**РЕПУБЛИКА СРБИЈА**
**МИНИСТАРСТВО УНУТРАШЊИХ ПОСЛОВА**
**СЕКТОР ЗА АНАЛИТИКУ ТЕЛЕКОМУНИКАЦИОНЕ И ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ**
**ОДЕЉЕЊЕ ЗА ИНФОРМАЦИОНУ БЕЗБЕДНОСТ**
**ОДСЕК ЗА СЕРТИФИКАЦИОНО ТЕЛО**

# ПРАКТИЧНА ПРАВИЛА РАДА СЕРТИФИКАЦИОНОГ ТЕЛА МУП РС (CPS – Certificate Practice Statement)

## OID CPS документа: 1.3.6.1.4.1.33589.3.1.1.1

**Верзија. 1.1**

**Београд, јануар 2016.**

# Садржај

На основу члана 5. став 2. тачка 2. Правилника о ближим условима за издавање квалификованих електронских сертификата („Службени гласник РС“ број 26/2008) Закона о електронском потпису („Службени гласник РС“ број 135/2004)

Министар унутрашњих послова доноси

# ПРАКТИЧНА ПРАВИЛА РАДА СЕРТИФИКАЦИОНОГ ТЕЛА МУП РС

## 1. Увод и преглед основних претпоставки

Сертификационо тело за потребе издавања сертификата на електронским идентификационим документима са чипом (e-ID) у оквиру Министарства унутрашњих послова Републике Србије (MUP CA) издаје квалификоване електронске сертификате за грађане тако што формира електронски потпис сертификата на основу свог приватног кључа и асиметричног криптографског алгоритма.

У тако формираном електронском сертификату, MUP CA се идентификује као издавалац квалификованог електронског сертификата у складу са Законом о електронском потпису и одговарајућим подзаконским актима.

MUP CA издаје квалификоване електронске сертификате грађанима у складу са документима:

- ETSI ESI TS 101 862 „Qualified Certificate Profile”,
- RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile“,
- RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” i
- ETSI TS 102 280 „X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons"

и са обавезним садржајем дефинисаним у члану 17. Закона о електронском потпису (у даљем тексту - Закон).

### 1.1 Преглед основних претпоставки

MUP CA је одговорно за пружање комплетних услуга сертификације, које укључују следеће сервисе:

- Регистрацију корисника,
- Формирање првог асиметричног пара кључева за кориснике и придруженог квалификованог сертификата за потребе аутентикације/шифровања,
- Формирање другог асиметричног пара кључева за кориснике и придруженог квалификованог електронског сертификата за потребе креирања квалификованог елетктронског потписа. Овај пар кључева се генерише у оквиру

самог средства за генерисање квалификованог електронског потписа (SSCD) у поступку доперсонализације e-ID картица грађана.
- Дистрибуцију приватног кључа и квалификованих електронских сертификата корисницима на начин прописан Законом (e-ID картица грађана као SSCD),
- Управљање процедуром опозива квалификованих електронских сертификата
- Обезбеђивање статуса опозваности квалификованих електронских сертификата.

MUP CA обезбеђује средство за формирање квалификованог електронског потписа корисницима (e-ID као SSCD) и придружени PIN код за активацију средства (password), као и њихову безбедну дистрибуцију до корисника.

MUP CA утврђује Општа правила пружања услуге сертификације (у даљем тексту: Општа правила) у складу са Законом.

Општа правила сертификације MUP CA уграђују се у документа:

1. Политика сертификације - CP (Certificate Policy);
2. Практична правила пружања услуге Сертификације - CPS (Certificate Practices Statement) (у даљем тексту: Практична правила) – овај документ.

Политика сертификације и Практична правила су јавни документи. Политика сертификације дефинише предмет рада сертификационог тела, а Практична правила дефинишу процесе и начин њиховог коришћења при формирању и управљању квалификованим електронским сертификатима.

Политика сертификације дефинише захтеве пословања сертификационог тела, док Практична правила дефинишу оперативне процедуре у циљу испуњења тих захтева. Практична правила дефинишу начин на који сертификационо тело испуњава техничке, организационе и процедуралне захтеве пословања који су идентификовани у Политици сертификације.

Политика сертификације је мање специфичан и детаљан документ у односу на Практична правила која представљају много детаљнији опис начина пословања, као и пословне и оперативне процедуре које сертификационо тело примењује у издавању и управљању квалификованим електронским сертификатима.

Политика сертификације се дефинише независно од специфичног оперативног окружења сертификационог тела, док Практична правила дају детаљан опис организационе структуре, оперативних процедура, као и физичко и рачунарско окружење сертификационог тела.

Општа правила функционисања MUP CA су у складу са документима:

- RFC 3647 „Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework”
- ETSI TS 101 456 „Policy Requirements for Certification Authorities Issuing Qualified Certificates”.

MUP CA утврђује и Посебна интерна правила рада сертификационог тела и заштите система сертификације (у даљем тексту: Посебна правила) у којима су садржани и

детаљно описани поступци и мере који се примењују приликом издавања и руковања електронским сертификатима и квалификованим електронским сертификатима. Посебна правила су приватни документи и представљају пословну тајну сертификационог тела.

Посебна интерна правила садрже детаљне одредбе о:

- систему физичке контроле приступа у поједине просторије сертификационог тела;
- систему логичке контроле приступа рачунарским ресурсима сертификационог тела;
- систему за чување приватног кључа сертификационог тела;
- систему дистрибуиране одговорности при активацији приватног кључа сертификационог тела;
- мерама заштите у ванредним ситуацијама (пожари, поплаве, земљотреси, друге временске непогоде, злонамерни упади у просторије или информациони систем сертификационог тела).

## 1.2 Име документа и идентификација

Овај документ представља Практична правила MUP CA које издаје квалификоване електронске сертификате грађанима Србије на електронском идентификационом документу са чипом (eID) – електронска лична карта.

MUP CA издаје квалификоване електронске сертификате за потребе реализације функција аутентикације/шифровања и квалификованог електронског потписа.

Идентификациони подаци MUP CA су:

**MUP CA**
**Министарство унутрашњих послова Републике Србије**
**Кнеза Милоша 101**
**11000 Београд**
**Србија**

Јединствено име (Dname – issuer):

**C=RS**
**L= Beograd**
**O=MUP Republike Srbije**
**CN= MUP CA Root**

## 1.3 Учесници у PKI систему MUP CA

У овом поглављу су дате основне информације о учесницима у оквиру PKI система MUP CA.

### 1.3.1 MUP CA

Регистровано сертификационо тело је организација која издаје квалификоване електронске сертификате у Републици Србији. MUP CA је одговорно за публикацију ових практичних правила у циљу подршке издавању квалификованих електронских сертификата. У том смислу, Политика сертификације (CP) и овај документ MUP CA CPS (Certificate Practice Statement), представљају одговарајућу политику и практична правила која се примењују при издавању MUP CA квалификованих електронских сертификата.

У циљу објављивања трећим странама информација које се односе на опозване квалификоване електронске сертификате, неопходно је да се изврши одговарајућа публикација листе опозваних сертификата (CRL – Certificate Revocation List). MUP CA периодично објављује такву листу у складу са условима дефинисаним у овом документу.

MUP CA представља хијерархијску PKI структуру за издавање електронских сертификата. У поменутој архитектури постоји:

- MUPCA Root
- MUPCA Gradjani
- MUPCA Sluzbenici
- MUPCA Resursi

Ова Практична правила се односе само на MUP CA за издавање квалификованих сертификата грађанима на електронским личним картама са чипом (e-ID).

Сертификат MUPCA Root је самопотписани сертификат. Сертификати e-ID корисника су дигитално потписани приватним кључем MUP CA.

MUP CA сертификати за e-ID кориснике се генеришу на основу валидног захтева за издавањем сертификата који се формира на основу података о ID кориснику који се узимају у процесу регистрације корисника, након подношења захтева за издавањем електронског идентификационог документа грађана (лична карта са чипом) – ID картица. Захтев за издавањем сертификата за креирање квалификованог електронског потписа подноси се посебно, након преузимања идентификационог документа од стране грађанина.

Кориснички сертификати могу бити намењени за аутентикацију корисника и шифровање, као и за креирање квалификованог електронског потписа.

Сва наведена сертификациона тела се налазе и управљају на централној локацији МУП, а у оквиру Управе за информационе технологије МУП РС.

Хијерархијски PKI систем MUP CA може укључити и било које екстерно Intermediate CA за које MUP CA обавља сертификационе услуге у складу са одговарајућим Уговором. Наиме, MUP CA омогућује имплементацију сертификационих сервиса и другим CA, као трећим странама, у складу са одговарајућим договореним условима.

У оквиру датог сертификационог окружења, таква CA представљају Intermediate CA у оквиру MUP CA хијерархије. Међутим, ова тела морају да пружају ниво сервиса који је еквивалентан нивоу које MUP CA обезбеђује.

У том смислу, спроводи се одговарајућа процедура акредитације, контроле и примене одговарајућих процедура у којима MUP CA проверава способност датог CA треће стране да издаје електронске сертификате у складу са овим Практичним правилима.

Прво што се мора обезбедити у том случају је да дато CA треће стране има Политику сертификације и Практична правила рада који су еквивалентни одговарајућим документима MUP CA. Другим речима, MUP CA ће проверити и анализирати практична правила и процедуре рада датог сертификационог тела (укључујући Политику сертификације и Практична правила (CPS – Certificate Practice Statement) и на основу тога одобрити укључење датог CA у PKI хијерархију MUP CA.

**Обавезе MUP CA**

MUP CA гарантује да ће спроводити све процедуре дефинисане у овим Практичним правилима. MUP CA користи кориснички уговор, CP и Практична правила у циљу спровођења легалних услова коришћења MUP CA сертификата од стране корисника и трећих страна.

Учесници од интереса за ова Практична правила су одговарајући ентитети у читавој MUP CA PKI инфраструктури који имају одговарајуће обавезе укључују CA, RA, кориснике, треће стране и друге учеснике.

До нивоа специфицираног у одговарајућим поглављима CP и овим Практичним правилима, MUP CA се обавезује на:

- Пуну сагласност са CP и овим Практичним правилима, као и свим одговарајућим додацима у тренутку када се публикују.
- Регуларно и периодично ажурирање CP документа и ових Практичних правила, као и њихово јавно публиковање,
- Објављивање контакт детаља сертификационог тела,
- Обезбеђивање услуга сертификације у складу са Законом, подзаконским актима и осталим нормативним актима,
- Обезбеђивање инфраструктуре и сертификационих услуга, укључујући успоставу и одржавање MUP CA репозиторијума и одговарајућег web сајта у циљу пружања сертификационих услуга.
- Обезбеђивање сигурних механизама који укључују механизам генерисања кључева, заштите кључева, као и процедуре дељења тајни у складу са својом сопственом PKI инфраструктуром.
- Обезбеђивање хитног обавештавања у случају компромитације сопственог приватног кључа.
- Издавање квалификованих електронских сертификата у складу са CP и овим Практичним правилима, као и испуњавање сопствених преузетих обавеза.

- Обавештавање корисника да су сертификати генерисани за њих, као и о начину како корисници могу да преузму сертификате.
- Обавештавање апликанта уколико MUP CA није способно да изврши валидацију корисничке апликације за добијање сертификата у складу са CP и овим Практичним правилима.
- Након пријема валидног захтева од стране PA које ради у оквиру MUP CA мреже издаје сертификате у складу са CP и овим Практичним правилима.
- Опозив сертификата који су издати у складу са CP и овим Практичним правилима након пријема валидног захтева за опозив сертификата од стране ауторизованог лица које може да захтева опозив.
- Објављивање издатих сертификата у складу са условима дефинисаним у CP и овим Практичним правилима.
- Обезбеђивање подршке корисницима и трећим странама као што је описано у CP и овим Практичним правилима.
- Регуларно и периодично објављивање листе опозваних сертификата (CRL листе) у складу са CP и овим Практичним правилима која је увек доступна свим заинтересованим странама,
- Обавештавање трећих страна о статусу сертификата путем публиковања CRL листа на MUP CA online репозиторијуму.
- Достављања копије CP и ових Практичних правила, као и осталих примењливих докумената по захтеву неке од страна.

MUP CA потврђује да, осим горе наведених, нема других обавеза по овом CPS документу.

**Одговорности MUP CA**

- MUP CA је одговорно за извршавање горе наведених обавеза у обиму који одређује законска регулатива Републике Србије.
- MUP CA није одговорно за заштиту приватних кључева корисника намењених за креирање квалификованог електронског потписа.
- MUP CA није одговорно за неодговарајућу проверу валидности сертификата од стране која се поуздаје у сертификат издат од стране MUP CA.
- MUP CA није одговорно за могућу злоупотребу сертификата која је настала услед неиспуњавања обавеза корисника или треће стране која се поуздаје у сертификат издат од стране MUP CA.
- MUP CA није одговорно за неизвршавање својих обавеза које је последица било ког проблема Надлежног органа за послове акредитације и супервизије PKI система у Србији или неког другог јавног ауторитета.
- MUP CA није одговорно за неизвршавање својих обавеза које су последица ванредне ситуације или више силе.

## 1.3.2 Регистрациона тела MUP CA

Захтеви за издавањем сертификата за грађане се прикупљају на аквизиционим локацијама у полицијским станицама које играју улогу Регистрационих ауторитета (RA – Registration Authority) MUP CA.

