanje istovetnosti operativnega osebja

- Z uporabo mehanizmov in delovanja CA aplikacije in sistemske programske opreme je omejeno delovanje osebja ponudnika storitev, glede na njihove funkcije.
- Uporabniški računi in potrdila, ki so potrebna za dostop do programske ali sistemske opreme so ustvarjena ali izdana, določeni fizični osebi.
- Pred dodelitvijo nalog in pooblastil se osebje ponudnika storitev preveri v skladu s točko 5.3.

5.2.4 Nezdružljivost nalog

Naloge so razdeljene na ločene skupine zaupanja vrednih oseb. Zloraba je onemogočena z organizacijskimi in tehničnimi ukrepi:

- Število oseb, dodeljenih po vlogah.
- Pravilo štirih oči.
- Omejitev fizičnega dostopa.

5.3 Zahteve za osebje ponudnika storitev

5.3.1 Kvalifikacije, izkušnje in varnostno preverjanje

NLB d.d. (ponudnik storitev) zaposluje osebje z ustreznimi kvalifikacijami v skladu s politiko zaposlovanja v NLB d.d.

5.3.2 Preverjanje primernosti osebja

Kadrovska služba NLB d.d. skrbi za preverjanje primernosti kadra za ponudnika storitev, v okviru svojih postopkov. Osebje je pred imenovanjem dolžno izročiti potrdilo iz katerega izhaja, da ni bilo kaznovano za katerokoli kaznivo dejanje.

5.3.3 Usposabljanje osebja

Osebje ponudnika storitev se redno izobražuje na področjih:

- Programska oprema CA.
- Varnost komunikacijskih in informacijskih sistemov.
- Specifična znanja pri za opravljanje svojih funkcij.
- Ukrepanje ob incidentih in obnova poslovanja (angl. Disaster Recovery).

Osebje ponudnika storitev z RA nalogami se izobražuje v okviru rednega dela v NLB d.d.

5.3.4 Pogostost dodatnih usposabljanj

Usposabljanja se izvajajo po potrebi, glede na zahteve ponudnika storitev in vrste operativnih zahtev ter sprememb vezanih na infrastrukturo ponudnika storitev.

5.3.5 Kroženje med delovnimi mesti

Kroženje med delovnimi mesti ni predvideno.

5.3.6 Ukrepi ob zlorabi pooblastil

V primeru zlorabe pooblastil se osebju prekličejo vsa pooblastila in onemogočijo dostopi, potrebni za opravljanje funkcije.

V primeru ugotovljenih kršitev postopkov ali zlorabe pooblastil se zoper osebje lahko uvedejo vsi postopki skladno s predpisi, ki veljajo v NLB d.d.

5.3.7 Zahteve za pogodbene in zunanje izvajalce

Za funkcije, navedene v poglavju 5.2.1 se ne angažira zunanjih izvajalcev.

5.3.8 Dokumentacija za osebje ponudnika storitev

Javno dostopna dokumentacija se nahaja na spletni strani, kot je opisano v točki 2. Osebju ponudnika storitev, so na voljo tudi interni operativni priročniki, dokumentacija programske in strojne opreme, infrastrukturni načrti in sheme ter priročniki iz sklopa izobraževanj glede na funkcijo osebja ponudnika storitev.

5.4 Postopki zbiranja in upravljanja revizijskih sledi

5.4.1 Vrste beleženih dogodkov

Revizijski podatki se zbirajo avtomatsko in ročno:

- Dogodki vezani na delo s potrdili.
- Dogodki vezani na delo ponudnika storitev.
- Dogodki na operacijskih sistemih, strojni opremi, mrežni opremi.
- Dogodki vezani s fizičnim dostopom do sistemov ponudnika storitev.
- Dogodki vezani na kadrovske spremembe ponudnika storitev.

5.4.2 Pogostost pregleda revizijskih dnevnikov

Osebje ponudnika storitev pregleduje revizijske dnevnike in izvaja naslednje aktivnosti:

- Dnevno pregledovanje avtomatiziranih sporočil s sistema AC NLB.
- Mesečno pregledovanje strojne opreme, mrežnih dogodkov in fizičnih dostopov do sistemov ponudnika storitev.
- Ob dogodku: izvedba analize v primeru suma odstopanja od rednega delovanja.

5.4.3 Obdobje hranjenja revizijskih dnevnikov

Podatki se hranijo najmanj, kot je trajanje potrdil + sedem (7) let.

5.4.4 Zaščita revizijskih dnevnikov

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

5.4.5 Varnostne kopije revizijskih dnevnikov

Dnevniki se vsak dan hranijo na disk in se prenašajo tudi na rezervno lokacijo. Za izdelavo varnostnih kopij so zadolženi skrbniki sistemov.

5.4.6 Način zbiranja revizijskih dnevnikov

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

Beleženi dogodki	**Zbiranje podatkov**	**Odgovorna oseba/sistem**
Dogodki, povezani s CA uporabniki	avtomatsko	CA aplikacija
Dogodki, povezani s CA ključi	avtomatsko	CA aplikacija
Dogodki, povezani s CA, RA aplikacijo	avtomatsko	CA aplikacija
Dogodki na operacijskem sistemu	avtomatsko	Operacijski sistem
Dogodki na mreži	avtomatsko	Usmerjevalniki, operacijski sistem
Backup/restore CA baze uporabnikov	avtomatsko	CA aplikacija, operacijski sistem
Backup/restore CA logov, konfiguracije	avtomatsko	CA aplikacija, operacijski sistem
Backup/restore direktorija	avtomatsko	Direktorij aplikacija, Operacijski sistem
Fizični dostop do CA	avtomatsko	CA osebje

Spremembe konfiguracije HW na sistemu	Ročno	CA osebje
Vzdrževalna dela na sistemu/prostoru	Ročno	CA osebje
Kadrovske spremembe	Ročno	CA osebje
Uničenje za to predvidenih podatkov	Ročno	CA osebje

5.4.7 Obveščanje povzročitelja dogodka

Povzročitelja dogodka v dnevniku o tem ni treba obvestiti.

5.4.8 Ocena tveganja

Ponudnik storitev ima narejeno oceno tveganja, ki jo redno pregleduje, dopolnjuje in osvežuje.

