РЕПУБЛИКА СРБИЈА
МИНИСТАРСТВО УНУТРАШЊИХ ПОСЛОВА
СЕРТИФИКАЦИОНО ТЕЛО

На основу члана 31. став 2. Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС“, број 94/17) и члана 4. Уредбе о условима за пружање квалификованих услуга од поверења, („Службени гласник РС“, број 37/18)

министар унутрашњих послова доноси

Практична правила за пружање услуге издавања квалификованих електронских сертификата на личним картама

1. Увод

Министарство унутрашњих послова (у даљем тексту „МУП“) као пружалац квалификоване услуге од поверења, уписан 07.05.2018. године у „Регистар пружалаца квалификованих услуга од поверења“ решењем број: 345-01-258/2018-12, пружа услугу издавања квалификованих електронских сертификата на личним картама у складу са Законом о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању (Службени гласник РС“, број 94/17), у даљем тексту: „Закон“ и сагласно Уредби о условима за пружање квалификованих услуга од поверења, („Службени гласник РС“, број 37/18), у даљем тексту „Уредба“. МУП пружа услугу издавања квалификованих електронских сертификата сагласно захтевима стандарда:

- *ETSI EN 319 401 „Electronic Signatures and Infrastructures (ETSI); General Policy Requirements For Trust Service Providers" [EN 319 401];*
- *ETSI EN 319 411-2 „Electronic Signatures and Infrastructures (ETSI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates" [EN 319 411-2],*
- *ETSI EN 319 411-1. „Electronic Signatures and Infrastructures [EN 319 411-1],* одељак *6.3.6 „Certificate renewal"*

Сертификати које МУП издаје испуњавају услове прописане Правилником о условима које морају да испуњавају квалификовани електронски сертификати ("Службени гласник РС", број 34/18 и број 81/18) и у складу су са препорученим стандардима:

- *ITU-T Recommandation X.509 Version 3*
- *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 TS 119 312 „Electronic Signatures and Infrastructures (ESI) – Cryptographic*

Suites".

- *IETF RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"*
- *IETF RFC 3739„Internet X.509 Public Key Infrastructure: Qualified Certificates Profile*

Структура овог акта је у складу са *RFC 3647 "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework" [RFC3647].*

МУП је дефинисао опште услове пружања услуге издавања квалификованих електронских сертификата, који су прецизирани у актима: Политика пружања услуге издавања квалификованих електронских сертификата на личним картама (Политика издавања сертификата) и Практична правила за пружање услуге издавања квалификованих електронских сертификата на личним картама (Практична правила за издавање сертификата). Политика издавања сертификата дефинише и прецизира правила пружања услуге издавања квалификованих електронских сертификата, а Практична правила за издавање сертификата дефинишу оперативне процедуре и друге услове у циљу испуњења захтева одређених политиком пружања услуге. Политика издавања сертификата и Практична правила за издавање сертификата су јавни акти.

МУП је утврдио Посебна интерна правила рада и заштите система издавања сертификата која детаљно описују поступке и мере које се примењују приликом руковања криптографским параметрима (алгоритмима и кључевима) за издавање идентификационих докумената и квалификованих електронских сертификата . Интерна правила нису јавна и означена су ознаком тајности „ДРЖАВНА ТАЈНА", у складу са Законом о тајности података.

МУП је одговоран за пружање комлетне услуге издавања сертификата која укључује следеће:
1) регистрацију корисника;
2) формирање сертификата;
3) дистрибуцију сертификата корисницима;
4) управљање животним веком (обнављање, суспензија, реактивација и опозив сертификата);
5) обезбеђивање поузданог и јавно доступног сервиса за проверу статуса сертификата.

1.2 Назив акта и идентификација

Назив акта:	Практична правила за пружање услуге издавања квалификованих електронских сертификата на личним картама
OID:	1.3.6.1.4.1.33589.1.1.1
Важење акта:	Ова верзија акта важи до издања следеће верзије

1.3 Учесници у ПКИ систему

Основна улога инфраструктуре система са јавним кључевима, ПКИ система (*PKI - Public Key Infrastructure)* је поуздано успостављање електронског идентитета корисника специфицираног у облику електронског сертификата. ПКИ систем МУП-а је хијерархијске структуре. На првом нивоу хијерархије је врховно самопотписујуће сертификационо тело *(RootCA)*, а на следећем нивоу су подређена сертификациона тела, издаваоци корисничких сертификата. Учесници ПКИ система су сертификационо тело, регистрациона тела, корисници и поуздајуће стране.

1.3.1 Сертификационо тело

Сертификационо тело *(CA - Certificate Authority)* представља највишу тачку поверења у ПКИ систему. Основна улога сертификационог тела је да процедуром електронског потписа на бази асиметричног криптографског алгоритма и свог приватног кључа, који мора бити најстроже чувана тајна, гарантује везу између јавног кључа и идентитета корисника сертификата.

RootCA издаје и својим приватним кључем потписује сертификате сертификационих тела, која су му по ПКИ хијерархији подређена, а то су СА издаваоци корисничких сертификата. *RootCA* опозива сертификате које је издао и потписује листе опозваних СА сертификата (*CRL – Certificate Revocation List).*

СА издавалац корисничких сертификата издаје и потписује корисничке сертификате, опозива их и потписује листе опозваних корисничких сертификата.

1.3.2 Регистрациона тела

Регистрациона тела су организационе јединице МУП-а, које врше регистрацију корисника за издавање сертификата, односно организационе јединице надлежне за издавање личних идентификационих докумената. Захтеви за издавање квалификованих електронских сертификата се подносе регистрационим телима. Регистрација корисника за потребе издавања квалификованих електронских сертификата се врши у оквиру процедуре аквизиције података за издавање идентификационих докумената, у складу са законски дефинисаним процедурама.

1.3.3 Корисници

Корисници су физичка лица којима се пружа услуга издавања квалификованих електронских сертификата.

1.3.4 Поуздајуће стране

Поуздајуће стране су физичка или правна лица која се поуздају у квалификоване електронске сертификате, у циљу верификовања квалификованог електронског потписа и

потврде идентитета корисника. Пре него што се поуздају у сертификат поуздајуће стране треба да изврше проверу статуса квалификованог електронског сертификата, спрам листе опозваних сертификата, која се ажурира на дневном нивоу.

1.3.5 Други учесници

Ова одредба није применљива.

1.4 Употреба сертификата

1.4.1 Прихватљива употреба сертификата

Сертификат за аутентикацију и шифровање и квалификовани сертификат за електронски потпис уписани у чип личне карте представљају шему електронске идентификације високог нивоа поузданости.

Сертификат се може користити за већину сервиса електронске управе и електронског пословања који су базирани на употреби квалификованих електронских сертификата. Корисник је дужан да сертификат користи у складу са важећим законским прописима. Домен коришћења сертификата дефинисан је у пољу Key Usage сертификата.

1.4.2 Забрањена употреба сертификата

Свака употреба сертификата ван оквира дефинисаног одредбом 1.4.1 овог акта није дозвољена.

1.5 Администрација правних аката

1.5.1 Организациона јединица надлежна за администрацију правних акта

Организациона јединица у МУП-у надлежна за израду, измене и допуне Политике издавања сертификата и овог акта је Одсек за сертификациони систем, Одељења за информациону безбедност, Сектора за аналитику, телекомуникационе и информационе технологије, Министарства унутрашњих послова.

1.5.2 Контакт подаци

Министарство унутрашњих послова
Сектор за аналитику, телекомуникационе и информационе технологије
Одељење за информациону безбедност
Одсек за сертификациони систем
Кнеза Милоша 103, 11000 Београд

e-mail: ca@mup.gov.rs

website: http://ca.mup.gov.rs

1.5.3 Усклађивање аката са праксом издавања сертификата

Запослени у Одсеку за сертификациони систем МУП-а усклађују форму и садржај Политике издавања сертификата и овог акта са важећом законском регулативом и евентуалним променама насталим у пракси издавања сертификата. Оцену усаглашености даје тело за оцењивање усаглашености у складу са законом.

1.5.4 Процедура одобравања аката

Политика издавања сертификата и овај акт се прегледају и ажурирају једном годишње или чешће у случају ванредних промена одређених одредби које проистичу из евентуалних промена у законској регулативи или техничким карактеристикама примењених криптографских алгоритама и дужина криптографских кључева. Свака нова верзија пре објављивања мора проћи процедуру одобравања.

Након креирања или ажурирања аката од стране запослених у Одсеку за сертификациони систем, акта прегледају Шеф Одсека за сертификациони систем и начелник Одељења за информациону безбедност. Кад се они сагласе, акти иду на одобрење код начелника Сектора за аналитику, телекомуникационе и информационе технологије. Акта која су одобрена од стране начелника Сектора се шаљу Секретаријату Министарства на мишљење. Након усклађивања са мишљењем Секретаријата акта потписује министар унутрашњих послова.