Подаци грађана за потребе издавања квалификованих електронских сертификата се прикупљају у оквиру процедуре издавања електронског идентификационог документа, а у складу са законски дефинисаним процедурама МУП-а.

РА тела интерактивно комуницирају и са корисницима и са MUP CA у циљу испоруке сертификационих услуга крајњим корисницима.

У том смислу, регистрациона тела MUP CA:

- Аутоматски региструју кориснике за коришћење MUP CA сертификационих услуга у склопу процедуре подношења захтева за ID картицу.
- Спроводе све кораке у процедури идентификације корисника што је дефинисано важећим законским документима и Општим правилима рада МУП.
- Користе службене и оверене документе у циљу провере корисникове апликације.
- Након потврде апликације корисника, достављају све неопходне информације до MUP CA у циљу издавања сертификата.
- Аутоматски иницирају процес генерисања квалификованог сертификата корисника за аутентикацију/шифровање.
- Врше доперсонализацију ID картица грађана у циљу генерисања асиметричног пара кључева и одговарајућег квалификованог електронског сертификата за потребе креирања квалификованог електронског потписа. Ова процедура се извршава након преузимања ID картице од стране грађана у датој полицијској станици.
- Иницирају процес опозива, суспензије и активације сертификата од стране MUP CA.

MUP CA регистрациона тела делују у складу са праксом, процедурама и основним документима рада MUP CA. Не постоји ограничење на број регистрационих тела која могу бити придружена MUP CA PKI инфраструктури.

### Обавезе РА тела

Сумарно, РА тело се обавезује на:

- Пријем апликација за издавање MUP CA сертификата у складу са CP и овим Практичним правилима.
- Извршавање свих активности на верификацији и провери аутентичности апликаната у складу са описом MUP CA процедура, CP и овим Практичним правилима (Провера идентитета особе која је поднела захтев).

- Достављање захтева апликаната до MUP CA у електронски потписаној поруци (захтев за издавањем сертификата), у складу са процедурама које су описане Политиком сертификације (CP) и Практичним правилима рада (CPS) MUP CA:
- Записивање свих активности у журналу догађаја.
- Пријем, верификацију и прослеђивање ка MUP CA свих захтева за опозивом, суспензијом и активацијом MUP CA издатих сертификата у складу са MUP CA процедурама, CP и овим CPS.
- Доперсонализација ID картице грађана са другим паром асиметричних кључева и квалификованим сертификатом за потребе креирања и верификације квалификованог електронског потписа.

RA је одговорно за извршавање горе наведених обавеза.

### 1.3.3 Корисници

Корисници представљају кориснике сертификационих услуга MUP CA. То су грађани који подносе захтев за електронски идентификациони документ са чипом.

**Обавезе корисника**

Сем ако није другачије дефинисано у CP и овим Практичним правилима (CPS), корисници сертификационих услуга MUP CA су одговорни за:

- Поседовање одговарајућих знања и ако је неопходно, похађање одговарајуће обуке за коришћење квалификованих електронских сертификата и других сертификационих услуга.
- Поштовање Политике сертификације (CP) и Практичних правила рада (CPS) публикованих од стране MUP CA.
- Обезбеђивање коректних и прецизних информација у њиховој комуникацији са RA и/или MUP CA.
- Упознавање, разумевање и сагласност са свим ставовима и условима у CP и овим CPS, као и другим документима који су објављени на MUP CA репозиторијуму.
- Уздржавање од нарушавања интегритета и произвођења неисправних сертификата издатих од стране MUP CA.
- Коришћење MUP CA сертификата само за легалне и ауторизоване сврхе у складу са CP и овим CPS, као и важећим законским документима.
- Обавештавање MUP CA или RA о било којим променама информација које су раније достављене.
- Прекид коришћења MUP CA издатог сертификата уколико је било која информација у сертификату постала невалидна.
- Прекид коришћења MUP CA издатог сертификата уколико сам сертификат постане невалидан.
- Одстрањивање серверског сертификата који је невалидан из било које апликације и/или било ког уређаја где је био инсталиран.

- Коришћење само једног квалификованог сертификата за квалификовани електронски потпис у датом тренутку.
- Спречавање компромитације, губљења, објављивања, модификације или било ког другог неауторизованог коришћења свог приватног кључа.
- Коришћење безбедних уређаја и производа који обезбеђују одговарајућу заштиту приватних кључева.
- За било које активности и пропусте партнера или агената у смислу генерисања, задржавања, одлагања, или уништавања било ког приватног кључа.
- Уздржавање од достављања до MUP CA, или било ког MUP CA директоријума, било каквог материјала који садржи ставове који угрожавају било који закон или било које право било које стране.
- Захтевање опозива сертификата у случају догађаја који материјално утиче на интегритет издатог сертификата од стране MUP CA.
- Пријављивање сваке могуће злоупотребе свог приватног кључа и захтевање да се сертификат опозове у том случају.

### 1.3.4 Треће стране

Треће стране су ентитети физичка лица (појединци) која прихватају квалификоване сертификате и верификују квалификовани електронски потпис одређених електронских докумената која су потписана од стране корисника MUP CA сертификата, као и која врше валидацију квалификацију сертификата издатих од стране MUP CA.

Верификација квалификованог електронског потписа се врши на бази јавног кључа који се налази у корисниковом сертификату.

У циљу провере валидности примењеног квалификованог електронског сертификата, треће стране морају увек да провере статус опозваности датог сертификата у оквиру CRL листе издате од стране MUP CA пре него што прихвате информације које су наведене у сертификату.

**Обавезе трећих страна**

Страна која се ослања на квалификовани сертификат издат од стране MUP CA обавезна је да:

- Поседује одговарајућа знања о коришћењу електронских сертификата и других технологија везаних за услуге сертификације.
- Упозна се са Политиком сертификације (CP) и овим Практичним правилима рада (CPS) у вези наведених услова који важе за треће стране.
- Поштује и спроводи одредбе из CP и ових CPS.
- Верификује MUP CA издати сертификат применом: провере валидности сертификата, провере CA које је издало сертификат, провере електронског потписа сертификата и провере статуса датог сертификата у важећој CRL

листи (MUP CA CRL), а у складу са процедуром валидације сертификата и комплетног ланца сертификата.

- Провери комплетност података у сертификату издатом од стране MUP CA, као и да провери да ли дати сертификат служи одговарајућој области примене која је наведена у сертификату.
- Верује у MUP CA издати сертификат само уколико се све информације које се односе на такав сертификат могу верификовати да су коректне и ажурне.
- Се разумно ослони и поуздa на MUP CA издати сертификат у складу са одговарајућим околностима.

## 1.3.5 Други учесници

**Обавезе везане за репозиторијум који одржава MUP CA**

Стране у комуникацији (укључујући кориснике и треће стране) које приступају MUP CA репозиторијуму и web сајту MUP CA у потпуности су сагласне са одредбама CP и ових CPS, као и са било којим другим условима коришћења које је MUP CA могло учинити доступним.

Стране у комуникацији демонстрирају прихватање услова коришћења наведених у CP и овим CPS достављањем упита везаних за статус квалификованих електронских сертификата или било којим другим начином који показује коришћење или ослањање на обезбеђене информације или услуге.

MUP CA репозиторијум укључује, обезбеђује или садржи:

- Јавну доступност свих својих сертификата (MUP CA Root и Intermediate MUP CA сертификата).
- Јавну доступност важеће листе опозваних сертификата (CRL).
- Верификацију статуса квалификованог електронског сертификата издатог од стране MUP CA, односно јавну доступност апликације eDocSigner која се користи за дигитално потписивање електронских докумената, али и проверава статус сертификата којим је документ потписан.
- Информације публиковане на MUP CA web сајту (CP, CPS, кориснички уговор, итд.).
- Било које друге услуге које MUP CA може рекламирати или обезбедити путем свог web сајта.

MUP CA чини све у својој моћи у циљу осигурања да стране које приступају његовом репозиторијуму добијају поуздане, ажурне и тачне информације. MUP CA, међутим, не може прихватити било какву одговорност која је ван ограничења дефинисаних у CP и овим CPS.

## 1.4 Коришћење сертификата издатих од стране MUP CA

У овом поглављу је дат акценат на прихватљивом коришћењу квалификованих електронских сертификата издатих од стране MUP CA.

### 1.4.1 Прихватљиво коришћење сертификата

MUP CA квалификовани сертификати се могу користити за већину трансакција електронске управе и електронског пословања које се базирају на употреби електронских и квалификованих електронских сертификата.

У такве трансакције спадају:

- Трансакције електронског пословања грађана са електронском управом,
- Електронска пошта,
- Електронски уговори,
- Приступ безбедним web сајтовима (SSL аутентикација) и другим online садржајима,
- Електронско потписивање докумената,
- Верификацију електронског потписа,
- Шифровање и дешифровање докумената у електронском облику, итд.

### 1.4.2 Забрањено коришћење сертификата

Ово поглавље није применљиво у оквиру ових CPS.

## 1.5 Администрација Практичних правила рада MUP CA

У овом поглављу су описане активности у вези администрације ових Практичних правила рада (CPS) MUP CA.

### 1.5.1 Организација администрирања Практичних правила рада

MUP CA је одговорно за прописну администрацију ових CPS и то у смислу периодичног прегледа и ажурирања, као и ванредних промена одговарајућих одредби које проистичу из евентуалних промена у законској регулативи или техничким карактеристикама примењених криптографских алгоритама и дужина кључева.

### 1.5.2 Контакт особа

Контакт особа у MUP CA за CPS документ је:

**Шеф Одсека за сертификационо тело**
**e-mail**: ca@mup.gov.rs

### 1.5.3 Особа која одређује погодност CPS документа

Ово поглавље није применљиво у оквиру ових CPS.

### 1.5.4 Процедура одобравања CPS документа

Документ Практична правила рада (CPS) MUP CA се редовно периодично прегледа и по потреби ажурира. Интерном процедуром се дефинише период прегледа ове CPS, а који не може бити ређи од једном у току календарске године.

Према датој интерној процедури, CPS се може евалуирати и по потреби ажурирати и чешће него једном годишње уколико се стекну услови за то. Такви услови се односе, између осталог на ванредне промене у законској регулативи или одговарајућа сазнања о критичним слабостима примењених криптографских алгоритама и дужина криптографских кључева.

## 1.6 Дефиниције и скраћенице

У овом документу поједини изрази имају следеће значење:

**Активациони подаци** – Подаци, који нису кључеви, који су захтевани у циљу рада криптографских модула и који морају бити заштићени (као на пример PIN, password, или мануелно размењивање кључева).

**CA сертификат** – Сертификат за дато CA издат (дигитално потписан) од стране другог CA или самопотписан (уколико се ради о MUPCARoot).

**Политика сертификације** – Именован скуп правила који индицира применљивост сертификата на одређено окружење и/или на класу апликација са заједничким безбедносним захтевима.

**Ланац (пут) сертификата** – Уређена секвенца сертификата која се, заједно са јавним кључем иницијалног објекта у ланцу (путу), процесира у циљу провере истог у последњем објекту на путу.

**Certificate Practice Statement (CPS)** – Јавна Практична правила и процедуре које сертификационо тело примењује у процедури издавања сертификата.

**Сертификационо тело – издавач сертификата (issuing CA)** – У контексту одређеног сертификата, сертификационо тело – издавалац сертификата је оно CA које је издало (дигитално потписало) сертификат.

**Квалификатор политике** – Информација која зависи од политике сертификације и која је придружена идентификатору политике сертификације у оквиру X.509 сертификата. Може да укључи и URL на коме се налази публикован CPS датог сертификационог тела.

**Регистрационо тело (RA)** – Ентитет који је одговоран за идентификацију и аутентикацију корисника/власника сертификата, као и креирање захтева за

издавање сертификата, али који не издаје и не потписује сертификат (тј. RA врши одговарајуће послове (идентификацију корисника) и у том смислу је делегирано од CA). Често се и термин LRA (Local Registration Authority) користи у истом контексту.

**Трећа страна** – Прималац сертификата који проверава дати сертификат и/или проверава дигитални потпис добијеног електронског документа применом јавног кључа потписника из сертификата. Такође, трећа страна проверава валидност сертификата у истом процесу. Трећа страна може бити такође корисник сертификата издатог од стране истог сертификационог тела, али и не мора.

**Електронски документ** – документ у електронском облику који се користи у правним пословима и другим правним радњама, као и у управном, судском и другом поступку пред државним органом.

**Електронски потпис** – скуп података у електронском облику који су придружени или су логички повезани са електронским документом и који служе за идентификацију потписника.

**Квалификовани електронски потпис** – Електронски потпис који се креира применом средства за креирање квалификованог електронског потписа (SSCD – Secure Signature Creation Device) и који се проверава путем квалификованог електронског сертификата потписника. Овај потпис је правно еквивалентан својеручном потпису по Закону о електронском потпису.

**Потписник** – лице које поседује средства за електронско потписивање и врши електронско потписивање у своје име или у име правног или физичког лица.

**Подаци за формирање електронског потписа** – јединствени подаци, као што су кодови или приватни криптографски кључеви, које потписник користи за израду електронског потписа;

**Средства за формирање електронског потписа** – одговарајућа техничка средства (софтвер и хардвер) која се користе за формирање електронског потписа, уз коришћење података за формирање електронског потписа.

