ПОЛИТИКА СЕРТИФИКАЦИЈЕ ЗА КВАЛИФИКОВАНЕ ЕЛЕКТРОНСКЕ СЕРТИФИКАТЕ

(*Certificate Policy - CP)*

Верзија: 1.2

Историја промена

Верзија	Датум	Разлог промене
1.0	09.10.2018.	Иницијална верзија
1.1	19.06.2019.	Промене у складу са коментарима оцењивача
1.2	02.04.2026.	Промена пословног имена и друга усклађивања

Садржај

1. УВОД

„Пошта Србије“ д.о.о. (у даљем тексту: Сертификационо тело Поште) изградило је инфраструктуру јавних криптографских кључева (*Public Key Infrastructure - PKI*) и на тржишту је присутно као сертификационо тело које пружа услуге издавања квалификованих електронских сертификата за електронски потпис и електронски печат (у даљем тексту: квалификовани сертификат).

Сертификационо тело Поште као квалификовани пружалац услуга од поверења омогућава стварање односа поверења потребног за коришћење и развој електронског пословања (е-пословање) и електронске јавне управе (е-управа). Промовисањем ових услуга од поверења и њиховим коришћењем Сертификационо тело Поште жели да подстакне и олакша развој е-пословања и е-управе. Пословна мрежа Сертификационог тела Поште има националну покривеност, а њена информатичка повезаност гарантује брзину и поузданост извршења захтева коју користе регистрациона тела Сертификационог тела Поште.

Као трећа страна од поверења Сертификационо тело Поште пружа услуге издавања сертификата од 2008. године. Сертификационо тело Поште издавање квалификованих сертификата врши у складу са законом и другим прописима донетим на основу закона, као и општим актима Сертификационог тела Поште, који регулишу ову област и област заштите података о личности.

Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС“, бр. 94/17 и 52/21) и подзаконска акта чине правни оквир за обављање делатности издавања квалификованих сертификата Сертификационог тела Поште.

Сертификационо тело Поште издавање квалификованих сертификата врши у складу са одговарајућим међународним стандардима и препорукама, односно другим стандардима, документима и препорукама, које се односе на издавање квалификованих сертификата.

1.1. Преглед

Инфраструктура јавног кључа (PKI) је инфраструктура успостављена у Сертификационом телу Поште којом се пружа услуга од поверења, а која се односи на издавање и управљање животним циклусом квалификованих сертификата.

Сертификационо тело Поште користи у својој инфраструктури за издавање квалификованих сертификата хијерархију више *CA* (*Certification Authority*) сервера. Инфраструктуру Сертификационог тела Поште чине следећа сертификациона тела:
- „*Pošta Srbije CA Root 2026* “, као *Root* сертификационо тело које потписује своју CRL и издаје сертификате подређеним сертификационим телима (*subordinate* CA),
- „*Pošta Srbije CA 2*“, као подређено (*subordinate*) сертификационо тело које потписује своју CRL и издаје квалификоване сертификате,
- „*Pošta Srbije CA Root* “, као *Root* сертификационо тело које потписује своју CRL до истека сертификата подређених (*subordinate* CA) које је издало,
- „*Pošta Srbije CA 1*“, као подређено (*subordinate*) сертификационо тело које потписује CRL до истека квалификованих сертификата које је издало.

„*Pošta Srbije CA Root 2026*“ сервер ради као *Root* сертификационо тело на основу сертификата издатог самом себи (*self-signed certificate*) у процесу генерисања приватног криптографског кључа апликације сертификационог тела (*Root Key Generation Ceremony*). „*Pošta Srbije CA Root 2026*“ сервер издаје сертификате подређеним сертификационим телима која су део инфраструктуре Сертификационог тела Поште и потписује своју CRL листу.
„*Pošta Srbije CA 2*“ сервер као подређено (*subordinate*) сертификационо тело, издато од стране „*Pošta Srbije CA Root 2026*“, издаје квалификоване сертификате физичким лицима и правним лицима/организацијама (у даљем тексту: правним лицима), а запосленима у Сертификационом телу Поште који раде на пословима сертификације сертификати се издају у складу са поверљивом улогом коју запослени обавља и потписује своју CRL листу.
„*Pošta Srbije CA Root*“ сервер ради као *Root* сертификационо тело на основу сертификата издатог самом себи (*self-signed certificate*) у процесу генерисања приватног криптографског кључа апликације сертификационог тела (*Root Key Generation Ceremony*). „*Pošta Srbije CA Root*“ сервер потписује своју CRL листу до истека подређених сертификата које је издало.
„*Pošta Srbije CA 1*“ сервер као подређено (*subordinate*) сертификационо тело, издато од стране „*Pošta Srbije CA Root*“, потписује своју CRL до истека квалификованих сертификата које је издало.

Опсег овог документа су услуге од поверења које пружа Сертификационо тело Поште, а које се односе на издавање и управљање животним циклусом квалификованих сертификата.

Структура овог документа је у складу са стандардима RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“ и 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“.

Поступци који се примењују у издавању квалификованих сертификата описани су у документу Практична правила пружања услуге сертификације за квалификоване електронске сертификате (у даљем тексту: Практична правила).

Сертификати које издају *Root* и његова подређена *CA* тела намењени су за коришћење у електронском пословању унутар и изван Републике Србије.

Root издаје следеће сертификате:
- *Root* Сертификат,
- Сертификате за подређена *CA* тела.

Root сертификати не издају корисничке сертификате.