2. Објављивања информација и локација где се објављују

Све инфомације које се односе на пружање услуге издавања квалификованих електронских сертификата МУП објављује на веб страни сертификационог тела МУП-а, http://ca.mup.gov.rs

Сертификационо тело Министарства унутрашњих послова ће кориснике о свим изменама Политике издавања сертификата, Практичних правила издавања сертификата, Уговора и свим другим изменама обавештавати путем странице Обавештења на сајту сертификационог тела Министарства унутрашњих послова.

2.1 Веб страна сертификационог тела МУП-а

Веб страна сертификационог тела МУП-а је јавно доступна као и све информације које се на њој објављују. Објављене информације се периодично ажурирају.

2.2 Информације које се објављују

МУП објављује следеће информације које се односе на пружање услуге издавања квалификованих електронских сертификата:

- акт Политика пружања услуге издавања квалификованих електронских сертификата на личним картама,

- акт Практична правила за пружање услуге издавања квалификованих електронских сертификата на личним картама (овај акт),
- акт Општи услови пружања услуге издавања квалификованих електронских сертификата,
- Образац Уговора о пружању услуге издавања квалификованих електронских сертификата,
- Образац захтева за пружање услуге издавања и обнављање квалификованих електронских сертификата (Образац 1.),
- Образац захтева за деблокадом ПИН-а личне карте (Образац 2.),
- Образац захтева за промену статуса квалификованих електронских сертификата (Образац 3.),
- CA сертификате,
- Листе опозваних сертификата,
- Корисничка упутства,
- друга акта и обавештења.

2.3 Фреквенција објављивања информација

Листе опозваних сертификата се објављују на 24 сата.
Акти и остали подаци се објављују након измена које су усвојене и одобрене.

2.4 Контрола приступа веб сајту сертификационог тела МУП-а

Веб сајт сертификационог тела МУП-а има имплементиране логичке и физичке сигурносне механизме за заштиту података од неовлашћеног брисања, додавања или промена. Приступ објављеним подацима ограничен је само на могућност читања и преузимања.

3. Идентификација и аутентикација

3.1 Имена

3.1.1 Врсте имена

У квалификованим електронским сертификатима које издаје МУП, име сертификационог тела које издаје сертификате, поље Issuer и име корисника сертификата, поље Subject, су јединствена имена (Distinguished Name - DN).

3.1.2 Значење имена

Име корисника сертификата једнозначно потврђује идентитет корисника.

3.1.3 Анонимност или псеудоними корисника

Корисници не могу да буду анонимни и не могу да користе псеудониме.

3.1.4 Правила за тумачење различитих врста имена

Имена корисника сертификата представљена су одговарајућим латиничним/ћириличним словима српског језика.

3.1.5 Јединственост имена

Јединственост имена корисника сертификата се остварује помоћу јединственог серијског броја X.509 сертификата.

3.1.6 Препознавање, аутентикација и улога заштитног знака

Додавање заштитног знака имену корисника сертификата није дозвољено. Имена којима би се кршила интелектуална или ауторска права других нису дозвољена.

3.2 Идентификација и аутентикација корисника

Након подношења захтева за издавање квалификованог електронског сертификата врши се провера идентитета корисника коме се издаје сертификат.

Сертификат за аутентикацију и шифровање и квалификовани сертификат за електронски потпис уписани у чип личне карте представљају шему електронске идентификације високог нивоа поузданости.

3.2.1 Метод доказивања поседа приватног кључа

Ово није применљиво, јер корисник не генерише свој приватни кључ, већ се у процесу издавања квалификованог електронског сертификата приватни кључ генерише у самом чипу личне карте.

3.2.2 Идентификација и аутентикација правног лица

Ова одредба није применљива, јер МУП издаје сертификате искључиво физичким лицима.

3.2.3 Идентификација и аутентикација физичког лица

Идентитет физичког лица се приликом подношења захтева за издавање сертификата потврђује на основу важећег идентификационог документа.

3.2.4 Непроверени подаци о кориснику

Корисник сноси одговорност за тачност података наведених у захтеву за издавање сертификата.

3.2.5 Провера тачности података правног лица

Ова одредба није применљива, јер МУП не издаје сертификате правним лицима.

3.2.6 Критеријуми интероперабилности

Ова одредба није применљива.

3.3 Идентификација и аутентикација при захтеву за заменом кључа

Замена кључа у оквиру истог сертификата није дозвољена. Када се мења кључ генерише се нови сертификат.

3.4 Идентификација и аутентикација при захтеву за опозивом сертификата

Поступак идентификације корисника при подношењу захтева за опозив сертификата је идентичан као при подношењу захтева за издавањем сертификата.

4. Оперативни захтеви у вези животног века сертификата

4.1 Подношење захтева за пружање услуге издавање сертификата

4.1.1 Ко може поднети захтев за пружање услуге издавање сертификата?

Захтев за пружање услуге издавања квалификованог електронског сертификата може да поднесе:

- Држављанин Републике Србије, који има важећу личну карту са чипом,
- Страни држављанин, који има важећу биометријску личну карту за странце. (Сертификати се не издају на привременим личним картама за странце.)

4.1.2 Услови за издавање квалификованог електронског сертификата

Услови за издавање сертификата кориснику су:

- да корисник поседује важећу личну карту са чипом,
- да корисник регистрационом телу лично поднесе уредно попуњен и својеручно потписан Захтев за пружање услуге издавања квалификованог електронског сертификата,
- да се корисник пре подношења захтева упозна са Општим условима пружања услуге издавања квалификованог електронског сертификата,
- да корисник са МУП-ом закључи Уговор о пружању услуге издавања квалификованог електронског сертификата.

Корисник уз Захтев прилаже два примерка својеручно потписаног документа „Општи услови пружања услуге издавања квалификованог електронског сертификата“ чиме потврђује да је упознат са садржајем тог документа. Уговор се закључује у два примерка, по један за сваку уговорну страну. Уговором су регулисана међусобна права и обавезе уговорних страна.

4.2 Обрада захтева за издавање сертификата

4.2.1 Идентификација и аутентикација при пријему захтева

Корисник регистрационом телу лично подноси захтев за издавање сертификата. Службеник регистрационог тела врши идентификацију корисника на основу важећег идентификационог документа.

4.2.2 Прихватање или одбијање захтева за издавање сертификата

Захтев ће бити прихваћен ако су испуњени услови из одредбе 4.1.2 овог акта, а одбијен ако било који од услова није испуњен. Службеник регистрационог тела потврђује да је захтев прихваћен својим потписом на захтеву.

4.2.3 Време обраде захтева за издавање сертификата

Захтев се сматра обрађеним прихватањем захтева од стране службеника регистрационог тела, након чега службеник започиње процес издавања сертификата.

4.3 Издавање сертификата

4.3.1 Активности током издавања сертификата

У процесу издавања сертификата неопходно је унети активациони податак (ПИН) који је познат само кориснику. Корисник активациони податак добија у заштићеној коверти приликом преузимања личне карте са чипом. Потребно је омогућити кориснику да, у процесу издавања сертификата у кораку који захтева унос активационог податка, сам унесе свој активациони податак. У случају да је корисник заборавио свој ПИН потребно је да пре подношења захтева за издавање сетификата, поднесе захтев за деблокадом ПИН-а. У процесу деблокаде ПИН-а, поставља се нови ПИН који корисник сам одређује. У сертификат ће бити уписан е-маил корисника ако је корисник тако навео у захтеву.

Након уписа сертификата у чип личне карте службеник кориснику предаје личну карту и по један примерак Уговора и Општих услова издавања сертификата. На овај начин је завршен поступак издавања сертификата

4.3.2 Обавештавање корисника о издавању сертификата

Ова одредба није применљива, јер се поступак издавања сертификата спроводи у присуству корисника.

4.4 Прихватање сертификата

4.4.1 Поступак прихватања сертификата

Сертификат се кориснику лично уручује и сматра се прихваћеним првом употребом сертификата од стране корисника.

4.4.2 Објављивање сертификата

Сертификати корисника се не објављују.

4.4.3 Обавештавање поуздајуће стране о издавању сертификата

Обавештавање поуздајуће стране о издавању сертификата се не врши.

4.5 Коришћење сертификата и асиметричног пара кључева

4.5.1 Коришћење приватног кључа корисника и сертификата

Приватни криптографски кључ корисника се користи за креирање квалификованог електронског потписа. Корисник приступа свом приватном кључу уношењем активационог податка (ПИН-а). Квалификовани електронски сертификат се користи за верификовање квалификованог електронског потписа.

4.5.2. Коришћење јавног кључа корисника и сертификата

Јавни кључ и квалификовани сертификат корисника поуздајуће стране користе за верификацију електронског потписа. Поуздајуће стране пре него што се поуздају у сертификат треба да осим верификације изврше и валидацију сертификата, односно треба да провере ланац поверења (ланац CA сертификата издаваоца) и статус сертификата спрам листе опозваних сертификата.