**Средства за формирање квалификованог електронског потписа** – средства за формирање електронског потписа која испуњавају додатне услове утврђене Законом о електронском потпису.

**Подаци за проверу електронског потписа** – подаци, као што су кодови или јавни криптографски кључеви, који се користе за проверу и оверу електронског потписа.

**Средства за проверу електронског потписа** – одговарајућа техничка средства (софтвер и хардвер) која служе за проверу електронског потписа, уз коришћење података за проверу електронског потписа.

**Средства за проверу квалификованог електронског потписа** – средства за проверу електронског потписа која испуњавају додатне услове утврђене Законом о електронском потпису.

**Електронски сертификат** – електронски документ којим се потврђује веза између података за проверу електронског потписа и идентитета потписника.

**Квалификовани електронски сертификат** – електронски сертификат који је издат од стране сертификационог тела за издавање квалификованих електронских сертификата и садржи податке предвиђене Законом о електронском потпису.

**Корисник** – физичко лице коме се издаје електронски сертификат.

**Сертификационо тело** - правно лице које издаје електронске сертификате у складу са одредбама Закона о електронском потпису.

**Акредитација** – Формална декларација од стране потврдног ауторитета да извесне функције/ентитети задовољавају специфичне формалне захтеве.

**Апликација за сертификат** – Захтев послат од стране корисника који захтева сертификат (апликант) ка Сертификационом телу у циљу издавања електронског сертификата.

**Архива** – Специфична база података за чување записа за одређени период времена у циљу безбедности, backup-а или audit-а.

**Идентификација** – утврђивање да дато име појединца одговара реалном идентитету појединца.

**Аутентикација** – процедура безбедног логичког представљања корисника, тј. утврђивања његовог електронског идентитета, одговарајућој апликацији или сервису.

**Ауторизација** – процедура утврђивања права које неки аутентиковани корисник има за коришћење одговарајуће апликације или сервиса.

**Екстензије у сертификату** – Додатна поља у сертификату, поред основних, која дају ближе информације о власнику (кориснику) и издавачу (CA) сертификата, као и о процесу сертификације.

**Хијерархија сертификата** – Секвенца сертификата базирана на нивоима која има један Root CA сертификат и subordinate/intermediate ентитете, као што су сертификати других CA и корисници.

**Управљање сертификатима** – Активности придружене управљању сертификатима укључују чување, испоруку, објављивање и опозив сертификата.

**Листа опозваних сертификата (CRL – Certificate Revocation List)** – Листа издата и електронски потписана од стране CA која укључује опозване сертификате, као и разлоге њиховог опозива. Таква листа се мора користити од стране трећих страна увек када треба проверити валидност сертификата и/или верификацију електронског потписа.

**Серијски број сертификата** – Секвенцијални број који јединствено идентификује сертификат у домену датог CA.

**Захтев за добијање сертификата (CSR – Certificate Service Request)** – Стандардна форма (по PKCS#10 препоруци) која се користи за слање захтева за добијањем сертификата.

**Сертификација** – Процес издавања електронског сертификата.

**Асиметрични пар кључева (key pair)** – Приватни кључ и јавни кључ, као математички пар који се користе за потребе рада асиметричног криптографског алгоритма, као што је на пример RSA алгоритам.

**Приватни кључ** – Математички податак који се користи као кључ за креирање електронског потписа и за распакивање дигиталне енвелопе - дешифровање симетричног кључа којим је шифрован документ за датог корисника применом асиметричног криптографског алгоритма.

**Јавни кључ** – Математички податак који може бити јавно објављен (најчешће се објављује у форми X.509v3 електронског сертификата) и који се користи за верификацију електронског потписа, креираног помоћу одговарајућег приватног кључа који је математички пар са датим јавним кључем, као и за шифровање података за корисника који поседује одговарајући приватни кључ.

**Шифровање** – трансформација која, применом одговарајућег криптографског алгоритма и одговарајућег криптографског кључа, претвара оригиналну информацију у облик у којем садржај те информације постаје недоступан неовлашћеним лицима (шифрат).

**Дешифровање** – трансформација којом се из шифрата добија оригинална информација применом одговарајућег криптографског алгоритма и одговарајућег криптографског кључа.

**Криптографија** – наука о заштити тајности информација.

**Криптографски алгоритми** – алгоритми по којима се врши трансформација оригиналне информације у шифровану информацију (шифрат) и обратно, из шифрата у оригиналну инфомацију, коришћењем одговарајућег криптографског кључа.

**Криптографски кључ** – тајна и случајна информација одговарајуће дужине у битовима (на пример 128 или 256 бита) која се користи у криптографским алгоритмима, у процедурама шифровања и дешифровања.

**Симетрични криптографски алгоритми** – криптографски алгоритми који се користе за реализацију шифровања у циљу заштите тајности информација. Алгоритми се називају симетричним зато што се исти криптографски кључ користи за шифровање и за дешифровање.

**Асиметрични криптографски алгоритми** – криптографски алгоритми који се користе за реализацију технологије дигиталног потписа којом се обезбеђује: аутентичност, интегритет и непорецивост трансакција. Алгоритми се називају асиметричним зато што се различити криптографски кључеви користе за шифровање и за дешифровање. Асиметрични криптографски алгоритам користи пар

кључева, јавни и приватни и то јавни у поступку шифровања и приватни у поступку дешифровања.

**Hash алгоритми** – једносмерни криптографски алгоритми помоћу којих се врши криптографска трансформација информације произвољне величине у hash вредност фиксне величине (160, 224, 256, 384, 512 битова (или више)).

**Идентификатор објекта (Object identifier)** – Секвенца бројчаних компоненти која може бити придружена неком регистрованом објекту и која има карактеристику да је јединствена у свим идентификаторима објеката у оквиру специфичног домена.

**Репозиторијум** – База података и/или директоријум на коме су јавно доступни основни документи рада CA, као и евентуалне друге информације које се односе на пружање сертификационих услуга од стране датог CA (као на пример објављивање свих издатих сертификата, итд.).

**Опозив сертификата** – Перманентно укидање валидности датог сертификата и његово смештање на CRL листу.

**Дељена тајна** – Део криптографске тајне која је подељена на унапред дефинисан број смарт картица.

**Смарт картица** – Хардверски токен који садржи чип на коме може да се изврше одговарајуће криптографске функције, као што су: електронски потпис, шифровање, генерисање пара асиметричних кључева, итд.

**Кориснички уговор** – Уговор између корисника и CA у циљу обезбеђења сертификационих услуга.

Скраћенице које се користе у овом документу:

**CA** – Certification Authority

**RA** – Registration Authority

**ID** – Identification document

**PKI** – Public Key Infrastructure

**OID** – Object IDentifier

**TSA** – Time Stamping Authority

**CRL** – Certificate Revocation List

**CSR** – Certificate Service Request

**CDP** – CRL Distribution Point

**AIA** – Authority Information Access

**AKI** – Authority Key Identifier

**SKI** – Subject Key Identifier

**RFC** – Request For Comments

**ETSI** – European Telecommunication Standardization Institute

**CP** – Certificate Policy

**CPS** – Certificate Practise Statement

**URL** – Uniform Resource Locator

**JMBG** – Jedinstveni Matični Broj Građana

# 2. Одговорности за публиковање и репозиторијуме

Ово поглавље се односи на неке аспекте публиковања информација, као и на локације где се те информације публикују, у оквиру MUP CA.

## 2.1 Репозиторијуми

MUP CA публикује информације у вези електронских сертификата које издаје на online репозиторијумима односно на web серверу. MUP CA задржава право да публикује статусне информације о сертификатима и на репозиторијуму неке треће стране уколико је то погодно.

MUP CA има online репозиторијум докумената у којима се објављују информације о практичним правилима и процедурама рада, укључујући CP као и ове CPS.

MUP CA задржава право да учини расположивим и публикује информације у вези сопствених политика и процедура рада путем било ког погодног начина.

## 2.2 Публиковање информација о сертификатима

MUP CA публикује информације о сертификатима на претходно поменутим репозиторијумима и то:

- Сертификате MUP CA (MUP CA Root сертификат и Intermediate MUP CA сертификате),
- Информације о статусима опозваности сертификата (CRL),
- Основне документе рада MUP CA (CP, ова CPS; стандардне форме апликација за добијање сертификата, стандардне корисничке уговоре, итд.).

Учесници у сертификационим услугама се обавештавају да ће MUP CA публиковати поједине информације које су они доставили на јавно приступачним директоријумима уз придружене статусне информације о електронским сертификатима у формату и садржају који прописује Закон.

Из разлога њихове осетљивости и пословне тајне, MUP CA неће публиковати интерна правила рада која се односе на подкомпоненте и елементе који укључују извесне безбедносне контроле, процедуре које се односе на управљање кључевима, дистрибуирану одговорност, безбедност регистрациона тела и све остале безбедносно осетљиве процедуре.

## 2.3 Време и фреквенција публиковања

MUP CA публикује информације о статусу опозваности издатих дигиталних сертификата (CRL листе) периодично и то у тачно одређеним интервалима, како је то назначено и прецизирано у овом CPS документу.

## 2.4 Контроле приступа репозиторијумима

Све информације објављене у online репозиторијуму MUP CA су доступне преко Интернета свим заинтересованим странама, без ограничења.

MUP CA одржава потпуно расположивим приступ до свог јавног репозиторијума трећим странама са сврхом:

- Добављања CA сертификата MUP CA,
- Добављања CRL листа MUP CA у циљу валидације сертификата издатог од стране MUP CA.

MUP CA може ограничити или забранити приступ одређеним услугама, као што су публиковање статусних информација о базама података треће стране, одређеним приватним директоријумима, итд.

Иако је приступ MUP CA репозиторијуму и директоријумима бесплатан, MUP CA задржава право да наплаћује одређена специфична коришћења својих сервиса.

# 3. Идентификација и аутентикација корисника

MUP CA одржава документована практична правила (овај документ) и процедуре у циљу аутентикације идентитета и/или других атрибута апликаната/крајњих корисника који захтевају издавање сертификата од стране MUP CA, а што се извршава пре издавања сертификата.

MUP CA аутентикује захтеве страна које желе да опозову сертификате у складу са CP и овим CPS.

## 3.1 Називи

### 3.1.1 Типови имена

У циљу идентификације корисника, MUP CA спроводи одговарајућа правила додељивања имена и идентификације која укључује типове имена придружених субјекту, као на пример X.500 “distinguished” имена.

### 3.1.2 Потреба да имена буду са реалним значењем

Када аплицира за добијање сертификата од стране MUP CA, име апликанта мора бити у потпуности реално и са одговарајућим значењем, сем ако то није експлицинтно дозвољено у релевантном опису процедуре у оквиру MUP CA, као и у овом документу. MUP CA издаје сертификате апликантима који достављају документоване апликације које садрже име које се може верификовати.

### 3.1.3 Анонимност корисника

MUP CA не издаје анонимне сертификате корисницима.

### 3.1.4 Правила за интерпретацију различитих форми имена

Ово поглавље није применљиво у оквиру ових CPS.

### 3.1.5 Јединственост имена

Имена придружена корисницима сертификата су јединствена у домену MUP CA пошто се увек користе заједно са јединственим идентификационим бројем корисника које се уписује у Dname поље корисника. Као јединствени идентификацини број корисника у MUP CA се користи ЈМБГ (Јединствени Матични Број Грађана).

### 3.1.6 Препознавање, аутентикација и улога робних марки („trademarks“)

MUP CA не прихвата “trademarks” ознаке, лога или друге графичке или текстуалне материјале који су заштићени од копирања, а предложени су за укључење у квалификоване сертификате које издаје.

## 3.2 Иницијална провера идентитета

Провера идентитета корисника коме се издаје квалификовани сертификат од стране MUP CA је укључена у законски дефинисану процедуру издавања електронског идентификационог документа.

### 3.2.1 Метода доказивања поседовања приватног кључа

Ово поглавље није применљиво у оквиру ове CPS зато што не постоји удаљено слање захтева за израдом сертификата од стране корисника већ MUP CA издаје два квалификована електронска сертификата кориснику, и то:

- Квалификовани електронски сертификат за потребе аутентикације/шифровања – креиран аутоматски у склопу процеса персонализације ID картице, а на основу асиметричног пара кључева генерисаног у оквиру MUP,
- Квалификовани електронски сертификат за верификацију квалификованог електронског потписа – захтеван од стране службеника MUP RA на основу асиметричног пара кључева генерисаног на самој ID картици у склопу процедуре доперсонализације која се врши у току преузимања ID картице од стране грађана.

### 3.2.2 Аутентикација идентитета организације

Ово поглавље није применљиво у оквиру ове CPS зато што MUP CA издаје квалификоване електронске сертификате грађанима на e-ID картицама и у том процесу се не захтевају подаци о евентуалном запослењу корисника.

### 3.2.3 Аутентикација идентитета појединца

У циљу идентификације и аутентикације индивидуалног корисника који аплицира за добијање MUP CA сертификата у склопу подношења захтева за добијање електронског идентификационог документа, MUP CA утврђује идентитет датог појединца на бази достављене документације у складу са Законом.

### 3.2.4 Информације корисника које се не верификују

Ово поглавље није применљиво у оквиру ових CPS.