Кориснички сертификати које издаје „*Pošta Srbije CA 2“* су:
- Квалификовани сертификат за електронски потпис намењен физичким лицима,
- Квалификовани сертификат за електронски потпис намењен физичким лицима која су припадници правних лица,
- Квалификовани сертификат за електронски печат намењен правним лицима.

1.2. Назив документа и идентификациони подаци

Назив документа је: Политика сертификације за квалификоване електронске сертификате (у даљем тексту: Политика сертификације).

Документ се објављује у „Службеном ПТТ-гласнику“ који се идентификује бројем и датумом објављивања.

Важећа верзија документа може да се преузме са веб сајта Сертификационог тела Поште: https://www.ca.posta.rs.

1.3. Учесници у PKI систему

Учесници у PKI систему су:

- Сертификационо тело (*Certification Authority - CA*);
- Регистрациона тела (*Registration Authority - RA*) која се састоје од централног и локалних регистрационих тела (*Local Registration Authority - LRA*);
- корисници;
- поуздајуће стране (трећа лица);
- остали учесници.

Сертификациона тела из опсега овог документа су: „*Pošta Srbije CA Root 2026*“, „*Pošta Srbije CA 2*“, „*Pošta Srbije CA Root*“ и „*Pošta Srbije CA 1*“.

„*Pošta Srbije CA Root 2026“* издаје сертификате подређеним сертификационим телима која су део инфраструктуре Сертификационог тела Поште.

„*Pošta Srbije CA 2*“ као подређено (*subordinate*) сертификационо тело издаје квалификоване сертификате корисницима Сертификационог тела Поште.

Наведена *CA* тела чине хијерархијску структуру која је описана у поглављу 1.1. овог документа.

У седишту Сертификационог тела Поште налази се Централно регистрационо тело, док су локална регистрациона тела овлашћене јединице поштанске мреже (у даљем тексту: поште) на територији Републике Србије. Успостављање екстерних локалних регистрационих тела може се извршити, а регулише се посебним уговором са заинтересованим правним лицем.

Пословима регистрације координира Централно регистрационо тело.

Корисници квалификованих сертификата у смислу овог документа су особе које са Сертификационим телом Поште уговарају коришћење услуга.

Корисници Сертификационог тела Поште могу бити:

- физичка лица - индивидуални корисници,
- правна лица / државни органи / организације (у даљем тексту: правно лице), односно у том субјекту ангажована физичка лица која су у радном односу или су по другом основу који нема карактер радног односа ангажовани у правном лицу (у даљем тексту: физичко лице у правном лицу).

Поуздајуће стране, односно трећа лица су физичка лица (појединци) и/или правна лица, односно државни органи и организације која прихватају сертификате и верификују електронски потпис одређених електронских докумената која су потписана од стране корисника Сертификационог тела Поште, као и која врше валидацију сертификата издатих од стране Сертификационог тела Поште. Поуздајуће стране су обавезне да провере статус квалификованог сертификата на основу сервиса за проверу опозваности сертификата Сертификационог тела Поште пре него што прихвате информације које су наведене у сертификату.

Остали учесници су правна лица која доприносе или учествују у обезбеђивању квалитета рада Сертификационог тела Поште: осигуравајућа друштва, произвођачи и дистрибутери опреме и софтвера.

1.4. Употреба сертификата

„Pošta Srbije CA Root 2026“ сертификат се искључиво користи за издавање сертификата њему подређених *CA* тела и за издавање регистра опозваних сертификата.

Сертификати подређених *CA* тела користе се за издавање корисничких сертификата, издавање припадајућих регистара опозваних сертификата и за издавање сертификата за потписивање *OCSP* одговора.

Свака употреба квалификованог сертификата која није у сагласности са прописима и другим подзаконским актима, као и општим актима и препорукама Сертификационог тела Поште и другим документима који регулишу ову област и област заштите података о личности, није дозвољена.

1.5. Политика администрирања документа

Документ Политика сертификације креира и ажурира Сертификационо тело Поште. Промене садржаја документа обављају се на основу интерних предлога и захтева за усклађивањем са законском регулативом и меродавним актима.

Лице за контакт је руководилац организационе целине надлежне за електронско пословање Сертификационог тела Поште.

Управна структура Сертификационог тела Поште редовно процењује усклађеност практичних правила са важећом законском регулативом и меродавним актима.

Измене и/или допуне Политике сертификације врше се у складу са прописима, општим актима и другим актима која регулишу ову област. Предлог измена и/или допуна Политике сертификације сачињава пословна функција надлежна за информационе технологије, електронске комуникације и развој, а правно - техничку редакцију врши пословна функција надлежна за правне послове. Директор Поште Србије доноси измене и/или допуне тог акта, уз претходну верификацију овлашћених запослених, у смислу правилника Поште Србије којим се уређује израда аката у Пошти Србије, а која лица својим потписима (парафима) потврђују тај предлог акта, у својству запослених који предлог акта обрађује, контролише, даје сагласност, односно одобрава.