4.6 Обнављање сертификата

Под обнављањем сертификата подразумева се генерисање новог пара криптографских кључева и издавање квалификованог електронског сертификата на личној карти, која већ има уписан квалификовани електронски сертификат, који је шест месеци или мање пред истицањем или му је истекла важност.

4.6.1 Околности за обнављање сертификата

Сертификат се издаје са роком важења до 5 година или краће, односно до истека периода важности личне карте. У случају када је лична карта и даље важећа, а до истека важности сертификата је остало шест месеци или мање, или му је важност истекла, корисник може захтевати обнављање сертификата.

Услови за обнављање сертификата су да корисник поднесе захтев за обнављање сертификата, да има важећи Уговор о пружању услуге издавања квалификованог електронског сертификата и важећу личну карту.

4.6.2 Ко може захтевати обнављање сертификата?

Обнављање сертификата може да захтева корисник сертификата.

4.6.3 Обрада захтева за обнављање сертификата

Захтев за обнављање сертификата корисник подноси регистрационом телу, које захтев прихвата ако су испуњени услови из одредбе 4.6.1, а одбија захтев ако услови нису испуњени. Након прихватања захтева службеник регистрационог тела врши обнављање и упис сертификата у чип личне карте.

4.6.4 Обавештавање корисника о обнављању сертификата

Ова одредба није применљива, јер се поступак обнављања сертификата спроводи у присуству корисника.

4.6.5 Прихватање обновљеног сертификата

Обновљени сертификат се сматра прихваћеним након прве употребе од стране корисника.

4.6.6 Објављивање обновљеног сертификата

Ова одредба није применљива, јер се сертификати корисника не објављују.

4.6.7 Обавештавање поуздајуће стране о обнављању сертификата

Ова одредба није применљива

4.7 Замена јавног кључа у сертификату

Замена кључева у сертификату се не врши. Када се генерише нови пар кључева издаје се нови сертификат.

4.7.1 Околности за замену јавног кључа у сертификату

Ова одредба није применљива.

4.7.2 Ко може да захтева нови јавни кључ?

Ова одредба није применљива.

4.7.3 Обрада захтева за заменом јавног кључа

Ова одредба није применљива.

4.7.4 Обавештавање корисника о замени јавног кључа

Ова одредба није применљива.

4.7.5 Прихватање сертификата са замењеним јавним кључем

Ова одредба није применљива.

4.7.6 Објављивање сертификата са замењеним јавним кључем

Ова одредба није применљива.

4.7.7 Обавештавање поуздајуће стране о замени јавног кључа сертификата

Ова одредба није применљива.

4.8 Модификација сертификата

Модификација сертификата подразумева промену података у сертификату без промене јавног кључа сертификата.

Модификација сертификата се не врши.

4.8.1 Околности за модификацију сертификата

Ова одредба није применљива.

4.8.2 Ко може захтевати модификацију сертификата?

Ова одредба није применљива.

4.8.3 Обрада захтева за модификацију сертификата

Ова одредба није применљива.

4.8.4 Обавештавање корисника о модификацији сертификата

Ова одредба није применљива.

4.8.5 Прихватање модификованог сертификата

Ова одредба није применљива.

4.8.6 Објављивање модификованог сертификата

Ова одредба није применљива.

4.8.7 Обавештавање поуздајуће стране о модификацији сертификата

Ова одредба није применљива.

4.9 Опозив, суспензија и реактивација сертификата

Опозив сертификата је потпуно укидање важења сертификата и његово објављивање на листи опозваних сертификата (CRL листи).

Суспензија сертификата је привремено укидање важења сертификата и његово објављивање на CRL листи. Суспензија траје онолико дуго колико трају услови због којих је захтевана. Када ови услови престану да важе, корисник може захтевати реактивацију сертификата.

Реактивација сертификата је поновно активирање сертификата који је био суспендован и његово брисање са CRL листе.

4.9.1 Околности за опозив сертификата

Опозив сертификата се врши када:
1) опозив сертификата захтева власник сертификата или његов пуномоћник,
2) власник сертификата изгуби пословну способност;
3) се утврди да је податак у сертификату погрешан;
4) се утврди да су подаци за проверу квалификованог електронског потписа угрожени на начин који утиче на безбедност и поузданост сертификата;
5) се утврди да су подаци за електронско потписивање угрожени на начин који утиче на безбедност и поузданост електронског потписа;
6) издавалац сертификата престаје са радом или му је рад забрањен.

4.9.2 Ко може захтевати опозив сертификата?

Опозив сертификата може захтевати корисник или његов овлашћени пуномоћник.
Корисник је дужан да одмах затражи опозив свог сертификата у случају губитка или оштећења средства или података за креирање електронског потписа или у случају компромитације или сумње у компромитацију свог приватног кључа.

4.9.3 Поступак опозива сертификата

Корисник регистрационом телу подноси захтев за опозив сертификата. Службеник регистрационог тела након пријема захтева без одлагања врши опозив сертификата. Службеник потврђује да је примио Захтев за опозивом сертификата својим потписом. Након подношења Захтева за опозивом сертификата службеник започиње процес опозива

сертификата. Службеник одлаже на чување Захтев за опозивом сертификата, а корисника обавештава да је корисников сертификат опозван, што подразумева трајно укидање важења сертификата и његово објављивање на листи опозваних сертификата (без могућности реактивације).

4.9.4 Време обраде захтева за опозивом

Захтев за опозивом се обрађује одмах након пријема без одлагања и сертификат се одмах опозива.

4.9.5 Време за које се сертификат који је опозван уписује на листу опозваних сертификата

Чим се опозове сертификат се уписује на листу опозваних сертификата. Након опозива сертификата генерише се нова листа опозваних сертификата.

4.9.6 Провера статуса сертификата

Поуздајуће стране пре него што се поуздају у сертификат врше проверу статуса сертификата, односно проверавају да ли се сертификат налази на листи опозваних сертификата (CRL- Certificate Revocation List).

4.9.7 Фреквенција објављивања листе опозваних сертификата (CRL листе)

CRL листа се објављује сваких 24 сата.

4.9.8 Максимално кашњење у објављивању CRL листе

У случају опозива или суспензије сертификата генерише нова CRL листа и објављује одмах након генерисања, пре редовне објаве.

4.9.9 Расположивост провере статуса сертификата

Ажурна CRL листа је увек доступна на веб сајту сертификационог тела МУП-а.

4.9.10 Захтеви за проверу статуса сертификата

Поуздајуће стране су дужне да провере статус сертификата у који се поуздају на основу јавно доступне листе опозваних сертификата.

4.9.11 Друге форме регистра опозваних сертификата

Ова одредба није применљива.

4.9.12 Посебни захтеви у случају компромитације кључа

У случају сумње у компромитацију свог приватног кључа корисник је дужан да одмах престане са његовим коришћењем и поднесе захтев за опозив сертификата.

4.9.13 Околности за суспензију и реактивацију сертификата

Суспензија сертификата се може извршити ако одређени период не постоји потреба за коришћењем сертификата. У случају да се после одређеног периода поново појави потреба за коришћењем, суспендовани сертификат се може реактивирати.

4.9.14 Ко може да захтева суспензију и реактивацију сертификата?

Суспензију и реактивацију сертификата захтева корисник.

4.9.15. Поступак суспензије и реактивације сертификата

4.9.15.1 Поступак суспензије

Корисник регистрационом телу подноси захтев за суспензијом сертификата. Службеник по пријему захтева за суспензијом без одлагања врши суспензију сертификата. Након извршене суспензије службеник одлаже на чување захтев за суспензијом сертификата, а корисника обавештава да је корисников сертификат суспендован, што подразумева привремено укидање важења сертификата и његово објављивање на листи опозваних сертификата.

4.9.15.2 Поступак реактивације

Корисник регистрационом телу подноси захтев за реактивацијом сертификата. Службеник по пријему захтева за реактивацијом без одлагања врши реактивацију сертификата. Након извршене реактивације службеник одлаже на чување захтев за реактивацијом сертификата, а корисника обавештава да је корисников сертификат реактивиран, што подразумева брисање сертификата са листе опозваних сертификата и враћање у активан статус.

4.10 Сервиси провере статуса сертификата

4.10.1 Оперативне карактеристике

Опозвани и суспендовани сертификати објављују се на листи опозваних сертификата (CRL листа) која се објављује на 24 сата, а у случају опозива и суспензије ажурира се пре редовне објаве.

4.10.2 Доступност сервиса

Листа опозваних сертификата је стално доступна (24/7) на веб сајту сертификационог тела МУП-а.

4.10.3 Додатне карактеристике

Листа опозваних сертификата садржи серијске бројеве сертификата, датум, време и разлог

опозива сертификата.

4.11 Престанак коришћења сертификата

Корисник престаје да користи сертификат након опозива сертификата.

