ПРАКТИЧНА ПРАВИЛА ПРУЖАЊА УСЛУГЕ СЕРТИФИКАЦИЈЕ ЗА КВАЛИФИКОВАНЕ ЕЛЕКТРОНСКЕ СЕРТИФИКАТЕ

(Certification Practices Statement - CPS)

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).

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

Осим Политике сертификације за квалификоване електронске сертификате (у даљем тексту: Политика сертификације) и ових практичних правила, Сертификационо тело Поште утврђује и интерна правила рада Сертификационог тела Поште и заштите система сертификације.

Интерна правила су интерни документ и представљају пословну тајну 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

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.

Функционисање хијерархијске инфраструктуре у потпуности је у складу са Политиком сертификације и Практичним правилима која су обавезујућа за Сертификационо тело Поште, лица којима је Сертификационо тело Поште издало квалификовани сертификат и трећа лица која се поуздају у сертификат издат од стране Сертификационог тела Поште (у даљем тексту: поуздајуће стране).

Квалификовани сертификати су стандардни сертификати *X*.509 верзије 3 који су намењени за валидацију квалификованог електронског потписа или печата.

Корисници квалификованих сертификата Сертификационог тела Поште поседују један пар криптографских кључева (јавни и приватни кључ). Приватни криптографски кључ користи се за квалификовано електронско потписивање или печатирање, а јавни криптографски кључ користи се за валидацију квалификованог електронског потписа или печата.

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“.

1.2. Назив документа и идентификациони подаци

Овај документ носи назив „Практична правила пружања услуге сертификације за квалификоване електронске сертификате“ (у даљем тексту: Практична правила), као што је означено на почетној страни документа.

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.

1.3.1. Сертификациона тела

Сертификационо тело Поште, обухвата следећа сертификациона тела (*Certification Authority - CA*): „*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.

1.3.2. Регистрациона тела

Регистрациона тела (*Registration Authority - RA*) Сертификационог тела Поште су:

- Централно регистрационо тело које ради у седишту Сертификационог тела Поште и које је овлашћено за одобравање и прослеђивање података за издавање квалификованих сертификата и захтева за промену статуса сертификата према апликацији сертификационог тела;
- Локална регистрациона тела (*Local Registration Authority - LRA*), која раде у седишту Сертификационог тела Поште и на удаљеним локацијама, а то су овлашћене јединице поштанске мреже (у даљем тексту: поште) на територији Републике Србије, овлашћене за проверавање идентитета корисника и за прослеђивање података о извршеној личној идентификацији у поступцима издавања квалификованих сертификата и захтева за промену статуса сертификата према централном регистрационом телу.

1.3.3. Корисници

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

Корисници Сертификационог тела Поште могу да буду:

- 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 по другом основу који нема карактер радног односа ангажовани у правном лицу (у даљем тексту: физичко лице у правном лицу).

1.3.4. Поуздајуће стране

Поуздајуће стране, односно трећа лица су физичка лица (појединци) и/или правна лица 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 обавезне су 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.

Регистар опозваних сертификата ажурира се на дневном нивоу. Поуздајуће стране проверавају најновије расположиве информације о опозваности да би имале комплетну и правовремену информацију о опозивању и суспензији сертификата.

Ни под којим условима се не треба ослањати на пружени податак о опозваности сертификата дуже од максималног рока важења примљеног одговора (*CRL* или *OCSP*) који садржи податак о опозваности.

1.3.5. Остали учесници

Остали учесници су правна лица која, на неки начин, доприносе или учествују у обезбеђивању квалитета рада Сертификационог тела Поште: осигуравајуће друштво, произвођачи и дистрибутери опреме и софтвера.

1.4. Употреба сертификата

1.4.1. Подручје примене

Квалификовани сертификати и припадајући приватни криптографски кључеви користе се за:

- квалификовано електронско потписивање или печатирање и
- аутентификацију корисника.

Приватни криптографски кључеви који су придружени квалификованим сертификатима користе се у процесу квалификованог електронског потписивања или печатирања електронског документа, који се може користити у општењу органа и општењу органа и странака, у правним пословима и другим правним радњама, као и у управном, судском и другом поступку пред државним органом, ако је законом којим се утврђује тај поступак, прописана употреба квалификованог електронског потписа или печата.

Квалификовани сертификати потврђују везу између јавног криптографског кључа корисника и идентитета корисника који је извршио квалификовано електронско потписивање или печатирање електронског документа.

1.4.2. Недозвољене примене

Свака друга употреба квалификованог сертификата која није дефинисана овим документом и није у сагласности са одредбама закона којим се уређује електронски потпис или печат и другим документима који регулишу ову област, није дозвољена.

1.5. Политика администрирања документа

1.5.1. Организација управљања документом

Документ Практична правила креира и ажурира Сертификационо тело Поште:

„Пошта Србије д.о.о.
Сертификационо тело Поште
Таковска 2
11120 Београд
Република Србија
Телефон: 011/3607-895
Факс: 011/3651-412
Е-пошта: cepp@posta.rs
Веб сајт: https://www.ca.posta.rs

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

1.5.2. Лица за контакт

Лица за контакт Сертификационог тела Поште су руководилац организационе целине надлежне за електронско пословање у Сертификационом телу Поште, запослени који обављају послове техничке подршке и други запослени овлашћени за давање информација у вези примене Практичних правила и других аката Сертификационог тела Поште.

Контакт адресе запослених у Пошти Србије д.о.о. који обављају послове техничке подршке и других запослених који су овлашћени за давање информација у вези примене Практичних правила и других аката Сертификационог тела Поште објављене су на званичном веб сајту Сертификационог тела Поште.

1.5.3. Лица одређена за усклађивање документа са праксом издавања сертификата

Управна структура Сертификационог тела Поште усклађује форму и садржај ових практичних правила са евентуалним променама насталим у пракси издавања квалификованих сертификата.

Такође, управна структура Сертификационог тела Поште редовно процењује усклађеност ових практичних правила са важећим законима.

1.5.4. Процедуре за одобрење Практичних правила

Измене или допуне Практичних правила врше се у складу са прописима, општим актима и другим актима која регулишу ову област, те зато могу бити предмет давања одобрења надлежног државног органа. Предлог измена и/или допуна Практичних правила 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 скраћеним потписом (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 овим практичним правилима 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 Поште 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 електронских 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
AES (Advanced Encryption Standard)	Алгоритам симетричне криптографије намењен за шифровање
CA (Certification Authority)	Сертификационо тело
CPS (Certification Practice Statement)	Практична правила пружања услуга сертификације сертификационог тела
CRL (Certificate Revocation List)	Регистар опозваних сертификата
EAL (Evaluation Assurance Level)	Тестирани ниво сигурности (постоји седам нивоа сигурности 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 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
OID (Object Identifier)	Идентификатор објекта
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 Protocol)	Протокол за приступ јавном директоријуму
UTC (Coordinated Universal Time)	Координисано универзално време
ETSI (European Telecommunications Standards Institute)	Европски институт за стандарде из области телекомуникација
IPS (Intrusion Prevention System)	Систем за превенцију упада
NTP (Network Time Protocol)	Протокол мрежног времена

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. Веб сајт је јавно доступан, као и документација која се на њој налази.

2.2. Објављивање података о сертификацији

Сертификационо тело Поште објављује на својој веб страни:
- Политику сертификације,
- 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 законским актима и друге информације објављују се пре почетка примене законских аката 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. Објављивање ових докумената обавља се без претходне најаве, а старије верзије докумената се уклањају.

2.3. Учесталост објављивања података о сертификацији

Сертификационо тело Поште ажурира објављене податке следећом динамиком:

- регистре опозваних сертификата објављује на свака 24 сата.
- све остале податке и документе објављује после евентуалних измена које су усвојене и одобрене од стране надлежних органа Сертификационог тела Поште или надлежног државног органа.

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 логичке и физичке сигурносне мере у циљу спречавања неауторизованог додавања, брисања или промене, као и заштите интегритета и аутентичности. Приступ објављеним документима и информацијама је ограничен на могућност читања.

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

3. ИДЕНТИФИКАЦИЈА И АУТЕНТИФИКАЦИЈА

3.1. Одређивање имена

3.1.1. Врсте имена

У квалификованим електронским сертификатима које издаје Сертификационо тело Поште, име сертификационог тела које издаје сертификате, поље *Issuer* (Табела 2, Табела 3, Табела 4. и Табела 5.) и име корисника сертификата, поље *Subject* (Табела 6, Табела 7. и Табела 8.), су јединствена имена (*Distinguished Name - DN*).

Табела 2. Структура имена *Root* сертификационог тела „*Pošta Srbije CA Root 2026*“ у квалификованим сертификатима

Име *CA* сервера (CN) =	*Pošta Srbije CA Root 2026*

Организација (O) =	*Pošta Srbije d.o.o.*
Идентификатор организације (2.5.4.97) =	*VATRS-100002803*
Место (L) =	*Beograd*
Ознака државе (C) =	*RS*

Табела 3. Структура имена подређеног сертификационог тела „*Pošta Srbije CA 2*“ у квалификованим сертификатима

Име *CA* сервера (CN) =	*Pošta Srbije CA 2*
Организација (O) =	*Pošta Srbije d.o.o.*
Идентификатор организације (2.5.4.97) =	*VATRS-100002803*
Место (L) =	*Beograd*
Ознака државе (C) =	*RS*

Табела 4. Структура имена *Root* сертификационог тела „*Pošta Srbije CA Root*“ у квалификованим сертификатима

Име *CA* сервера (CN) =	*Pošta Srbije CA Root*
Организација (O) =	*Javno preduzeće Pošta Srbije*
Идентификатор организације (2.5.4.97) =	*VATRS-100002803*
Место (L) =	*Beograd*
Ознака државе (C) =	*RS*

Табела 5. Структура имена подређеног сертификационог тела „*Pošta Srbije CA 1*“ у квалификованим сертификатима

Име *CA* сервера (CN) =	*Pošta Srbije CA 1*
Организација (O) =	*Javno preduzeće Pošta Srbije*
Идентификатор организације (2.5.4.97) =	*VATRS-100002803*
Место (L) =	*Beograd*
Ознака државе (C) =	*RS*

Табела 6. Структура имена корисника квалификованог сертификата за електронски потпис

Јединствено име (CN) =	*Ime prezime JIK* (Име и презиме корисника са додатком јединственог идентификатора корисника (ЈИК)).
Име (G) =	*Ime*
Презиме (SN) =	*Prezime*
Серијски број (SERIALNUMBER) =	*PNORS-JMBG* (Јединствени матични број (ЈМБГ) физичког лица).*
Серијски број (SERIALNUMBER) =	*CA:RS-JIK* (Јединствени идентификатор корисника).
Организациона јединица (O) =	*Naziv pravnog lica**
Идентификатор организације (2.5.4.97) =	*MB:RS-MB* (Матични број правног лица).*
Идентификатор организације (2.5.4.97) =	*VATRS-PIB* (Порески идентификациони број (ПИБ) број правног лица).*

Ознака државе (C) =	*RS*

* Подаци означени звездицом су опциони.

Табела 7. Структура имена корисника квалификованог сертификата за електронски потпис који је издат странцу на основу путне исправе (пасоша)

Јединствено име (CN) =	*Ime prezime JIK* (Име и презиме корисника са додатком јединственог идентификатора корисника (ЈИК)).
Име (G) =	*Ime*
Презиме (SN) =	*Prezime*
Серијски број (SERIALNUMBER) =	*PASXX-Broj pasoša* (Двословна ознака државе издаваоца и број пасоша).
Серијски број (SERIALNUMBER) =	*CA:RS-JIK* (Јединствени идентификатор корисника).
Организациона јединица (O) =	*Naziv pravnog lica**
Идентификатор организације (2.5.4.97) =	*MB:RS-MB* (Матични број правног лица).*
Идентификатор организације (2.5.4.97) =	*VATRS-PIB* (Порески идентификациони број (ПИБ) број правног лица).*
Ознака државе (C) =	*XX* (Двословна ознака државе издаваоца пасоша).