5.5 Arhiviranje podatkov

5.5.1 Vrste arhiviranih podatkov

Ponudnik storitev hrani naslednje podatke:

- Revizijske dnevnike iz točke 5.4.5.
- Pogodbe z uporabniki in njihove vloge.
- Vloge o preklicih potrdil in prijave ogrožanja ključev.
- Potrdila, različice politik oz. javnih delov notranjih pravil ponudnika storitev.

5.5.2 Čas hrambe

Arhivirani podatki se hranijo najmanj, kot je trajanje potrdil + sedem (7) let.

5.5.3 Zaščita arhiva

Varnostna kopija arhiva se hrani na drugi lokaciji, zaščitena z enakimi varnostnimi mehanizmi, kot so vzpostavljeni na osnovni lokaciji.

5.5.4 Varnostna kopija arhiva

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

5.5.5 Zahteva za časovno žigosanje zapiskov

Časovno žigosanje zapiskov ni predpisano.

5.5.6 Sistem za arhiviranje (interni ali zunanji)

Arhivski podatki se hranijo na infrastrukturi ponudnika storitev in infrastrukturi NLB d.d.

5.5.7 Postopek za dostop do arhivskih podatkov in verifikacija

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

5.6 Obnova potrdila ponudnika storitev

Ponudnik storitev ob vsaki obnovi lastnega potrdila tvori nov par ključev. Postopek je izveden nadzorovano v varnih prostorih in ob upoštevanju ostalih določil poglavja 5 Fizično varovanje, organizacijski varnostni ukrepi in zahteve za osebje, ter določil poglavja 6 Tehnične varnostne zahteve.

5.7 Postopki v primeru ogrožanja zasebnega ključa in okrevalni načrt

5.7.1 Postopki za odzivanje na varnostne incidente in nepravilnosti

Obvladovanje varnostnega incidenta poteka po naslednjih fazah:

- Priprava na incident.
- Zaznava in prijava incidenta.
- Ukrepanje ob incidentu.
- Omejitev posledic incidenta.
- Zavarovanje sledi.
- Odstranitev vzroka.
- Vzpostavitev delujočega stanja.
- Priprava zaključnega poročila.
- Obveščanje vodstva IT in ostalih organov v NLB d.d. ter regulatorja .
- Ponudnik storitev izvaja postopke za odzivanje na varnostne incidente in nepravilnosti v skladu z internimi dokumenti NLB d.d.

5.7.2 Uničenje programske, strojne opreme ali podatkov

V primeru okvare strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ ponudnika storitev ni bil uničen, bodo storitve ponudnika storitev vzpostavljene nazaj v najkrajšem možnem času.

5.7.3 Ogrožanje ali uničenje zasebnega ključa ponudnika storitev

V primeru ogrožanja zasebnega ključa ponudnika storitev, ponudnik storitve:

- o tem obvesti vse, ki imajo z njim sklenjeno kakršno koli naročniško razmerje,
- prekliče vsa izdana potrdil uporabnikom,
- objavi preklic potrdila ponudnika storitev,
- izdela nov ključ ponudnika storitev,
- izda nova potrdila uporabnikom, ki so jim bila potrdila preklicana.

V primeru uničenja zasebnega ključa ponudnika storitev, ponudnih storitev:

- o tem obvesti vse, ki imajo z njim sklenjeno kakršno koli naročniško razmerje,
- umakne vse CRL liste, podpisane s tem ključem in ukine storitev OCSP,
- izdela nov ključ ponudnika storitev,
- izda nova potrdila uporabnikom, ki so jim bila preklicana potrdila.

5.7.4 Okrevalni načrt v primeru naravne in druge nesreče

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

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

5.8 Prenehanje delovanja ponudnika storitev

Če ponudnik storitev preneha z opravljanjem storitve, prekliče vsa potrdila, ki jih je do tedaj izdal, zagotovi objavo registra preklicanih potrdil in hrambo arhiva za obdobje, kot je določeno v 5.5.2.

Če ponudnik storitev AC NLB preneha z delovanjem, prekliče vsa potrdila, ki jih je do tedaj izdal, vodenje registra preklicanih potrdil in hrambo arhiva pa preda drugemu ponudniku storitev.

6 Tehnične varnostne zahteve

6.1 Tvorjenje in namestitev para ključev

6.1.1 Tvorjenje para ključev

Par ključev ponudnika storitev za podpisovanje je ustvarjen ob namestitvi CA-programske opreme v okviru nadzorovanega in dokumentiranega postopka. Uporabljena je zaščita, ki velja za prostore ponudnika storitev [poglavje 5.1], večkratno preverjanje istovetnosti pooblaščenih oseb [poglavje 6.2.2] in strojni šifrirni modul (HSM – Hardware Security Module) [poglavje 6.2.1].

Ustvarjanje ključev uporabnikov je v domeni aplikacijskega okolja uporabnika. Za vse vrste potrdil, ki jih izdaja ponudnik storitev AC NLB, se par ključev za podpisovanje ustvari v aplikaciji na strani uporabnika oziroma na pametni kartici.

6.1.2 Prenos zasebnega ključa imetniku

Par ključev za podpisovanje se vedno ustvari pod nadzorom uporabnika. Zasebni ključ za podpisovanje, se nikdar ne hrani na strojni ali programski opremi ponudnika storitev, razen za kvalificirana potrdila za fizične osebe za oddaljen podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa, kjer se zasebni ključ hrani na posebni certificirani strojni opremi ponudnika storitev (glej 6.2.1).

6.1.3 Prenos imetnikovega javnega ključa ponudnika storitev

Javni ključ za podpisovanje, imetniki potrdil dostavijo ponudniku storitev po protokolu PKCS#10 ali SPKAC.

6.1.4 Dostop do javnega ključa ponudnika storitev

Javni ključi ponudnika storitev so dostopni na naslovih:

- https://www.nlb.si/images/content/_doc/ACNLB.cer

6.1.5 Dolžina asimetričnega ključa

Zasebni ključi ponudnika storitev za podpisovanje so dolžin:

- ACNLB RootCA in ACNLB SubCA: RSA 3072 bitov
- ACNLB RSA: 2048 bitov

Uporabniki morajo ustvariti RSA par ključev dolžine najmanj 2048 bitov.