4.12 Откривање и обнова приватног кључа корисника

Приватни кључ квалификованог сертификата за електронски потпис генерише се у самом чипу личне карте и нигде се осим на чипу не чува, тако да се не може открити нити обновити.

5. Физичка, процедурална и кадровска безбедносна контрола

5.1 Физичка контрола

5.1.1 Локација

Целокупна опрема безбедних система за издавање сертификата (сервери, криптографски уређаји и остала опрема) смештени су у Београду, у згради Министарства унутрашњих послова у улици Кнеза Милоша број 103. Опрема система за издавање сертификата налази се у просторији, која одговара потребама извршења операција високе безбедности (Фарадејев кавез).

5.1.2 Контрола физичког приступа

Фарадејев кавез у коме се налази опрема система за издавање сертификата смештен је у безбедној зони зграде, у оквиру Центра за персонализацију идентификационих докумената (Персоцентар). У безбедној зони имплементиран је механизам физичке контроле приступа заснован на бесконтактним смарт картицама. Просторијама у оквиру безбедне зоне могу да приступе само запослени у Персоцентру и запослени у Одсеку за сертификациони систем, који имају смарт картице са додељеним дозволома за приступ одређеним просторијама у безбедној зони. Контрола приступа Фарадејевом кавезу, где је смештена опрема система за издавање сертификата, ограничена је на запослене у Одсеку за сертификациони систем. У Фарадејевом кавезу постављене су сигурносне камере, тако да је под сталним надзором. Систем контроле физичког приступа електронски евидентира сваки улазак у Фарадејев кавез.

5.1.3 Напајање и климатизација

Целокупна опрема система за издавање сертификата прикључена је на систем за непрекидни извор напајања електричном енергијом и стабилизацију напона. Систем за климатизацију омогућава контролу и одржавање температуре и влажности ваздуха у дефинисаном опсегу. Напајање и вентилација се извршавају са редундансом високог

нивоа.

5.1.4 Заштита од поплава

У Фарадејевом кавезу нема водоводних инсталација. Предузете су техничке мере заштите од евентуалних поплава од водоводних инсталација у окружењу.

5.1.5 Заштита од пожара

Фарадејев кавез опремљен је системом за рано откривање и аутоматску дојаву пожара, детекторима дима и системом за гашење пожара, који није штетан за људе, рачунарску и комуникациону опрему.

5.1.6 Чување медија

Сви рачунарски медији, који садрже продукциони софтвер, архиву логова и резервне копије података система за издавање сертификата, смештају се у ватроотпорне безбедне сефове, заштићене системима физичке и логичке контроле приступа.

5.1.7 Бацање отпада

Након престанка потребе за коришћењем података, документације и уређаја, везаних за рад система за издавање сертификата, подаци, документација и уређаји се уништавају.

Папирна документација се уништава пропуштањем кроз машину за сечење папира. Подаци са рачунарских медија се неповратно бришу, а рачунарски медији се физички уништавају. Криптографски уређаји се физички унуштавају.

5.1.8 Чување резервних копија

Имплементиран је систем за прављење резервних копија *(backup)* података и логова система за издавање сертификата. Резервне копије се чувају у безбедним сефовима заштићеним системима физичке и логичке контроле приступа. Резервна копија за процедуру опоравка од катастрофе *(disaster recovery)* се чува на удаљеној локацији.

5.2 Процедурална контрола

5.2.1 Поверљиве улоге

Запосленима у Одсеку за сертификационо тело додељене су безбедносне функције које подразумевају следеће поверљиве улоге:

- **главни администратор безбедности,** одговоран за администрирање и имплементацију безбедносних функција и процедура, као и управљање активностима на додатном унапређењу послова издавања и управљања животним веком сертификата,
- **систем администратори**, одговорни за инсталацију, конфигурисање и одржавање безбедних система за издавање сертификата,
-

- **систем оператори**, одговорни за рад безбедних система за издавање сертификата и за имплементацију система за формирање резервних копија и процедуре опоравка,
- **систем евидентичари**, одговорни за прегледање и одржавање архива и лог фајлова безбедних система за издавање сертификата.

5.2.2 Потребан број запослених за извршавање процедуре

Имплементирана је строга процедурална контрола, која захтева вишеструку ауторизацију за извршавање процедура високог нивоа поверљивости. Неопходна је аутентикација најмање два запослена са поверљивим улогама да би био могућ физички и логички приступ критичним системима за издавање сертификата и криптографским уређајима.

5.2.3 Идентификација и аутентикација за сваку улогу

Имплементирана контрола физичког и логичког приступа омогућава:
- да се физички приступ безбедним зонама остварује двоструком аутентикацијом, заснованом на примени смарт картица;
- да се за логички приступ безбедним системима захтева ауторизација запослених, заснована на додели одговарајућих поверљивих улога.

5.2.4 Поверљиве улоге које захтевају раздвајање дужности

Извршавање процедура високог нивоа поверљивости захтева присуство и учешће најмање два запослена са поверљивим улогама. Према томе, раздвајање дужности у оквиру једне поверљиве улоге није потребно.

5.3 Кадровска безбедносна контрола

Пре заснивања радног односа врши се провера подобности и компетенције кандидата за одређено радно место. Кандидат не сме бити кажњаван нити кривично гоњен.

5.3.1 Квалификација и искуство

Кандидат мора да задовољи одређене захтеве у погледу стручне квалификације и радног искуства на истим или сличним пословима. Неопходно је да кандидат, за свако радно место на које се ангажује, има одговарајући степен стручне спреме из области информационо комуникационих технологија и потребно радно искуство у области одржавања и безбедности информационих система.

5.3.2 Безбедносна контрола

Пре заснивања радног односа у МУП-у врше се безбедносне провере кандидата у складу са законом и на начин прописан подзаконским актима.

5.3.3 Захтеви за обученошћу

Запослени са поверљивим улогама треба да поседују експертско знање из области одржавања и безбедности информационих система.

5.3.4 Фреквенција поновних обука

Потребно је да запослени са поверљивим улогама најмање једном годишње похађају обуке и семинаре у циљу обнављања знања о новим безбедносним претњама и актуелним безбедносним процедурама.

5.3.5 Ротација послова

Ова одредба није применљива.

5.3.6 Санкционисање неауторизованих активности

Запослени са поверљивим улогама дужни су да предузимају само оне активности за које су ауторизовани и да се придржавају прописаних интерних процедура рада и заштите система издавања сертификата. Неауторизоване активности и кршење прописаних процедура рада сматраће се повредом службене дужности.

5.3.7 Захтеви за спољне сараднике

Поверљиве улоге се не додељују спољним сарадницима. У случају потребе за ангажовањем спољних сарадника, спољним сарадницима се дозвољава приступ уз пратњу и надзор ауторизованих запослених са поверљивим улогама.

5.3.8 Документација која се доставља запосленима

Запосленима са поверљивим улогама, пре почетка вршења дужности, доставља се документација, која садржи интерне процедуре рада и заштите система издавања сертификата, како би могли да своје дужности обављају у складу да прописаним процедурама.

5.4 Процедуре бележења догађаја

Сви догађаји који се односе на обављање делатности пружања услуге издавања сертификата се бележе у лог фајлове *(Audit Logging)*, а целокупна документација примљена уз захтев за издавање сертификата се чува у евиденцијама у складу законом који уређује евиденције и обраду података у области унутрашњих послова.

5.4.1 Врсте догађаја који се бележе

Бележе се све активности предузете у процесу пријема захтева и издавања сертификата,

укључујући датум и време подношења захтева и податке о запосленом, који је примио захтев.

5.4.2 Фреквенција прегледа лог фајлова

Подаци из лог фајлова се једном недељно прегледају.

5.4.3 Период чувања лог фајлова

Након архивирања лог фајлови се чувају најмање десет година.

5.4.4 Заштита лог фајлова

Лог фајлови су заштићени од неауторизованог прегледања, модификације и брисања.

5.4.5 Процедура прављења резервнх копија лог фајлова

Резервне копије лог фајлова праве се једном месечно.

5.4.6 Систем сакупљања података лог фајлова

Систем сакупља податке и лог фајлове чува у реалном времену.

5.4.7 Обавештавање запосленог који је изазвао инцидентан догађај

У случају инцидентног догађаја, запослени који је догађај изазвао се не обавештава. О инцидентном догађају обавештава се шеф Одсека за сертификациони систем.

5.4.8 Процена рањивости система

Анализа ризика и процена рањивости система врши се једном годишње.

5.5 Архивирање података

5.5.1 Врсте података који се архивирају

МУП у складу са чланом законом који уређује евиденције и обраду података у области унутрашњих послова чува у својој архиви целокупну документацију у вези са пружањем услуге издавања сертификата:

- документацију корисника (захтеве о пружању услуге издавања сертификата, уговоре о пружању услуге издавања сертификата, захтеве за променом статуса сертификата, захтеве за деблокадом ПИН-а личне карте...);
- процедуре рада (посебна интерна правила рада и заштите система за издавање сертификата);
- инсталационе фајлове апликација система за издавање сертификата;
- лог фајлове.