### 3.2.5 Валидација ауторитета

Ово поглавље није применљиво у оквиру ових CPS.

### 3.2.6 Критеријуми за интероперабилност

Ово поглавље није применљиво у оквиру ових CPS.

## 3.3 Идентификација и аутентикација захтева за обнављање кључева

Ово поглавље није применљиво у оквиру ових CPS.

### 3.3.1 Идентификација и аутентикација за рутинско обнављање кључева

Ово поглавље није применљиво у оквиру ових CPS.

### 3.3.2 Идентификација и аутентикација за обнављање кључева након опозива

Ово поглавље није применљиво у оквиру ових CPS.

## 3.4 Идентификација и аутентикација захтева за суспензију/опозив сертификата

У циљу спровођења процедура идентификације и аутентикације захтева за суспензију/опозив сертификата корисника, дефинисано је да корисници контактирају службенике RA или да захтеве евентуално достављају коришћењем одговарајућег online аутентикационог механизма (аутентикација путем дигиталног сертификата, PIN броја, ауторизационог кода, итд.). У случају опозива личне карте опозива се и сертификат.

При томе, захтеви се могу упутити одговарајућем RA или путем web комуникације до самог MUP CA. Добијене захтеве, RA спроводи до MUP CA у циљу реализације процедуре суспензије/опозива сертификата.

# 4. Оперативни захтеви у вези животног циклуса сертификата

Корисници имају сталну обавезу да информишу MUP CA о свим променама у информацијама које су објављене у сертификату за читав период оперативног рада таквог сертификата.

Одређене друге обавезе се такође могу додатно применити.

## 4.1 Апликација за добијање сертификата

### 4.1.1 Ко може да достави апликацију за издавање сертификата?

Што се тиче апликације за издавање квалификованог корисниковог сертификата, MUP CA захтева да апликант лично поднесе апликацију за квалификован

сертификат и то у склопу процедуре подношења захтева за добијањем електронског идентификационог документа (личне карте са чипом).

Захтев за издавање сертификата од стране MUP CA може да поднесе свако ко испуњава следеће услове:

- Корисник мора бити прихватљив крајњи корисник MUP CA како то дефинише политика сертификације и овај CPS документ.
- Захтев који предаје корисник мора да у себи садржи све неопходне податке, укључујући довољно података да корисник може да буде идентификован на јединствен начин.

### 4.1.2 Процес достављања захтева за издавањем сертификата (enrollment) и одговорности

Грађани подносе захтев за добијање квалификованог електронског сертификата за аутентикацију/шифровање и квалификованог електронског сертификата за дигитални потпис аутоматски приликом подношења захтева за издавањем електронског идентификационог документа са чипом.

Квалификовани електронски сертификат за дигитални потпис грађана се добија у оквиру процедуре доперсонализације електронског идентификационог документа која се спроводи од стране службеника RA након уручења електронског идентификационог документа са чипом.

## 4.2 Процесирање апликације за добијање сертификата

### 4.2.1 Извршавање функције идентификације и аутентикације корисника

Након пријема апликације датог корисника за добијање електронског идентификационог документа, службеник RA врши дефинисану идентификациону и аутентикациону процедуру у циљу валидације достављене апликације.

### 4.2.2 Потврђивање или одбијање апликације за добијање сертификата корисника

Захтев за добијање квалификованог сертификата за аутентикацију/шифровање се процесира аутоматски у оквиру процеса издавања електронског идентификационог документа грађана.

Ово важи само за грађане који захтевају лични идентификациони документ са чипом.

Захтев за добијање квалификованог сертификата за дигитално потписивање се спроводи у оквиру процедуре доперсонализације електронског идентификационог документа од стране службеника RA.

### 4.2.3 Потребно време за процесирање апликације корисника

Време потребно да се изда први квалификовани сертификат се уклапа у законско време које је потребно да се изда лични идентификациони документ (електронска лична карта) са чипом. Други сертификат или квалификовани електронски сертификат за дигитални потпис издаје се на лицу места по пријему захтева корисника и у присуству корисника који у поступку доперсонализације сам укуцава свој PIN код.

## 4.3 Издавање сертификата

### 4.3.1 Активности CA током процеса издавања сертификата

Да би сертификат био издат неопходно је да буду испуњени следећи услови:

- Корисник који је поднео захтев за издавање сертификата позитивно је идентификован и његов идентитет је потврђен.
- Подаци које је навео у пријави су истинити.
- Корисник не поседује претходно издати валидан електронски идентификациони документ.

Након доставе валидног захтева корисника за издавањем личног идентификационог документа са чипом од стране RA, MUP CA спроводи процес издавања одговарајућих сертификата који се састоји од:

- Генерисања асиметричног пара кључева и квалификованог сертификата за аутентикацију/шифровање и њихов упис на лични идентификациони документ са чипом током процеса персонализације.
- Генерисања асиметричног пара кључева и квалификованог сертификата за дигитални потпис у самом чипу електронског идентификационог документа у процесу доперсонализације од стране службеника RA,

Операцију доперсонализације врши службеник RA која подразумева следеће акције:

1. генерисање пара кључева за квалификовани електронски потпис на ID смарт картици корисника,
2. генерисање захтева за издавањем сертификата за квалификовани електронски потпис и слање до MUP CA путем web сајта MUP CA,
3. генерисање сертификата за квалификовани електронски потпис у MUP CA,
4. упис изгенерисаног сертификата за квалификовани електронски потпис на ID смарт картицу корисника.

### 4.3.2 Обавештење корисника од стране CA о издатом сертификату

Квалификовани сертификати се генеришу у оквиру MUP CA и уписују на SSCD – Secure Signature Creation Device (ID картицу грађана) која се уручује лично кориснику.

Ако се деси да захтев за добијање електронског идентификационог документа буде одбијен корисник ће бити информисан о разлозима одбијања који су дефинисани Законом.

## 4.4 Прихватање сертификата

### 4.4.1 Спровођење процеса прихватања сертификата

Издати сертификат од стране MUP CA се сматра прихваћеним од стране корисника уколико се испуни било који од доле наведених услова:

- Коришћење стандардне online форме уз одговарајући квалификовани електронски потпис корисника где је то могуће применити,
- Коришћење сертификата први пут уз одговарајући квалификовани електронски потпис корисника,
- Петнаест (15) дана након преузимања уколико корисник не јави да постоје било какви проблеми у издатом сертификату.

### 4.4.2 Објављивање сертификата од стране CA

Ово поглавље није применљиво у оквиру ових CPS.

### 4.4.3 Обавештење других ентитета о издатом сертификату

Ово поглавље није применљиво у оквиру ових CPS.

## 4.5 Коришћење сертификата и асиметричног пара кључа

У овом поглављу се дефинишу одговорности које се односе на коришћење асиметричног пара кључева и сертификата.

### 4.5.1 Коришћење приватног кључа и сертификата од стране корисника

Одговорности корисника – корисник се обавезује да ће користити приватни кључ и изгенерисани квалификовани сертификат од стране MUP CA у складу са дефинисаним начином коришћења кључа у самом сертификату (Key Usage и Enhanced Key Usage екстензије).

Коришћење приватног кључа и сертификата представља део корисниковог уговора са CA. У том смислу, корисник може користити свој приватни кључ само након прихватања одговарајућег сертификата.

Такође, корисник мора престати да користи свој приватни кључ након истицања периода валидности или опозива издатог сертификата.

### 4.5.2 Коришћење јавног кључа и сертификата од стране трећих страна

Одговорност треће стране – трећа страна је обавезна да прихвата издате квалификоване сертификате MUP CA само уколико се користе у складу са предвиђеним начином коришћења сертификата дефинисаним у самом сертификату. Трећа страна је обавезна да прописно и успешно примењује операцију јавног кључа који екстрахује из издатог сертификата и одговорна је да спроводи проверу статуса опозваности датог сертификата коришћењем метода који је дефинисан у CP и CPS документима MUP CA.

## 4.6 Обнављање сертификата

### 4.6.1 Услови за обнављање сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 4.6.2 Ко може захтевати обнављање сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 4.6.3 Процесирање захтева за обнављањем сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 4.6.4 Обавештење корисника да му је издат обновљени сертификат

Ово поглавље није применљиво у оквиру ових CPS.

### 4.6.5 Спровођење процеса прихватања обновљеног сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 4.6.6 Објављивање обновљеног сертификата од стране CA

Ово поглавље није применљиво у оквиру ових CPS.

### 4.6.7 Обавештење других ентитета од стране CA о обнови датог сертификата

Ово поглавље није применљиво у оквиру ових CPS.

## 4.7 Генерисање новог пара кључева и сертификата корисника

Ово поглавље није применљиво у оквиру ове CP.

Нови асиметрични парови приватних кључева и квалификованих сертификата се издају са новим електронским идентификационим документом са чипом.

### 4.7.1 Услови за генерисање новог пара кључева и сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 4.7.2 Ко може захтевати нови сертификат са новим јавним кључем

Ово поглавље није применљиво у оквиру ових CP.

### 4.7.3 Процесирање захтева за новим паром кључева и сертификатом

Ово поглавље није применљиво у оквиру ових CPS.

### 4.7.4 Обавештење корисника да му је издат нови сертификат

Ово поглавље није применљиво у оквиру ових CPS.

### 4.7.5 Спровођење процеса прихватања новог сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 4.7.6 Објављивање новог сертификата од стране CA

Ово поглавље није применљиво у оквиру ових CPS.

### 4.7.7 Обавештење других ентитета од стране CA о издавању новог сертификата

Ово поглавље није применљиво у оквиру ових CPS.

## 4.8 Модификације сертификата корисника

### 4.8.1 Услови за модификацију сертификата корисника

Ово поглавље није применљиво у оквиру ових CPS.

### 4.8.2 Ко може захтевати модификацију сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 4.8.3 Процесирање захтева за модификацијом сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 4.8.4 Обавештење корисника да му је издат нови модификовани сертификат

Ово поглавље није применљиво у оквиру ових CPS.

### 4.8.5 Спровођење процеса прихватања новог модификованог сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 4.8.6 Објављивање новог модификованог сертификата од стране CA

Ово поглавље није применљиво у оквиру ових CPS.

### 4.8.7 Обавештење других ентитета од стране CA о издавању новог модификованог сертификата

Ово поглавље није применљиво у оквиру ових CPS.

## 4.9 Суспензија, реактивација и опозив сертификата

### 4.9.1 Услови за суспензију сертификата

Сертификат се суспендује у следећим ситуацијама:

- Ако суспензију сертификата захтева власник сертификата или одговарајући службеник MUP CA или RA;
- Ако суспензију сертификата захтева надлежни орган за заштиту података или неки други виши орган који има оправдане сумње да сертификат садржи неисправне податке или да се приватни кључ који одговара јавном кључу из сертификата може користити без сагласности власника;
- Ако суспензију сертификата захтева суд, тужилац или институције које врше криминалну истрагу да би спречили даље злочине.

### 4.9.2 Ко може захтевати суспензију сертификата

Суспензију сертификата датог корисника може захтевати сам корисник, овлашћени службеник RA, MUP CA, суд, тужилац или институције које врше криминалну истрагу.

### 4.9.3 Процедура захтева за суспензијом сертификата

Захтев за суспензијом сертификата може бити достављен од стране корисника или службеника RA. Захтев се у овом случају доставља одговарајућом дигитално потписаном поруком од стране службеника RA.

Операција суспензије сертификата је идентична опозиву с тим што се статус сертификата у бази поставља на суспендован што оставља могућност да се сертификат после одређеног времена поново активира.

## 4.9.4 Реактивација сертификата

Суспензија сертификата траје онолико дуго колико трају и услови због којих је суспензија и захтевана. Када ови услови престану да важе, корисник може захтевати реактивацију свог сертификата.

MUP CA публикује серијске бројеве свих опозваних и суспендованих сертификата у својој CRL листи.

За време суспензије, или након опозива сертификата, период оперативног рада датог сертификата се истовремено сматра завршеним.

Сертификат се реактивира у следећим ситуацијама:

- Ако активирање сертификата захтева власник сертификата, његов овлашћени представник, или одговарајући службеник MUP CA или RA на основу чијег захтева је и извршена суспензија.
- Ако активирање сертификата захтева надлежни орган за заштиту података или неки други виши орган на основу чијег захтева је извршена суспензија.
- Ако активирање сертификата захтева суд, тужилац или институција на основу чијег захтева је извршена суспензија, или ако је прошло време суспензије.

Операцију активирања сертификата из стања суспендован врши RAO. Она подразумева брисање серијског броја сертификата корисника из листе опозваних сертификата.

## 4.9.5 Услови за опозив сертификата корисника

Након одговарајућег захтева од стране службеника RA или самог корисника, MUP CA врши опозив издатог електронског сертификата у случају:

- Губитка, крађе, модификације, неауторизованог објављивања или неке друге компромитације приватног кључа корисника сертификата.
- Да је субјект сертификата нарушио материјалне обавезе које су дефинисане у CP или у овом CPS документу.
- Да извршење одговарајућих обавеза лица која су наведена у CP и у овим CPS касни или је спречено услед природне катастрофе, рачунарског или комуникационог отказа, или услед другог узрока који излази ван контроле датог лица и као резултат, информације о другом лицу су материјално угрожене или компромитоване.
- Да се десила промена одређених информација која се садрже у сертификату датог лица.