1.6. Дефиниције и скраћенице

Поједини изрази који се користе у овој политици сертификације имају следеће значење:

1) **Апликација централног регистрационог тела -** апликација на администраторској радној станици посредством које се прихватају и обрађују захтеви корисника за издавање квалификованих сертификата и захтеви за промену статуса сертификата;
2) **Апликација локалног регистрационог тела** - апликација за пријем захтева за издавање и прихватање захтева за промену статуса сертификата;
3) **Апликација сертификационог тела** - апликација на серверима Сертификационог тела Поште која генерише и потписује квалификоване сертификате и регистре опозваних сертификата, што се ради у хардверском криптографском модулу;
4) **Електронски дневник** - електронска форма записа о спроведеним активностима;
5) **Електронски документ** - документ у електронском облику који се користи у пословним и другим радњама;
6) **Компромитовање приватног криптографског кључа -** нарушавање безбедности којом се приватни криптографски кључ излаже могућем неовлашћеном приступу, као што су неовлашћено откривање, мењање или коришћење;
7) **Корисник -** физичко или правно лице које користи квалификовани сертификат издат од стране Сертификационог тела Поште и чији се подаци налазе у сертификату;
8) **Квалификовани електронски потпис или печат** - електронски потпис којим се поуздано гарантује идентитет потписника или печатиоца, интегритет електронских докумената, и онемогућава накнадно порицање одговорности за њихов садржај, и који испуњава услове утврђене законом;
9) **Квалификовани електронски сертификат -** електронски сертификат који је издат од стране сертификационог тела за издавање квалификованих сертификата и садржи податке предвиђене законом;
10) **Подаци за креирање квалификованог електронског потписа или печата** - подаци за креирање електронског потписа односно печата су јединствени подаци које користи потписник односно печатилац за креирање електронског потписа односно печата и који су логички повезани са одговарајућим подацима за валидацију електронског потписа односно печата;
11) **Подаци за валидацију квалификованог електронског потписа или печата** - подаци за валидацију електронског потписа односно печата су подаци на основу којих се проверава да ли електронски потпис односно печат одговара подацима који су потписани односно печатирани;
12) **Приватни криптографски кључ апликације сертификационог тела** - приватни криптографски кључ генерисан приликом иницијализације апликације сертификационог тела који служи за потписивање издатих квалификованих сертификата и регистара опозваних сертификата, што се ради у хардверском криптографском модулу;
13) **Регистар опозваних сертификата** (*Certificate Revocation List - CRL*) - листа у коју се уписују серијски бројеви и други подаци свих опозваних сертификата које је издало сертификационо тело;
14) **Сертификационо тело** - правно лице које издаје квалификоване сертификате;
15) **Квалификована средства за креирање квалификованих потписа и печата** - средство за креирање електронског потписа односно печата је техничко средство (софтвер односно хардвер) које се користи за креирање електронског потписа односно печата уз коришћење података за креирање електронског потписа односно печата;

16) **Средства за валидацију квалификованог потписа и печата** - одговарајућа техничка средства (софтвер и хардвер) која служе за валидацију квалификованог потписа и печата, уз коришћење података за валидацију електронског потписа и печата;
17) **Централно регистрационо тело** (*Registration Authority - RA*) - тело које ради у седишту сертификационог тела и које је овлашћено за одобравање и прослеђивање података за издавање квалификованих електронских сертификата и захтева за промену статуса сертификата према апликацији сертификационог тела;
18) **Локална регистрациона тела** (*Local Registration Authority - LRA*) - тела овлашћена за проверавање идентитета корисника и за прослеђивање података за издавање квалификованих сертификата и захтева за промену статуса сертификата према централном регистрационом телу;
19) **Запослени -** лице у радном односу или по другом основу ангажовано у Сертификационом телу Поште.

Списак скраћеница које се помињу у документу приказан је у оквиру Табеле 1.

Табела 1. Списак скраћеница

Скраћеница	Објашњење
CA (Certification Authority)	Сертификационо тело
CRL (Certificate Revocation List)	Регистар опозваних сертификата
EAL (Evaluation Assurance Level)	Тестирани ниво сигурности. Постоји седам (7) нивоа и то од *EAL*1 до *EAL7*
FIPS (Federal Information Processing Standards)	Стандард захтеваног нивоа сигурности за криптографске модуле (*Security Requirements for Cryptographic Modules*). Постоји четири (4) нивоа
HSM (Hardware Security Module)	Хардверски криптографски модул за операције са приватним криптографским кључем
LRA (Local Registration Authority)	Локално регистрационо тело
OCSP (Online Certificate Status Protocol)	Протокол за *on-line* проверу статуса сертификата, описан у документу *RFC* 6960
PKI (Public Key Infrastructure)	Инфраструктура јавних криптографских кључева
RA (Registration Authority)	Регистрационо тело
RFC (Request for Comments)	Документа која дефинишу Интернет стандарде и препоруке
QSCD (Qualified Signature Creation Device)	Квалификовано средство за креирање електронских потписа и електронских печата (смарт картица, *USB* смарт токен,...)
X.509	Стандард за електронске сертификате, описан у документу *RFC* 5280
LDAP (Lightweight Directory Access	Протокол за приступ јавном директоријуму

Protocol)	
UTC (Coordinated Universal Time)	Координисано универзално време
ETSI (European Telecommunications Standards Institute)	Европски институт за стандарде из области телекомуникација

2. ОБЈАВЉИВАЊЕ И ЛОКАЦИЈА ПОДАТАКА О СЕРТИФИКАЦИЈИ

2.1. Локација за објављивање података о сертификацији

Сертификационо тело Поште објављује податке и сву документацију која се односи на издавање квалификованих сертификата на веб сајту https://www.ca.posta.rs, који је јавно доступан, као и документација која се на њој налази.

2.2. Објављивање података о сертификацији

На веб сајту Сертификационог тела Поште јавно су објављени документи и информације о пружању услуга сертификације.

Репозиторијум се састоји од дела који је доступан на веб сајту Сертификационог тела Поште и дела који је доступан преко јавног LDAP именика.