5.5.2 Период чувања архиве

Комплетна документација о издатим и опозваним сертификатима и лог фајлови се чувају 10 година по престанку важења сертификата у складу са законом.

5.5.3 Заштита архиве

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

5.5.4 Процедуре прављења резервних копија архиве

Резервне копије архиве се праве једном месечно.

5.5.5 Временска ознака архивираних података

Архивирани подаци носе временску ознаку са сервера који је синхронизован са извором тачног времена.

5.5.6 Систем архивирања (интерни или екстерни)

Користи се комбиновани систем архивирања. Запослени са поверљивим улогама су одговорни за архивирање електронских података.

5.5.7 Процедуре за приступ подацима из архиве

Архивирани електронски подаци чувају се у сигурносним сефовима, за чије отварање су потребна два кључа. Сефови су постављени у заштићеним просторијама са рестриктивним и ауторизованим приступом.

5.6 Замена кључева сертификационог тела

Замена кључева сертификационог тела подразумева генерисање нових кључева сертификационог тела и врши се у случају истицања периода важности кључа, компромитације кључа или промена одговарајућих одредби, које проистичу из евентуалних промена у законској регулативи или техничким карактеристикама примењених криптографских алгоритама и дужина кључева. Замена кључева врши се у складу са процедуром дефинисаном у посебним интерним правилима рада и заштите система за издавање сертификата.

5.7 Опоровак система после катастрофе

5.7.1 Процедуре у случају инцидената

У случају појаве инцидента, током рада система за издавање сертификата, запослени са поверљивим улогама поступају у складу са својим интерним процедурама рада.

5.7.2 Процедуре у случају уништења техничких средстава

У случају штете настале на техничким средствима (хардверу и софтверу) или подацима,

сервиси апликације система за издавање сертификата биће поново успостављени у најкраћем могућем року.

5.7.3 Процедуре у случају компромитације приватног кључа сертификационог тела

МУП у случају компромитације или сумње у компромитацију приватног кључа сертификационог тела:

- престаје са издавањем сертификата;
- информише све кориснике и поуздајуће стране о компромитацији приватног кључа;
- јавно објављује информације о томе да издати сертификати, као и информације о статусу опозваности сертификата, више нису важеће;
- врши опозив свих издатих сертификата одмах, а најкасније у року од 24 часа у складу са Законом.

5.7.4 Наставак рада након катастрофе

Након катастрофе и отклањања њених последица МУП ће у најкраћем року да доведе систем у продукционо стање и настави са пружањем услуге издавања сертификата.

5.8 Престанак пружања услуге издавања сертификата

У случају престанка пружања услуге од поверења МУП ће настојати да корисницима обезбеди наставак пружања услуге код другог пружаоца услуге од поверења, коме ће доставити сву документацију и неопходна техничка средства. Ако није могуће обезбедити наставак пружања услуге код другог пружаоца услуге, МУП ће три месеца пре престанка пружања услуге обавестити кориснике и поуздајуће стране о намери престанка обављања делатности, након чега ће извршити раскид уговора и опозив свих издатих сертификата.

6. Техничке безбедносне контроле

6.1 Генерисање и инсталација пара криптографских кључева

6.1.1 Генерисање пара криптографских кључева сертификационог тела

Приватни кључеви сертификационог тела генеришу се на безбедан начин, коришћењем безбедних и поузданих система и у складу са препорученим стандардима. Примењују се неопходне превентивне мере у циљу спречавања компромитације или неауторизованог коришћења приватних кључева сертификационог тела. Приватни кључеви сертификационог тела генеришу се у криптографским уређајима, хардверско-криптографским модулима *(Hardware Security Module - HSM)* у процедури „Церемоније кључева“, која захтева вишеструку ауторизацију запослених са поверљивим улогама.

6.1.2 Генерисање пара криптографских кључева и предаја приватног кључа кориснику

Пар криптографских кључева корисника генерише се на смарт картици (личној карти са чипом), која је средство за формирање квалификованог електронског потписа *(Secure Signature CreationDevice - SSCD).* Приватни кључ и сертификат корисника генеришу се у присуству корисника и кориснику се уручују одмах након генерисања.

6.1.3 Достава јавног криптографског кључа сертификационог тела корисницима

Јавни криптографски кључ сертификационог тела је део сертификата сертификационог тела МУП-а, који је доступан корисницима на веб сајту сертификационог тела МУП-а.

6.1.4 Достава јавног криптографског кључа сертификационог тела поуздајућим странама

Јавни криптографски кључ сертификационог тела доступан је поуздајућим странама на исти начин као и корисницима, што је описано у тачки 6.1.3.

6.1.5 Дужине криптографских кључева

Криптографски кључеви врховног сертификационог тела (RootCA) су дужине 4096 бита, криптографски кључеви подређеног сертификационог тело, издаваоца корисничких сертификата су дужине 3072 бита, а криптографски кључеви корисника су дужине 2048 бита.

6.1.6 Генерисање криптографских параметара и провера квалитета

Криптографски параметри, тј. асиметрични парови кључева се генеришу помоћу хардверских генератора случајних бројева, који су реализовани на криптографско-хардверским уређајима:

- HSM *(Hardver Security Module)* уређаји – за криптографске кључеве сертификационог тела
- Смарт картица (лична карта) – за криптографске кључеве корисника.

Квалитет начина генерисања поменутих криптографских параметара искључиво зависи од квалитета хардверског генератора случајних бројева на HSM уређајима и смарт картицама.

С обзиром да су и HSM уређаји и смарт картице сертификоване по стандарду *FIPS 140-2 Level 3*, квалитет генерисаних криптографских параметара је загарантован.

6.1.7 Намена кључа

Намена кључа дефинисана је у X.509 в.3 пољу Key Usage сертификата.

Приватни криптографски кључ сертификационог тела се користи за потписивање сертификата које издаје и за потписивање листе опозваних сертификата. Јавни криптографски кључ сертификационог тела се користи за верификацију потписа. Сертификат сертификационог тела у пољу Key Usage има уписане вредности *Certificate Signing, Off-line CRL Signing, CRL Signing.*

Приватни криптографски кључ корисника се користи за креирање квалификованог електронског потписа. Јавни криптографски кључ корисника се користи за верификовање квалификованог електронског потписа и обезбеђивање непорецивости. Сертификат корисника у пољу Key Usage има уписане вредности *Digital Signature, Non-Repudiation.*

6.2 Заштита приватног криптографског кључа и контрола криптографског уређаја

6.2.1 Заштита приватног криптографског кључа

Приватни криптографски кључеви сертификационог тела генеришу се и чувају у криптографским HSM уређајима, који задовољавају одговарајуће захтеве у складу са међународним стандардом FIPS 140-2 L3. Испуњење овог стандарда гарантује да је било који покушај нарушавања интегритета уређаја или криптографске меморије истовремено детектован.

Приватни криптографски кључеви корисника генеришу се на смарт картицама (личним картама) корисника и за њихово чување одговоран је корисник.

6.2.2 Контрола приступа приватном кључу и криптографском уређају

HSM уређаји смештени су у Фарадејевом кавезу, коме физички приступ имају само запослени са поверљивим улогама. Приступ приватном кључу захтева вишеструку ауторизацију, при чему се ***n*** од ***m*** запослених са поверљивим улогама мора аутентификовати да би приступ кључу био могућ.

6.2.3 Безбедно чување и руковање приватним криптографским кључевима

Приватни криптографски кључеви који се чувају у HSM уређајима никад не напуштају уређај у отвореном облику. Процедуре чувања и руковања приватним криптографским кључевима су део Посебних интерних правила рада и заштите система издавања сертификата.

6.2.4 Креирање резервне копије приватног кључа

Копија приватног кључа сертификационог тела креира се у складу са процедуром за креирање копије приватног кључа сертификационог тела описаном у оквиру Посебних интерних правила рада и заштите система издавања сертификата. Креирање резервне копије приватног кључа захтева вишеструку ауторизацију. Резервна копија приватног кључа чува се у шифрованом облику. Фајл који садржи резервну копију приватног кључа

шифрован је AES алгоритмом. Дешифровање фајла могуће је само у HSM уређају, при чему се такође захтева вишеструка ауторизација

6.2.5 Архивирање приватног кључа

Након креирања резервне копије приватни криптографски кључ сертификационог тела се архивира и смешта у ватроотпорни безбедни сеф, заштићен системима физичке и логичке контроле приступа.

6.2.6 Пребацивање приватног кључа у други криптографски модул

Приватни кључ никада не напушта HSM уређај у отвореном облику. Експорт кључа из HSM уређаја за потребе креирања резервне копије, подразумева крерање шифрованог фајла, који се може дешифровати само у HSM уређају. У случају квара и замене криптографског модула (HSM уређаја), криптографски кључ ће бити импортован у нови HSM уређај, уз вишеструку ауторизацију запослених са поверљивим улогама.