* Подаци означени звездицом су опциони.

Табела 8. Структура имена корисника квалификованог сертификата за електронски печат

Јединствено име (CN) =	*Naziv pravnog lica JIK* (Назив правног лица са додатком јединственог идентификатора корисника (ЈИК)).
Серијски број (SERIALNUMBER) =	*CA:RS-JIK* (Јединствени идентификатор корисника).
Организациона јединица (O) =	*Naziv pravnog lica*
Идентификатор организације (2.5.4.97) =	*MB:RS-MB* (Матични број правног лица).
Идентификатор организације (2.5.4.97) =	*VATRS-PIB* (Порески идентификациони број (ПИБ) број правног лица).
Ознака места (L) =	*Naziv mesta* (седиште правног лица/државног органа)
Ознака државе (C) =	*RS*

Табела 8а. Структура имена корисника квалификованог сертификата за електронски печат који се користи за валидацију временских жигова

Јединствено име (CN) =	*Naziv jedinice JIK* (Назив јединице за формирање временских жигова са додатком јединственог идентификатора корисника (ЈИК)).
Серијски број (SERIALNUMBER) =	*CA:RS-JIK* (Јединствени идентификатор корисника).
Организациона јединица (O) =	*Naziv pravnog lica*

Идентификатор организације (2.5.4.97) =	*MB:RS-MB* (Матични број правног лица).
Идентификатор организације (2.5.4.97) =	*VATRS-PIB* (Порески идентификациони број (ПИБ) број правног лица).
Ознака државе (C) =	*RS*

3.1.2. Смисленост имена

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, које је запослено 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.

3.1.3. Анонимност или псеудоними корисника

Корисници не могу да буду анонимни.

Сертификационо тело Поште одбија било који захтев за анонимношћу.

Корисници не могу да користе псеудоним.

3.1.4. Правила за тумачење различитих врста имена

У квалификованим сертификатима су имена корисника верно представљена одговарајућим латиничним словима из српског језика.

Коришћење специјалних знакова у именима корисника није дозвољено. Исте је потребно изоставити или заменити другим знацима.

3.1.5. Јединственост имена

Сертификационо тело Поште гарантује јединственост имена у свом домену. Сертификационо тело Поште додељује сваком кориснику јединствено име (*Distinguished Name - DN*), које се уписује у поље *Subject* квалификованог сертификата.

3.1.6. Признавање, аутентификација и улога заштитног знака

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.

Сертификационо тело Поште ће, што је могуће пре, извршити све судске налоге који су издати у складу са законима, а који се тичу правних лекова за било какво кршење права трећих лица приликом издавања квалификованих сертификата по овим практичним правилима.

3.2. Почетна провера идентитета

Почетна провера тачности идентитета је део поступка подношења захтева за издавање сертификата.

3.2.1. Метод доказивања поседа приватног кључа

Приватни криптографски кључ корисника генерише се у Сертификационом телу Поште на квалификованом средству за креирање електронских потписа и електронских печата. У случају квалификованог сертификата за електронски печат који се издаје на HSM уређају корисника, који је квалификовано средство за електронски печат, приватни криптографски кључ се генерише у HSM уређају корисника у присуству представника Сертификационго тела Поште.

3.2.2. Аутентификација идентитета правног лица

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 се може издати само правном лицу.

Уколико Сертификационо тело Поште издаје квалификовани сертификат физичком лицу, које је запослено у правном лицу, у оквиру атрибута који идентификују корисника налазе се: пословно име правног лица, матични број и порески идентификациони број правног лица.

Уколико је корисник физичко лице у правном лицу, неопходно је:

- да се утврди тачан идентитет правног лица и ауторизовање коришћења његовог имена,
- да би се проверила ваљаност имена правног лица, подносилац захтева мора да обезбеди службена документа о том правном лицу не старија од 30 дана од дана подношења захтева (оригинал/копија решења о упису/регистрацији правног лица или оригинал/копија извода о регистрацији правног лица или копија извода о основним регистрованим подацима правног лица штампаним са веб сајта одговарајућег регистра, који садржи датум штампе),
- доказ да је корисник овлашћен од стране правног лица за добијање квалификованог електронског сертификата.

3.2.3. Аутентификација идентитета физичког лица

Корисник мора да буде идентификован у складу са овим практичним правилима.

Током регистрације корисник мора да поседује важећи идентификациони документ са фотографијом (важећа лична карта, пасош или други). Приликом регистрације корисник треба да приложи квалитетну фотокопију идентификационог документа.

Будући корисник квалификованог електронског сертификата може да захтева квалификовани електронски сертификат у своје лично име (физичка лица) или у име корисника у оквиру правног лица, као овлашћено лице правног лица/државног органа. Регистрационо тело проверава и потврђује идентитет будућег корисника квалификованог електронског сертификата.

Приликом уручења овлашћено лице Сертификационог тела Поште фотографију у документу за идентификацију пореди са корисником који је физички присутан (карактеристике лица, старост, пол и сл).

3.2.4. Непроверени подаци о кориснику

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

3.2.5. Провера тачности података правног лица

Корисник доставља важећу документацију за пословно име правног лица, које ће бити укључено у квалификовани сертификат. Избор речи у имену правног лица које треба уписати у квалификовани сертификат мора да буде идентичан речима у достављеној документацији.

Сагласно закону којим се уређују електронски потпис и печат, коришћење пословног имена правног лица морају дозволити и ауторизовати одговорни представници правног лица, и то:

- коришћење пословног имена правног лица које је регистровано у надлежном регистру морају да ауторизују одговорни представници,
- коришћење имена правног лица које има једног власника, мора да ауторизује власник,
- коришћење пословног имена правног лица које је власништву више партнера, мора да ауторизује партнер који је наведен у уговору о партнерству,
- коришћење пословног имена правног лица које је власништво неке заједнице (верске заједнице, организације, удружења и др.), мора да ауторизује одговарајући субјект права својине.

3.2.6. Критеријуми за међусобну сарадњу

Сертификационо тело Поште не предвиђа унакрсно сертификовање.

3.3. Идентификација и аутентификација захтева за обновом кључа

3.3.1. Идентификација и аутентификација захтева за рутинском обновом кључа

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

3.3.2. Идентификација и аутентификација захтева за заменом кључа после опозива

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 или овлашћено лице правног лица/државног органа које је поднело захтев за издавање сертификата захтева опозив квалификованог сертификата по једној од следећих процедура:

- корисник предаје својеручно потписан захтев локалном регистрационом телу или
- корисник шаље образац захтева за промену статуса потписан важећим квалификованим сертификатом издатим од стране сертификационог тела уписаног у Регистар пружалаца квалификованих услуга од поверења у Републици Србији путем електронске поште Сертификационом телу Поште, на унапред одређену адресу електронске поште.

4. ОПЕРАТИВНИ ЗАХТЕВИ У ПРОЦЕСУ ИЗДАВАЊА СЕРТИФИКАТА

4.1. Подношење захтева за издавање сертификата

4.1.1. Ко може да поднесе захтев за издавање сертификата

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

4.1.2. Услови за издавање сертификата

За издавање квалификованог сертификата корисник који се идентификује као физичко лице дужан је да:

- попуни и потпише захтев за издавање квалификованог електронског сертификата,
- попуни и потпише уговор,
- испуни захтеве за идентификацију,
- испуни финансијске обавезе према ценовнику.

За издавање квалификованог сертификата за електронски печат или квалификованог сертификата за електронски потпис физичком лицу у правном лицу, корисник је дужан да:

- достави документацију потребну за закључење уговора,
- попуни и потпише уговор,
- испуни захтеве за идентификацију,
- испуни финансијске обавезе према ценовнику.

Документација за издавање квалификованог сертификата садржи податке на основу којих Сертификационо тело Поште може да ступи у контакт са корисником квалификованог сертификата.

Уговор о пружању услуга Сертификационог тела Поште садржи услове издавања и коришћења сертификата, а ступа на снагу потписивањем обе уговорне стране.

Коришћење сертификата, по правилу, уговара се са роком важности од 1 (једне) до 5 (пет) година и везује се за датум издавања сертификата. Под датумом издавања сертификата сматра се датум када је он креиран у Сертификационом телу Поште и уписан на средство за креирање квалификованог електронског потписа или печата.

4.2. Обрада захтева за издавање сертификата

4.2.1. Обављање функција идентификације и потврђивања аутентичности

Сертификационо тело Поште идентификује корисника на основу докумената за идентификацију које корисник подноси (важећа лична карта, пасош или други).

4.2.2. Одобрење или одбијање захтева за издавање сертификата

Сертификационо тело Поште ће одобрити захтев за издавање квалификованог електронског сертификата, уколико су испуњени следећи услови:

- корисник је поднео идентификациону документацију,
- сва документација је успешно примљена и проверена,
- сви подаци унети у захтев сматрају се одговарајућим и комплетним.

Ако корисник не испуни услове из става 1. ове тачке или ако на било који начин повреди одредбе ових практичних правила, Сертификационо тело Поште ће одбити захтев за издавање квалификованог електронског сертификата.

4.2.3. Време обраде захтева за издавање сертификата

Сертификационо тело Поште врши обраду захтева одмах после приспећа захтева од стране локалног регистрационог тела, тако да обрада може да траје најдуже 10 радних дана од дана пријема захтева, уколико је документација комплетна и уплата извршена у складу са инструкцијама.

Ако подносилац захтева не комплетира документацију за издавање сертификата у року од 60 дана од дана подношења захтева и не изврши уплату по достављеном предрачуну, сматра се да је одустао од захтева за издавање сертификата.

4.3. Издавање сертификата

4.3.1. Активности током издавања сертификата

Издавање квалификованог електронског сертификата, врши се на следећи начин:

1) корисник електронски попуњава, преузима и штампа Захтев за издавање квалификованог електронског сертификата преко веб сајта Сертификационог тела Поште,
2) корисник се идентификује пред регистрационом телом,
3) после успешне идентификације, регистрационо тело шаље потписан захтев корисника сертификацоном телу.
4) Сертификационо тело проверава захтев корисника и прихвата или одбија захтев корисника,
5) у случају прихватања захтева, кориснички приватни криптографски кључ се генерише у квалификованом средству за креирање електронских потписа и електронских печата у сертификационом телу,
6) корисник лично преузима квалификовани сертификат на изабраној локацији на територији Републике Србије,
7) припадајућа лозинка се доставља кориснику одвојено од квалификованог средства за креирање електронских потписа и печата.

4.3.2. Обавештавање корисника о издавању сертификата

Сертификационо тело Поште корисника обавештава о издавању сертификата коришћењем контакт података које је он навео приликом регистрације.

4.4. Преузимање сертификата

4.4.1. Поступак преузимања сертификата

Кориснику се квалификовани сертификат уручује лично на изабраној локацији на територији Републике Србије.

Првом употребом квалификованог сертификата од стране корисника, сертификат се сматра прихваћеним.
Уколико се накнадно утврди да у квалификованом сертификату постоје погрешни подаци, корисник је дужан да се обрати Сертификационом телу Поште, ради издавања новог квалификованог сертификата.

4.4.2. Објављивање сертификата

Квалификовани сертификат јавно се не објављује од стране Сертификационог тела Поште.

4.4.3. Обавештење о издавању сертификата трећих лица

Трећа лица се не обавештавају о издавању квалификованог сертификата.

4.5. Коришћење пара криптографских кључева и сертификата

4.5.1. Коришћење приватног кључа корисника и сертификата корисника

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

4.5.2. Коришћење јавног кључа и сертификата од стране трећег лица

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.

4.6.1. Околности за обнову сертификата

Не врши се.

4.6.2. Ко може да захтева обнову сертификата

Не врши се.

4.6.3. Обрада захтева за обнову сертификата

Не врши се.

4.6.4. Обавештење корисника о обнови сертификат

Не врши се.

4.6.5. Поступак прихватања обавештења о обнови сертификата

Не врши се.

4.6.6. Објављивање сертификата код кога је извршена обнова

Не врши се.