Сертификационо тело Поште објављује на својој веб сајту:

- Политику сертификације за квалификоване електронске сертификате (у даљем тексту: Политика сертификације),
- Практична правила пружања услуга сертификације за квалификоване електронске сертификате (у даљем тексту: Практична правила),
- корисничка упутства,
- сертификате CA сервера са придруженим hash вредностима,
- регистре опозваних сертификата,
- ценовник,
- опште услове пружања услуга,
- обрасце за кориснике,
- законску регулативу из подручја пружања услуга сертификације,
- друга акта и обавештења.

Путем *OCSP* сервиса Сертификационог тела Поште доступне су информације о статусу опозваности квалификованих сертификата издатих од стране Сертификационог тела Поште. Адреса *OCSP* сервиса Сертификационог тела Поште је: *http://ldap-ocsp.ca.posta.rs/ocsp.*

Сертификационо тело Поште јавно не објављује поверљиве податке.

LDAP именик је доступан на адреси*: ldap://ldap-ocsp.ca.posta.rs*

У делу који је доступан преко јавног *LDAP* именика објављују се регистри опозваних сертификата које издају *CA* тела Сертификационог тела Поште и *CA* сертификати.

Објављивање докумената по одобрењу обавља овлашћени запослени задужен за управљање садржајем веб сајта.

Обавештења корисницима, информације о прописима, општима актима и друге информације објављују се пре почетка примене у Сертификационом телу Поште.

Сертификати *CA* тела Сертификационог тела Поште и припадајуће информације објављују се после њиховог издавања.

Објављивање корисничких упутстава и образаца за кориснике на веб сајту одобрава Сертификационо тело Поште, без претходне најаве, тако да се старије верзије докумената уклањају.

2.3. Учесталост објављивања података о сертификацији

Сертификационо тело Поште аутоматски објављује припадајуће *CRL* у јавном именику и на веб сајту после њиховог издавања.

Учесталост објављивања CRL које издаје Сертификационо тело Поште дефинисана је у Практичним правилима.

2.4. Контрола приступа подацима о сертификацији

Документи и информације објављени на веб сајту Сертификационог тела Поште су бесплатни и јавно доступни.

Сертификационо тело Поште има успостављене контроле приступа у циљу спречавања неауторизованог додавања, брисања или промене, као и заштите интегритета и аутентичности. Приступ објављеним документима и информацијама омогућен је само за читање.

Право додавања, промене и брисања података на веб сајту Сертификационог тела Поште имају само овлашћени запослени у Сертификационом телу Поште.

3. ИДЕНТИФИКАЦИЈА И АУТЕНТИФИКАЦИЈА

Идентификација и аутентификација корисника којима подређено (*subordinate*) сертификационо тело издаје сертификате су описани у Практичним правилима.

3.1. Одређивање имена

У квалификованим сертификатима које издаје Сертификационо тело Поште, име сертификационог тела које издаје сертификате, поље *Issuer* и име корисника, поље *Subject*, су јединствена имена (*Distinguished Name - DN*).

Имена и називи у атрибутима поља *Subject* која идентификују физичко лице и правно лице су смислени.

У поље *Subject* квалификованог сертификата уписују се подаци о физичком лицу онако како су наведени у важећем идентификационом документу, односно у службеном

матичном регистру. Подаци о правном лицу који се уписују у поље *Subject* наводе се онако како су регистровани у надлежном регистру.

Уколико Сертификационо тело Поште издаје квалификовани сертификат физичком лицу у правном лицу, у оквиру атрибута који идентификују корисника налазе се и регистровани подаци правног лица.

Садржај поља сертификата *Subject Alternative Name* може бити адреса е-поште која не мора бити смислена.

Корисници не могу да буду анонимни.

У квалификованим сертификатима су имена корисника верно представљена одговарајућим латиничним словима српског језика.
Сертификационо тело Поште гарантује јединственост имена у свом домену.

Имена којима би се кршила интелектуална или ауторска права других нису дозвољена. Сертификационо тело Поште није обавезно да верификује да ли је коришћење таквих имена законито. Корисник сноси одговорност за то да обезбеди законито коришћење одабраног имена.

3.2. Почетна провера идентитета

Корисник мора да буде физички присутан у циљу утврђивања идентитета. Ближи услови регулисани су Практичним правилима.

Приватни криптографски кључ корисника генерише се у Сертификационом телу Поште на квалификованом средству за креирање електронских потписа и електронских печата.

Квалификовани сертификат за електронски потпис може се издати само физичком лицу. Физичко лице има право да у име правног лица користи квалификовани сертификат за електронски потпис, уколико му то дозволи правно лице. Квалификовани сертификат за електронски печат може се издати само правном лицу.

Сертификационо тело Поште врши проверу података о правном лицу на основу регистрованих података у службеним регистрима.

Поступак идентификације корисника описан је у Практичним правилима.

Сви подаци о кориснику које захтевају законски прописи морају да буду проверени.

Сви подаци о физичком лицу у правном лицу морају да буду проверени.

Сертификационо тело Поште не предвиђа унакрсно сертификовање.

3.3. Идентификација и аутентификација захтева за обновом кључа

Сертификационо тело Поште не дозвољава обнову кључа. Цео процес се извршава издавањем новог квалификованог сертификата.

Сертификационо тело Поште не дозвољава замену кључа после опозива. Цео процес се извршава издавањем новог квалификованог сертификата.

3.4. Идентификација и аутентификација захтева за опозивом

Корисник сертификата захтева опозив квалификованог сертификата у складу с поступком описаним у Практичним правилима.