## 4.9.6 Ко може захтевати опозив сертификата

Опозив сертификата датог корисника може захтевати сам корисник или овлашћени службеник RA или MUP CA. Другим речима, захтев за опозивом сертификата може да поднесе власник сертификата, након прописне аутентикације, или одговарајући

службеник MUP CA или PA уз доказ да је испуњен један од услова за опозив сертификата, наведен у 4.9.1.

## 4.9.7 Процедура захтева за опозивом сертификата

Ако се деси неки од горе поменутих догађаја, корисник мора што пре да контактира службенике RA или MUP CA у циљу достављања захтева за опозивом сертификата. Поменути контакт може бити online или путем неких недигиталних канала.

MUP CA опозива сертификат одмах након верификације идентитета стране која је захтевала опозив и потврдом да је захтев поднет у складу са процедуром захтеваном у CP, као и у овом CPS документу. Верификација идентитета може бити извршена на основу информационих елемената који су садржани у идентификационим подацима које је корисник доставио до RA. Након испуњења поменутих услова, MUP CA извршава хитну активност у циљу опозива сертификата.

Конкретно у MUP CA, операцију опозива корисничких сертификата врши оператор PA (PAO). Она подразумева упис серијског броја сертификата корисника у листу опозваних сертификата.

## 4.9.8 Grace период захтева за опозивом сертификата

Ово поглавље није применљиво у оквиру ових CPS.

## 4.9.9 Време за које CA мора да процесира захтев за опозивом сертификата

Ово поглавље није применљиво у оквиру ових CPS.

## 4.9.10 Захтеви за треће стране у вези провере статуса сертификата

Треће стране морају користити online ресурсе које MUP CA чини расположивим путем репозиторијума у циљу провере статуса сертификата на које они желе да се ослоне.

Треће стране морају бити у сагласности са MUP CA политиком сертификације а посебно са обавезама трећих страна публикованим у CP или овом CPS документу.

## 4.9.11 Фреквенција издавања CRL листе

Листа опозваних сертификата (CRL – Certificate Revocation List) MUP CA се ажурира на сваких 24 сата.

## 4.9.12 Максимално кашњење у издавању CRL листе

Ово поглавље није применљиво у оквиру ових CPS.

## 4.9.13 Расположивост процедуре online провере статуса сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 4.9.14 Захтеви online провере статуса сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 4.9.15 Расположивост других форми објављивања статуса сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 4.9.16 Специјални захтеви у односу на компромитацију приватног кључа

Ово поглавље није применљиво у оквиру ових CPS.

## 4.10 Сервиси провере статуса сертификата

### 4.10.1 Оперативне карактеристике

MUP CA објављује све опозване и суспендоване сертификате у својој CRL листи. Листа опозваних сертификата (CRL – Certificate Revocation List) MUP CA се ажурира на сваких 24 сата.

### 4.10.2 Расположивост сервиса

Треће стране морају користити online ресурсе које MUP CA чини расположивим путем репозиторијума у циљу провере статуса сертификата на које они желе да се ослоне.

### 4.10.3 Опциона обележја

Ово поглавље није применљиво у оквиру ових CPS.

## 4.11 Престанак коришћења сертификата

Након престанка коришћења сертификата издатог од стране MUP CA, дати сертификат мора бити опозван.

Престанак коришћења сертификата може бити из следећих разлога:

- Корисник жели да прекине коришћење сертификационих сервиса MUP CA.
- MUP CA је престало са пружањем услуга сертификације.

## 4.12 Чување и реконструкција приватног кључа корисника

### 4.12.1 Политика и пракса чувања и реконструкције приватног кључа

MUP CA обезбеђује услове за генерисање вишеструких парова асиметричних кључева за кориснике.

Први пар кључева и први сертификат служе за аутентикацију корисника и за шифровање докумената путем процедуре дигиталне енвелопе за датог корисника.

У циљу омогућавања дешифровања докумената шифрованих за датог корисника у инцидентним случајевима, као и за евентуалне службене потребе, неопходно је да се дати приватни кључ чува у оквиру МУП-а на заштићен начин (шифрован) у одговарајућој бази.

Други пар кључева и други сертификат (квалификовани електронски сертификат за дигитални потпис) служе за електронско потписивање квалификованим електронским потписом.

Приватни кључ корисника којим се врши квалификовани електронски потпис се нигде не чува изузев на смарт картици корисника (e-ID картици).

### 4.12.2 Енкапсулација сесијског кључа и политика и пракса за реконструкцију

Ово поглавље није применљиво у оквиру ових CPS.

# 5. Управне, оперативне и физичке безбедносне контроле

Ово поглавље описује све оне безбедносне контроле које не спадају директно у техничке контроле, а које се користе од стране MUP CA као подршка у циљу реализације функција генерисања кључева, аутентикације субјеката, издавања сертификата, опозива сертификата, ревизије и архивирања.

Ове не-техничке безбедносне контроле су критичне за поверење у сертификате издате од стране MUP CA пошто недостатак безбедности може компромитовати оперативни рад CA резултујући на пример у креирању сертификата и CRL са погрешним информацијама или компромитацијом приватног кључа CA.

## 5.1 Физичке безбедносне контроле

MUP CA имплементира одговарајуће механизме физичке контроле у својим просторијама.

### 5.1.1 Локација и конструкција сајта

MUP CA се налази у просторијама МУП РС у Београду, Кнеза Милоша 101.

MUP CA безбедне просторије су лоциране у простору који одговара потребама извршења операција високе безбедности. Постоје означене зоне са физичком контролом приступа и закључане канцеларије са одговарајућим сефовима.

### 5.1.2 Физички приступ

Приступ просторијама MUP CA је омогућен само овлашћеном особљу које поседује бесконтактне смарт картице из система MUP CA.

Физички приступ је ограничен имплементацијом одговарајућих механизама контроле приступа из једне у другу зону безбедности, као и у зону високе безбедности. У том смислу, CA операције су лоциране у оквиру безбедне рачунарске собе (Фарадејев кавез) која је подржана физичким надгледањем и безбедносним алармима, а обезбеђена је и подршка да прелазак из зоне у зону може бити изведен само коришћењем бесконтактних картица, као и листи контроле приступа.

### 5.1.3 Електрично напајање и климатизација

Сва опрема MUP CA је прикључена на јединице за непрекидно напајање.

Температура и влажност ваздуха се у просторијама одржава у оквиру унапред специфицираних интервала помоћу клима уређаја.

Напајање и вентилација се извршавају са редундансом високог нивоа.

### 5.1.4 Изложеност поплавама и временским непогодама

Унутар просторија MUP CA нема водоводних инсталација.

Просторије MUP CA су заштићене од поплава.

### 5.1.5 Превенција и заштита од пожара

Превенција и заштита од пожара су имплементиране.

Просторије MUP CA су опремљене детекторима дима и системом за гашење пожара.

### 5.1.6 Медијуми за чување података

Медијуми се чувају на безбедан начин. Backup медијуми се такође чувају на одвојеној локацији која је физички обезбеђена и заштићена од пожара и поплава.

### 5.1.7 Одлагање смећа

Изношење смећа се такође контролише.

Папирни отпад се пропушта кроз машине за сечење папирног отпада. Електронски медијуми се пре одлагања морају физички/механички уништити.

### 5.1.8 Одлагање резервних копија

Ово поглавље није применљиво у оквиру ових CPS.

## 5.2 Процедуралне контроле

MUP CA спроводи кадровску и управну праксу која обезбеђује разумну сигурност у поверљивост и компетенцију запослених, као и задовољавајуће перформансе у вези са њиховим дужностима у домену технологија које се односе на електронски потпис и PKI системе.

Сваки запослени MUP CA потписује изјаву да ће се придржавати правне регулативе у вези заштите података, као и да ће задовољити све постављене захтеве у вези са поверљивошћу.

### 5.2.1 Поверљиве улоге

Сви запослени у MUP CA који извршавају операције повезане са управљањем кључевима, као и било које друге операције које материјално утичу на такве операције, сматрају се дужностима на поверљивим позицијама. Поверљиве улоге/дужности у MUP CA, између осталих, су:

- Администратор безбедности,
- Систем администратори,
- Систем оператер и
- Систем евидентичар

MUP CA спроводи иницијално истраживање свих запослених који су кандидати за поверљиве улоге у циљу разумног покушаја стицања увида у њихову поверљивост и компетенције.

### 5.2.2 Број особа које се захтевају по сваком задатку

Тамо где се захтева дуална контрола, потребно је да најмање два поверљива запослена MUP CA искажу њихова подељена знања у циљу омогућавања извршења текућих операција. Другим речима, у оквиру MUP CA, ниједну осетљиву операцију не може извршити само један запослени.

### 5.2.3 Идентификација и аутентикација за сваку улогу

Свака улога/дужност дефинише одговарајуће захтеве у погледу идентификације и аутентикације корисника.

### 5.2.4 Улоге које захтевају раздвајање дужности

У оквиру MUP CA дефинисано је које улоге/дужности могу бити комбиноване од стране једног запосленог, а које то не смеју.

## 5.3 Кадровске безбедносне контроле

### 5.3.1 Квалификација и искуство

MUP CA извршава неопходне активности у циљу провере захтеване биографије, квалификација, као и неопходног искуства у циљу реализације у оквиру контекста компетенције специфичног посла. Запослени у MUP CA не смеју бити законски кажњавани.

Такве провере биографије типично укључују:

- Криминалне осуде за озбиљне злочине,
- Погрешне презентације информација од стране кандидата,
- Одговарајуће референце.

За рад у MUP CA су неопходни стручњаци који су технолошки и професионално компетентни и који имају потребна знања из криптографије, дигиталног потписа, PKI система, смарт картица, HSM-ова, итд.

### 5.3.2 Процедура провере биографије

MUP CA реализује релевантне провере евентуалних запослених на бази статусних извештаја који су издати од стране компетентних ауторитета, изјава трећих страна или изјава самих потенцијалних запослених.

### 5.3.3 Захтеви за обученошћу

MUP CA обезбеђује обуку за своје запослене у циљу реализације функција пословања CA и RA.

### 5.3.4 Фреквенција и захтеви за поновну обуку

Периодична дообука може такође бити извршена у циљу успоставе континуитета и ажурности знања запослених, као и одговарајућих процедура.

### 5.3.5 Фреквенција и секвенца ротације послова

Ово поглавље није применљиво у оквиру ових CPS.

### 5.3.6 Казнене мере за неовлашћење активности

MUP CA има одговарајуће мере за кажњавање запослених за неовлашћене активности, неовлашћено коришћење ауторитета, као и неовлашћено коришћење система у циљу спровођења санкција за одређено непословно и ризично понашање, а које може бити различито у зависности од различитих околности.

### 5.3.7 Захтеви за независне уговараче

Независни уговарачи су субјекти истих процедура заштите приватности и услова поверљивости као и запослени у MUP CA.

### 5.3.8 Документација која се доставља запосленима

MUP CA чини доступном сву документацију запосленима која се односи на MUP CA за потребе иницијалне обуке, дообуке или за друге сврхе.

## 5.4 Процедуре безбедносних провера логова/ревизија

Процедуре audit логовања укључују логовање догађаја и ревизију система и имплементиране су за сврху одржавања безбедног окружења. У том смислу, MUP CA имплементира контроле наведене у наредном тексту.

### 5.4.1 Типови забележених догађаја

MUP CA записује догађаје који укључују, али нису ограничени на операције везане за животни циклус сертификата, покушаје приступа систему, као и захтеве достављене систему.

### 5.4.2 Фреквенција процесирања логова

MUP CA чува audit логове у реалном времену, који се касније процесирају на дневном нивоу и архивирају на седмичном нивоу.

### 5.4.3 Период чувања audit логова

MUP CA процесира и архивира audit логове на седмичном нивоу, који се трајно чувају.

### 5.4.4 Заштита audit логова

Audit логови се само могу видети од стране ауторизованог особља.

### 5.4.5 Процедуре backup-а audit логова

MUP CA имплементира процедуре backup-а audit логова.

### 5.4.6 Систем сакупљања audit логова

MUP CA сакупља и чува audit логове у реалном времену.

### 5.4.7 Обавештење субјекта који је проузроковао догађај

У случају аларма или инцидентног догађаја, обавештава се администратор мреже MUP CA.

Субјекат који је проузроковао одређени audit догађај се не обавештава о самој audit активности.

### 5.4.8 Оцена рањивости система

MUP CA реализује с времена на време процену рањивости система.

## 5.5 Архивирање записа/логова

Захтеви за чувањем записа се примењују како на MUP CA тако и на RA. Опште политике чувања записа MUP CA укључују одредбе наведене у наставку текста.

### 5.5.1 Типови архивираних записа

MUP CA на безбедан начин чува записе о MUP CA издатим квалификованим електронским сертификатима, информације о апликацијама за издавање сертификата, као и документацију о самим апликацијама за издавање сертификата.

### 5.5.2 Период чувања архиве

MUP CA чува на безбедан начин поменуте записе о MUP CA квалификованим електронским сертификатима за период који је назначен у Закону о електронском потпису и одговарајућем подзаконском акту.