4.6.7. Обавештење трећих лица о издавању сертификата

Не врши се.

4.7. Замена јавног кључа у сертификату

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

4.7.1. Околности за замену јавног кључа у сертификату

Не врши се.

4.7.2. Ко може да захтева замену јавног кључа у сертификату

Не врши се.

4.7.3. Обрада захтева за замену јавног кључа у сертификату

Не врши се.

4.7.4. Обавештење корисника о замени јавног кључа у сертификату

Не врши се.

4.7.5. Поступак прихватања обавештења о замени јавног кључа у сертификату

Не врши се.

4.7.6. Објављивање сертификата код кога је извршена замена јавног кључа

Не врши се.

4.7.7. Обавештење трећих лица о издавању сертификата

Не врши се.

4.8. Промена података у сертификату

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

4.8.1. Околности за промену података у сертификату

Не врши се.

4.8.2. Ко може да захтева промену података у сертификату

Не врши се.

4.8.3. Обрада захтева за промену података у сертификату

Не врши се.

4.8.4. Обавештење корисника о промени података у сертификату

Не врши се.

4.8.5. Поступак прихватања обавештења о промени података у сертификату

Не врши се.

4.8.6. Објављивање сертификата код кога је извршена промена података

Не врши се.

4.8.7. Обавештење трећих лица о издавању сертификата

Не врши се.

4.9. Опозив и суспензија сертификата

4.9.1. Околности опозива сертификата

Сертификационо тело Поште дужно је да опозове квалификовани сертификат из следећих разлога:

- губитка, оштећења или злоупотребе техничких средстава (хардвера или софтвера) или приватног криптографског кључа, односно компромитовања или сумње у компромитовање приватног криптографског кључа,
- промене података у издатом сертификату,
- неиспуњавања обавеза корисника сертификата одређених овим практичним правилима и уговором,
- накнадног утврђивања да подаци које је доставио корисник при идентификацији нису тачни,
- уколико опозив квалификованог сертификата захтева корисник сертификата, или овлашћено лице правног лица које је захтевало издавање сертификата за корисника,
- уколико корисник квалификованог сертификата изгуби пословну способност или правно лице којем припада корисник престане да постоји,
- уколико се промене околности које битно утичу на важење сертификата,
- из других разлога који су утврђени законом и другим прописима који регулишу ову област.

4.9.2. Ко може да захтева опозив сертификата

Опозив квалификованог сертификата може да захтева:

- корисник квалификованог сертификата, или овлашћено лице правног лица које је захтевало издавање сертификата за корисника,
- Сертификационо тело Поште,
- надлежни државни орган на основу закона.

4.9.3. Процедуре за опозив сертификата

4.9.3.1. Опозив сертификата услед компромитовања приватног криптографског кључа

Опозив квалификованог сертификата услед компромитовања или сумње у компромитовање приватног криптографског кључа, врши се по једној од следећих процедура, и то:

1) Корисник електронски попуњава, преузима и штампа Захтев за промену статуса електронског сертификата преко веб сајта Сертификационог тела Поште, идентификује се и предаје својеручно потписан захтев регистрационом телу;

2) Корисник електронски попуњава и преузима Захтев за промену статуса електронског сертификата преко веб сајта Сертификационог тела Поште, а Захтев потписује важећим квалификованим сертификатом издатим од стране сертификационог тела уписаног у Регистар пружалаца квалификованих услуга од поверења у Републици Србији и доставља на унапред одређену адресу електронске поште.

Сертификационо тело Поште у оба случаја проверава захтев корисника и опозива квалификовани сертификат, или одбија захтев.
Сертификационо тело Поште обавештава корисника о опозиву квалификованог сертификата електронском поштом, или о разлозима за одбијање захтева.

Сертификационо тело Поште може да се одлучи за опозив квалификованог сертификата и без захтева корисника, уколико установи да је дошло до компромитовања приватног криптографског кључа и у другим случајевима предвиђеним Законом.

После опозива квалификованог сертификата, корисник може да захтева издавање новог квалификованог сертификата.

4.9.3.2. Опозив сертификата услед промене података у сертификату

Опозив квалификованог електронског сертификата услед промене података у сертификату, врши се на исти начин како је одређено у тачки 4.9.3.1.

Сертификационо тело Поште може да се одлучи за опозив квалификованог сертификата и без захтева корисника, уколико процени да је дошло до промене података у сертификату.

После опозива квалификованог сертификата, корисник може да захтева издавање новог квалификованог сертификата.

4.9.3.3. Опозив сертификата услед неиспуњења обавеза корисника

У случају да корисник не испуњава своје обавезе, Сертификационо тело Поште спроводи процедуру опозива квалификованог сертификата корисника:
1) опозива квалификовани сертификат корисника,
2) обавештава корисника о опозиву квалификованог сертификата електронском поштом.

После опозива квалификованог сертификата, корисник може да захтева издавање новог квалификованог сертификата.

4.9.4. Време од пријаве до опозива сертификата

После подношења захтева за опозив квалификованог сертификата од стране корисника, Сертификационо тело Поште ће приступити обради захтева за опозив сертификата, без одлагања.

4.9.5. Временски рок у коме сертификационо тело спроводи захтев за опозив сертификата

Сертификационо тело Поште извршава опозив квалификованог сертификата одмах по пријему захтева за опозив сертификата, а после спроведене идентификације.

4.9.6. Захтев за проверу опозваности сертификата од стране поуздајућих страна

Током рада са квалификованим сертификатима издатим од стране Сертификационог тела Поште, поуздајуће стране имају обавезу да проверавају опозваност сертификата.

4.9.7. Учесталост објављивања регистра опозваних сертификата

Регистар опозваних сертификата подређеног (*subordinate*) сертификационог тела редовно се објављује на свака 24 сата.

Регистар опозваних сертификата *Root* сертификационог тела редовно се објављује на сваких 12 месеци и приликом опозива подређеног (*subordinate*) сертификационог тела.

4.9.8. Максимално кашњење у објављивању регистра опозваних сертификата

У случају да пре редовне објаве, дође до опозива или суспензије квалификованог сертификата, Сертификационо тело Поште може да објави нови регистар опозваних сертификата и пре истека рока важности регистра опозваних сертификата.

4.9.9. Расположивост *on-line* провере опозваности/статуса сертификата

Регистар опозваних сертификата и *OCSP* сервис су стално доступни за *on-line* проверу опозваности квалификованих сертификата.

4.9.10. Захтеви за *on-line* проверу опозваности сертификата

Корисници и поуздајуће стране дужни су да провере статус квалификованог сертификата на основу јавно доступног регистра опозваних сертификата или *OCSP* сервиса Сертификационог тела Поште.

4.9.11. Друге форме регистра опозваних сертификата

Регистар опозваних сертификата је расположив на веб страни и *LDAP* серверу Сертификационог тела Поште.

4.9.12. Посебни захтеви у случају компромитовања кључа

Ако корисник зна или сумња у компромитацију његовог приватног кључа дужан је да одмах престане са његовим коришћењем и поднесе захтев за опозив квалификованог сертификата.

4.9.13. Околности суспензије и прекида суспензије сертификата

Суспензија је намењена привременом деактивирању квалификованог сертификата који је издат кориснику.

Сертификационо тело Поште може да суспендује квалификовани сертификат у току проверавања околности у вези са могућим опозивом сертификата.

Прекидом (укидањем) суспензије квалификовани сертификат постаје активан, тако да има све функционалности које је имао и пре суспензије.

4.9.14. Ко може да захтева суспензију и прекид суспензије сертификата

Суспензију квалификованог сертификата може да захтева:
- корисник квалификованог сертификата,
- Сертификационо тело Поште,
- надлежни државни орган, на основу закона.

Прекид суспензије може да захтева:
- корисник квалификованог сертификата, када установи да су разлози за суспензију престали,
- Сертификационо тело Поште, када установи да су разлози за суспензију престали,
- надлежни државни орган, на основу закона.

4.9.15. Процедуре за суспензију и прекид суспензије сертификата

Суспензија или прекид суспензије квалификованог сертификата, на захтев корисника, врши се на следећи начин:
1) корисник подноси Захтев за промену статуса електронског сертификата по једној од следећих процедура:
- корисник електронски попуњава, преузима и штампа тај захтев са веб сајта Сертификационог тела Поште, својеручно га потписује и предаје регистрационом телу или
- корисник електронски попуњава и преузима тај захтев са веб сајта Сертификационог тела Поште, потписује га важећим квалификованим сертификатом издатим од стране сертификационог тела уписаног у Регистар пружалаца квалификованих услуга од поверења у Републици Србији и доставља на унапред одређену адресу електронске поште;
2) Сертификационо тело Поште, у оба случаја, проверава захтев корисника, спроводи га или одбија.
3) Сертификационо тело Поште обавештава корисника о суспензији или прекиду суспензије квалификованог сертификата електронском поштом, или о разлозима за одбијање захтева.

Сертификационо тело Поште може да се одлучи за суспензију квалификованог сертификата и без захтева корисника, уколико сумња да је дошло до компромитовања приватног криптографског кључа корисника или сумња да је дошло до промене података у сертификату.

4.9.16. Ограничење периода на који се сертификат суспендује

Суспензија сертификата траје онолико дуго колико трају и услови због којих је суспензија и захтевана, а максимално 30 дана. По истеку овог рока Сертификационо тело Поште опозива сертификат.

4.10. Услуге о статусу сертификата

4.10.1. Оперативне карактеристике

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

4.10.2. Доступност услуге

Регистар опозваних сертификата и *OCSP* сервис су стално доступни.

4.10.3. Додатне карактеристике

У регистру опозваних сертификата и *OCSP* одговору поред података о серијском броју, датуму и времену опозива квалификованог сертификата уписан је и разлог опозива сертификата.

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

4.12.1. Политика откривања и обнове приватног кључа корисника

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

4.12.2. Политика енкапсулације кључа сесије и обнове

Не врши се.

5. КОНТРОЛА ФИЗИЧКОГ ПРИСТУПА, ПРОЦЕДУРА И ОВЛАШЋЕНИХ ЛИЦА

Ово поглавље описује контролу физичког окружења, процедура и овлашћених лица, која је имплементирана у Сертификационом телу Поште да би се заштитило функционисање система.

5.1. Контрола физичког приступа

5.1.1. Локација и размештај просторија

Најважнија опрема Сертификационог тела Поште која служи за обављање делатности из ових практичних правила, 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, и то на следећи начин:

- приступ у заштићене просторије електронски се бележи и уноси у електронски дневник за приступ просторији, а исти се периодично прегледа,
- приступ без пратње ограничен је на лица која се налазе на листи за приступ,
- приступ са пратњом уз претходно одобрење овлашћеног лица Сертификационог тела Поште захтева се за сва лица која се не налазе на листи за приступ,
- приступ због одржавања система мора бити унапред најављен, осим у случају хитне интервенције,
- зидови су ојачане конструкције,
- браве, електронски системи заштите и системи противпожарне заштите одобрени су од стране организационог дела Сертификационог тела Поште, надлежног за безбедност и заштиту,
- простор и систем надгледани су 24 сата/7 дана у недељи од стране овлашћених лица организационог дела Сертификационог тела Поште и заштићени системом противпровалне заштите, односно сензорима који су повезани са централним уређајем за надзор просторија,
- заштићене просторије су обезбеђене од излива воде.

5.1.2. Контрола физичког приступа за појединце

Сертификационо тело Поште обезбеђује да је приступ систему сертификације ограничен искључиво на поуздано ауторизоване запослене.

Запослени Сертификационог тела Поште мора да се придржава следећих обавеза:

- извршава своје администраторске дужности у заштићеним просторијама, у које је улазак могућ искључиво уз идентификацију са бесконтактном картицом,
- штити лозинке које омогућавају приступ приватним криптографским кључевима,
- смешта картице *HSM* администратора и оператера и друге медије који садрже криптографске кључеве у безбедну касу-контејнер, за чије отварање је потребан пар кључева и шифра,
- смешта резервне копије приватног кључа у безбедну касу-контејнер,
- одјављује се са свих апликација у случају да напушта рачунар, а рачунар остаје без надзора,
- закључава металне ормане у којима се налазе сервери Сертификационог тела Поште, после завршетка рада.