4. ОПЕРАТИВНИ ЗАХТЕВИ У ПРОЦЕСУ ИЗДАВАЊА СЕРТИФИКАТА

4.1. Подношење захтева за издавање сертификата

Захтев може да поднесе физичко или правно лице које испуњава услове наведене у Практичним правилима.

4.2. Обрада захтева за издавање сертификата

Сертификационо тело Поште идентификује корисника и одобрава захтев за издавање квалификованог сертификата уколико су испуњени услови прописани Практичним правилима. Сертификационо тело Поште може да одбије захтев уколико нису испуњени услови прописани Практичним правилима.

4.3. Издавање сертификата

Сертификационо тело Поште издаје квалификовани сертификат после свих извршених процеса провере података и после одобрења захтева за издавање сертификата. Издавање сертификата врши се на начин којим се обезбеђује и осигурава аутентичност. Из тог разлога Сертификационо тело Поште има примењене мере којима се спречава фалсификовање сертификата. Поступци и обавештавање корисника од стране *CA* тела су описани у Практичним правилима.

4.4. Преузимање сертификата

Прихватање и преузимање квалификованог сертификата од стране корисника описано је у Практичним правилима.

4.5. Коришћење пара криптографских кључева и сертификата

Приватни криптографски кључ корисника користи се за креирање квалификованог потписа или печата, а квалификовани сертификат за валидацију квалификованог потписа или печата.

Трећа страна користи јавни кључ и квалификовани сертификат за валидацију квалификованог потписа или печата.

4.6. Обнова сертификата

Обнова квалификованог сертификата се не врши. Цео процес се извршава издавањем новог квалификованог сертификата.

4.7. Замена јавног кључа у сертификату

Замена јавног кључа у квалификованом сертификату се не врши. Цео процес се извршава издавањем новог квалификованог сертификата.

4.8. Промена података у сертификату

Промена података у квалификованом сертификату се не врши. Цео процес се извршава издавањем новог квалификованог сертификата.

4.9. Опозив и суспензија сертификата

Опозив и суспензија сертификата су регулисани Практичним правилима.

4.10. Услуге о статусу сертификата

Сертификационо тело Поште пружа услугу провере статуса/опозваности квалификованог сертификата посредством регистра опозваних сертификата и *OCSP* сервиса.

4.11.Престанак коришћења сертификата

Корисник престаје са коришћењем квалификованог сертификата после:
- истека рока важности квалификованог сертификата,
- извршеног опозива или суспензије квалификованог сертификата.

4.12.Откривање и обнова приватног кључа корисника

Сертификационо тело Поште не чува приватне кључеве корисника и не може да их открије нити обнови.

5. КОНТРОЛА ФИЗИЧКОГ ПРИСТУПА, ПРОЦЕДУРА И ОВЛАШЋЕНИХ ЛИЦА

5.1. Контрола физичког приступа

Најважнија опрема Сертификационог тела Поште која служи за пружање услуга сертификације, налази се у заштићеним просторијама, у објектима на централној и резервној локацији Сертификационог тела Поште.

Контрола физичког приступа, надзора и заштите заштићених просторија имплементирана је у складу са стандардима заштите Сертификационог тела Поште.

Сертификационо тело Поште обезбеђује да је приступ заштићеним просторијама ограничен искључиво на поуздано ауторизоване запослене.

Заштићене просторије Сертификационог тела Поште опремљене су:
- системом за непрекидни извор напајања електричном енергијом,
- системом за климатизацију,
- системом за рано откривање и аутоматску дојаву пожара.

5.2. Контрола процедура

Сертификационо тело Поште гарантује да послови, које обављају овлашћени запослени Сертификационог тела Поште, могу да буду накнадно прегледани по активностима.

Послови, обавезе и одговорности запослених дефинисани су са становишта раздвајања дужности и привилегија, односно подељени према одговарајућим поверљивим улогама.

За обављање појединих безбедносно осетљивих задатака у заштићеним просторијама захтева се учествовање прописаног броја лица са одређеним поверљивим улогама и дефинисаним задацима.

5.3. Контрола овлашћених лица

Сертификационо тело Поште има довољан број запослених са знањем, искуством и квалификацијама које су потребне за пружање услуга сертификације из опсега ове политике сертификације и Практичних правила.

Запослени у Сертификационом телу Поште морају бити квалификовани за обављање послова и подлежу провери радне способности пре почетка рада у Сертификационом телу Поште.

Врши се периодично обнављање и усавршавање знања запослених са одговарајућим поверљивим улогама.

5.4. Процедуре надгледања рада система

Догађаји који се односе на обављање делатности Сертификационог тела Поште записују се у електронске дневнике (*audit log*) и електронске евиденције, са датумом и временом догађања.

Овлашћени администратори Сертификационог тела Поште прегледају електронске дневнике и електронске евиденције једанпут недељно.

Копије електронских дневника и електронских евиденција чувају се најмање 10 година.

Електронски дневници и електронске евиденције чувају се на безбедан начин, а приступ је ограничен и могућ само лицима која имају одговарајуће поверљиве улоге.

Електронски дневници се свакодневно ажурирају.

5.5. Архивирање података

Сертификационо тело Поште врши архивирање података.

Сертификационо тело Поште је дужно да чува комплетну документацију о издатим и опозваним квалификованим сертификатима 10 година по престанку важења сертификата.

Сертификационо тело Поште обезбеђује тајност текућих и архивираних записа о квалификованим сертификатима.

5.6. Замена кључева сертификационог тела

Сертификационо тело Поште настоји да континуирано пружа услугу сертификације. Из тог разлога Сертификационо тело Поште ће довољно времена пре истека *CA* сертификата извршити генерисање нових кључева. Генерисање кључева *CA* тела могуће је спровести и раније.