### 5.5.3 Заштита архиве

Услови за заштиту архиве укључују:

- Записе које само систем запослени којима су придружене дужности чувања података могу да виде и архивирају.
- Заштиту у односу на модификацију архиве, као што је чување података на медијуму на кога се може уписати само једном.
- Заштиту у односу на брисање архиве.

- Заштиту у односу на кварење карактеристика медијума временом на којима се архива чува, као на пример реализација захтева да се подаци периодично мигрирају на свеже медијуме.

### 5.5.4 Процедура backup-а архиве

MUP CA спроводи одговарајућу процедуру backup-а архиве.

MUP CA реализује захтеве за процедуром чувања барем две одвојене копије архиве које су под контролом две различите особе.

### 5.5.5 Захтеви за timestamping записима

Ово поглавље није применљиво у оквиру ових CPS.

### 5.5.6 Систем сакупљања записа

MUP CA спроводи одговарајући систем сакупљања записа/логова који се архивирају.

### 5.5.7 Процедуре за добијање и верификацију информација из архиве

У оквиру MUP CA, дефинисане су процедуре у циљу добијања и верификације архивских информација.

У циљу добијања и верификације архивских информација, MUP CA и RA одржавају записе под јасном хијерархијском контролом и са јасним описом посла. MUP CA чува записе у електронској или папирној форми.

MUP CA може захтевати од својих RA или корисника да доставе одговарајућа документа у циљу подршке овог захтева. Ови записи могу бити чувани у електронској, папирној и у било којој другој форми за коју MUP CA сматра да је одговарајућа.

MUP CA може да измени начин чувања записа ако је то евентуално потребно да буде у сагласности са одговарајућом акредитационом и супервизионом шемом коју спроводи Надлежни орган за акредитацију и супервизију PKI система у Србији.

## 5.6 Измена кључева

MUP CA поседује процедуру, детаљно описану у овом CPS документу, која се спроводи у случају истека сертификата сертификационог тела или опозива сертификата сертификационог тела у складу са условима дефинисаним у CP.

У оба случаја, врши се генерисање новог пара кључева серитификационог тела и дистрибуција сертификата CA свим корисницима и заинтересованим странама, као и у случају првог генерисаног сертификата CA.

# 5.7 Компромитација и опоравак у случају катастрофе

## 5.7.1 Процедуре за поступање у инцидентним и компромитујућим ситуацијама

MUP CA документује процедуре које треба извршити при решавању инцидената, као и извештавања у вези са евентуалном компромитацијом кључева CA.

## 5.7.2 Рачунарски ресурси, софтвер или подаци који су оштећени

MUP CA такође документује процедуре опоравка које се користе уколико су рачунарски ресурси, софтвер или подаци неисправни или се сумња да су неисправни.

## 5.7.3 Процедуре које се спроводе код компромитације приватног кључа корисника

MUP CA тежи да поново успостави безбедно окружење у корацима који укључују, али нису ограничени само на опозив неисправних сертификата одговарајућих ентитета. Након тога, MUP CA може поново издати нови сертификат датом ентитету.

## 5.7.4 Могућности континуитета пословања након катастрофе

План континуитета пословања се имплементира да осигура наставак пословања након природне или друге катастрофе.

# 5.8 Завршетак рада CA или RA

Пре него што прекине своје активности пружања сертификационих услуга MUP CA:

- Обезбеђује својим корисницима који имају валидне сертификате обавештење о намери да престане са пружањем сертификационе услуге, тј. да престане да извршава активности у својству CA.
- Повлачи све сертификате који су још увек валидни (тј. оне који нису опозвани или им је истекао рок важности) након обавештења, а без неопходне сагласности корисника.
- Благовремено обавештава о опозиву сертификата све кориснике на које се то односи.
- Чини разумне мере у циљу заштите записа које чува у складу са CP и овим CPS.
- Уколико је то могуће, обезбеђује одговарајуће мере обезбеђења сукцесије у смислу поновног издавања сертификата од стране другог CA које је сукцесор – настављач издавања сертификата датог CA – и које поштује исте/еквивалентне CP и CPS документе.

# 6. Техничке безбедносне контроле

Ово поглавље дефинише техничке безбедносне мере које примењује MUP CA у циљу заштите криптографских кључева и активационих података (као на пример PIN-ови, лозинке, итд.). Безбедносно управљање кључевима је критично у циљу осигурања да су сви кључеви и активациони подаци заштићени и да се користе искључиво од стране ауторизованих запослених.

Такође, дефинисане су и друге техничке безбедносне контроле које се користе од стране CA да се безбедно извршавају функције генерисања кључева, аутентикације корисника, регистрације корисника, издавања сертификата, опозива сертификата, ревизије и архивирања. Техничке контроле укључују животни циклус безбедносних контрола као и оперативне безбедносне контроле.

У овом поглављу се такође дефинишу техничке безбедносне контроле над репозиторијумима, регистрационим телима, корисницима и другим учесницима.

## 6.1 Генерисање и инсталација асиметричног пара кључева

### 6.1.1 Генерисање асиметричног пара кључева

MUP CA безбедно генерише и штити своје сопствене приватне кључеве, коришћењем безбедних и поузданих система и примењује неопходне превентивне мере у циљу спречавања компромитације или неауторизованог коришћења. MUP CA имплементира и документује процедуре генерисања кључева у складу са CP и овим CPS. MUP CA примењује јавне, интернационалне и Европске стандарде у вези безбедних и поузданих система.

MUP CA генерише следеће асиметричне парове кључева:

- За потребе Intermediate MUP CA (intermediate у MUP CA PKI хијерархији) – асиметрични пар кључева се генерише на хардверском безбедносном модулу (HSM – Hardware Security Module).
- За потребе корисника – аутентикација/шифровање (дигитална енвелопа) – овај асиметрични пар кључева се генерише у оквиру система MUP CA и приватни кључ, заједно са сертификатом, се уписују на ID смарт картицу корисника током процеса персонализације електронског идентификационог документа.
- За потребе корисника – квалификовани електронски потпис – овај асиметрични пар кључева се генерише на ID смарт картици корисника и никада не напушта смарт картицу. Генерисање се врши у току процеса доперсонализације ID смарт картице приликом уручења електронског идентификационог документа.

MUP CA користи безбедан процес генерисања свог Root приватног кључа у складу са документованом процедуром. MUP CA дистрибуира дељене тајне за своје приватне кључеве. MUP CA је власник приватних кључева и поседује ауторитет да пренесе одговарајуће дељене тајне на ауторизоване носиоце дељених тајни.

Приватни кључ MUP CA Root се користи за електронско потписивање MUP CA сертификата (издавање Intermediate CA сертификата), листе опозваних сертификата, као и евентуалних акредитованих Root-потписаних ентитета (CA трећих страна). Друге сврхе коришћења приватног кључа MUP CA Root су забрањене.

### 6.1.2 Испорука приватног кључа кориснику

MUP CA испоручује два приватна кључа кориснику на смарт картици (један генерисан у оквиру самог система MUP CA, а други генерисан на самој ID смарт картици).

### 6.1.3 Достава јавног кључа до издаваоца сертификата

Што се тиче квалификованог сертификата за аутентикацију/шифровање, јавни кључ корисника, као део асиметричног пара кључева се доставља до MUP CA кроз персонализациони софтвер у оквиру самог MUP CA (приликом припреме података за персонализацију ID смарт картице) и то у облику захтева за издавање сертификата у PKCS#10 формату.

Што се тиче квалификованог сертификата за верификацију квалификованог електронског потписа, достављање захтева за издавање сертификата крајњег корисника у PKCS#10 формату врши оператер регистрационог ауторитета (RAO) у оквиру процедуре доперсонализације. Оператер регистрационог ауторитета дигитално потписује захтев на бази свог приватног кључа који се налази на службеној смарт картици (RAO) и припрема поруку коју шаље MUP CA.

### 6.1.4 Достава јавног кључа издаваоца сертификата трећим странама

MUP CA доставља своје јавне кључеве Root и Intermediate CA, у облику X.509v3 сертификата путем свог online репозиторијума коме могу да приступају сви корисници и треће стране.

### 6.1.5 Дужине кључева

За потребе свог Root приватног кључа и одговарајуће потписивање, MUP CA Root користи SHA-1/RSA комбинацију hash и асиметричног алгоритма са дужином кључа од 4096 бита и периодом валидности сертификата од 20 година са периодом издавања сертификата (периодом валидности приватног кључа) од 10 година.

За свој Intermediate /оперативне/online CA приватни кључ и одговарајући алгоритам за електронско потписивање, MUP CA користи SHA-1/RSA комбинацију hash и асиметричног алгоритма са дужином кључа од 2048 бита, као и период валидности сертификата од 10 година са периодом издавања сертификата (период валидности приватног кључа) од 5 година.

MUP CA задржава право на измену горе наведених комбинација алгоритама и дужина кључева уколико се у криптографској теорији и пракси покажу слабости наведених алгоритама и светска криптографска јавност препоручи поузданије

алгоритме, као и у случајевима дефинисања нових стандарда за hash и асиметричне алгоритме.

### 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 криптографским хардверским уређајима:

- HSM – за асиметричне кључеве CA и за први пар асиметричних кључева за кориснике – за дигиталну енвелопу
- Смарт картица – за кључеве корисника за потребе квалификованог електронског потписа

Квалитет начина генерисања поменутих криптографских параметара искључиво зависи од квалитета хардверског генератора случајних бројева на HSM-овима и смарт картицама коришћеним у MUP CA.

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

### 6.1.7 Могуће „Key Usage " опције

У електронским сертификатима (Root и Intermediate CA сертификати) издатим од стране MUP CA и квалификованим електронским сертификатима (кориснички сертификати) издатим од стране MUP CA користе се следеће вредности у екстензији „Key Usage“:

Root CA сертификат:

- Certificate Signing, Off-Line CRL Signing, CRL Signing

Intermediate CA сертификат:

- Certificate Signing, Off-Line CRL Signing, CRL Signing

Сертификат за аутентикацију корисника и дигиталну енвелопу:

- Digital Signature, Key Encipherment, Data Encipherement

Квалификовани сертификат за квалификовани електронски потпис корисника:

- Digital Signature, Non-Repudiation

## 6.2 Заштита приватног кључа и контрола криптографског хардверског модула

MUP CA користи одговарајуће криптографске уређаје у циљу реализације задатака управљања и заштите кључева MUP CA. Поменути криптографски уређаји су познати под именом Хардверски безбедносни модули (HSM - Hardware Security Modules).

### 6.2.1 Стандарди и контроле криптографског хардверског модула

Генерисање приватног кључа MUP CA се врши у оквиру безбедног криптографског уређаја који задовољава одговарајуће захтеве у складу са међународним стандардом FIPS 140-2 L3. Испуњење овог стандарда гарантује, између осталог, да је било који покушај нарушавања интегритета уређаја или криптографске меморије истовремено детектован.

HSM уређаји не смеју да напуштају MUP CA просторије изузев ретких прилика унапред дефинисаних премештања и пресељења. MUP CA чува записе у вези свих тих премештања или пресељења.

У случају да одговарајући HSM захтева одржавање или поправку, која се не може извршити у оквиру MUP CA просторија, они се онда безбедно преносе до њиховог произвођача уз поштовање свих неопходних безбедносних мера, детаљно описаних у овом CPS документу.

### 6.2.2. *k* од *n* дистрибуција одговорности контроле приватног кључа

Генерисање приватног кључа MUP CA захтева контролу од више од једног, на одговарајући начин ауторизованог, запосленог који има поверљиве позиције и дужности у оквиру MUP CA. Ауторизација процедуре генерисања кључева се мора извршити од стране више од једног члана управне структуре MUP CA.

Процедура дељених тајни MUP CA користи вишеструке ауторизоване носиоце у циљу да заштити и побољша поверљивост приватних кључева и обезбеди одговарајућу процедуру опоравка кључа.

Приватни кључ MUP CA се користи под условима дефинисаним у оквиру ***k*** од ***n*** контроле од стране више запослених са поверљивим улогама.

Пре него што носилац дељене тајне прихвати дељену тајну он мора лично да се упозна са креирањем, поновним креирањем и дистрибуцијом тајне на његовог следећег члана ланца поверљивости.

Носилац дељене тајне може примити дељену тајну на физичком медијуму, као што је одређени хардверски криптографски модул (на пример смарт картица) који је одобрен за коришћење од стране MUP CA. MUP CA чува писане записе у вези дистрибуције дељене тајне.

MUP CA документује сопствену дистрибуцију дељених тајни за активацију свог приватног кључа и има могућност да измени начин дистрибуције смарт картица у

случају да носиоци смарт картице захтевају да буду замењени у њиховим ролама као носиоци смарт картица.

### 6.2.3 Безбедно чување приватног кључа

MUP CA користи безбедни криптографски уређај да чува своје приватне кључеве у складу са захтевима исказаним у стандарду FIPS 140-2 L3.

Процедура чувања приватног кључа MUP CA захтева вишеструке контроле од стране, на одговарајући начин ауторизованог особља са поверљивим ролама. Ауторизација процедуре чувања кључева и ауторизација одговарајућег особља мора бити извршена од стране више од једног члана управне структуре.

Хардверски и софтверски механизми који штите приватне кључеве CA су документовани у Посебним интерним правилима рада. Документи приказују да су механизми заштите CA кључа у најмању руку еквивалентне снаге као и сами CA кључеви који се штите.