Запослени који обавља послове пријема захтева за издавање квалификованог сертификата и захтева за промену статуса сертификата у оквиру регистрационог тела, дужан је да се придржава следећих обавеза:

- извршава своје дужности у зони пријема,
- штити лозинке које омогућавају пријављивање на апликацију за пријем захтева за издавање квалификованог сертификата и пријем захтева за промену статуса сертификата,

- одјављује се са свих апликација у случају да напушта рачунар, а рачунар остаје без надзора.

5.1.3. Напајање и климатизација

Сертификационо тело Поште је опремљено:

- системом за непрекидни извор напајања електричном енергијом и стабилизацију напона за рачунарску и комуникациону опрему, који је повезан са агрегатом,
- независним системом за климатизацију који омогућава контролу температуре и влажности ваздуха унутар просторија Сертификационог тела Поште.

5.1.4. Заштита од поплаве

Унутар заштићене просторије на централној локацији Сертификационог тела Поште не постоји водоводна инсталација. Сертификационо тело Поште је предузело све техничке мере заштите од евентуалних поплава од водоводних инсталација у окружењу.

Зграде на централној и резервној локацији Сертификационог тела Поште, у којима се налази опрема која служи за обављање делатности из ових практичних правила, удаљене су од речних и других водених токова.

5.1.5. Заштита од ватре

Просторије на централној и резервној локацији Сертификационог тела Поште, заштићене су системом за рано откривање и аутоматску дојаву пожара.

Просторије на централној локацији се посебно штите локалним системом за аутоматско гашење пожара који није штетан за људе, рачунарску и комуникациону опрему.

5.1.6. Смештање медија

Сви рачунарски медији који садрже податке о пословима Сертификационог тела Поште, укључујући и медије са резервним копијама података, смештају се у ватроотпорне безбедне касе-контејнере, од којих се једна налази на централној локацији Сертификационог тела Поште, а друга на удаљеној, безбедној локацији.

5.1.7. Одлагање непотребних података

Непотребна папирна документација и рачунарски медији за смештај података се комисијски секу на комадиће и физички уништавају.

Подаци са средстава, као што су криптографски кључеви, подаци за активирање или електронски дневници, неповратно се бришу, пре него што се средства расходују.

5.1.8. Смештај резервних копија података на удаљеној локацији

Сертификационо тело Поште користи безбедну удаљену локацију за смештај медија са подацима. Медији се смештају у касу-контејнер. Просторију у којој је смештена ватроотпорна безбедна каса-контејнер на поменутој удаљеној локацији надзиру

овлашћена лица организационог дела Сертификационог тела Поште надлежног за безбедност и заштиту.

5.2. Контрола процедура

5.2.1. Поверљиве улоге овлашћених лица

Апликација сертификационог тела и апликација централног регистрационог тела користе поверљиве улоге, које се додељују овлашћеним лицима Сертификационог тела Поште у зависности од њихових дужности.

Сертификационо тело Поште гарантује, да послови из ових практичних правила које обављају овлашћена лица Сертификационог тела Поште, могу да буду накнадно прегледани по активностима. Наиме, активности запослених на административним пословима, у зависности од врсте активности, уписују се у електронске дневнике или ручне евиденције.

5.2.1.1. Поверљиве улоге овлашћених лица сертификационог и централног регистрационог тела

Овлашћена лица Сертификационог тела Поште, у зависности од додељене улоге, могу да имају одређене налоге, и то:

- на серверима Сертификационог тела Поште,
- на хардверским криптографским модулима - HSM уређајима,
- на апликацији сертификационог тела,
- на апликацији централног регистрационог тела,
- на *firewall*-овима и радној станици за администрирање *firewall*-ова.

Привилегије одређених налога на оперативним системима рачунара и налога у апликацијама, ограничавају приступ овлашћеним лицима Сертификационог тела Поште на радње које су им потребне у обављању њихових дужности и укључују следеће улоге:

- главног администратора безбедности - свеукупну одговорност за администрирање и имплементацију безбедносних функција и процедура, као и управљање активностима на додатном унапређењу послова генерисања, опозива и суспензије квалификованих сертификата,
- систем администраторе - ауторизовану одговорност за инсталацију, конфигурисање и одржавање безбедних система издаваоца квалификованих сертификата тела за регистрацију корисника, генерисање квалификованих сертификата, обезбеђење квалификованих средстава за креирање електронског потписа за кориснике и управљање опозивом квалификованих сертификата,
- систем операторе - одговорност за рад безбедних система издаваоца сертификата у текућем раду на дневном нивоу и ауторизовану одговорност за имплементацију система за формирање резервних копија и процедуре опоравка,
- систем евидентичаре - ауторизовану одговорност за прегледање и одржавање архива и лог фајлова безбедних система издаваоца сертификата.

5.2.1.2. Поверљиве улоге овлашћених лица локалног регистрационог тела

Овлашћена лица локалног регистрационог тела добијају налоге на радним станицама на

којима је инсталисана апликација локалног регистрационог тела и налоге на апликацији локалног регистрационог тела.

Овлашћена лица локалног регистрационог тела имају дужности да:

- примају и региструју захтеве за издавање квалификованог електронског сертификата коришћењем апликације локалног регистрационог тела,
- примају и региструју захтеве за промену статуса квалификованог електронског сертификата (опозив, суспензија и прекид суспензије) коришћењем апликације локалног регистрационог тела,
- проверавају идентитет корисника,
- шаљу централном регистрационом телу документацију и податке о корисницима квалификованих сертификата.

5.2.2. Потребан број овлашћених лица за оперативне послове

Сертификационо тело Поште има имплементирану вишеструку ауторизацију за оперативне послове наведене у овој тачки.

Две ауторизације потребне су да би се извршили следећи послови:

- креирање и обнова профила HSM администратора и HSM оператера,
- промена заборављене лозинке HSM администратора и HSM оператера,
- генерисање приватног криптографског кључа апликације сертификационог тела,
- приступ безбедним касама-контејнерима.

Остали послови који нису наведени у овој тачки, извршавају се уз ауторизацију једног овлашћеног лица Сертификационог тела Поште.
За послове овлашћених лица локалног регистрационог тела, потребна је ауторизација једног лица.

5.2.3. Идентификација и аутентификација овлашћених лица

Сертификационо тело Поште врши проверу својих запослених, пре него што им додели одређене привилегије које могу да буду:

- упис у одговарајуће приступне листе за улазак у заштићене просторије Сертификационог тела Поште,
- идентификациона бесконтактна картица за улазак у заштићене просторије,
- налог на оперативном систему сервера и радних станица Сертификационог тела Поште,
- налог на апликацији сертификационог тела и HSM смарт картица,
- налог на апликацији централног регистрационог тела и смарт картица са сертификатом,
- налог на апликацији локалног регистрационог тела.

Налози и сертификати из става 1. ове тачке, креирају се посебно за свако овлашћено лице Сертификационог тела Поште.

Заједничко коришћење налога или сертификата између овлашћених лица Сертификационог тела Поште забрањено је.

5.2.4. Разграничење овлашћења овлашћених лица

Активности запослених у Сертификационом телу Поште ограничене су путем овлашћења дефинисаних на нивоу:

- оперативног система сервера и радних станица,
- апликације сертификационог тела,
- апликације централног регистрационог тела,
- апликације локалног регистрационог тела.

5.3. Контрола овлашћених лица

Послове Сертификационог тела Поште, у смислу ових практичних правила, обављају запослени који су у радном односу.

Запослени у Сертификационом телу Поште морају бити квалификовани за обављање послова из ових практичних правила и подлежу провери радне способности.

Запослени у Сертификационом телу Поште дужни су да не објављују, односно не саопштавају неовлашћеним лицима, поверљиве информације везане за безбедност Сертификационог тела Поште или информације о корисницима квалификованих сертификата.

Запосленима у Сертификационом телу Поште не додељују се послови изван делокруга послова за које су ангажовани, а који би могли да доведу до сукоба интереса са овим пословима.

Запослени у Сертификационом телу Поште добијају од руководиоца послова Сертификационог тела Поште документацију са детаљним описом процедура којих су дужни да се придржавају.

5.3.1. Захтеви у вези са претходним радним ангажовањем, квалификацијама, искуством и безбедносна провера овлашћених лица

Запослени у Сертификационом телу Поште морају да задовоље одређене захтеве у погледу стручне квалификације за свако радно место на које се ангажује, као и у погледу радног искуства и искуства на сличним радним дужностима.

Приликом запошљавања узима се у обзир да лице које се ангажује није било осуђивано.

5.3.2. Поступци за проверу претходног радног ангажовања

Провера претходног радног ангажовања лица за рад у Сертификационом телу Поште врши се у складу са кадровском политиком Сертификационог тела Поште.

5.3.3. Обука

Обука запослених у Сертификационом телу Поште обухвата:

- упознавање са инфраструктуром Сертификационог тела Поште,
- упознавање са поступцима заштите инфраструктуре и података,

- оспособљавање за коришћење апликације сертификационог тела, централног регистрационог тела и локалног регистрационог тела, у складу са додељеном улогом,
- оспособљавање за креирање резервних копија података,
- предузимање поступака за опоравак система после катастрофе,
- упознавање са другим дужностима везаним за рад Сертификационог тела Поште.

За лица која врше дужности у локалним регистрационим телима, обука укључује:

- упознавање са делатношћу Сертификационог тела Поште, врстама сертификата и захтевима за издавање/промену статуса сертификата,
- оспособљавање за коришћење апликације локалног регистрационог тела,
- упознавање са другим дужностима везаним за рад Сертификационог тела Поште.

Лица која похађају обуку, добијају одговарајућу литературу, у складу са темом обуке.

5.3.4. Учесталост поновних обука

Запослени у Сертификационом телу Поште и у локалним регистрационим телима похађају обуке за обнављање и усавршавање знања најмање једанпут годишње, а ванредно када се изврше промене техничких средстава (хардвера и софтвера) Сертификационог тела Поште и начина обављања делатности.

5.3.5. Учесталост и редослед ротације послова овлашћених лица

Сертификационо тело Поште није установило правила ротације послова, како не би дошло до нарушавања правила вршења различитих овлашћења и дужности, у вези са различитим поверљивим улогама запослених у Сертификационом телу Поште.

5.3.6. Санкције за неауторизоване активности

У случају извршене или сумње на извршене неауторизоване активности од стране овлашћеног лица Сертификационог тела Поште, истом ће бити онемогућен даљи приступ техничким средствима (хардверу и софтверу) Сертификационог тела Поште, а Сертификационо тело Поште ће суспендовати или опозвати квалификоване сертификате који су издати том лицу.

Извршене неауторизоване активности, пријављују се надлежним организационим деловима Сертификационог тела Поште, државним органима и институцијама, у складу са важећим законским и интерним прописима.

5.3.7. Захтеви за спољне сараднике

У случају да се додели поверљива улога спољном сараднику, за то лице важе исти услови као за запослене у Сертификационом телу Поште.

5.3.8. Документација за потребе овлашћених лица

Запосленима се даје одговарајућа документација са детаљним описом процедура којих морају да се придржавају.

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.

5.4.1. Врсте догађаја који се евидентирају

Догађаји који се евидентирају су у вези са:

- корисничким криптографским кључевима и квалификованим сертификатима: издавање, преузимање, опозив, суспензија, прекид суспензије и други,
- криптографским кључевима апликације сертификационог тела,
- техничким средствима (хардвер и софтвер) Сертификационог тела Поште,
- администрацијом, креирањем резервних копија, сигурносним правилима и коришћењем апликација сертификационог тела, централног регистрационог тела, локалних регистрационих тела,
- физичким приступом систему Сертификационог тела Поште,
- кадровским променама у оквиру Сертификационог тела Поште.