6.1.6 Parametri za generiranje javnih ključev in preverjanje parametrov

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

6.1.7 Namen ključev in potrdil (definirani v X.509 v3 keyUsage in extKeyUsage)

Kvalificirana potrdila za elektronski podpis:
- keyUsage: nonRepudiation, digitalSigniture, keyEncipherment

Kvalificirana potrdila za oddaljen elektronski podpis
- keyUsage:: nonRepudiation

Kvalificirana potrdila za elektronski žig:
- keyUsage: nonRepudiation, digitalSigniture

Potrdila za ostale namene:
- keyUsage: nonRepudiation, digitalSigniture, keyEncipherment

Potrdila za OCSP:
- keyUsage: digitalSigniture
- extKeyUsage: id-kp-OCSPSigning

6.1.7.1 Korenski izdajatelj

Zasebni ključ ponudnika storitev se uporablja samo za podpisovanje podrejenih ponudnikov storitev, registrov preklicanih potrdil za storitev OCSP in skrbniških potrdil potrebnih za upravljanje aplikacije korenskega izdajatelja.

6.1.7.2 Izdajatelj potrdil uporabnikom (AC NLB SubCA)

Namen uporabe ključev je označen v razširitvenem polju keyUsage, vsakega izdanega potrdila v skladu s priporočili RFC 5280.

Zasebni ključ ponudnika storitve se uporablja samo za podpisovanje potrdil in registrov preklicanih potrdil. Javni ključ ponudnika storitve, se uporablja za preverjanje veljavnosti potrdil in registrov preklicanih potrdil.

6.2 Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov

6.2.1 Standardi za kriptografski modul

Ustvarjanje kriptografskih ključev ponudnika storitve za digitalni podpis ter digitalni podpis s kriptografskimi ključi ponudnika storitve se izvaja na strojnem varnostnem modulu (HSM), ki ima potrdilo o skladnosti s FIPS 140-2 level 3.

Ustvarjanje kriptografskih ključev imetnikov potrdil za oddaljeni podpis ter podpis se izvaja na strojnem varnostnem modulu (HSM), ki ima potrdilo o skladnosti s FIPS 140-2 level 3 in QSCD.

Vse ostale kriptografske operacije CA aplikacije ponudnika storitev se izvajajo v kriptografskih modulih s stopnjo najmanj FIPS 140-2 level 2.

6.2.2 Nadzor zasebnega ključa z pooblaščenimi osebami

Operacije so navedene v točki 5.2.2.

6.2.3 Odkrivanje (angl. Escrow) zasebnega ključa

Ponudnik storitev ne podpira odkrivanja zasebnih ključev.

6.2.4 Varnostno kopiranje zasebnih ključev

Pri kreiranju zasebnega ključa ponudnika storitve , se zasebni ključ ponudnika storitev izdela na primarnem in sekundarnem kriptografskem modulu istočasno. Ni dodatnega kopiranja zasebnega ključa ponudnika storitve.

Imetniških zasebnih ključev za podpisovanje, se ne hrani, razen za kvalificirana potrdila za fizične osebe za oddaljen podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa, kjer se zasebni ključ hrani na posebni strojni opremi ponudnika storitev (glej 6.2.1).

6.2.5 Arhiviranje zasebnega ključa

Glej 6.2.4.

6.2.6 Prenos zasebnega ključa v kriptografski modul in iz njega

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

6.2.7 Hranjenje zasebnega ključa ponudnika storitev v kriptografskem modulu

Ključi ponudnika storitev se uporabljajo v strojnem varnostnem modulu, v katerem so bili tvorjeni, oziroma, na katerem je bila odobrena in omogočena uporaba.

6.2.8 Postopek za aktiviranje zasebnega ključa

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

6.2.9 Postopek za deaktiviranje zasebnega ključa

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

6.2.10 Postopek za uničenje zasebnega ključa

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

6.2.11 Stopnja varnosti kriptografskih modulov

Glej 6.2.1.

6.3 Ostali vidiki upravljanja s pari ključev

Ni ostalih vidikov.

6.3.1 Arhiviranje javnega ključa

Se izvaja po postopkih iz poglavja 5.5 Arhiviranje podatkov.

6.3.2 Obdobje veljavnosti ključev in potrdil

- Javni ključi ponudnika storitev za overjanje imajo veljavnost:
    - Korenski izdajatelj 20 let.
    - Podrejeni izdajatelji do 20 let.
- Imetniški javni ključ za overjanje velja do 5 let.
- Imetniški javni ključ za šifriranje in/ali avtentikacijo velja do 5 let.
- Javni ključ storitve OCSP velja do 3 let-a.

Veljavnost imetniških ključev je lahko do 5 let. Ponudnik storitev lahko kadarkoli prilagodi veljavnost posameznih imetniških ključev glede na politiko in vrsto potrdila.

6.4 Aktivacijski podatki

6.4.1 Generiranje in instalacija aktivacijskih podatkov

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

6.4.2 Zaščita aktivacijskih podatkov

- Avtorizacijske kode in referenčne številke se varno ustvarijo v aplikativni programski opremi CA ponudnika storitev in shranijo šifrirani v bazi.
- Avtorizacijske kode se tiskajo na slepe kuverte.
- Referenčna številka in avtorizacijska koda se dostavita naročniku po različnih komunikacijskih kanalih.
- Avtorizacijska koda se dostavi naročniku s pisemsko pošiljko.
- Uporabniki morajo do prevzema potrdila skrbno varovati vse aktivacijske podatke.

6.4.3 Drugi vidiki aktivacijskih podatkov

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

6.5 Varnostne zahteve za računalnike

6.5.1 Specifične tehnične varnostne zahteve za računalnike

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

- Nadzor dostopa do CA-postopkov in dodeljenih pooblastil za opravljanje nalog.
- Razdelitev nalog za posamezno funkcijo.
- Uporabo šifrirnih modulov za hranjenje kriptografskih ključev osebja ponudnika storitev.
- Varno sejo med aplikativno programsko opremo CA in aplikacijo za prevzem potrdil
- Šifrirano bazo podatkov ponudnika storitev.
- Varen arhiv ponudnika storitev in uporabniških kriptografskih ključev ter varnostnih beležk.
- Varnostne beležke vseh varnostno veljavnih dogodkov.
- Vzpostavljene mehanizme restavriranja sistema, šifrirnih ključev ponudnika storitev ter baze podatkov ponudnika storitev.