### 6.2.4 Backup приватног кључа

MUP CA приватни кључ се backup-ује у складу са процедуром дефинисаном у интерним правилима рада MUP CA. У процедури backup-а користе се процедуре backup-а кључа које су подржане од стране датог HSM уређаја.

Копије приватног кључа MUP CA се чувају на екстерној меморији (flash меморија, CD, ...) на сигурном месту у шифрованом облику.

### 6.2.5 Архивирање приватног кључа

Backup-ован приватни кључ MUP CA се архивира према процедури описаној у интерним правилима рада MUP CA.

### 6.2.6 Трансфер приватног кључа на хардверски криптографски модул

Процедура безбедног експортовања приватног кључа MUP CA у циљу backup-а, као и процедура безбедног импорта архивираног приватног кључа на HSM су описане у посебним интерним правилима рада MUP CA:

### 6.2.7 Чување приватног кључа на хардверском криптографском модулу

Када се приватни кључ MUP CA налази и користи на HSM уређају, он се чува у шифрованом облику у меморији HSM уређаја.

### 6.2.8 Метода активације приватног кључа

Носиоци дељених тајни (стараоци) MUP CA имају задатак да активирају и деактивирају приватни кључ. Приватни кључ је тада активан у дефинисаном периоду времена.

### 6.2.9 Метода деактивирања приватног кључа

Носиоци дељених тајни (стараоци) MUP CA имају задатак да активирају и деактивирају приватни кључ. Приватни кључ је тада активан у дефинисаном периоду времена.

### 6.2.10 Метода уништења приватног кључа

Приватни кључ MUP CA се не обнавља.

Приватни кључ MUP CA ће бити уништен на крају свог животног циклуса.

MUP CA приватни кључеви се уништавају на крају њиховог животног века у циљу гаранције да они неће никада бити поново активирани и коришћени.

Приватни кључеви MUP CA се уништавају тако што се исти униште, као и брисањем њихових дељених делова/тајни.

Процес уништавања кључева је документован у Посебним интерним правилима рада и одговарајући записи су архивирани.

Након генерисања новог асиметричног пара кључева и новог сертификата MUP CA, претходни приватни кључ се брише из HSM-а, а backup копије се уништавају на најсигурнији могући начин.

### 6.2.11 Рангирање криптографских хардверских модула

Ово поглавље није применљиво у оквиру ових CPS.

## 6.3 Други аспекти управљања паром кључева

### 6.3.1 Архивирање јавног кључа

MUP CA архивира свој сопствени јавни кључ.

### 6.3.2 Периоди валидности сертификата и приватног кључа

MUP CA издаје корисничке сертификате за периодом коришћења као што је назначено у самим сертификатима.

Време валидности приватног кључа MUP Root CA је 10 година, док је валидност самог MUP Root CA сертификата 20 година.

Време валидности приватног кључа MUP CA Intermediate CA је 5 година, док је валидност самог MUP CA Intermediate сертификата 10 година.

## 6.4 Активациони подаци

### 6.4.1 Генерисање и инсталација активационих података

MUP CA безбедно процесира активационе податке придружене приватним кључевима CA, као и свим другим приватним кључевима у датом PKI систему (Intermediate CA, RA, корисници).

### 6.4.2 Други аспекти у вези активационих података

Ово поглавље није применљиво у оквиру ових CPS.

## 6.5 Безбедносне контроле рачунара

### 6.5.1 Специфични захтеви за безбедност рачунара

MUP CA имплементира специфичне безбедносне контроле над рачунарима који се користе у оквиру датог PKI система.

Рачунари који се користе у оквиру MUP CA чувају се унутар специјалне просторије која је физички обезбеђена. Приступ преко рачунарске мреже се штити помоћу специјалних апликативних firewall уређаја - крипто комуникационих сервера.

Неауторизован приступ рачунарима MUP CA није дозвољен. MUP CA систем могу стартовати само две или више овлашћених особа која поседују одговарајуће смарт картице и која знају њихове PIN-ове.

### 6.5.2 Рангирање безбедности рачунара

Ово поглавље није применљиво у оквиру ових CPS.

## 6.6 Животни циклус техничких безбедносних контрола

### 6.6.1 Контроле развоја система

MUP CA реализује периодичне развојне управљачке контроле.

### 6.6.2 Контроле управљања безбедношћу

MUP CA реализује периодичне безбедносне управљачке контроле.

### 6.6.3 Животни циклус безбедносних контрола

Ово поглавље није применљиво у оквиру ових CPS.

## 6.7 Мрежне безбедносне контроле

MUP CA одржава и примењује висок ниво система мрежне безбедности, укључујући примену firewall уређаја и система за превенцију и заштиту од напада.

## 6.8 Временски печат

Ово поглавље није применљиво у оквиру ових CPS.

# 7. Профили сертификата и CRL листа

Ово поглавље специфицира формате сертификата и CRL листа које издаје MUP CA.

## 7.1 Профили сертификата

MUP CA издаје следеће врсте сертификата у оквиру MUP CA PKI хијерархије:

- MUP CA Root
- MUP CA Gradjani
- MUP CA Sluzbenici
- MUP CA Resursi

MUP CA издаје следеће врсте сертификата:

- Квалификоване сертификате грађанима на личним електронским идентификационим документима са чипом

MUP CA публикује у оквиру овог CPS документа профиле сертификата које користи за све типове сертификата које издаје.

### 7.1.1 Број верзије

MUP CA издаје сертификате у формату X.509v3 тако да су сви сертификати верзије 3.

### 7.1.2 Екстензије у сертификату

Профили сертификата који се издају од стране MUP CA су наведени у наставку.

**Општи профил сертификата**

Општи профил MUP CA сертификата:

| | |
|---|---|
| Ime profila | |
| Period validnosti sertifikata | |
| Basic Constraints Ekstenzija | End Entity\|CA, Path length=x |

| | | |
|---|---|---|
| Čuvanje ključeva | Smart kartica \| HSM | |
| Zajedničke ekstenzije | Authority Key Identifier<br>Subject Key Identifier<br>Authority Information Access<br>CRL Distribution Point | |
| Dužina ključeva | 1024, 2048, 4096 | |
| Key Usage ekstenzija – moguće vrednosti | Digital Signature<br>Non-Repudiation<br>Key Encipherment<br>Data Encipherment | Certificate Signing<br>CRL Signing<br>Encipher Only<br>Decipher Only |
| Enhanced Key Usage Ekstenzija | Client Authentication<br>Server Authentication<br>e-mail Protection<br>Code Signing | |
| QC (Qualified Certificate) statement ekstenzija | OID ekstenzije (1.3.6.1.5.5.7.1.3) sa standardnim vrednostima iz ETSI dokumenta | |
| OID Politike | | |
| URL za politiku certifikacije | | |

**Профил MUP CA Root сертификата**

Профил MUP CA Root сертификата:

| | |
|---|---|
| Ime profila | MUP CA Root |
| Period validnosti sertifikata | 20 godina |
| Period izdavanja sertifikata | 10 godina |
| Ekstenzija osnovnih ograničenja | CA |
| Čuvanje ključeva | HSM |
| Zajedničke ekstenzije | Subject Key Identifier |
| Primenljiva dužina ključeva | 4096 |
| Ekstenzija korišćenja ključa | Certificate Signing<br>OffLine CRL Signing<br>CRL Signing |

**Профил MUP CA Gradjani сертификата**

Профил MUP CA грађани сертификата:

| | |
|---|---|
| Ime profila | MUP CA gradjani |
| Period validnosti sertifikata | 10 godina |
| Period izdavanja sertifikata | 5 godina |
| Ekstenzija osnovnih ograničenja | CA |
| Čuvanje ključeva | HSM |
| Zajedničke ekstenzije | Authority Key Identifier<br>Subject Key Identifier |

| | |
|---|---|
| | Authority Information Access<br>CRL Distribution Point |
| Primenljiva dužina ključeva | 2048 |
| Ekstenzija korišćenja ključa | Certificate Signing<br>Off-Line CRL signing<br>CRL Signing |

**Профил сертификата корисника**

У следеће две табеле су приказани профили квалификованих сертификата за дигитални потпис и за аутентикацију које издаје MUP CA.

**Квалификовани сертификат за аутентикацију/шифровање**

| Ime profila | Kvalifikovani sertifikat za autentikaciju/šifrovanje |
|---|---|
| Period validnosti sertifikata | 5 godina |
| Ekstenzija osnovnih ograničenja | End Entity |
| Čuvanje ključeva | Smart kartica - SSCD |
| Zajedničke ekstenzije | Authority Key Identifier<br>Subject Key Identifier<br>Authority Information Access<br>CRL Distribution Point<br>Certificate Policies |
| Primenljiva dužina ključeva | 1024 |
| Ekstenzija korišćenja ključa | Digital Signature<br>Key Encipherement<br>Data Encipherement |
| Ekstenzija naprednog korišćenja ključa | Client Authentication (1.3.6.1.5.5.7.3.2)<br>Email Protection (1.3.6.1.5.5.7.3.4) |
| QC (Qualified Certificate) statement ekstenzija | OID ekstenzije (1.3.6.1.5.5.7.1.3) sa standardnim vrednostima iz ETSI dokumenta |
| OID Politike | 1.3.6.1.4.1.33589.3.1.1.1 |
| URL za CPS | http://ca.mup.gov.rs |

**Квалификовани сертификат за квалификовани електронски потпис**

| Ime profila | Kvalifikovani sertifikat za kvalifikovani elektronski potpis |
|---|---|
| Period validnosti certifikata | 5 godina |
| Ekstenzija osnovnih ograničenja | End Entity |
| Čuvanje ključeva | Smart kartica - SSCD |
| Zajedničke ekstenzije | Authority Key Identifier<br>Subject Key Identifier |

| | |
|---|---|
| | Authority Information Access<br>CRL Distribution Point<br>Certificate Policies |
| Primenljiva dužina ključeva | 1024 |
| Ekstenzija korišćenja ključa | Digital Signature<br>Non-Repudiation |
| Ekstenzija naprednog korišćenja ključa | Client Authentication (1.3.6.1.5.5.7.3.2)<br>e-mail Protection (1.3.6.1.5.5.7.3.4) |
| QC (Qualified Certificate) statement ekstenzija | OID ekstenzije (1.3.6.1.5.5.7.1.3) sa standardnim vrednostima iz ETSI standarda uz korišćenje SSCD |
| OID Politike | 1.3.6.1.4.1.33589.3.1.1.1 |
| URL za CPS | http://ca.mup.gov.rs |

### 7.1.3 Објектни идентификатори алгоритама

MUP CA у сертификатима које издаје користи комбинацију алгоритама:

- **SHA1RSA** са OID-ом: **1.2.840.113549.1.1.5**

Међутим, MUP CA PKI систем подржава имплементацију било којих комбинација hash и асиметричног криптографског алгоритма.

### 7.1.4 Форме имена

Ово поглавље није применљиво у оквиру ових CPS.

### 7.1.5 Ограничења имена

Ограничења која се односе на имена корисника у квалификованим електронским сертификатима проистичу из одговарајућег и важећег подзаконског акта Закона о електронском потпису.

У наставку су наведена поменута ограничења.

- Поље „subject” квалификованог електронског сертификата мора да има атрибут „commonName”.
- У атрибут „commonName” треба да је уписано пуно име и презиме потписника, јединствени идентификатор потписника унутар сертификационог тела и опционо ЈМБГ. Подаци се уписују следећим редом: име, размак, презиме, размак, јединствени идентификатор унутар сертификационог тела и на крају, опционо, цртица и ЈМБГ. За атрибут „commonName“ треба користити UTF8String кодирање, тако да сва слова из имена и презимена буду верно представљена одговарајућим карактерима.
- Сертификационо тело је дужно да кориснику јасно стави до знања да ли ће сертификат садржати ЈМБГ.

- Сертификати који се користе у општењу органа, општењу органа и странака, достављању и изради одлуке органа у електронском облику у управном, судском и другом поступку пред државним органом, треба да садрже ЈМБГ. Сертификате који садрже ЈМБГ или лични број сертификационо тело не сме учинити јавно доступним.

### 7.1.6 Објектни идентификатор политике сертификације

У овом поглављу је дефинисана OID структура за потребе Политика сертификације и CPS-а која се користи при издавању сертификата у оквиру PKI система МУП РС.

Формат структуре OID-а је следећи:

**1.3.6.1.4.1.33589.а.б.ц.д**

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.

Слова иза PEN-а имају следећа предложена значења:

**а. Тип електронског документа**
1 – ресурсна картица
2 – службена картица EID
3 – лична карта ID

**б. Тип документа**
1 – CP - Certificate Policy
2 – CPS - Certificate Practice Statement

**ц. Тип сертификата**
1 – Квалификовани ITU-T X.509 електронски сертификат
2 - Неквалификовани ITU-T X. 509 електронски сертификат

**д. медиј**
1 – смарт картица (лична карта)

### 7.1.7 Коришћење „Policy Constraints“ екстензије

Ово поглавље није применљиво у оквиру ових CPS.

### 7.1.8 Синтакса и семантика „Policy Qualifier“-са

Ово поглавље није применљиво у оквиру ових CPS.