5.4.2. Учесталост прегледа електронских дневника и евиденција

Овлашћена лица Сертификационог тела Поште прегледају електронске дневнике и електронске евиденције једанпут недељно.
Под прегледом, подразумева се:

- прикупљање свих електронских дневника и евиденција од последњег прегледа,
- преглед и анализа записа у електронским дневницима и евиденцијама,
- разрешавање евентуалних проблема или пријава руководиоцу послова Сертификационог тела Поште, који преузима даље кораке у циљу решавања проблема.

5.4.3. Време чувања евиденција

Копије електронских дневника и евиденција чувају се најмање 10 (десет) година.

5.4.4. Заштита електронских дневника

Приступ просторијама у којима се налази опрема дозвољен је само овлашћеним лицима, како је то дефинисано интерним правилима за приступ.

За електронске дневнике оперативног система се употребљавају заштите које омогућава сам оперативни систем, и могу да их прегледају само овлашћена лица Сертификационог тела Поште.

Електронски дневници апликације сертификационог тела су шифровани тако да могу да их прегледају само овлашћена лица Сертификационог тела Поште.

5.4.5. Креирање резервних копија електронских дневника

Електронски дневници се ажурирају свакодневно. За креирање резервних копија задужена су овлашћена лица Сертификационог тела Поште. Резервне копије

електронских дневника, чувају се на централној и резервној локацији Сертификационог тела Поште.

5.4.6. Систем прикупљања података за електронске дневнике и евиденције

Подаци за електронске дневнике и евиденције се прикупљају аутоматски и ручно, како је дато у Табели 7.

Табела 7. Догађаји који се записују у електронске дневнике и евиденције, и начин прикупљања

Догађаји који се записују у електронске дневнике и ручне евиденције	**Начин прикупљања података**	**Одговорно лице или систем**
Догађаји повезани са корисничким квалификованим сертификатима	аутоматско	апликација сертификационог тела и централног регистрационог тела
Догађаји повезани са апликацијом сертификационог и централног регистрационог тела	аутоматско	апликација сертификационог и централног регистрационог тела
Догађаји на апликацији локалног регистрационог тела	аутоматско	апликација локалног регистрационог тела
Догађаји на оперативном систему	аутоматско	оперативни систем
Догађаји на рачунарској мрежи	аутоматско	*firewall*-ови, оперативни систем
Креирање резервних копија и обнова базе корисника квалификованог сертификата	аутоматско	оперативни систем, апликација сертификационог тела
Креирање резервних копија и обнова логова конфигурације сертификационог тела	аутоматско	оперативни систем, апликација сертификационог тела
Физички приступ до заштићене просторије сертификационог тела	ручно, аутоматско	запослени Сертификационог тела, систем за контролу приступа
Промене хардвера и софтвера на систему	ручно	запослени Сертификационог тела
Техничко одржавање на систему и у заштићеним просторијама	ручно	запослени Сертификационог тела
Кадровске промене	ручно	запослени Сертификационог тела

5.4.7. Обавештавање лица које је изазвало догађај

О догађају се обавештава руководилац организационе целине надлежне за електронско пословање у Сертификационом телу Поште. Лице које је изазвало догађај се не обавештава.

5.4.8. Процена рањивости система

Процена рањивости система врши се у склопу свакодневних активности које се спроводе на систему, анализама ризика, разменом искустава са сертификационим телима из окружења и прегледом електронских дневника и евиденција.

Тест пенетрације се спроводи једном годишње или после великих промена на систему.

5.5. Архивирање података

5.5.1. Подаци који се архивирају

Сертификационо тело Поште архивира следеће податке и документа:
- електронске дневнике,
- уговоре и документацију корисника,
- захтеве за издавање квалификованог електронског сертификата,
- захтеве за промену статуса електронског сертификата (опозив, суспензија, прекид суспензије и друго),
- квалификоване електронске сертификате,
- регистре опозваних сертификата,
- општа акта Сертификационог тела Поште везана за обављање делатности Сертификационог тела Поште.

5.5.2. Период чувања података у архиви

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

5.5.3. Заштита архиве

Архива докумената се чува на централној локацији Сертификационог тела Поште.

Архива је заштићена одговарајућим сигурносним механизмима Сертификационог тела Поште (физичко-техничком заштитом и надзором, ограниченим приступом, шифрама и кључевима). Приступ архивама дозвољен је само овлашћеним лицима.

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

5.5.4. Процедуре архивирања

Папирни документи архивирају се на централној локацији Сертификационог тела Поште.

Сертификационо тело Поште свакодневно ради архивирања израђује копије електронских дневника и података.

5.5.5. Временска ознака архивираних података

Архивирани подаци носе временску ознаку са сервера који је синхронизован са извором тачног времена. Временска ознака није криптографски/електронски временски жиг.

5.5.6. Систем архивирања (интерни или екстерни)

Сертификационо тело Поште користи интерни систем архивирања. Архивирање електронских података извршава се аутоматски техничким средствима за архивирање у заштићеним просторијама Сертификационог тела Поште.

Документација у папирном облику се прикупља и архивира ручно на централној локацији Сертификационог тела Поште, а може да се архивира и у електронском облику.

5.5.7. Процедуре контроле приступа архивираним подацима

Архивирани електронски подаци чувају се у касама-контејнерима за чије отварање су потребна два кључа и шифра. Касе-контејнери се налазе у заштићеним просторијама на централној и удаљеној локацији. Просторије су са рестриктивним и ауторизованим приступом. Приступ подацима који се чувају у уређајима ограничен је физичким и логичким контролама приступа са рестриктивним и ауторизованим приступом.

5.6. Замена кључева сертификационог тела

Замена криптографских кључева Сертификационог тела Поште, врши се 6 (шест) година пре истека рока важности постојећих кључева.
Замену кључева могуће је спровести и раније, због :

1) промене криптографског алгоритма којим сертификационо тело потписује сертификате и регистре опозваних сертификата;
2) промене дужине кључева сертификационог тела;
3) промене рока важности кључева сертификационог тела;
4) промене *hash* алгоритам сертификационог тела, применом кога се израчунава *hash* вредност сертификата и регистра опозваних сертификата;
5) промене садржаја постојећих поља (екстензија) сертификата сертификационог тела или додавања нових поља (екстензије) сертификата сертификационог тела;
6) оштећења или компромитовања приватног криптографског кључа сертификационог тела.

5.7. Опоравак система после катастрофе

5.7.1. Процедуре рада у инцидентним ситуацијама приликом компромитације система

Сертификационо тело Поште врши континуирани надзор рада система и у случају појаве грешке или инцидентне ситуације на систему спроводи правовремене и координисане активности у складу са интерним правилима рада. Обавештавање у случају појаве грешке или инцидентне ситуације врши се у складу са овим практичним правилима и интерним правилима.

У случају компромитовања или сумње у компромитовање приватног криптографског кључа апликације сертификационог тела, спроводе се следеће операције:

- опозив издатих квалификованих сертификата корисника,
- опозив сертификата апликације сертификационог тела,
- објављивање опозваних сертификата у регистру опозваних сертификата.

Затим се, уколико је то могуће, врши отклањање узрока компромитације.

5.7.2. Уништење техничких средстава или података

У случају штете настале на техничким средствима (хардверу и софтверу) или подацима, при чему приватни криптографски кључ апликације сертификационог тела није уништен или оштећен, сервиси апликације сертификационог тела биће поново успостављени у најкраћем могућем року.

У случају уништења или оштећења приватног криптографског кључа апликације сертификационог тела, после отклањања узрока уништења или оштећења, спроводи се поступак реконструисања кључа.

5.7.3. Компромитовање приватног криптографског кључа апликације сертификационог тела

Сертификационо тело Поште ће, у случају компромитовања приватног криптографског кључа апликације сертификационог тела, одмах да:

- опозове издате квалификоване сертификате,
- опозове сертификат апликације сертификационог тела,
- објави регистар опозваних сертификата,
- обавести кориснике издатих квалификованих сертификата.

Сертификационо тело Поште ће, у случају компромитовања приватног криптографског кључа апликације сертификационог тела, после отклањања узрока компромитовања, да:

- генерише нове криптографске кључеве апликације сертификационог тела,
- изда корисницима нове квалификоване сертификате.

5.7.4. Наставак рада 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.

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.

Сертификационо тело Поште ће о планираном престанку обављања послова сертификације обавестити своје кориснике и надлежни државни орган писаним путем најмање три месеца пре престанка рада, у складу са важећим прописима. 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.

Сертификационо тело Поште ће предузети све што могућности у датом тренутку буду дозвољавале, како би обезбедило наставак обављања услуге сертификације код другог сертификационог тела за своје кориснике. Сертификационо тело Поште има обавезу да сертификационом телу, код кога је обезбедило наставак пружања услуге сертификације према својим корисницима, достави сву постојећу документацију и архиву, која се односи на обављање услуге сертификације.

Ако се не постигне пренос обавеза на друго сертификационо тело, Сертификационо тело Поште има обавезу да сву постојећу документацију и архиву, која се односи на обављање услуга сертификације достави надлежном државном органу.

Уколико нема могућности за пренос обавеза пружања услуге сертификације на друго сертификационо тело, Сертификационо тело Поште ће раскинути уговоре о издавању и коришћењу квалификованих електронских сертификата са својим корисницма и опозвати све важеће квалификоване сертификате, о чему ће обавестити кориснике и надлежни државни орган.

6. КОНТРОЛЕ ТЕХНИЧКЕ ЗАШТИТЕ

6.1. Генерисање пара криптографских кључева и инсталација

Пар криптографских кључева апликације сертификационог тела је генерисан током церемоније генерисања (*Key Generation Ceremony*) по прецизно дефинисаној процедури. 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*), оперативни систем, апликација сертификационог тела и вишеструка аутентификација овлашћених лица.

6.1.1. Генерисање пара криптографских кључева

Пар криптографских кључева апликације сертификационог 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*).

6.1.2. Уручење приватног криптографског кључа кориснику

Уручење приватног кључа кориснику врши се уручивањем квалификованог средства за креирање електронског потписа и печата на изабраној локацији на територији Републике Србије.

6.1.3. Слање сертификационом телу јавног криптографског кључа корисника

Корисников јавни и приватни криптографски кључ генеришу се у Сертификационом телу Поште на квалификованом средству за креирање електронског потписа и печата.

6.1.4. Уручење јавног криптографског кључа трећим лицима

Јавни криптографски кључ апликације сертификационог тела у форми сертификата је јавно доступан на веб сајту Сертификационог тела Поште.

Корисничке јавне криптографске кључеве и сертификате, Сертификационо тело Поште јавно не објављује, нити уручује трећим лицима.

6.1.5. Дужине криптографских кључева

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

- Криптографски кључеви апликације сертификационог тела: RSA кључеви дужине 4096 бита.
- Кориснички кључеви: RSA кључеви дужине 4096 бита.

6.1.6. Генерисање параметара јавног криптографског кључа и провера квалитета

Генерисање параметара јавног криптографског кључа апликације сертификационог тела врши се у хардверским криптографским модулима Сертификационог тела Поште, а параметри јавних криптографских кључева корисника генеришу се у квалификованим средствима за креирање електронског потписа и печата. Параметри су врста алгоритма и дужина кључа.

Провера квалитета параметара криптографских кључева и сертификата апликације сертификационог тела се врши током и непосредно после генерисања криптографских кључева.

Управна структура Сертификационог тела Поште задаје параметре јавних кључева апликације сертификационог тела и корисника.

6.1.7. Намена кључа (дефинисано у *X*.509 вер. 3 пољу *Key Usage* сертификата)

За потписивање квалификованих сертификата и регистра опозваних сертификата употребљава се искључиво приватни криптографски кључ апликације сертификационог тела. Јавни криптографски кључ апликације сертификационог тела се употребљава за валидацију електронског потписа квалификованих сертификата и регистра опозваних сертификата (*Key Usage = Certificate Signing, Off-line CRL Signing, CRL Signing*).

Намена јавног криптографског кључа квалификованог сертификата корисника је валидација квалификованог електронског потписа или печата и обезбеђивање непорецивости, како је дато у Табели 8. Додатна намена јавног криптографског кључа квалификованог сертификата корисника за електронски печат који се користи за валидацију временских жигова је валидација временских жигова (*Extended Key Usage = Time Stamping*).