6.5.2 Nivo varnostne zaščite računalnikov

Strežniški operacijski sistemi ponudnika storitev so komercialni produkti, ki so dodatno varnostno okrepljeni za zagotavljanje varnega izvajanja postopkov ponudnika storitev.

6.6 Tehnični nadzor življenjskega cikla ponudnika storitev

6.6.1 Nadzor razvoja sistema

CA-programska oprema ponudnika storitev je verificirana po kriterijih Common Criteria (CC) EAL4+.

6.6.2 Upravljanje varnosti

Ponudnik storitev ima vzpostavljene postopke za upravljanje problemov, sprememb in konfiguracij za vse komponente svoje infrastrukture ter postopke za nadzor celovitosti programske opreme.

6.6.3 Upravljanje varnosti čez življenjski cikel

Razvoj in vzdrževanje programske kode CA-aplikacije izvaja dobavitelj. Postopki dobavitelja so v skladu s postopki za doseganje skladnosti CC EAL4+. (glej tudi 6.6.1).

6.7 Varnostne kontrole na ravni računalniškega omrežja

Računalniško omrežje ponudnika storitev sestavlja več ločenih segmentov, na katerih se nahajajo strežniki in delovne postaje. Segmenti so med seboj ločeni s požarnimi pregradami.

Računalniška omrežja so prek požarnih pregrad, povezana z računalniškim omrežjem NLB. Varnostna pravila na požarnih pregradah dovoljujejo prehod samo protokolom, potrebnim za dostop do CA-servisov ter varnostni nadzor in upravljanje strežnikov.

6.8 Časovno žigosanje

Časovno žigosanje ni predpisano.

7 Profil potrdil in registrov preklicanih potrdil

7.1 Profil potrdil

7.1.1 Različica potrdil

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

Signature *(signature)*	Podpis ponudnika storitev
Issuer *(issuer)*	Edinstveno razločevalno ime ponudnika storitev (glej 1.3.1)
Validity *(thisUpdate, nextUpdate)*	Datum aktiviranja in poteka veljavnosti potrdila
Subject	Edinstveno razločevalno ime imetnika potrdila

(subject)	(glej 3.1.1)
Subject Public Key Info (subjectPublicKeyInfo)	Oznaka algoritma ključa
Version (version)	Različica potrdila X.509
Serial Number (serialNumber)	Edinstvena serijska številka

7.1.2 Razširitvena polja

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

7.1.2.1 Standardna razširitvena polja

Naziv atributa	**Opis**
Authority Key Identifier (authorityKeyIdentifier)	Odtis javnega ključa ponudnika storitev AC NLB, s katerim je podpisano potrdilo
Subject Key Identifier (subjectKeyIdentifier)	Odtis imetnikovega javnega ključa
Key Usage (keyUsage)	Kot je opisano v 6.1.7 Polje je označeno kot kritično v vseh potrdilih.
Certificate Policies (certificatePolicies)	OID oznaka vrste potrdila v skladu s poglavjem 1.2 in URI objave pravil delovanja. Glej tudi poglavje 7.1.2.3.
CRL Distribution Points (cRLDistributionPoints)	Naslovi na katerih je objavljen register preklicanih potrdil
Subject Alternative Name (subjectAlternativeName)	Alternativno ime imetnika v skladu z RFC5280 (Elektronski poštni naslov, domensko ime strežnika, ...)
Basic Constraints (basicConstraint)	Doda CA aplikacija Polje je označeno kot kritično v CA potrdilih.
Qualified Certificate Statements qCStatements	Oznaka Kvalificiranega potrdila v skladu z ETSI EN 319 412-5 Glej tudi 7.1.2.4 in 7.1.2.5
Extended Key Usage (extKeyUsage)	Razširjena uporaba, neobvezen atribut, uporabi se lahko v glede na zahteve aplikativnega okolja (glej tudi 6.1.7)
Authority Information Access (authorityInfoAccess)	Vsebuje spletni naslov storitve OCSP in spletni naslov na katerem je dostopno potrdilo izdajatelja. Gelj tudi 7.1.2.2.

7.1.2.2 Razširitveno polje authorityInfoAccess

Razširitveno polje *authorityInfoAccess* (RFC 5280, Authority Information Access) vsebuje spletni naslov na katerem je objavljeno potrdilo izdajatelja, ki je izdal potrdilo in spletni naslov storitve OCSP.

Spletni naslov na katerem je objavljeno potrdilo izdajatelja (glej 6.1.4) je objavljen v razširitvene polju *id-ad-caIssuers*.

Spletni naslov storitve OCSP (http://acldap.nlb.si/ocsp) je objavljen v razširitvenem polju *id-ad-ocsp*.

7.1.2.3 Razširitveno polje certificatePolicies

Razširitveno polje *id-ce-certificatePolicies* potrdil vsebuje identifikacijo oznako ponudnika storitev AC NLB (glej 1.2) in identifikacijsko oznako politik kvalificiranih potrdil v skladu z ETSI EN 319411-2..

V ostalih (nekvalificiranih) potrdilih vsebuje razširitveno polje *id-ce-certificatePolicies* identifikacijo oznako ponudnika storitev AC NLB (glej 1.2).

Kvalificirana potrdila za elektonski podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa, vsebujejo ETSI EN 319 411-2 identifikacijsko oznako politike *qcp-natural-qscd* (0.4.0.194112.1.2). Ostala kvalificirana digitalna potrdila za elektronski podpis vsebujejo ETSI EN 319 411-2 identifikacijsko oznako politike *qcp-natural* (0.4.0.194112.1.0).