5.7. Опоравак система после катастрофе

После престанка катастрофе и отклањања њеног узрока, Сертификационо тело Поште ће у најкраћем могућем року да доведе систем у продукционо стање и настави са радом у складу са Политиком управљања континуитетом пословања у Јавном предузећу „Пошта Србије“, Београд („Службени ПТТ-гласник“, број 1758/24) и Планом опоравка од катастрофе.

5.8. Престанак рада сертификационог тела

Сертификационо тело Поште, у случају престанка рада, има обавезу да:

- обавести све заинтересоване стране о престанку обављања услуга сертификације;
- пренесе своје обавезе другом сертификационом телу, уколико постоје могућности за то;
- опозове све издате квалификоване сертификате, којима није истекао рок важности, уколико не успе да пренесе своје обавезе на друго сертификационо тело;
- уништи или потпуно онемогући коришћење својих приватних кључева, који су коришћени за креирање сертификата и регистра опозваних сертификата, тако да се исти не могу реконструисати.

Корисници издатих квалификованих сертификата биће обавештени о престанку рада, преко веб сајта Сертификационог тела Поште или на други начин, посредством средстава јавног информисања или електронском поштом.

6. КОНТРОЛЕ ТЕХНИЧКЕ ЗАШТИТЕ

6.1. Генерисање пара криптографских кључева и инсталација

Пар криптографских кључева *CA* тела генерише се у хардверском криптографском модулу.

Пар криптографских кључева корисника генерише се у квалификованом средству за креирање електронских потписа и печата (*Qualified Signature Creation Device - QSCD*).

6.2. Заштита приватног криптографског кључа

У току генерисања пара криптографских кључева користи се заштита која важи за просторије Сертификационог тела Поште, заштита коју пружа хардверски криптографски модул (*Hardware Security Module - HSM*) који је у складу са стандардом *FIPS* 140-2 нивоа 3 и *EAL* 4+, оперативни систем, апликација сертификационог тела и вишеструка аутентификација овлашћених лица. *Root CA* тело је у *off-line* режиму.

Дужине криптографских кључева за које Сертификационо тело Поште издаје квалификоване сертификате су:

- Криптографски кључеви *CA* тела: *RSA* кључеви дужине 4096 бита,
- Кориснички кључеви: Прецизирано у Практичним правилима.

Сертификационо тело Поште има имплементирану вишеструку ауторизацију за присуп приватном криптографском кључу апликације сертификационог тела. Управљање приватним кључем *CA* тела спроводи се уз ауторизацију најмање две овлашћене особе са поверљивим улогама у Сертификационом телу Поште. Сертификационо тело Поште не нуди могућност откривања приватног криптографског кључа *CA* тела.

Сертификационо тело Поште врши чување сигурносних копија приватних кључева *CA* тела у *HSM* уређајима на централној и резервној локацији. Изван *HSM* кључеви се чувају у шифрованом облику у ватроотпорним безбедним касама-контејнерима, од којих се једна налази на централној локацији Сертификационог тела Поште, а друга на удаљеној, безбедној локацији. Не постоје друге копије приватних кључева. Сертификационо тело Поште не чува копије приватних кључева квалификованих сертификата.

За време док су изван *HSM* приватни кључеви *CA* тела су заштићени шифровањем. Шифровање приватних кључева спроводи се строгим придржавањем захтева наведених у документацији *HSM*, па се на тај начин осигурава једнаки ниво сигурности кључа, као када је у *HSM*. Пренос приватног кључа се врши уз ауторизацију две или више особа са поверљивим улогама у Сертификационом телу Поште уз дуалну контролу.

Пренос приватних кључева *CA* тела врши се у *HSM* једнаког или вишег нивоа сигурности у односу на криптографски модул из ког се приватни кључ преноси.

Приватни кључеви *CA* тела заштићени су хардверским криптографским модулом и могу се користити једино ако су прописно активирани.

Активацију приватних кључева *CA* тела спроводе најмање два запослена са поверљивим улогама у Сертификационом телу Поште. Сваки од запослених овлашћених за активацију *HSM* употребљава припадајућу смарт картицу и припадајућу лозинку.
Приватни кључ *CA* тела деактивира се:

- заустављањем серверског процеса *CA* тела,
- искључењем сервера на ком се налази *CA* тело,
- искључењем *HSM*.

Корисничке апликације деактивирају приватни криптографски кључ корисника после електронског потписивања и извлачења смарт картице из читача картица, односно извлачења *USB* токена из *USB* порта рачунара.

Приватни криптографски кључ *CA* тела се уништава само у случају планираног престанка рада *CA* тела, а што се спроводи само уз писану одлуку управне структуре највишег нивоа Сертификационог тела Поште. Поступком уништавања трајно су онеспособљене све сигурносне копије тог приватног кључа, па њихова употреба више није могућа.

6.3. Остали видови управљања паром кључева

Рок важности сертификата *Pošta Srbije CA Root 2026 CA* тела Сертификационог тела Поште је 25 (двадесетпет) година. Рок важности сертификата *Pošta Srbije CA 2 CA* тела Сертификационог тела Поште је 15 (петнаест) година.

Рок важности сертификата *Pošta Srbije CA Root CA* тела и сертификата *Pošta Srbije CA 1 CA* тела Сертификационог тела Поште је 25 (двадесетпет) година.