Табела 8. Садржај поља *Key Usage* у квалификованим сертификатима које издаје Сертификационо тело Поште

Врста сертификата	Садржај поља *Key Usage*
Квалификовани сертификат	*Digital Signature, Non-Repudiation* (електронски потпис и непорецивост)

6.2. Заштита приватног криптографског кључа

6.2.1. Стандарди за хардверски криптографски модул

Хардверски криптографски модул на серверу апликације сертификационог тела задовољава стандард *FIPS* 140-2 ниво 3 и *EAL* 4+.

Квалификовано средство за креирање електронског потписа и печата корисника задовољава стандард *FIPS* 140-2 ниво 2 или виши или *EAL* 4+.

6.2.2. Контрола приступа приватном криптографском кључу од стране *n* од *m* овлашћених лица

Сертификационо тело Поште има имплементирану вишеструку ауторизацију за присуп приватном криптографском кључу апликације сертификационог тела. *Root* сертификационо тело је у *off-line* режиму.

Приступ корисничком приватном криптографском кључу ограничен је само на корисника.

6.2.3. Откривање приватног криптографског кључа

Сертификационо тело Поште не нуди могућност откривања приватног криптографског кључа.

6.2.4. Креирање копије приватног криптографског кључа

После генерисања криптографских кључева апликације сертификационог тела (*Key Generation Ceremony*), уз присуство овлашћених лица Сертификационог тела Поште креира се копија приватног криптографског кључа апликације сертификационог тела. Приватни криптографски кључ апликације сертификационог тела је шифрован *AES* (*Rijndael*) алгоритмом и никад се не налази изван хардверског криптографског модула у дешифрованом облику. Дешифровање приватног криптографског кључа је могуће само у хардверском криптографском модулу, на основу копије приватног криптографског кључа, уз помоћ две администраторске и оператерске *HSM* смарт картице за приступ хардверском криптографском модулу и њихових лозинки.

Креирање копија приватних криптографских кључева корисника се не ради.

6.2.5. Архивирање приватног криптографског кључа

Сертификационо тело Поште архивира копију приватног криптографског кључа апликације сертификационог тела после његовог креирања, на локацији

Сертификационог тела Поште и на другој удаљеној локацији, у заштићеним просторијама у касама-контејнерима за дуготрајно чување.

Архивирање приватних криптографских кључева корисника се не ради.

6.2.6. Пребацивање приватног криптографског кључа у криптографски модул или из њега

Приватни криптографски кључ апликације сертификационог тела је генерисан у хардверском криптографском модулу. Само уколико наступи хардверски квар хардверског криптографског модула апликације сертификационог тела, он ће бити замењен новим модулом, а приватни кључ пребачен (импортован) у тај модул, уз писану одлуку управне структуре највишег нивоа Сертификационог тела Поште и уз вишеструку ауторизацију запослених Сертификационог тела Поште.

Приватни криптографски кључ корисника генерисан је у квалификованом средству за креирање електронског потписа и печата и не експортује се.

6.2.7. Чување приватног криптографског кључа у криптографском модулу

Криптографски кључеви се чувају у хардверским криптографским модулима и могу да се користе само уколико су на правилан начин активирани.

6.2.8. Поступак за активирање приватног криптографског кључа

За реконструкцију и активирање приватног криптографског кључа апликације сертификационог тела потребна је ауторизација два *HSM* администратора и два *HSM* оператера са својим картицама и лозинкама. Приватни криптографски кључ апликације сертификационог тела се активира после стартовања апликације сертификационог тела.

Корисник активира QSCD картицу/токен пре прве употребе коришћењем одговарајућег софтвера. Када је активација приватног криптографског кључа спроведена уношење лозинке QSCD уређаја активира кориснички приватни криптографски кључ који може да се користи после успешне аутентификације корисника са лозинком у корисничкој апликацији приликом електронског потписивања или печатирања.

6.2.9. Поступак за деактивирање приватног криптографског кључа

Приватни криптографски кључ апликације сертификационог тела се деактивира заустављањем апликације сертификационог тела, искључењем сервера на ком се налази апликација сертификационог тела или искључењем хардверског криптографског модула.

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, односно деактивирања квалификованог средства за креирање електронског потписа и печата.

6.2.10. Поступак за уништавање приватног криптографског кључа

Приватни криптографски кључ апликације сертификационог тела се уништава само у случају планираног престанка рада сертификационог тела, а спроводе га овлашћени запослени са поверљивим улогама у Сертификационом телу Поште.

Приватни криптографски кључ корисника се уништава уколико га корисник обрише са квалификованог средства за креирање електронског потписа и печата или физички оштети квалификовано средство за креирање електронског потписа и печата.

6.2.11. Класификовање криптографских модула

Стандарди за криптографске модуле према којима може да се врши њихово класификовање су *FIPS* и *EAL*, и наведени су у тачки 6.2.1.

6.3. Остали видови управљања паром кључева

6.3.1. Архивирање јавног криптографског кључа

Сертификационо тело Поште архивира јавни криптографски кључ апликације сертификационог тела и јавне криптографске кључеве корисника.

6.3.2. Рок важности сертификата и криптографских кључева

Рок важности сертификата Сертификационог тела Поште је:

- Сертификати апликације сертификационог тела дефинисани су у Политици сертификације.
- Квалификовани сертификати корисника: од 1 (једне) до 5 (пет) година.
- Квалификовани сертификати за електронски печат који се користе за валидацију временских жигова: 6 (шест) година.

Временски период важности приватног кључа апликације сертификационог тела једнак је временском периоду важности припадајућег 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 1 (једна) година.

6.4. Подаци за активирање

6.4.1. Генерисање и употреба података за активирање

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

Лозинку за активирање приватног кључа корисника генерише генератор лозинке, после чега се она доставља кориснику одвојено од квалификованог средства за креирање електронског потписа и печата.

Лозинка има најмање пет или више нумеричких карактера.

Корисник има могућност промене лозинке и њене дужине.

6.4.2. Заштита података за активирање

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

Корисници су дужни да чувају лозинке за приступ приватним криптографским кључевима који се налазе на квалификованом средству за креирање електронског потписа и печата.

6.4.3. Остали видови података за активирање

Не постоје.

6.5. Безбедносне контроле рачунарског система

6.5.1. Специфични безбедносно-технички захтеви за рачунаре

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.

Сертификационо тело Поште спроводи континуирано праћење и поседује алармни систем који се користи у сврху откривања, бележења и правовременог реаговања на покушаје недозвољеног приступа ресурсима система.

6.5.2. Ниво заштите рачунара

Оперативни систем на серверима Сертификационог тела Поште, је оперативни систем компаније *Microsoft*, који је у складу са *EAL* стандардом заштите, како би се омогућио сигуран рад апликације сертификационог тела.

6.6.Технички надзор у току обављања делатности

6.6.1. Развој система

Приликом развоја система спроводи се анализа безбедносних захтева како би се осигурало да је безбедност имплементирана у *PKI* систему за издавање квалификованих сертификата. Софтвер који се користи приликом пружања услуге издавања квалификованих сертификата је од поузданог произвођача. Нове верзије софтвера тестирају се у тестном окружењу. Имплементација софтвера у продукционом окружењу спроводи се у складу са документованим поступцима. Сертификационо тело Поште омогућава издавање сертификата за потребе тестирања. Сертификати за потребе тестирања су јасно означени.

6.6.2. Управљање безбедношћу

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

У случају нарушавања безбедности система Сертификационог тела Поште или губитка његовог интегритета који може да има значајан утицај на пружање услуге издавања квалификованих сертификата или на заштиту личних података, Сертификационо тело Поште ће у року од 24 сата о томе обавестити надлежни државни орган. У случају да губитак интегритета може да има негативан утицај на кориснике услуга од поверења, Сертификационо тело Поште ће о томе без одлагања обавестити сва физичка и правна лица на које нарушавање безбедности може да има утицај.

6.6.3. Животни циклус безбедносне контроле

Безбедносна контрола се периодично извршава проверавањем рада компонената Сертификационог тела Поште. Интегритет компонената система и података штити се антивирусном заштитом и употребом ауторизованог софтвера.

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 подељени у логичке целине, односно зоне са различитим нивоима безбедности. 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.

Мрежни сегмент у ком се налазе радне станице за администрацију сертификационог тела је одвојен *firewall* уређајем од осталих мрежних сегмената и рачунара који се налазе у тим сегемнтима.

Опрема за заштиту рачунарске мреже бележи саобраћај и покушаје приступа сервисима Сертификационог тела Поште применом *IPS* система.

Непотребне комуникације, кориснички налози, портови, протоколи и сервиси су експлицитно забрањени или деактивирани.

Интерна рачунарска мрежа Сертификационог тела Поште заштићена је од неовлашћеног приступа, укључујући приступ корисника и трећих лица.

Сви критични системи за пружање услуге издавања квалификованих сертификата смештени су у заштићену просторију и распоређени су у више различитих безбедносних мрежних зона.

Системи Сертификационог тела Поште посебно су безбедносно подешени и ојачани.

Мрежне компоненте система Сертификационог тела Поште чувају се у физички и логички сигурном окружењу. Усклађеност њихове конфигурације се периодично проверава.

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 применом *NTP* (*Network Time Protocol*) протокола, најмање једном у 24 сата.

7. ПРОФИЛ СЕРТИФИКАТА, РЕГИСТРА ОПОЗВАНИХ СЕРТИФИКАТА И OCSP

7.1. Профил сертификата

7.1.1. Верзија сертификата

Сертификационо тело Поште издаје *X*.509 сертификате верзије 3. Профил квалификованог сертификата је у складу са документима: *RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“, RFC 3739 „Internet X.*509 *Public Key Infrastructure: Qualified Certificates Profile“, 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”* и *ETSI EN 319 412-5 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements”.*

Сертификати *X*.509 Сертификационог тела Поште садрже основна поља *X*.509 сертификата (Табела 9.) и екстензије *X*.509 сертификата (Табеле 10. и 11.).

Табела 9. Основна поља *X*.509 сертификата

Назив поља	Опис поља

Version	Верзија *X*.509 сертификата.
Serial Number	Јединствени серијски број квалификованог сертификата
Signature Algorithm	*Hash* алгоритам и асиметрични криптографски алгоритам коришћен за потписивање сертификата од стране апликације сертификационог тела
Issuer	Јединствено име сертификационог тела
Valid From	Датум и време почетка важења квалификованог електронског сертификата
Valid To	Датум и време престанка важења квалификованог електронског сертификата
Subject	Јединствено име корисника сертификата
Subject Public Key Info	Јавни криптографски кључ корисника сертификата, дужина јавног кључа и назив алгоритма јавног кључа
Signature	Електронски потпис квалификованог сертификата приватним криптографским кључем апликације сертификационог тела

7.1.2. Екстензије сертификата

Екстензије *X*.509 сертификата које апликација сертификационог тела уписује у квалификоване сертификате, и њихов опис, дати су у Табели 10.