Kvalificirana potrdila za elektronski žig na napravi za ustvarjanje kvalificiranega elektronskega žiga vsebujejo ETSI EN 319 411-2 identifikacijsko oznako politike *qcp-legal-qscd* (0.4.0.194112.1.3). Ostala kvalificirana digitalna potrdila za elektronski žig vsebujejo ETSI EN 319 411-2 identifikacijsko oznako politike *qcp-legal* (0.4.0.194112.1.1).

7.1.2.4 Razširitveno polje QCStatements

Razširitveno polje QCStatements vsebuje oznake v skladu z ETSI EN 319 412-5.

Kvalificirana potrdila za elektronski podpis

Razširitveno polje *qCStatements* v kvalificiranih digitalnih potrdilih za elektronski podpis na napravi za ustvarjanje kvalificiranega elektronskega podpisa vsebuje oznake:

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

Razširitveno polje *qCStatements* v ostalih kvalificiranih potrdilih za elektronski podpis vsebuje oznake:

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

Kvalificirana potrdila za elektronski žig

Razširitveno polje *qCStatements* v kvalificiranih digitalnih potrdilih za elektronski žig na napravi za ustvarjanje kvalificiranega elektronskega žiga vsebuje oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)
- QCstatement QcType (0.4.0.1862.1.6)
    - id-etsi-qct-eseal (0.4.0.1862.1.6.2)

Razširitveno polje *qCStatements* v ostalih kvalificiranih potrdilih za elektronski žig vsebuje oznake:

- id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
- id-etsi-qcs-QcPDS (0.4.0.1862.1.5)
- QCstatement QcType (0.4.0.1862.1.6)
  - id-etsi-qct-eseal (0.4.0.1862.1.6.2)

7.1.2.5 Razširitveno polje QCStatements: id-etsi-qcs-QcPDS

Razširitveno polje *id-etsi-qcs-QcPDS* vsebuje spletne naslove na katerih je objavljen dokument PDS v slovenskem in angleškem jeziku:

PdsLocation:
url: https://www.nlb.si/ac-nlb/en/
jezik: en
PdsLocation:
url: https://www.nlb.si/ac-nlb/
jezik: sl

7.1.3 Identifikacijske oznake (angl. Object identifiers) algoritmov

Algoritem	Identifikacijska oznaka
sha1WithRSAEncryption	1.2.840.113549.1.1.5
sha256WithRSAEncryption	1.2.840.113549.1.1.11
RSA Encryption	1.2.840.113549.1.1.1

7.1.4 Oblike imen

Potrdila ponudnika storitev vsebujejo polno razločevalno ime ponudnika storitev in imetnika potrdila v poljih »issuer name« ter »subject name«. Razločevalna imena so v obliki X.501 *PrintableString*.

7.1.5 Omejitve imen

Ne uporablja se omejitve imen.

7.1.6 Identifikacijska oznaka potrdila

Uporablja se polje *id-ce-certificatePolicies* za označevanje vrste potrdil. Glej 7.1.2.3.

7.1.7 Uporaba omejitve imen

Ne uporablja se omejitve imen.

7.1.8 Policy qualifiers

Polje RFC 5280 *id-ce-certificatePolicies:id-qt-cps* se uporablja za objavo spletnega naslova, kjer je objavljena Politika AC NLB.

7.1.9 Procesiranje oznake kritičnosti razširitvenih polj potrdila

Tretje strani, ki procesirajo potrdila ponudnika storitev AC NLB, morajo preverjati kritičnost razširitvenih polj v skladu z RFC 5280.

7.2 Profil registra preklicanih potrdil

7.2.1 Različica

Version	V2
Signature	Podpis ponudnika storitev
Issuer	Razločevalno ime izdajatelja
thisUpdate	Čas izdaje liste
nextUpdate	Čas izdaje naslednje liste
revokedCertificate	Serijske številke preklicanih potrdil

7.2.2 CRL and CRL entry extension

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

7.3 Profil OCSP

7.3.1 Različica

Uporablja se različica 1 protokola OCSP v skladu s specifikacijami v RFC2560, RFC 5019 in RFC 6960.

7.3.2 OCSP razširitvena polja

Razširitvena polja so v skladu s priporočili RFC navedenimi v 7.3.1.

8 Preverjanje skladnosti in ostale oblike nadzora

8.1 Pogostost ali okoliščine izvajanja nadzornih pregledov

Preverjanje skladnosti z zakonodajo izvaja pristojni certifikacijski in nadzorni organ v skladu z Uredbo eIDAS, člen 17. Ponudnik storitev izvaja redne notranje preglede delovanja.

8.2 Pogoji za izvajalca nadzora

Zunanji izvajalec nadzora mora biti akreditiran v skladu z Uredbo eIDAS in je pristojen za ugotavljanje skladnosti ponudnika kvalificiranih storitev zaupanja in kvalificiranih storitev zaupanja, ki jih ta zagotavlja. Ponudnik storitev določi izvajalca notranjih pregledov po svoji presoji.

8.3 Relacija med izvajalcem nadzora in ponudnikom storitev

Urejeno v točki 8.1 in 8.2.

8.4 Področja nadzora

Nadzor izvaja pristojni certifikacijski in nadzorni organ, skladno z zakonodajo.

Postopek odobritve in preverjanje skladnosti delovanja ponudnika storitev s Politiko AC NBL izvaja Center notranje revizije NLB d.d. (CNR). V okviru postopka odobritve se izvaja preverjanje infrastrukture ter vzpostavljenih postopkov glede na določila Politike AC NLB in priporočila dobre prakse.

8.5 Postopki po opravljenem nadzornem pregledu

Ponudnik storitev pripravi načrt za odpravo pomanjkljivosti in poročilo o odpravi pomanjkljivosti, v primeru, da le-te obstajajo.

8.6 Prejemniki in objava ugotovitev

Ugotovitve se posreduje Upravnemu odboru AC NLB.

9 Ostale poslovne in pravne zadeve

9.1 Cenik

9.1.1 Cena izdaje in upravljanja potrdil

NLB d.d. določi cenik uporabe potrdil in svojih storitev ter vsakokrat veljaven cenik objavi na svojih spletnih straneh.

9.1.2 Cena dostopa do potrdil v javnem imeniku

Dostop do javnega imenika ni možen.