6.2.7 Чување приватног криптографског кључа у криптографском модулу

Приватни криптографски кључеви сертификационог тела чувају се у меморији криптографског уређаја и могу да се користе само ако су на правилан начин активирани.

6.2.8 Активација приватног кључа

Приватни криптографски кључ се активира уношењем активационог податка.

Активациони податак за приватни криптографски кључ сертификационог тела састоји се из више делова (дељених тајни), при чему је за унос сваког дела одговоран један запослени са поверљивим улогама.

6.2.9 Деактивација приватног кључа

Након гашења апликације приватни кључ се деактивира.

6.2.10 Метод уништења приватног кључа

Приватни кључеви сертификационог тела се не обнављају и биће уништени на крају свог животног циклуса у циљу гаранције да се неће никада поново активирати и користити. Процедура уништења приватних кључева подразумева брисање кључева из HSM уређаја, уништавање резервних копија кључева и делова активационих података (дељених тајни), што се документује записником.

6.2.11 Класификовање криптографских модула

Ова одредба није применљива.

6.3 Остали аспекти управљања паром кључева

6.3.1 Архивирање јавног криптографског кључа

Јавни криптографски кључеви се налазе у сертификатима и чине њихов саставни део. Архивирањем сертификата архивирају се и јавни криптографски кључеви.

6.3.2 Рок важности сертификата и криптографских кључева

Рок важности сертификата врховног сертификационог тела RootCA је 20 година.

Рок важности сертификата подређеног сертификационог тела, издаваоца сертификата крајњих корисника је 10 година.

Рок важности корисничких сертификата је 5 година или краће, ако је до истека рока важности личне карте остало мање од 5 година, тада се сертификат издаје на рок важности личне карте.

6.4 Активациони подаци

Активациони подаци су лозинке или ПИН кодови потребни за активацију приватног криптографског кључа.

6.4.1 Генерисање и употреба активационоих података

Активациони подаци приватног кључа сертификационог тела, лозинке, генеришу се током извођења „Церемоније кључева" и користе их искључиво запослени са

поверљивим улогама током извршавања интерних процедура рада и заштите система за издавање сертификата.

Активациони податак корисника, ПИН код, генерише се у процесу персонализације идентификационог документа (личне карте) и заједно са њим се уручује кориснику у заштићеној коверти. Кориснички ПИН има четири нумеричка карактера.

6.4.2 Заштита активационих података

Запослени са поверљивим улогама су дужни да чувају лозинке за активацију приватног кључа сертификационог тела у складу са прописаним интерним процедурама рада и заштите система за издавање сертификата.

Корисник је дужан да чува свој ПИН за активацију приватног кључа од неовлашћеног приступа и употребе.

6.4.3 Остали аспекти у вези активационих података

Ова одредба није применљива.

6.5 Безбедносне контроле рачунара

6.5.1 Специфични захтеви за безбедност рачунара

Сервери система за издавање сертификата заштићени су системима физичке и логичке заштите. Сервери се налазе у Фарадејевом кавезу, коме физички могу приступити само запослени са поверљивим улогама. Логички приступ серверима остварује се вишеструком ауторизацијом.

6.5.2 Класификација безбедности рачунара

Ова одредба није применљива.

6.6 Животни циклус техничко-безбедносних контрола

6.6.1 Контрола развоја система за издавање сертификата

Имплементиране су следеће контроле развоја система:

- Софтверске компоненте су дизајниране и развијене у контролисаном окружењу, на основу документоване развојне технологије, са дефинисаним и документованим развојним процесима,
- Хардверске и софтверске компоненте система су испоручене на безбедан начин, који гарантује да није било неовлашћеног приступа ниједној од компоненти система,
- У систему за издавање сертификата налазе се само софтверске и хардверске компоненте неопходне за рад система; не постоје инсталиране друге апликације, уређаји, мрежне конекције или софтверске компоненте које нису неопходне за рад система,
- Води се рачуна да се злонамеран код не учита у систем,
- Све компоненте система инсталиране су од стране запослених са поверљивим улогама на начин прописан интерним процедурама рада и заштите система за издавање сертификата.

6.6.2 Управљање безбедносним контролама

Конфигурација система за издавање сертификата, као и све модификације и надоградње система се документују и контролишу.

6.6.3 Животни циклус безбедносних контрола

Имплементиране безбедносне контроле се по потреби унапређују.

6.7 Контроле безбедности рачунарске мреже

Имплементиран је механизам мрежне безбедности високог нивоа, заснован на примени

firewall уређаја и система за превенцију и заштиту од напада.

6.8 Временска ознака

Сертификати и листе опозваних сертификата имају временску ознаку датума и времена издавања, датума и времена престанка важења сертификата и датума и времена издавања следеће листе опозваних сертификата.

7. Профили сертификата, CRL листе и OCSP

7.1 Профил сертификата

Садржај сертификата смештен је у три дефинисана блока: *tbsCertificate, signature algorithm* и *signatureValue*.

Блок *tbsCertificate* се састоји од поља која на јединствен начин идентификују сертификат, корисника сертификата и сертификационо тело које је издало сертификат. То су следећа поља:

- *version* – верзија X.509 сертификата
- *serial number* – серијски број сертификата
- *signature* – идентификатор алгоритма коришћеног за потписивање сертификата
- *issuer* – назив сертификационог тела издаваоца и потписника сертификата
- *validity* – период важења сертификата
- *subject* – име корисника
- *subjectPublicKeyInfo* – подаци о јавном кључу корисника
- *extensions* – екстензије сертификата

Блок *signature algorithm* садржи идентификатор алгоритма који сертификационо тело користи за потписивање сертификата. Ово поље мора да садржи исти идентификатор алгоритма као што је наведено у пољу *signature* блока *tbsCertificate.*

Блок *signatureValue* садржи електронски потпис сертификационог тела које је издало сертификат. Сертификационо тело својим потписом гарантује за валидност података из блока *tbsCertificate*.

Authentication and Encryption certificate

Subject
CN = Јован Јовановић 123456789
G = Јован
SN = Јовановић
SERIALNUMBER=PNORS-1234567890123
SERIALNUMBER = CA:RS-123456789
L = Beograd
S = Srbija
C = RS

Qualified electronic certificate

Subject
CN = Јован Јовановић 123456789
G = Јован
SN = Јовановић
SERIALNUMBER=PNORS-1234567890123
SERIALNUMBER = CA:RS-123456789
L = Beograd
S = Srbija
C = RS

CN = Јован Јовановић 123456789 ◄——— ЛК (број личне карте)
SERIALNUMBER=PNORS-1234567890123 ◄——— ЈМБГ (јединствени матични број грађана)
SERIALNUMBER = CA:RS-123456789 ◄——— ЈИК (јединствени идентификатор корисника)

7.1.1 Верзија

МУП издаје X.509 сертификате верзије 3. Сертификати X.509 в3 осим основних поља која имају X.509 сертификати верзије 1 и 2 имају и додатне екстензије.

7.1.2 Екстензије сертификата

Сертификати које МУП издаје имају следеће екстензије:

Authority Key Identifier – идентификатор јавног кључа који је пар приватном кључу који је коришћен за потписивање сертификата
Subject Key Identifier - идентификатор јавног кључа корисника
Key Usage – дефинише намену кључа садржаног у сертификату
Certificate Policies – садржи идентификатор политике издавања сертификата *(Object Identifier - OID)* и униформни ресурсни локатор (*Uniform Resource Locator -URL*) за преузимање политика издавања сертификата
Subject Alternative Name - алтернативно име сертификата. У овом пољу може да се наведе адреса електронске поште корисника сертификата
Basic Constraints – ознака корисничког сертификата
CRL Distribution Points- URL за преузимање листе опозваних сертификата.
Qualified Certificate Statements – означава да је сертификат квалификован
Authority Information Access – URL за преузимање сертификата сертификационог тела

7.1.3 Идентификациона ознака алгоритма

За потписивање сертификата примењен је алгоритам SHA-512 са RSA енкрипцијом чија је идентификациона ознака **sha512RSA**

7.1.4 Форме имена

Имена корисника и издаваоца сертификата су јединствена имена *(Distinguished Name - DN).*

7.1.5 Ограничења у именима

У именима није дозвољено коришћење специјалних карактера.

Атрибут „*commonName*" поља „*subject*" не сме да се завршава са 13 или више узастопних нумеричких карактера, нити да се завршава цртицом иза које следе два словна карактера и низ нумеричких карактера.

7.1.6 Идентификатор политике издавања сертификата (OID)

Идентификатор политике издавања сертификата уписује се у поље *Certificate Policies* сертификата.