Табела 10. Екстензије *X*.509 сертификата

Назив поља - екстензије	Опис поља - екстензије
Authority Key Identifier	Идентификатор јавног криптографског кључа сертификационог тела који се рачуна као *SHA*-1 *hash* поља *Subject Public Key Info* сертификата сертификационог тела
Subject Key Identifier	Идентификатор јавног криптографског кључа корисника сертификата који се рачуна као *SHA*-1 *hash* поља *Subject Public Key Info* квалификованог сертификата корисника
Key Usage	Намена јавног криптографског кључа корисника квалификованог сертификата
Certificate Policies	Идентификација политике сертификације и адреса веб стране на којој се налазе ова практична правила
Subject Alternative Name	Алтернативно име корисника квалификованог сертификата. У овом пољу може да се наведе адреса електронске поште корисника сертификата, ако је адреса електронске поште наведена у уговору
Basic Constraints	Ознака која указује да је сертификат кориснички и она садржи „*Subject Type=End Entity*“
CRL Distribution Points	Локација на којој се налазе регистри опозваних сертификата

Qualified Certificate Statements	Ознака да је сертификат издат као квалификовани сертификат (*OID*: 1.3.6.1.5.5.7.1.3), која садржи објекте *QcCompliance, QcType, QcLegislation* и *QcSSCD*
Authority Information Access	Адреса OCSP сервера и адреса сертификата издавачког (Intermediate) сервера
Private Key Usage Period	Рок важности приватног криптографског кључа корисника, који је пар јавном криптографском кључу из квалификованог електронског сертификата за електронски печат који се користи за валидацију временских жигова.
Extended Key Usage	Додатна намена јавног криптографског кључа корисника квалификованог сертификата за електронски печат који се користи за валидацију временских жигова (*Time Stamping*)

Додатне екстензије *X*.509 сертификата које апликација Сертификационог тела Поште уписује у квалификовани сертификат за електронски потпис који је издат страницу на основу путне исправе (пасоша) и њихов опис, дате су у Табели 11.

Табела 11. Додатне екстензије X.509 сертификата за електронски потпис који је издат страницу на основу путне исправе (пасоша)

Назив поља - екстензије	**Опис поља - екстензије**
Broj pasoša	Број пасоша корисника сертификата (*OID*: 1.3.6.1.0.1).
Ime države koja je izdala pasoš	Име државе која је издала пасош кориснику сертификата (*OID*: 1.3.6.1.0.2).
Datum isteka pasoša	Последњи дан важности пасоша корисника сертификата (*OID*: 1.3.6.1.0.3).

7.1.3. Идентификациона ознака алгоритма

Сертификационо тело Поште потписује квалификоване сертификате и регистре опозваних сертификата, применом алгоритма *sha512RSA* (*OID*: 1.2.840.113549.1.1.13, *SHA-512 with RSA Encryption*) у складу са документима *RFC* 5280 *„Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“*, *RFC* 4055 *„Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.*509 *Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“* и *ETSI TS 119 312 „Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”* .

7.1.4. Форме имена

У квалификованим сертификатима које издаје Сертификационо тело Поште, име Сертификационог тела Поште које је наведено у пољу *Issuer,* и име корисника сертификата, које је наведено у пољу *Subject*, су јединствена имена (*Distinguished Name – DN*), као што је дефинисано у тачки 3.1.1. Јединствена имена су уписана у квалификованом сертификату применом *UTF8 String* кодирања.

7.1.5. Ограничења у именима

Коришћење специјалних знакова у именима корисника није дозвољено. Исте је потребно изоставити или заменити другим знацима.

7.1.6. Идентификациона ознака политике сертификације

Сертификационо тело Поште користи поље *Certificate Policies* сертификата, у коме објављује *Policy Identifier OID* (*Object Identifier*) идентификациону ознаку политике сертификације, које су дате у Табели 12.

Табела 12. Ознаке политике сертификације

Врста сертификата	Ознака политике (*OID*)
Квалификовани сертификат за електронски потпис	1.3.6.1.4.1.15672.10.152.1.0
Квалификовани сертификат за електронски потпис који је издат странцу на основу путне исправе (пасоша)	1.3.6.1.4.1.15672.10.156.1.0
Квалификовани сертификат за електронски печат	1.3.6.1.4.1.15672.10.128.1.0
Квалификовани сертификат за електронски печат који се користи за валидацију временских жигова	1.3.6.1.4.1.15672.10.822.1.0

7.1.7. Употреба екстензије за раздвајање политика

Не користи се.

7.1.8. Квалификатори политике сертификације

Сертификационо тело Поште користи потпоље *Policy Qualifier=CPS* поља *Certificate Policies* сертификата, у коме објављује адресу веб сајта на којем се налазе ова практична правила и друга акта Сертификационог тела Поште, и потпоље *Policy Qualifier=User Notice* у коме је наведено да је електронски сертификат квалификован.

7.1.9. Процесирање критичних екстензија сертификата

Корисничке апликације морају да процесирају екстензије сертификата које су означене као критичне (*critical*).

7.2. Профил регистра опозваних сертификата

7.2.1. Верзија регистра опозваних сертификата

Сертификационо тело Поште издаје *X*.509 регистре опозваних сертификата (*Certificate Revocation List - CRL*) верзије 2. Профил регистра опозваних сертификата је у складу са документом *RFC* 5280 „*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“*. Регистри опозваних сертификата Сертификационог тела

Поште садрже основна поља *X*.509 регистра (Табела 13.) и екстензије *X*.509 регистра (Табела 14.).

Табела 13. Основна поља *X*.509 регистра опозваних сертификата

***Н*азив поља**	**Опис поља**
Version	Верзија *X*.509 регистра опозваних сертификата.
Signature Algorithm	*Hash* алгоритам и асиметрични криптографски алгоритам коришћен за потписивање регистра опозваних сертификата од стране апликације сертификационог тела
Issuer	Јединствено име сертификационог тела
Effective Date (This Update)	Датум и време издавања регистра опозваних сертификата
Next Update	Датум и време следећег издавања регистра опозваних сертификата
Revoked Certificates	Списак серијских бројева опозваних сертификата и датума и времена њиховог опозивања
Signature	Електронски потпис регистра опозваних сертификата приватним криптографским кључем апликације сертификационог тела

7.2.2. Екстензије регистра опозваних сертификата

Екстензије *X*.509 регистра опозваних сертификата које апликација сертификационог тела уписује у регистре, и њихов опис, дати су у Табели 14.

Табела 14. Екстензије *X*.509 регистра опозваних сертификата

***Н*азив поља - екстензије**	**Опис поља – екстензије**
Authority Key Identifier	Идентификатор јавног криптографског кључа сертификационог тела који се рачуна као *SHA*-1 *hash* поља *Subject Public Key Info* сертификата сертификационог тела
CRL Number	Редни број регистра опозваних сертификата
Reason Code	Разлог опозива сертификата
Invalidity Date	Датум компромитовања или сумње у компромитовање приватног криптографског кључа или датум када је квалификовани сертификат на неки други начин престао да буде важећи (*OID*: 2.5.29.24)

7.3. *OCSP* профил

Сертификационо тело Поште омогућава *on-line* проверу статуса квалификованог сертификата посредством *OCSP* протокола (*Online Certificate Status Protocol*).

OCSP профил Сертификационо тела Поште је у складу са документом *RFC* 6960 „*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP“*.

7.3.1. *OCSP* верзија

Верзија *OCSP* је верзија 1.

7.3.2. *OCSP* екстензије

OCSP екстензије које се користе су: *Nonce* (произвољан број) и *Extended Revoked Definition. Extended Revoked Definition* екстензија указује да је статус неиздатог сертификата опозван (Revocation reason = Certificate Hold), а датум опозива је 1.1.1970. године.

8. РЕВИЗИЈА УСКЛАЂЕНОСТИ РАДА СЕРТИФИКАЦИОНОГ ТЕЛА И ДРУГЕ ПРОЦЕНЕ

Сертификационо тело Поште извршава редовне унутрашње ревизије рада (*internal audit*).

Надлежни орган има право да захтева спољну ревизију, у складу са законом и подзаконским актима.

8.1. Учесталост ревизије

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 законским 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. Законски заступник може да одлучи да се ревизија спроведе ангажовањем стручног лица из или ван Сертификационог тела Поште, које мора да има искуства на подручју:

- технологије инфраструктуре јавних криптографских кључева,
- вршења делатности сертификационог тела,
- спровођења ревизије сертификационог тела или другог информационо-комуникационог система.

Спољашњу ревизију спроводи Тело за оцењивање усаглашености које је, у складу са законом којим се уређује акредитација, акредитовано за оцењивање усаглашености пружалаца квалификованих услуга од поверења и квалификованих услуга од поверења које они пружају.

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 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 објављује ценовник за издавање квалификованих сертификата на свом веб сајту.

Свака промена цена издавања квалификованих сертификата биће објављена на веб сајту Сертификационог тела Поште и доступна свим заинтересованим лицима.

9.1.1. Надокнада за издавање сертификата

Сертификационо тело Поште наплаћује издавање квалификованог сертификата на основу ценовника, који је објављен на веб сајту Сертификационог тела Поште и доступан на захтев свим заинтересованим лицима.

9.1.2. Надокнада за приступ сертификату

Сертификационо тело Поште не објављује квалификоване сертификате, тако да они нису јавно доступни, па не може ни да наплаћује приступ квалификованом сертификату.

9.1.3. Надокнада за проверу опозваности и статуса сертификата

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

9.1.4. Надокнада за друге услуге

Сертификационо тело Поште задржава право да наплаћује различите услуге у зависности од пружених услуга у сваком конкретном случају.

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

9.1.5. Повраћај уплаћених средстава

Сертификационо тело Поште врши повраћај накнаде уколико је извршена погрешна уплата, плаћен виши износ накнаде и у складу са другим нормативно-правним прописима који регулишу права потрошача.

9.2. Одговорност

Сертификационо тело Поште сноси финансијску одговорност за обављање своје делатности у складу са законским прописима.

9.2.1. Осигурање

Сертификационо тело Поште је дужно да у складу са правилником којим се прописује најнижи износ осигурања од ризика одговорности за штету насталу вршењем квалификоване услуге од поверења, обезбеди најнижи износ осигурања од ризика за могућу штету насталу вршењем квалификоване услуге од поверења тако да:

- осигурана сума на коју мора бити уговорено осигурање по једном штетном догађају не може износити мање од 20.000 (двадесет хиљада) евра у динарској противвредности за квалификовану услугу од поверења, подразумевајући при том као штетни догађај појединачну штету насталу употребом једног квалификованог сертификата у једном акту у правном промету, у оквиру пружања квалификоване услуге од поверења;
- укупна осигурана сума на коју мора бити уговорено осигурање од одговорности сертификационог тела кумулативно на годишњем нивоу, по свим штетним догађајима, не може бити нижа од 1.000.000 (милион) евра у динарској противвредности укупно за све квалификоване услуге од поверења које пружалац услуге пружа.

9.2.2. Други фондови

Није примењено.

9.2.3. Осигурање или гаранција за крајње кориснике

Осигурање или гаранције за крајње кориснике описане су у оквиру тачке 9.2.1.

9.3. Тајност пословних података

9.3.1. Опсег тајних 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 лицима Сертификационог тела Поште и надлежним државним органима, ако су испуњени законом прописани услови.

9.3.2. Подаци који се не сматрају тајним

Подаци који се не сматрају тајним су:
- регистри опозваних сертификата, као и подаци које они садрже,
- Политика сертификације,
- Практична правила,
- подаци и документа која су објављена на званичном веб сајту Сертификационог тела Поште,
- документа за која постоји писана сагласност за јавно објављивање.

9.3.3. Одговорност за заштиту тајних података

Овлашћена лица Сертификационог тела Поште и корисници обавезују се:
- да чувају тајност података применом мера које користе за заштиту својих тајних података и да ће их користити само за потребе због којих су били прикупљени или формирани у односу на одредбе Практичних правила,
- да неће неовлашћено откривати тајне податке, без претходног одобрења, које даје корисник или надлежни орган, у писаној форми.

9.4. Заштита података о личности

Сертификационо тело Поште дужно је 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.

9.4.1. План чувања тајних података о личности

Наведено у тачкама 9.3 и 9.4.

9.4.2. Подаци о личности који се сматрају тајним

Сви подаци о корисницима који су заштићени законом сматрају се тајним подацима о личности.

9.4.3. Подаци о личности који се не сматрају тајним

Сви подаци који су јавно доступни се не сматрају тајним подацима о личности.

9.4.4. Одговорност за заштиту тајних података о личности

Сертификационо тело Поште одговорно је за тајне податке о личности и за заштиту тих података, у складу са тачком 9.3.3.

9.4.5. Упозорење и сагласност за коришћење тајних података о личности

Сертификационо тело Поште ће, за потребе пружања услуге сертификације, користити тајне податке о личности само ако корисник да сагласност током процеса регистрације. Сматра се да је корисник дао сагласност уколико је прихватио услове пружања услуге током процеса регистрације и потписао Уговор о издавању и коришћењу квалификованих електронских сертификата.