9.1.3 Cena dostopa do registra preklicanih potrdil

Dostop do registra preklicanih potrdila je brezplačen.

9.1.4 Cena ostalih storitev

Stroške potrebne strojne ali programske opreme, ki jo zahteva oz. priporoča AC NLB za varno shranjevanje in uporabo potrdil, krije imetnik potrdila.

9.1.5 Pravica vračila

Stranka lahko pisno zahteva povrnitev stroškov izdaje potrdila v primeru odstopa od zahtevka pred prevzemom oziroma pred potekom roka za prevzem potrdila.

9.2 Finančna odgovornost

9.2.1 Zavarovanje odgovornosti

NLB d.d. za ponudnika storitev zagotavlja zadostna finančna sredstva z obveznosti prostim premoženjem.

9.2.2 Druge oblike zavarovanja

Ni predvideno.

9.2.3 Zavarovanja ali jamstvo za druge uporabnike

Ni predvideno.

9.3 Zaupnost poslovnih informacij

9.3.1 Obseg zaupnih poslovnih informacij

Vsi podatki (zbrani, ustvarjeni, vzdrževani) s strani ponudnika storitev, štejejo za zaupne in so poslovna skrivnost ponudnika storitev oziroma NLB d.d.. Izjema so le podatki navedeni v poglavju 9.3.2.

9.3.2 Informacije izven obsega zaupnih poslovnih informacij

Vse informacije, ki so vsebovane v potrdilih, ali listah preklicanih potrdil, ali kakorkoli javno objavljene s strani ponudnika storitev, se ne štejejo za zaupne.

9.3.3 Odgovornost za zagotavljanje zaupnosti poslovnih informacij

Ponudnik storitev je odgovoren za zagotavljanje zaupnosti poslovnih informacij v skladu s predpisi veljavnimi v Republiki Sloveniji

9.4 Varovanje osebnih podatkov

9.4.1 Načrt zagotavljanja varovanja osebnih podatkov

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

9.4.2 Obseg varovanih osebnih podatkov

Vsi osebni podatki imetnika potrdila, ki jih ponudnik storitev pridobi, obdeluje ali posreduje v okviru izvajanja svoje storitve, imajo status varovanih osebnih podatkov in jih ponudnik storitev sporoča le na zahtevo imetnika potrdila ali na pisno zahtevo sodišča ter v drugih primerih, ki jih določa veljavna zakonodaja, ki ureja področje varstva osebnih podatkov in na njegovi podlagi izdanimi predpisi. Izjema so potrdila in register preklicanih potrdil.

Ponudnik storitev in imetnik potrdila sta dolžna zagotavljati visoko raven ukrepov, ki bodo zagotovili minimiziranje tveganj nepooblaščenega dostopa do podatkov, spreminjanja podatkov in/ali izgube podatkov.

9.4.3 Nevarovani osebni podatki

Vse informacije, ki so vsebovane v potrdilih, ali listah preklicanih potrdil, ali kakorkoli javno objavljene s strani ponudnika storitev, se ne štejejo za zaupne.

9.4.4 Odgovornost glede varovanja osebnih podatkov

Ponudnik storitev je odgovoren za zagotavljanje varovanja osebnih podatkov v skladu s predpisi veljavnimi v Republiki Sloveniji.

9.4.5 Dovoljenje za uporabo osebnih podatkov

Ponudnik storitev uporablja osebne podatke samo za namene, za katere je dal imetnik potrdila soglasje v postopku registracije oziroma v skladu z veljavnimi predpisi.

9.4.6 Posredovanje osebnih podatkov v sodnih in upravnih postopkih

Ponudnik storitev posreduje osebne podatke v sodnih in upravnih zadevah, če je tovrstno posredovanje v skladu z veljavnimi predpisi.

9.4.7 Druge okoliščine posredovanja osebnih podatkov

Ni predvideno.

9.5 Zaščita intelektualne lastnine

Zaščita intelektualne lastnine ni predpisana.

9.6 Odgovornosti in jamstva

9.6.1 Odgovornosti in jamstva ponudnika storitev

Ponudnik storitev je dolžan:

- delovati v skladu s svojimi notranjimi pravili in ostalimi veljavnimi predpisi in zakonodajo,
- delovati v skladu z mednarodnimi priporočili,
- objavljati vse pomembne dokumente, ki določajo njegovo delovanje (politike delovanja, zahtevke, cenik, navodila za varno uporabo Kvalificiranih potrdil ipd.),
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti ponudnika storitev, ki kakorkoli vplivajo na imetnike potrdil in tretje osebe,
- zagotoviti delovanje prijavnih služb v skladu z določili ponudnika storitev in ostalimi veljavnimi predpisi,
- spoštovati določila glede varnega ravnanja z osebnimi, poslovnimi in zaupnimi podatki o ponudniku storitev, imetnikih potrdil ali tretjimi osebami,
- preklicati potrdilo in objaviti preklicano potrdilo v registru preklicanih potrdil, ko ugotovi. da so podani razlogi po tej politiki ali drugih veljavnih predpisih,
- izdajati potrdila v skladu s to politiko in ostalimi predpisi ter priporočili,
- zagotoviti pravilnost podatkov izdanih potrdil.
- zagotoviti, da ima imetnik potrdila v času izdaje le-tega zasebni ključ, ki pripada v potrdilu navedenemu javnemu ključu (glej podpogl. 3.2.1),
- zagotoviti pravilnost objave registra preklicanih potrdil,
- zagotoviti pravilnost delovanja sprotnega preverjanja statusa potrdil.
- zagotoviti enoličnost razločevalnih imen,
- zagotoviti primerno fizično varnost prostorov in dostopov do samih prostorov ponudnika storitev,.
- kot dober gospodar skrbeti za nemoteno delovanje in čim večjo razpoložljivost storitve,
- kot dober gospodar skrbeti za čim večjo dostopnost storitev,
- kot dober gospodar skrbeti za nemoteno delovanje vseh ostalih spremljajočih storitev,
- poskušati odpraviti nastale probleme po najboljših močeh in v najkrajšem času,
- obveščati vse ustrezne subjekte o pomembnih zadevah,
- izpolnjevati vse druge zahteve v skladu s to politiko.