Временски период важности приватног кључа *CA* тела једнак је временском периоду важности припадајућег сертификата. Припадајући приватни кључеви *CA* сертификата не смеју се употребљавати после истека рока важности сертификата или после опозива сертификата.

Рок важности приватног кључа квалификованог сертификата једнак је временском периоду важности припадајућег сертификата, изузев квалификованог сертификата за електронски печат који се користи за валидацију временских жигова код кога је рок важности приватног кључа једна година.

6.4. Подаци за активирање

Подаци за активирање приватног кључа *CA* тела генеришу се приликом генерисања криптографских кључева (*Key Generation Ceremony*) и могу да их користе искључиво овлашћена лица Сертификационог тела Поште.

Овлашћена лица Сертификационог тела Поште су дужна да чувају лозинке које се користе за активирање кључева сертификационог тела.

Начин генерисања и достављања података за активирање приватног кључа корисника описани су у Практичним правилима.

6.5. Безбедносне контроле рачунарског система

У рачунарском систему Сертификационог тела Поште имплементиране су техничко-безбедносне контроле и механизми, и то:

- контрола приступа до системских сервиса сертификационог тела,
- контрола приступа функцијама апликације сертификационог тела,
- строга подела улога између овлашћених лица сертификационог тела,
- употреба смарт картица за смештање криптографских кључева овлашћених лица сертификационог тела,
- шифровање тајних података у бази података апликације сертификационог тела,

- безбедно архивирање података апликације сертификационог тела и електронских дневника,
- заштита електронских дневника, односно података у истима о свим догађајима који се односе на безбедност,
- успостављање механизама обнове система, криптографских кључева и базе података апликације сертификационог тела.

6.6. Технички надзор у току обављања делатности

Сертификационо тело Поште има механизме и процедуре које примењује у контроли и надзору свих техничких система сертификационог тела.

6.7. Управљање безбедношћу рачунарске мреже

Рачунарску мрежу Сертификационог тела Поште чине повезани мрежни сегменти, на којима се налазе сервери и радне станице. Сегменти су међусобно повезани *firewall*-овима. Безбедносна правила на *firewall*-овима дозвољавају саобраћај само између сервера и радних станица по протоколима који су потребни за обављање делатности Сертификационог тела Поште и за приступ сервисима Сертификационог тела Поште.

6.8. Временска ознака

Квалификовани сертификати и регистри опозваних сертификата имају временску ознаку датума и времена издавања, датума и времена престанка важења сертификата и датума и времена издавања следећег регистра опозваних сертификата. Временска ознака није криптографски/електронски временски жиг.

Криптографски/електронски временски жиг се не употребљава у опсегу услуга од поверења из овог документа.

Систем се усклађује са интерним сервисом тачног времена који је усклађен са спољним *UTC* (Coordinated Universal Time) извором тачног времена.

7. ПРОФИЛ СЕРТИФИКАТА, РЕГИСТРА ОПОЗВАНИХ СЕРТИФИКАТА И *OCSP*

7.1. Профил сертификата

Сертификационо тело Поште издаје *X*.509 сертификате верзије 3. Профили сертификата су описани у Практичним правилима.

7.2. Профил *CRL*

Сертификационо тело Поште издаје *X*.509 регистре опозваних сертификата (*Certificate Revocation List - CRL*) верзије 2. Профил регистра опозваних сертификата је описан у Практичним правилима.

7.3. *OCSP* профил

Сертификационо тело Поште омогућава *on-line* проверу статуса квалификованог сертификата посредством *OCSP* протокола (Online Certificate Status Protocol). *OCSP* профил је описан у Практичним правилима.

8. РЕВИЗИЈА УСКЛАЂЕНОСТИ РАДА СЕРТИФИКАЦИОНОГ ТЕЛА И ДРУГЕ ПРОЦЕНЕ

Надзор над радом Сертификационог тела Поште као квалификованог пружаоца услуга од поверења регулисан је законским прописима, општим актима и другим документима који регулишу ову област.

8.1. Учесталост ревизије

Провере усклађености рада Сертификационог тела Поште могу бити унутрашње или спољашње.

Сертификационо тело Поште извршава редовне унутрашње ревизије рада једанпут годишње.

Могуће је извршити и више од једне ревизије годишње уколико је то захтевано од надлежног органа или је то последица незадовољавајућих резултата претходне ревизије.

Учесталост и околности спољашње ревизије регулисани су прописима, општим актима и другим документима који регулишу ову област.

8.2. Квалификација лица које врши ревизију

Законски заступник Сертификационог тела Поште одговоран је за спровођење унутрашњих ревизија и одређивање лица која их спроводе.

Спољашњу ревизију спроводи Тело за оцењивање усаглашености.

8.3. Однос лица које врши ревизију према предмету ревизије

Лице које врши ревизију може бити запослени Сертификационог тела Поште или спољно стручно лице, према избору законског заступника Сертификационог тела Поште.

Тело за оцењивање усаглашености и његови ревизори независни су од Сертификационог тела Поште и не сме да постоји сукоб интереса.

8.4. Предмет ревизије

У оквиру ревизије проверава се:

- целовитост и тачност документације,
- усклађеност са законским прописима,
- организациони процеси и процедуре,
- технички процеси и процедуре,

- физичка сигурност предметних локација,
- примењене мере информационе безбедности.

8.5. Предузете активности као резултат пронађених недостатака

У случају пронађених недостатака, спроводе се активности на отклањању истих у што краћем року.

8.6. Објављивање извештаја ревизије

Извештај интерне ревизије представља интерни документ Сертификационог тела Поште и не објављује се јавно. Намењен је искључиво овлашћеним лицима Сертификационог тела Поште за потребе отклањања евентуално пронађених недостатака.