Формат структуре OID-a је следећи: **1.3.6.1.4.1.33589.а.б.в**
Број 1.3.6.1.4.1 представља општи префикс за *private-enterprize* број са сајта:
http://www.iana.org/assignments/smi-numbers,

33589 је *Private Enterprize Number (PEN)* додељен Министарству унутрашњих послова Републике Србије.

а - тип документа
1- лична карта

б.в - верзија документа
(пример б.в = 1.1)

7.1.7 Употреба екстензије *Policy Constraints*

Ова одредба није применљива.

7.1.8 Квалификатори политике

У оквиру екстензије *Certificate Policies* користи се *Policy Qualifier=User Notice* у коме је наведено да је електронски сертификат квалификован.

7.1.9 Процесирање критичних екстензија

Екстензије означене као критичне се обавезно процесирају.

7.2 Профил листе опозваних сертификата (CRL листе)

Листа опозваних сертификата садржи списак серијских бројева опозваних сертификата, датум и време опозива. Подаци који идентификују листу опозваних сертификата су организовани у три блока: *tbsCertList, signatureAlgorithm* и *signatureValue.*

Блок *tbsCertList* садржи следећа поља:
- *Version* - верзија X.509 листе опозваних сертификата.
- *Issuer* - име сертификационог тела које је потписало листу опозваних сертификата
- *Effective Date* - датум и време издавања листе опозваних сертификата.
- *Next Update* - датум и време следећег издавања листе опозваних сертификата.

Блок *signatureAlgorithm* садржи идентификатор алгоритма који сертификационо тело користи за потписивање листе опозваних сертификата.

Блок *signatureValue* садржи електронски потпис сертификационог тела које је потписало листу опозваних сертификата.

7.2.1 Верзија

Листа опозваних сертификата је X.509 верзије 2.

7.2.2 Екстензије CRL листе

CRL листе имају следеће екстензије:

- *Authority Key Identifier* - идентификатор јавног кључа који је пар приватном кључу који је коришћен за потписивање CRL листе
- *CRL Number* – редни број CRL листе
- *Reason code* - разлог опозива сертификата
- *Invalidity Date* - датум опозива сертификата

7.3 Профил OCSP (Online Certificate Status Protocol)

Министарство унутрашњих послова омогућава on-line проверу статуса квалификованог електронског сертификата посредством OCSP протокола.

OCSP профил је у складу са документом *RFC 2560: X.509 Internet Public Key*

Infrastructure Online Certificate Status Protocol - OCSP.

7.3.1 Верзија

Верзија OCSP је постављена на v1.0.

7.3.2 OCSP екстензије

OCSP екстензија која може да се користи је *Nonce* (произвољан број).

8. Ревизија усклађености и друге процене

МУП врши интерну ревизију усклађености пружања услуге издавања сертификата са важећим законским прописима који регулишу област квалификованих услуга од поверења и одредбама овог документа. Екстерну ревизију врши тело за оцењивање усаглашености у складу са законом. Након извршене ревизије сачињава се извештај о оцени усаглашености.

8.1 Фреквентност и околности ревизије

Редовна интерна ревизија врши се најмање једном у 12 месеци.
Редовна екстерна ревизија врши се најмање једном у 24 месеца.
Ванредна ревизија врши се у случају незадовољавајућих резултата претходне ревизије или ако наступи инцидент који у значајној мери угрожава или нарушава информациону безбедност.

8.2 Идентитет/квалификације ревизора

За спровођење интерне ревизије и одређивање лица која врше интерну ревизију одговоран је шеф Одсека за сертификациони систем. Лица која врше интерну ревизију морају имати искуства у подручју технологије инфраструктуре јавних кључева и пружања квалификованих услуга од поверења.

Екстерну ревизију врши тело за оцењивање усаглашености, које је у складу са законом којим се уређује акредитација, акредитовано за оцењивање усаглашености пружаоца квалификованих услуга од поверења и квалификованих услуга од поверења које они пружају.

8.3 Однос ревизора према предмету ревизије

Лица које врше интерну ревизију могу бити запослени у Одсеку за сертификациони систем. Предмет интерне ревизије су регистрациона тела.

Екстерну ревизију врши независно тело за оцењивање усаглашености.

8.4 Предмет ревизије

Ревизијом се проверава усклађеност пружања услуге издавања сертификата са важећим законским прописима који регулишу област квалификованих услуга од поверења и препорученим стандардима.

8.5 Предузете активности као резултат пронађених недостатака

У случају да се интерном или екстерном ревизијом утврде неправилности у пружању услуге издавања сертификата, предузимају се мере да се у што краћем року неправилности отклоне.

8.6 Објављивање резултата ревизије

Након извршене ревизије сачињава се извештај о оцени усаглашености. Извештај о оцени усаглашености сачињен након интерне ревизије је интерни акт и не објављује се.

9. Други пословни и правни аспекти

9.1 Накнаде

МУП бесплатно пружа услугу издавања квалификованих електронских сертификата на личним картама са чипом.

9.1.1 Накнада за пружање услуге издавања и обнављања сертификата

Издавања сертификата на личним картама са чипом се не наплаћује. Корисник коме је истекла важност сертификата, а лична карта је још увек важећа може поднети захтев за обнављање сертификата без плаћања накнаде.

9.1.2 Накнада за приступ сертификату

Сертификати сертификационог тела су јавно доступни на веб сајту сертификационог тела МУП-а и може им се приступити без плаћања накнаде. Кориснички сертификати се не објављују.

9.1.3 Накнада за проверу статуса сертификата

Провера статуса сертификата врши се спрам листе опозваних сертификата, која је јавно доступна на веб сајту сертификационог тела МУП-а и може им се приступити без плаћања накнаде.

9.1.4 Накнада за друге услуге

МУП задржава право да наплаћује друге услуге у зависности од врсте пружене услуге у конкретном случају.

9.1.5 Рефундација

Ова одредба није применљива.

9.2 Материјална одговорност

МУП сноси материјалну одговорност за пружање услуге издавања сертификата у складу са важећим законским прописима.

9.2.1 Осигурање

МУП је дужан да обезбеди најнижи износ осигурања од ризика одговорности за могућу штету насталу пружањем услуге издавања сертификата у складу са важећим прописима, тако да:

- осигурана сума на коју мора бити уговорено осигурање по једном штетном догађају не може износити мање од 20.000 € (евра) у динарској противвредности, подразумевајући при том као штетни догађај појединачну штету насталу употребом једног квалификованог електронског сертификата у једном акту у правном промету;
- 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 € (евра) у динарској противвредности.

9.2.2 Други фондови

Ова одредба није применљива.

9.2.3 Осигурање или гаранција за крајње кориснике

Осигурање или гаранција за крајње кориснике описано је у одредби 9.2.1 овог акта.

9.3 Поверљивост (тајност) података

9.3.1 Опсег тајних података

Тајни подаци су све информације и подаци који се односе на приватне криптографске кључеве сертификационог тела, активационе податке (лозинке за активацију приватног

кључа) и лог фајлове система за издавање сертификата. Овим подацима се рукује и подаци се чувају сагласно одредбама Закона о тајности података.

Посебна интерна правила рада и заштите система издавања сертификата у којима су детаљно описани поступци и мере, који се примењују приликом руковања криптографским параметрима (алгоритмима и кључевима) за издавање идентификационих докумената и квалификованих електронских сертификата, означена су ознаком тајности „ДРЖАВНА ТАЈНА“, у складу са Законом о тајности података.

9.3.2 Подаци који се не сматрају тајним

Не сматрају се тајним сви подаци и информације, које се објављују на веб сајту сертификационог тела МУП-а.

9.3.3 Одговорност за заштиту поверљивих информација

Запослени са поверљивим улогама, који у току обављања својих послова имају контакт са поверљивим информацијама и тајним подацима дефинисаним одредбом 9.3.1 овог акта, су у обавези да штите тајност података, да их не откривају неовлашћеним лицима и да при руковању тајним подацима примењују мере заштите тајних података дефинисане

посебним интерним правилима рада и заштите система издавања сертификата и Законом о тајности података.

9.4 Заштита података о личности

9.4.1 План заштите података о личности

МУП је дужан да се приликом пружања услуге издавања сертификата, према личним подацима корисника односи сагласно одредбама Закона о заштити података о личности.

9.4.2 Подаци о личности који су заштићени

Заштићени су сви подаци о корисницима на начин прописан Законом о заштити података о личности.

9.4.3 Подаци о личности који нису заштићени

Ова одредба није применљива, јер се одредбе Закона о заштити података о личности примењују на све податке о личности.

9.4.4 Одговорност за заштиту личних података

МУП је у обавези да штити податке о корисницима, да их не открива неовлашћеним лицима и да их користи искључиво у сврху пружања услуге издавања сертификата.