Ponudnik storitev zagotavlja čim večjo dostopnost svojih storitev, in sicer 24ur/7dni/365dni, razen v naslednjih primerih

- delovanje registracijske pisarne je samo v delovnem času,
- pri načrtovanih in vnaprej napovedanih tehničnih ali servisnih posegih na infrastrukturi,

- pri nenačrtovanih tehničnih ali servisnih posegih na infrastrukturi, kot posledica nepredvidenih okvar,
- pri tehničnih ali servisnih posegih zaradi okvare infrastrukture izven pristojnosti ponudnika storitev,
- zaradi nedostopnost, kot posledico višje sile ali izrednih dogodkov.

9.6.2 Odgovornost in jamstva prijavne službe

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

Registracijska pisarna ponudnika storitev jamči za:
- preverjanje točnosti podatkov na vlogah,
- preverjanje identitete prosilcev,
- posredovanje vlog centru ponudnika storitev.

9.6.3 Obveznosti in odgovornost imetnika

Imetnik oziroma bodoči imetnik potrdila je dolžan:
- seznaniti se s to politiko pred izdajo potrdila,
- ravnati v skladu s to politiko in ostalimi veljavnimi predpisi,
- po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti ponudnika storitev oziroma zahtevati preklic potrdila,
- če po oddaji zahtevka za pridobitev potrdila oz. drugo storitev od ponudnika storitev ne prejme obvestila po e-pošti, ki jo je navedel v zahtevku, potem se mora obrniti na pooblaščene osebe ponudnika storitev,
- spremljati vsa obvestila ponudnika storitev in ravnati v skladu z njimi,
- v skladu z obvestili ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
- vse spremembe, ki so povezane s potrdilom, nemudoma sporočiti ponudniku storitev,
- zahtevati preklic potrdila, če so bili zasebni ključi ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe,
- uporabljati potrdilo za namen določen v podpoglavju 1.4.1.

Imetnik odgovarja za:
- nastalo škodo v primeru zlorabe potrdila od prijave preklica do preklica,
- vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba imetnikovega potrdila s strani nepooblaščenih oseb,

vsako drugo škodo, ki izvira iz neupoštevanja določil te politike in drugih obvestil ponudnika storitev ter veljavnih predpisov.

Obveznosti imetnika glede uporabe potrdil so določene v 4.5.1.

9.6.4 Obveznosti in odgovornost tretjih oseb

Tretje osebe morajo proučiti vse zahteve in okoliščine, preden se odločijo za uporabo potrdil, ki jih izda ponudnika storitev.

Tretje osebe, ki uporabljajo izdana potrdila ponudnika storitev, morajo:
- skrbno proučiti vse možnosti tveganja in odgovornosti pri uporabi potrdil in določiti politiko za način uporabe,
- za overjanje podpisa oz. druge kriptografske operacije uporabljati programsko in strojno opremo, s katero lahko na verodostojen način preverijo vse zahteve za varno uporabo potrdil,
- obvestiti ponudnika storitev, če izvedo, da so bili zasebni ključi imetnika potrdila, na katerega se zanašajo, ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, navedeni v potrdilu,
- upoštevati druge določbe iz morebitnih medsebojnih dogovorov,

- upoštevati vsa navodila oz. priporočila ponudnika storitev glede zanesljive uporabe,
- ob morebitnih napakah ali problemih takoj obvestiti ponudnika storitev,
- seznaniti se s to politiko in upoštevati vsa določila glede njihove obveznosti, odgovornosti ter omejitve glede zaupanja in uporabe potrdil,
- spremljati vsa obvestila in objave ponudnika storitev in ravnati v skladu z le-temi,
- upoštevati morebitna druga pravila, ki so izven pristojnosti ponudnika storitev in so določena drugje.

Tretje osebe nosijo vse posledice, ki bi nastale zaradi morebitnega neupoštevanja določil te politike, morebitnega dogovora z ponudnikom storitev in veljavne zakonodaje.

9.6.5 Obveznosti in odgovornosti drugih subjektov

Obveznosti in odgovornosti drugih subjektov niso predpisane.

9.7 Zanikanje odgovornosti ponudnika storitev

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

- če je bilo potrdilo izdano zaradi napake, neverodostojnih podatkov ali drugih nepravilnosti na strani imetnika potrdila,
- če je potekla veljavnost potrdila,
- kadar je potrdilo uporabljeno po preklicu in objavi v registru preklicanih potrdil,
- če je potrdilo ponarejeno ali kakor koli predrugačeno ali spremenjeno,
- če prosilec, imetnik potrdila ali tretja oseba ne ravna v skladu z določbami tega dokumenta, pravili delovanja ponudnika storitev, ali veljavnimi zakoni in na njihovi podlagi izdanimi podzakonskimi predpisi,
- če je bil zasebni ključ imetnika ogrožen ali obstaja objektivno utemeljen sum, da je bil ogrožen,
- če je bilo varovanje gesel ali zasebnih ključev imetnikov nepravilno ali pomanjkljivo ali pa je prišlo do izdajanja zaupnih podatkov ali ključev tretjim osebam in neodgovornega ravnanja imetnika,
- če je bilo potrdilo uporabljeno v drugačne namene, kot je določeno z naročniško pogodbo, pravili delovanja ponudnika storitev, ali veljavnimi zakoni in na njihovi podlagi izdanimi podzakonskimi predpisi,
- če je prišlo do zlorabe oz. vdora v informacijski sistem imetnika potrdila in s tem do podatkov o potrdilih s strani nepooblaščenih oseb,
- če nastane škoda zaradi napake v delovanju strojne ali programske opreme prosilca, imetnika potrdila ali tretje osebe.

9.8 Omejitve odgovornosti ponudnika storitev

Ponudnik storitev zanika kakršnokoli odgovornost vseh vrst, za nadomestila, škodo ali druge terjatve ali obveznosti katerekoli vrste, ki izhajajo iz škod, pogodb ali iz katerihkoli drugih razlogov v zvezi s katerokoli storitvijo povezano z izdajo, uporabo, ali zanašanjem na digitalno potrdilo, ki ga je izdal ponudnik storitev in ki presega ceno digitalnega potrdila, ki je navedena na spletnih straneh NLB d.d.