### 7.1.9 Семантика процесирања критичне екстензије „Certificate Policies“

У сертификатима издатим од стране MUP CA, неопходно је да екстензија „Certificate Policies“ има следеће вредности:

- Одговарајући OID политике сертификације по којој се издаје дати сертификат
- Интернет локацију (URL) на којој се налази овај CPS документ ради преузимања.

## 7.2 Профил CRL листе

У складу са IETF PKIX RFC 2459, MUP CA подржава издавање CRL листа које су у сагласности са следећим условима:

- Бројеви верзија су подржани за CRL листе,
- CRL и CRL екстензије су попуњене и њихова критичност је посебно назначена.

Профил MUP CA CRL (Certificate Revocation List) листе је приказан у следећој табели:

| | | |
|---|---|---|
| **Version** | [Version 2] | |
| **Issuer Name** | CountryName=[Root Certificate Country Name],<br>OrganizationName=[Root Certificate Organization],<br>commonName=[Root Certificate Common Name] | |
| **This Update** | [Date of Issuance] | |
| **Next Update** | [Date of Issuance + 24 hours] | |
| | Signature Algoritham Identifier | |
| | Authority Key Identifier | |
| | CRL Number – redni broj CRL liste | |
| **Revoked sertificates** | CRL Entries | |
| | Certificate Serial Number | [Certificate Serial Number] |
| | Date and Time of Revocation | [Date and Time of Revocation] |

### 7.2.1 Број верзије

MUP CA генерише и објављује CRL листе верзије 2 (X.509v2).

### 7.2.2 CRL и CRL entry екстензије

CRL листа која се издаје од стране MUP CA има следеће екстензије:

- AKI (Authority Key Identifier)
- CRL Number – редни број CRL листе

- CRL entry екстензије су:
- Серијски број опозваног сертификата
- Датум и време опозива

## 7.3 OCSP профил

Ово поглавље није применљиво у оквиру ових CPS.

### 7.3.1 Број верзије

Ово поглавље није применљиво у оквиру ових CPS.

### 7.3.2 OCSP екстензије

Ово поглавље није применљиво у оквиру ових CPS.

# 8. Провера сагласности и друга оцењивања

## 8.1 Фреквенција или услови оцењивања

MUP CA прихвата периодичну проверу сагласности својих политика сертификације, укључујући овај CPS документ, што укључује и периодичну супервизију од стране Надлежног органа за послове акредитације и супервизије PKI система у Републици Србији.

Рад MUP CA је такође у сагласности са најважнијим међународним и Европским стандардима у овој области, као и са Европском директивом 1999/93/EC о електронским потписима.

У домену издавања квалификованих електронских серификата, MUP CA ради у оквиру ограничења дефинисаним у оквиру Закона о електронском потпису државе Србије, као и одговарајућим подзаконским актима.

## 8.2 Идентитет/квалификације процењивача

Супервизију рада MUP CA врши надлежна комисија формирана од стране Надлежног органа за послове акредитације и супервизије Републике Србије.

MUP CA спроводи такође редовне интерне провере усклађености пословања са CP, као и са овим CPS документом. Интерне провере спроводе одговарајући запослени са датим задужењима.

Након испуњења свих услова MUP CA за издавање квалификованих електронских сертификата у Србији, Надлежни орган за послове акредитације и супервизије PKI система (Министарство за телекомуникације и информатичко друштво) врши обавезну супервизију MUP CA редовно барем једном годишње.

## 8.3 Однос оцењивача према оцењиваном ентитету

Ово поглавље није применљиво у оквиру ових CPS.

## 8.4 Теме покривене у процесу оцењивања

У процесу оцењивања рада MUP CA, било екстерног од стране Надлежног органа или интерног од стране интерних аудитора, врши се провера сагласности оперативног рада MUP CA са политкама сертификације (CP) и овим практичним правилима рада (CPS), као и са интерним правилима рада.

## 8.5 Активности предузете као резултат утврђених недостатака

MUP CA треба да усклади свој оперативни рад у складу са евентуалним налазима екстерног или интерне ревизије.

## 8.6 Комуникација резултата

Резултати екстерног или интерне ревизије су расположиви свим корисницима и трећим странама и јавно се објављују на web сајту MUP CA.

# 9. Други пословни и правни аспекти

## 9.1 Цене

### 9.1.1 Цене издавања сертификата

MUP CA не наплаћује коришћење MUP CA издатих квалификованих сертификата корисницима.

MUP CA задржава права да мења услове коришћења сертификата од стране корисника.

### 9.1.2 Цена приступа сертификатима

Ово поглавље није применљиво у оквиру ових CPS.

### 9.1.3 Цена приступа информацијама о статусу сертификата

Ово поглавље није применљиво у оквиру ових CPS.

### 9.1.4 Сене за друге сервисе

Ово поглавље није применљиво у оквиру ових CPS.

### 9.1.5 Политика повраћаја новца

Ово поглавље није применљиво у оквиру ових CPS.

## 9.2 Финансијска одговорност

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

### 9.2.1 Покривање осигурања

Сертификационо тело је дужно да обезбеди најнижи износ осигурања од ризика одговорности за могућу штету насталу вршењем услуга издавања квалификованих електронских сертификата у складу са важећим прописима, тако да:
1) 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;
2) 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 Друга добра

Ово поглавље није применљиво у оквиру ових CPS.

### 9.2.3 Осигурање или гаранцијско покривање за крајње кориснике

Корисник је дужан да обештети MUP CA у односу на било које активности или пропусте у одговорности, било које губитке или штету, као и за било какве трошкове било које врсте, укључујући разумне накнаде адвоката, које би MUP CA могао да има као резултат:

- Било ког лажног или погрешно презентованог податка достављеног од стране корисника или њихових агената.
- Било ког пропуста корисника да достави материјалну чињеницу да је погрешна презентација или пропуст учињен из немарности или са намером да се превари MUP CA или било које лице које прима и односи се према добијеном сертификату.
- Необезбеђивања одговарајуће заштите корисниковог приватног кључа, некоришћења безбедног система како је захтевано или неизвршења одговарајућих превентивних мера неопходних да се спречи компромитација, губитак, објављивање, модификација или неауторизовано коришћење корисниковог приватног кључа или напада на интегритет MUP CA Root приватног кључа.
- Кршења било којих закона који су применљиви, укључујући оне који се односе на заштиту интелектуалних права, вирусе, приступ рачунарским системима итд.

## 9.3 Поверљивост пословних информација

Ово поглавље није применљиво у оквиру ових CPS.

### 9.3.1 Опсег поверљивих информација

Ово поглавље није применљиво у оквиру ових CPS.

### 9.3.2 Информације које нису у опсегу поверљивих информација

Ово поглавље није применљиво у оквиру ових CPS.

### 9.3.3 Одговорност за заштиту поверљивих информација

Ово поглавље није применљиво у оквиру ових CPS.

## 9.4 Приватност и заштита персоналних информација

### 9.4.1 План приватности

MUP CA се придржава правила заштите приватности персоналних података и правила поверљивости како је прописано у овом CPS документу, као и у одговарајућим законским документима.

### 9.4.2 Информације које се третирају као приватне

MUP CA третира приватним све информације које се односе на кориснике сертификата.

### 9.4.3 Информације које се не сматрају приватним

MUP CA не сматра приватним само оне информације корисника за које је сам корисник дао сагласност да се могу публиковати. Најчешће се то односи само на податке који се садрже у издатим квалификованим електронским сертификатима.

### 9.4.4 Одговорност за заштиту приватних информација

MUP CA је одговорно за заштиту приватности корисникових информација.

### 9.4.5 Откривање информација сходно правним и административним процесима

MUP CA не објављује, нити се захтева да објављује, било коју поверљиву информацију без аутентикованог и потврђеног захтева од стране:

- Саме стране за коју се таква информација чува,
- Одговарајућег суда.

MUP CA може наплатити одговарајућу административну цену за процесирање оваквих објављивања.

Стране у комуникацији које захтевају и добијају поверљиве информације имају дозволу за то на основу претпоставке да ће они те информације користити за захтеване сврхе, да ће их осигурати од компромитације и да ће се уздржавати од њиховог коришћења и објављивања трећим странама.

### 9.4.6 Друге околности за откривање информација

MUP CA и његови партнери могу учинити расположивом специфичну политику приватности у циљу заштите персоналних података апликанта који захтева издавање сертификата од стране MUP CA путем њихових web сајтова и/или CP или CPS докумената.

## 9.5 Права интелектуалног власништва

MUP CA поседује и задржава сва права интелектуалног власништва придружена његовим базама података, web сајтовима, електронским сертификатима које издаје, као и било којим другим публикацијама које на било који начин припадају или потичу од стране MUP CA, укључујући CP и ове CPS.

## 9.6 Представљање и гаранције

Ово поглавље није применљиво у оквиру ових CPS.

### 9.6.1 CA представљање и гаранције

Ово поглавље није применљиво у оквиру ових CPS.

### 9.6.2 RA представљање и гаранције

Ово поглавље није применљиво у оквиру ових CPS.

### 9.6.3 Корисничко представљање и гаранције

Ово поглавље није применљиво у оквиру ових CPS.

### 9.6.4 Представљање и гаранције трећих страна

Ово поглавље није применљиво у оквиру ових CPS.

### 9.6.5 Представљање и гаранције других учесника

Ово поглавље није применљиво у оквиру ових CPS.

## 9.7 Непризнавање гаранције

Ово поглавље није применљиво у оквиру ових CPS.

## 9.8 Ограничења одговорности

MUP CA не прихвата било какву другу одговорност осим оне која је експлицитно дефинисана у CP и у овом CPS документу.

Ни у ком случају (изузев злоупотребе или намере) MUP CA није одговорно за:

- Било какав губитак профита.
- Било какав губитак података.
- Било коју индиректну или случајну штету која је проузрокована или је везана за коришћење, испоруку, лиценцу, перформансе сертификата или електронских потписа.

- Било коју трансакцију или услугу понуђену у оквиру ових CPS.
- Било коју другу штету изузев оних које потичу од оправданог ослањања на верификоване информације које се налазе у издатом сертификату.
- Било коју одговорност која се појавила у случају грешке у верификованим информацијама која је резултат грешке, злоупотребе или намере апликанта.

## 9.9 Одштете

Ово поглавље није применљиво у оквиру ових CPS.

## 9.10 Период важности и крај валидности ових CPS

Ово поглавље није применљиво у оквиру ових CPS.

### 9.10.1 Важност

Ово поглавље није применљиво у оквиру ових CPS.

### 9.10.2 Крај валидности

Ово поглавље није применљиво у оквиру ових CPS.

### 9.10.3 Ефекат завршетка и поновног рада

Ово поглавље није применљиво у оквиру ових CPS.

## 9.11 Појединачна обавештења и комуникација са учесницима

Ово поглавље није применљиво у оквиру ових CPS.

## 9.12 Исправке

Ово поглавље није применљиво у оквиру ових CPS.

### 9.12.1 Процедуре за исправку

Ово поглавље није применљиво у оквиру ових CPS.

### 9.12.2 Механизам и период обавештавања

Ово поглавље није применљиво у оквиру ових CPS.

### 9.12.3 Услови промене објектног идентификатора (OID)

Ово поглавље није применљиво у оквиру ових CPS.

## 9.13 Процедуре решавања спорова

MUP CA се реферише на арбитражу у циљу решавања свих спорова који се односе на CP и ових CPS. Ако се спор не реши у оквиру десет (10) дана након иницијалног обавештења сходно правилима CP и ових CPS, стране у спору достављају спор на арбитражу. Арбитража се састоји од 3 арбитра, свака страна предлаже по једног, док трећег предлажу заједно обе стране у спору. Место за арбитражу је Београд, Србија, а арбитри одређују све трошкове арбитраже.

За све спорове који се односе на технологију, као и спорове који се односе на саме CP и CPS документе, стране у спору прихватају арбитражно тело које ће бити изабрано од стране Владе Србије.

## 9.14 Закон који се поштује

Овај CPS документ је издат у потпуности у складу са одговарајућом законском регулативом државе Србије и то пре свега са Законом о електронском потпису и одговарајућим подзаконским актима. Све правне ствари које се односе на MUP CA и/или који се односе на сертификате издате од стране MUP CA ће бити процесуиране од стране одговарајућег суда у Србији.

## 9.15 Сагласност са применљивим законима

Ово поглавље није применљиво у оквиру ових CPS.

## 9.16 Разне одредбе

Ово поглавље није применљиво у оквиру ових CPS.

### 9.16.1 Комплетан уговор

Ово поглавље није применљиво у оквиру ових CPS.

### 9.16.2 Додељивање

Ово поглавље није применљиво у оквиру ових CPS.

### 9.16.3 Озбиљност

Ово поглавље није применљиво у оквиру ових CPS.

### 9.16.4 Спровођење правног поступка

Ово поглавље није применљиво у оквиру ових CPS.

### 9.16.5 Виша сила

Ово поглавље није применљиво у оквиру ових CPS.

## 9.17 Друге одредбе

Ово поглавље није применљиво у оквиру ових CPS.

# 10. Референце

Закон о електронском потпису, Сл. Гласник Републике Србије, бр. 135/2004

Правилник о ближим условима за издавање електронских сертификата, Сл. Гласник Републике Србије, бр. 48/2005

RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework

RFC 5280 – Request For Comments 5280, Internet X.509 Public Key Infrastructure / Certificate and CRL Profile

Политика сертификације Сертификационог тела MUP CA