Извештај о оцењивању усаглашености Сертификационо тело Поште доставља надлежном органу у року од три радна дана од дана пријема од стране Тела за оцењивање усаглашености.

9. ОСТАЛИ ПОСЛОВИ И ПРАВНА ПИТАЊА

9.1. Ценовник

Сертификационо тело Поште и регистрациона тела обавештавају кориснике и трећа лица о свим услугама које се наплаћују. Уколико посебним уговором није другачије одређено, услуге се наплаћују у складу са ценовником. Ценовник свих услуга које се наплаћују објављен је на веб сајту Сертификационог тела Поште и доступан на захтев свим заинтересованим лицима.

Сертификационо тело Поште задржава право да измени ценовник.

Сертификационо тело Поште не наплаћује опозив, суспензију и прекид суспензије сертификата.

Сертификационо тело Поште не наплаћује услугу пружања информација о статусу опозваности путем регистра опозваних сертификата и *OCSP* сервиса.

Сертификационо тело Поште врши повраћај накнаде уколико је извршена погрешна уплата, плаћен већи износ накнаде и у складу са другим прописима и општим актима који регулишу права потрошача.

9.2. Одговорност

Сертификационо тело Поште сноси одговорност за обављање своје делатности у складу са важећим прописима. Износ осигурања је регулисан Практичним правилима.

9.3. Тајност пословних података

Тајни подаци су сви подаци које Сертификационо тело Поште прибави и креира у обављању своје делатности.

Приступ подацима, који се сматрају тајним, може бити одобрен овлашћеним запосленима Сертификационог тела Поште и надлежним државним органима, ако су испуњени законом прописани услови.

9.4. Заштита података о личности

Сертификационо тело Поште је дужно да се у свом пословању придржава одредби које се односе на заштиту података о личности у складу са важећим прописима.

Корисници пре издавања квалификованих сертификата потврђују да су сагласни да се врши обрада њихових података о личности.

9.5. Заштита права интелектуалне својине

Овај документ, као и друга документација Сертификационог тела Поште објављена на веб сајту Сертификационог тела Поште представља интелектуалну својину Сертификационог тела Поште, осим уколико то није другачије означено.

Сва права интелектуалне својине Сертификационог тела Поште укључујући заштитне знаке и ауторска права остају искључиво власништво Сертификационог тела Поште.

Сертификационо тело Поште не полаже право интелектуалне својине на софтвер који се користи у *PKI* систему за издавање квалификованих сертификата, а који је у власништву трећих лица.

Софтвер треће стране Сертификационо тело Поште користи у складу с одредбама важеће лиценце.

9.6. Права и обавезе

Сертификационо тело Поште гарантује пружање услуге сертификације, у складу са законом, другим прописима, овом политиком сертификације и другим општим актима Сертификационог тела Поште, који су усклађени са важећим прописима Републике Србије.

Обавезе свих учесника у *PKI* систему регулисане су Практичним правилима.

9.7. Непризнавање права

Сертификационо тело Поште признаје права корисника која су у складу са важећим прописима у Републици Србији.

9.8. Одговорност и ограничења од одговорности

Одговорност и ограничења од одговорности регулисани су Практичним правилима.

9.9. Накнаде

За пружање услуга Сертификационог тела Поште, корисник плаћа накнаде у складу са поглављем 9.1. ове политике сертификације.

9.10. Ступање на снагу и престанак важења правних аката

Правна акта Сертификационог тела Поште објављују се у „Службеном ПТТ-гласнику“, пре ступања на снагу и ступају на снагу у року утврђеном у сваком од тих аката, у складу са законом.
Ова политика сертификације и друга акта Сертификационог тела Поште доносе се и објављују на српском језику.

9.11. Појединачна обавештења и комуникација са корисницима

Сертификационо тело Поште комуницира са корисницима путем електронске поште, поште и веб сајта, осим ако није другачије одређено Практичним правилима.

9.12. Допуне Политике сертификације

Сертификационо тело Поште ће имплементирати промене у своје важеће акте у случају промене регулативе и процедура рада.

9.13. Спорови између сертификационог тела и корисника

Сви спорови између Сертификационог тела Поште, корисника и трећег лица биће решавани договором, а у случајевима када то није могуће, спор ће решавати надлежни суд у Београду.

9.14. Меродавно право

За тумачење и примену ове политике сертификације меродавно је право Републике Србије.

9.15. Усклађеност са важећим законодавством

Правна акта Сертификационог тела Поште доносе се у складу са законом и другим прописима Републике Србије, који регулишу ову област.

9.16. Остале одредбе

Сертификационо тело Поште ослобађа се одговорности за било коју штету причињену кориснику, другом учеснику или трећем лицу, приликом пружања услуга сертификације, уколико је до штете дошло услед разлога који су ван контроле Сертификационог тела Поште, односно услед више силе.

9.17. Друге одредбе

До ступања на снагу ове политике сертификације примењиваће се Политика сертификације Сертификационог тела Јавног предузећа „Пошта Србије“, Београд за квалификоване електронске сертификате са новог система (*Certificate Policy*) („Службени ПТТ-гласник“, број 1307/20), чија важност престаје по ступању на снагу ове политике.

Ова политика сертификације, ступа на снагу осмог дана од дана објављивања у „Службеном ПТТ-гласнику“.

„ПОШТА СРБИЈЕ“ д.о.о.
В. Д. ДИРЕКТОРА
Зоран Анђелковић, с. р.