9.9 Poravnava škode

Glej poglavji 9.7 in 9.8.

9.10 Začetek in prenehanje veljavnosti

9.10.1 Začetek veljavnosti

Pričujoča Politika začne veljati naslednji dan po objavi na spletni strani ponudnika storitev.

9.10.2 Prenehanje veljavnosti

Politika preneha veljati s trenutkom veljavnosti nove politike, ki jo nadomesti.

9.10.3 Učinek in posledice prenehanja veljavnosti

Z začetkom veljavnosti nove politike ostanejo za vsa potrdila izdana pred tem, v veljavi tista določila prej veljavne politike, ki se smiselno ne morejo nadomestiti z ustreznimi določili nove politike (na primer postopek, ki določa način, po katerem je bilo to potrdilo izdano ipd.).

9.11 Komuniciranje med subjekti

Kontaktni podatki ponudnika storitev oz. izdajatelja so objavljeni na spletnih straneh in podani v podpogl. 1.3.1. in 2.1

Kontaktni podatki imetnikov so podani v zahtevkih v zvezi s potrdili.

Kontaktni podatki tretjih oseb so podani v morebitnem medsebojnem dogovoru med tretjo osebo in ponudnikom storitev.

Ponudnik storitev ostale subjekte obvešča preko obvestil objavljenih na svojih spletnih straneh.

9.12 Spreminjanje dokumenta

9.12.1 Postopek uveljavitve sprememb

Ponudnik storitev bo izvajal uredniške in tipografske popravke katerega koli dela tega dokumenta in skrbel za njihovo objavo brez posebnega obvestila.

Vse spremembe te politike bodo stopile v veljavo naslednji dan po objavi na spletnih straneh ponudnika storitev.

9.12.2 Postopek obveščanja

Imetniki potrdil, tretje osebe in medsebojno priznani ponudniki storitev bodo o spremembah obveščeni na spletni strani ponudnika storitev.

9.12.3 Spremembe, ki zahtevajo novo identifikacijsko oznako politike

Ponudnik storitev se po lastni presoji odloči, ali so spremembe vsebine politike ponudnika storitev potrdil takšne, da zahtevajo objavo nove Politike z novo identifikacijsko oznako.

9.13 Postopek v primeru sporov

Stranke si bodo prizadevale za sporazumno reševanje sporov, če pa to ne bi bilo mogoče, je za reševanje sporov pristojno sodišče v Ljubljani. Stranke za reševanje sporov dogovorijo izključno uporabo predpisov Republike Slovenije.

9.14 Veljavna zakonodaja

Ponudnik storitev deluje v skladu z:

- UREDBO (EU) št. 910/2014 EVROPSKEGA PARLAMENTA IN SVETA o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (na kratko Uredbo eIDAS).

- Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/2004 - ZEPEP).
- Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 94/2007-UPB1 -ZVOP-1).
- drugimi predpisi veljavnimi v Republiki Sloveniji.

9.15 Skladnost z veljavno zakonodajo

Nadzor nad skladnostjo delovanja ponudnika storitev z veljavno zakonodajo in predpisi, določenimi v podpogl. 9.14, izvaja pristojni certifikacijski in nadzorni organ v skladu z Uredbo eIDAS, člen 17.

9.16 Splošne določbe

9.16.1 Ostali obvezujoči dokumenti

Določbe te politike v ničemer ne spreminjajo, omejujejo ali drugače vplivajo na obveznosti in odgovornosti ponudnika storitev na podlagi drugih pogodb ali dogovorov oziroma druge veljavne zakonodaje.

9.16.2 Prenos pravic in obveznosti

Potrdilo, ki ga ponudnik storitev izda imetniku ter morebitne pravice, povezane z uporabo potrdila, so namenjene izključno imetniku in niso prenosljive na tretje osebe.

9.16.3 Neodvisnost določil

Če katerokoli od določil politike ali morebitnega dogovora oz. pogodbe je ali postane neveljavno, to ne vpliva na ostala določila. Neveljavno določilo se nadomesti z veljavnim, ki mora čim bolj ustrezati namenu, ki ga je želelo doseči neveljavno določilo.

9.16.4 Uveljavljanje (povračila stroškov v primeru sporov in izjeme)

Zahtevki povračila stroškov v primeru sporov so obravnavajo v skladu s predpisi, ki veljajo v Republiki Sloveniji.

9.16.5 Višja sila

Višja sila so izredne nepremagljive in nepredvidljive okoliščine, ki nastopijo po sklenitvi pogodbe in so zunaj volje ali sfere pogodbenih strank (v celoti tuje pogodbenim strankam), kot na primer požar, potres, druge elementarne nezgode, vojna in podobno.

Za višjo silo štejejo tudi predpisi, posamični akti in dejanja ter drugi ukrepi organov Evropske skupnosti, ki izpolnjujejo pogoje iz prejšnjega odstavka.

Za višjo silo štejejo tudi predpisi, posamični akti ali ukrepi organov RS, ki pomenijo vključitev obveznih določb predpisov Evropske skupnosti v pravni red Republike Slovenije ali ki pomenijo izvrševanje neposredno uporabljivih pravil prava te skupnosti, ki izpolnjujejo pogoje za višjo silo iz prejšnjega odstavka.

Nobena stranka ne more uveljavljati zahtevkov, ki ji po tej politiki, pogodbi ali po zakonu pripadajo zaradi kršitve druge stranke, če je do ravnanja v nasprotju s pogodbo prišlo zaradi višje sile.

Če je zaradi višje sile začasno onemogočeno izvrševanje kakšne obveznosti v zvezi s to politiko, ali dogovoru, se rok za izvršitev ustrezno podaljša.

9.17 Ostale določbe

- Oblika in vsebina javne politike ponudnika storitev je usklajena z:
  - RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
  - RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
  - ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
  - ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
  - ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
  - ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
  - ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
  - ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
  - ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
- Imetniki potrdil, izdanih s strani AC NLB, lahko morebitne pritožbe v zvezi s storitvami in delovanjem AC NLB naslovijo na naslov, opredeljen v točki 1.3.1.