9.4.6. Откривање тајних података о личности у складу са судским или административним поступком

Сертификационо тело Поште ће открити или обелоданити тајне податке о личности на захтев надлежног органа и у другим случајевима, у складу са законом.

9.4.7. Друге околности за откривање тајних података о личности

Сертификационо тело Поште ће открити податке о личности заштићене законом уз предходну сагласност корисника или на захтев надлежног органа и у другим случајевима предвиђеним законом.

9.5. Заштита права интелектуалне својине

Овај документ, као и друга документација Сертификационог тела Поште објављена на веб сајту Сертификационог тела Поште, представља право интелектуалне својине и власништво је 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

9.6.1. Права и обавезе сертификационог тела

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

Сертификационо тело Поште има обавезу да:

- пре успостављања уговорног односа са корисником сертификата, јавно информише корисника сертификата о релевантним условима коришћења сертификата,
- изврши проверу идентитета корисника сертификата који учествују поступку издавања или промене статуса сертификата,у зависности да ли се корисник сертификата идентификује као физичко или правно лице, као и проверу тачност података у захтеву за издавање - промену статуса сертификата,
- подаци садржани у сертификату буду поуздани и тачни,
- са корисником сертификата закључи Уговор и исти чува 10 (десет) година по престанку важења сертификата,
- изда сертификат у складу са условима дефинисаним законом,
- обезбеди да сертификат садржи све потребне податке, у складу са важећим прописима и захтевима стандарда који су тим прописима прописани да се примењују,
- унесе у сертификат основне податке о свом идентитету и идентитету корисника сертификата, као и јавни криптографски кључ корисника сертификата који је пар његовом приватном криптографском кључу,
- обезбеди видљив податак у сертификату о тачном датуму и времену (сат и минут) издавања сертификата,
- изврши или одбије да изврши захтев за промену статуса сертификата, у складу са условима дефинисаним законом,
- води ажуран, тачан и безбедним мерама заштићен регистар опозваних сертификата који је јавно доступан,
- обезбеди видљив податак у регистру опозваних сертификата о тачном датуму и времену (сат и минут) опозива сертификата,
- врши надзор обављања делатности регистрационих тела,
- обавља делатност у складу са важећим прописима и општим актима Сертификационог тела Поште, којима се уређује пружање услуга издавања сертификата, као и прописима и општим актима којима се уређује заштита података о личности.

9.6.2. Права и обавезе регистрационих тела

Регистрациона тела, овлашћена од стране Сертификационог тела Поште, имају права и обавезе да:

- провере идентитет корисника у поступку издавања квалификованог сертификата и тачност података у Захтеву за издавање квалификованог електронског сертификата,
- провере идентитет корисника и тачност података у Захтеву за промену статуса електронског сертификата,

- проследе податке за издавање и промену статуса квалификованог сертификата, као и сву документацију централном регистрационом телу.

Сертификационо тело Поште одговара за обавезе регистрационих тела.

9.6.3. Права и обавезе корисника

Сертификационо тело Поште обезбеђује поштовање свих права корисника, односно омогућава остваривање обавеза корисника, која су утврђена прописима која се односе на квалификовани сертификат, овим практичним правилима.

Корисник је обавезан да:
- пружи тачне и поуздане податке о свом идентитету, у зависности да ли се идентификује као физичко или правно лице, информације о адреси за физичко лице, односно докаже својство овлашћеног лица у правном лицу за подношење захтева из тачке 9.6.1. став 2. алинеја друга Практичних правила и пружи тачне и поуздане податке о правном лицу (регистровани подаци) или другим атрибутима, који описују како се Корисник сертификата може контактирати, као и о осталим подацима садржаним у сертификату,
- у поступку провере идентитета, корисник сертификата, уколико се идентификује као физичко лице, буде физички присутан, као и овлашћено лице у правном лицу овлашћено за подношење захтева из тачке 9.6.1. став 2. алинеја друга Практичних правила,
- обавештава Сертификационо тело Поште о промени података о идентитету и осталих података садржаних у сертификату, најкасније у року од 24 сата од настанка промене,
- прегледа податке садржане у сертификату и обавештава Сертификационо тело Поште о евентуалним грешкама, после преузимања, а пре коришћења сертификата,
- користи средство за креирање електронских потписа или печата које обезбеђује Сертификационо тело Поште,
- употребљава сертификат само за намене одређене у овим практичним правилима,
- чува приватни криптографски кључ и у тајности чува лозинку за приступ приватном криптографском кључу,
- у случају губитка, оштећења или злоупотребе техничких средстава (хардвера или софтвера) или приватног криптографског кључа, односно компромитовања или сумње у компромитовање приватног криптографског кључа, без одлагања, поднесе захтев за опозив сертификата,
- испуњава друге обавезе у складу са законом и преузетим уговорним обавезама.

9.6.4. Права и обавезе поуздајућих страна

Поуздајућим странама гарантује се да Сертификационо тело Поште услуге сертификације пружа трећим лицима у складу са законом и другим сродним прописима, овим практичним правилима и другим општим актима и интерним правилима рада Сертификационог тела Поште, у складу са важећим прописима.

Обавезе поуздајућих страна, пре него што се поуздају у квалификовани сертификат издат од стране Сертификационог тела Поште су:
- да провере статус квалификованог сертификата,

- да се не поуздају у неважећи сертификат (опозван, суспендован или истекао),
- да се упознају са одговорностима и ограничењима одговорности Сертификационог тела Поште дефинисаним у овим практичним правилима и другим актима објављеним на веб сајту Сертификационог тела Поште.

9.6.5. Права и обавезе других учесника

Сваком учеснику гарантује се да Сертификационо тело Поште услуге сертификације пружа у складу са законом и другим сродним прописима, овим практичним правилима и другим општим актима и интерним правилима рада Сертификационог тела Поште.

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

9.8.1. Одговорност и ограничења од одговорности сертификационог тела

Сертификационо тело Поште дужно је да на прописан начин издаје квалификоване сертификате и одговорно је за штету причињену лицу које се поуздало у тај сертификат, у складу са законом, актима сертификационог тела и уговором закљученим између Сертификационог тела Поште и корисника.

Сертификационо тело Поште је дужно да чува доказе о томе да је поступало у складу са важећим прописима.

Сертификационо тело Поште не одговара за штету (директну или индиректну), губитке, трошкове и потраживања која произилазе из или су настала због употребе сертификата, ако је:

- сертификат био употребљен супротно овим практичним правилима, као и супротно другим прописима који регулишу ову област,
- сертификат био на било који начин промењен од стране корисника,
- дошло до злоупотребе техничких средстава (хардвера или софтвера) или приватног криптографског кључа код корисника, односно компромитовања приватног криптографског кључа, код корисника,
- дошло до нефункционисања или грешке у функционисању техничких средстава (хардвера или софтвера) корисника или трећег лица, у ком случају, Сертификационо тело Поште није дужно да пружи техничку подршку у отклањању проблема насталог у функционисању техничких средстава ових субјеката.

Сертификационо тело Поште не одговара за штету која настане као последица околности, које су изван контроле Сертификационог тела Поште.

9.8.2. Одговорност и ограничења од одговорности корисника квалификованог сертификата

Корисник сертификата је одговоран за штету која настане у случају коришћења сертификата после истека рока важности сертификата, опозива или суспензије, као и у другим случајевима недозвољеног коришћења сертификата, укључујући и неиспуњења обавеза утврђених у тачки 9.6.3. ових практичних правила.

Корисник сертификата одговара и за штету коју причини недозвољеним коришћењем сертификата.

Корисник сертификата одговора за штету уколико са намером, крајњом непажњом или из нехата обрише сертификат или криптографске кључеве са средства за креирање квалификованог електронског потписа или печата, као и када на било који начин оштети средство или перманентно блокира средство (*PUK Status = LOCKED*), тако да онемогући његово коришћење.

Корисник није одговоран за штету, ако докаже да је поступао у складу са законом, подзаконским актима и закљученим уговором.

9.9. Накнаде

За пружање услуга Сертификационог тела Поште, корисник плаћа накнаде у складу са тачком 9.1. ових практичних правила.

9.10. Ступање на снагу и престанак важења правних аката

9.10.1. Ступање на снагу 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 практична правила доступна су свим заинтересованим лицима и објављују се на веб сајту Сертификационог тела Поште.

9.10.2. Престанак важења правних аката

Престанак важења правних аката Сертификационог тела Поште објављују се „Службеном ПТТ-гласнику“.

9.10.3. Ефекат трајања

Сертификационо тело Поште ће и после престанка важења квалификованог сертификата поштовати тајност личних и других података корисника, као и после престанка важења својих аката.

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 овим практичним правилима.

9.12. Допуне Практичних правила

9.12.1. Поступак за допуну

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

Измене и допуне Практичних правила, које се односе на рад Сертификационог тела Поште и издавање квалификованих сертификата, по правилу се усвајају тридесет дана пре почетка важења. Измене и допуне Практичних правила, које по процени Сертификационог тела Поште не утичу битно на кориснике усвајају се седам дана пре почетка важења.

9.12.2. Механизам и период обевештавања

О изменама и допунама Практичних правила и осталих докумената везаних за Практична правила, Сертификационо тело Поште обавештава надлежни орган и исте објављује на веб сајту Сертификационог тела Поште.

9.12.3. Околности под којима *OID* мора да се промени

Промена *OID*-а ће се извршити уколико управна структура највишег нивоа Сертификационог тела Поште одлучи да направи промене у Политици сертификације и Практичним правилима, а наведене промене буду захтевале промену *OID*-а.

9.13. Спорови између сертификационог тела и корисника

Уколико дође до спора између Сертификационог тела Поште и корисника квалификованог сертификата, у вези међусобних права и обавеза и тумачења уговора и ових практичних правила, Сертификационо тело Поште ће настојати да спор реши мирним путем, споразумно, а уколико до споразума не дође, спор ће решавати надлежни суд у Београду.

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 ових практичних правила меродавно је право Републике Србије.

9.15. Усклађеност са важећим законодавством

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

9.16. Остале одредбе

9.16.1. Уговор са корисницима

Пружање услуга сертификације (издавање и коришћење квалификованог сертификата) регулише се посебним уговором између Сертификационог тела Поште и корисника, у складу са законом и другим прописима.

9.16.2. Преношење права

Корисник квалификованог сертификата нема право да права из закљученог уговора са Сертификационим телом Поште, у целини или делимично, пренесе на трећа лица.

Сертификационо тело Поште има право да уговор закључен са корисником, односно права и обавезе из тог уговора, у потпуности или делимично, без сагласности корисника, пренесе на друго регистровано сертификационо тело у Републици Србији или надлежни орган.

9.16.3. Измена или неважење одредби ових практичних правила

Измене или допуне појединих одредби ових практичних правила или аката донетих на основу ових практичних правила не утичу на важење осталих одредби ових практичних правила.

9.16.4. Применљивост за адвокатске накнаде и одрицање од права

Није применљиво.

9.16.5. Виша сила

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

9.17. Друге одредбе

9.17.1. Доступност услуге особама са инвалидитетом

Где је то могуће, Сертификационо тело Поште омогућава да услуге сертификације и производи за крајњег корисника који се користе при пружању тих услуга буду доступни особама с инвалидитетом.

9.17.2. Језик

Ова практична правила и друга акта Сертификационог тела Поште доносе се и објављују се на српском језику.

9.17.3. Прелазна одредба и ступање на снагу

За квалификоване електронске сертификате (*Certification Practices Statement - CPS*) издате по основу Практичних правила пружања услуге сертификације Сертификационог тела Јавног предузећа „Пошта Србије“, Београд за квалификоване електронске сертификате (*Certification Practices Statement - CPS*) („Службени ПТТ-гласник“, број 1307/20) примењиваће се та практична правила, до истека важења сертификата.

Ова практична правила, ступају на снагу осмог дана од дана објављивања у „Службеном ПТТ-гласнику“.

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