9.4.5 Сагласност за коришћење личних података

Ова одредба није применљива, јер за коришћење личних података о кориснику у сврху пружања услуге издавања сертификата није потребна сагласност корисника. Количина података о личности коју МУП обрађује у сврху издавања електронских сертификата дефинисана је законом који уређује евиденције и обраду података у области унутрашњих послова..

9.4.6 Откривање личних података у случају управног или судског поступка

Подаци о личности биће откривени на захтев надлежног органа и у другим случајевима предвиђеним законом.

9.4.7 Друге околности за откривање личних података

Околности за откривање личних података дефинисане су одредбом 9.4.6 овог акта.

9.4.8 Обавештавање о повреди података о личности

МУП је у обавези да у случају повреде података о личности о томе обавести Повереника и лице на које се подаци односе, на начин прописан Законом о заштити података о личности.

9.5 Право интелектуалне својине

Сва права интелектуалне својине остају искључиво власништво МУП-а.

9.5.1 Право интелектуалне својине над сертификатима и листама опозваних сертификата

МУП задржава право интелектуалног власништва над издатим сертификатима и листама опозваних сертификата. Корисници и поуздајуће стране имају право да сертификате и листе опозваних сертификата користе у складу са законским прописима и овим актом.

9.5.2 Право интелектуалне својине над актима

МУП задржава право интелектуалног власништва над овим актом и свим актима који се односе на инфраструктуру система са јавним кључевима МУП-а.

9.6 Права и обавезе

9.6.1 Права и обавезе МУП-а

МУП је одговоран за пружање комплетне услуге издавања сертификата која укључује: регистрацију корисника, формирање сертификата, дистрибуцију сертификата

корисницима, управљање животним веком (обнављање, суспензија, реактивација и опозив) сертификата, обезбеђивање поузданог и јавно доступног сервиса за проверу статуса сертификата.

МУП је у обавези да чува податке коришћене у регистрацији корисника и све информације о животном циклусу издатог сертификата корисника; да води ажурну и безбедну евиденцију неважећих (опозваних и суспендованих) сертификата и мора за сваки сертификат, за који је издао информацију о његовој валидности, ту информацију учини јавно доступном путем сервиса за проверу статуса опозваности електронских сертификата.

МУП је дужан да изврши опозив сертификата када:

- опозив сертификата захтева власник сертификата или његов пуномоћник,
- власник сертификата изгуби пословну способност;
- утврди да је податак у сертификату погрешан;
- утврди да су подаци за проверу квалификованог електронског потписа угрожени на начин који утиче на безбедност и поузданост сертификата;
- утврди да су подаци за електронско потписивање угрожени на начин који утиче на безбедност и поузданост електронског потписа;
- престаје са радом или му је рад забрањен.

МУП је у обавези да у случају компромитације свог приватног асиметричног приватног

кључа:

- престаје са издавањем сертификата;
- информише све кориснике и друге заинтересоване стране о компромитацији приватног кључа;
- јавно објављује информације о томе да издати сертификати, као и информације о статусу опозваности сертификата, више нису важеће;
- врши опозив свих издатих сертификата одмах, а најкасније у року од 24 часа у складу са Законом.

9.6.3 Права и обавезе корисника

Корисник је у обавези да:

- достави тачне и комплетне информације у складу са дефинисаном процедуром регистрације;
- искључиво користи свој асиметрични приватни кључ за формирање квалификованог електронског потписа у складу са одредбама Закона;
- онемогући неовлашћен приступ свом приватном кључу;
- одмах обавести издаваоца сертификата ако се пре истека важности сертификата назначеног у самом сертификату: корисников приватни кључ изгуби, украде или наступи основана сумња да је компромитован, престане контрола над коришћењем корисниковог приватног кључа из разлога компромитације активационог податка (ПИН) за средство за формирање квалификованог електронског потписа (лична карта) или других разлога, установи нетачност или измена садржаја сертификата;
- прекине коришћење свог приватног кључа уколико постоји основана сумња у

компромитацију кључа или контролу над активационом податком.

Корисник је дужан да одмах затражи опозив свог сертификата у случају губитка или оштећења средства или података за креирање електронског потписа.

9.6.4 Права и обавезе поуздајућих страна

Поуздајуће стране су у обавези пре него што се поуздају у сертификат:

- да изврше проверу статуса сертификата, спрам ажурне листе опозваних сертификата,
- да се упознају са одговорностима и ограничењима од одговорности дефинисаним овим актом, Уговором и важећим законским прописима.

9.6.5 Права и обавезе других учесника

Ова одредба није применљива.

9.7 Непризнавање одговорности

МУП не прихвата било какву другу одговорност осим оне која је изричито одређена овим

актом, Уговором и важећим законским прописима.

9.8 Ограничења одговорности

Свака употреба сертификата која није у сагласности са важећим законским прописима и овим актом није дозвољена. МУП не прихвата одговорност за штету насталу при коришћењу сертификата ван оквира истакнутих ограничења. За евентуалну штету насталу неправилним и недозвољеним коришћењем сертификата одговоран је корисник сертификата.

9.9 Обештећење

Корисник има право на обештећење за штету насталу коришћењем сертификата, ако се докаже да је штета настала при коришћењу сертификата сагласно важећим законским прописима и у оквиру истакнутих ограничења.

9.10 Почетак и престанак важења овог акта

9.10.1 Почетак важења овог акта

Овај акт почиње да се примењује даном доношења.

9.10.2 Престанак важења овог акта

Овај акт се примењује и важи до доношења новог акта, или до престанка пружања услуге издавања сертификата.

9.10.3 Обавезе у случају престанка пружања услуге

Обавезе МУП-а у случају престанка пружања услуге издавања сертификата дефинисане су одредбом 5.8 овог акта.

9.11 Обавештавање и комуникација са корисницима

Сва потребна обавештења намењена корисницима објављују се на веб сајту сертификационог тела МУП-а, http://ca.mup.gov.rs .
Питања у вези пружање услуге издавања сертификата корисници могу поставити на ca@mup.gov.rs .

Сертификационо тело Министарства унутрашњих послова ће кориснике о свим изменама Политике издавања сертификата, Практичних правила издавања сертификата, Уговора и свим другим изменама обавештавати путем странице Обавештења на сајту сертификационог тела Министарства унутрашњих послова.

9.11.1 Техничка подршка корисницима

Кориснички сервис за техничку подршку доступан је радним данима од 08 до 20 часова и

суботом од 08 до 14 часова на телефон: 011/3620-850

9.12 Ажурирање аката

9.12.1 Процедура ажурирања аката

У случају потребе за изменама или допунама овог акта, као и акта Политика пружања услуге издавања квалификованих сертификата на личној карти, након извршених измена или допуна, у табелу *Историја акта* уписује се нова верзија акта, датум извршене измене или допуне, име аутора, који је извршио измену или допуну и коментар. Коментар укратко описује извршену измену или допуну и разлог извршене измене или допуне.

9.12.2 Процедура одобравања аката и објављивање

Нова верзија акта, пре објављивања мора проћи процедуру одобравања описану у одредби 1.5.4 овог акта.

9.12.3 Околности под којима се мора променити OID

Верзија акта је саставни део OID-а, тако да се са сваком изменом верзије мења и OID.

9.13 Решавање спорова

Спорови настали између корисника и МУП-а у вези међусобних права и обавеза, тумачења уговора и овог акта решаваће се споразумно, а уколико споразум није могућ, 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 законским прописима

Овај акт донет је у складу са Законом о електронском документу, електронској документацији и услугама од поверења у електронском пословању (Службени гласник РС", број 94/17) и важећим прописима који произилазе из наведеног закона.

9.16 Остале одредбе

9.16.1 Уговор

Међусобна права, обавезе и одговорности корисника и МУП-а у вези са пружањем услуге издавања сертификата регулисана су Уговором о пружању услуге издавања квалификованог електронског сертификата, који се закључује између уговорних страна.

9.16.2 Преношење права

Корисник нема право да права из уговора у целини или делимично пренесе на треће лице.

МУП има право да сагласно одредби 5.8 овог акта права и обавезе из уговора, у потпуности или делимично, без сагласности корисника, пренесе на другог регистрованог пружаоца квалификоване услуге од поверења у Републици Србији или надлежни орган.

9.16.3 Измене и важење одредби

Измене или допуне појединих одредби не утичу на важење осталих одредби овог акта.

9.16.4 Извршење (адвокатске накнаде и одрицање од права)

Ова одредба није применљива.

9.16.5 Виша сила

МУП је ослобођен одговорности за било коју штету причињену корисницима приликом пружања услуге издавања сертификата, уколико је до штете дошло услед разлога, који су ван контроле МУП-а, односно услед више силе.

9.17 Прелазне и завршне одредбе

9.17.1 Престанак важења претходних аката

Доношењем овог акта престаје да важи „Практична правила рада сертификационог тела МУП РС 02/2010, 08/2014 и 06/2016“.

У Београду,
18-06-2021
01 Број: 3159/21-4

МИНИСТАР
Александар Вулин