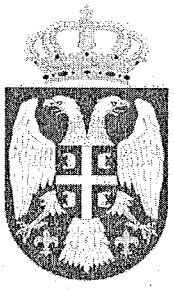
ГЕНЕРАЛШТАБ ВОЈСКЕ СРБИЈЕ
УПРАВА ЗА ТЕЛЕКОМУНИКАЦИЈЕ И ИНФОРМАТИКУ (Ј-6)
ЦЕНТАР ЗА ПРИМЕЊЕНУ МАТЕМАТИКУ И ЕЛЕКТРОНИКУ
Сертификационо тело Министарства одбране и Војске Србије



ПРАКТИЧНА ПРАВИЛА РАДА ЗА ПРУЖАЊЕ КВАЛИФИКОВАНЕ УСЛУГЕ ИЗДАВАЊА КВАЛИФИКОВАНИХ ЕЛЕКТРОНСКИХ СЕРТИФИКАТА ЗА КВАЛИФИКОВАНИ ЕЛЕКТРОНСКИ ПОТПИС/ПЕЧАТ

(верзија 3.0)

OID документа: 1.3.6.1.4.1.42922.10.1.2.1

Београд, јул 2026.

ЦЕНТАР ЗА ПРИМЕЊЕНУ МАТЕМАТИКУ И ЕЛЕКТРОНИКУ
Број _____
_____.20___. год.
Б Е О Г Р А Д

На основу Одлуке о Сертификационом телу Министарства одбране и Војске Србије (акт Управе за телекомуникације и информатику (Ј-6) инт. бр. 12911-1 од 15.11.2013. године), а у складу са чланом 31. Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС“, бр. 94/2017 и 52/ 2021.) и чланом 4. Уредбе о условима за пружање квалификованих услуга од поверења („Службени гласник РС“, бр. 37/2018) , доносим

ПРАКТИЧНА ПРАВИЛА РАДА ЗА ПРУЖАЊЕ КВАЛИФИКОВАНЕ УСЛУГЕ ИЗДАВАЊА КВАЛИФИКОВАНИХ ЕЛЕКТРОНСКИХ СЕРТИФИКАТА ЗА КВАЛИФИКОВАНИ ЕЛЕКТРОНСКИ ПОТПИС/ПЕЧАТ

које ступа на снагу даном доношења.

НАЧЕЛНИК УТИ (Ј-6)
генерал мајор
Миле Витезовић

Садржај

1. Увод и преглед основних претпоставки

Министарство одбране је квалификовани пружалац услуге издавања квалификованих електронских сертификата за квалификовани електронски потпис и квалификовани електронски печат. Сертификационо тело Министарства одбране и Војске Србије (у наставку: Сертификационо тело МО и ВС) за потребе Министарства одбране издаје квалификоване електронске сертификате. Сертификационо тело МО и ВС квалификоване електронске сертификате потписује користећи свој приватни кључ и асиметрични криптографски алгоритам.

У тако формираним сертификатима, Сертификационо тело МО и ВС се идентификује као квалификовани пружалац услуге издавања квалификованог електронског сертификата у складу са Законом о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању (Службени гласник РС, 94/17 и 52/21), у даљем тексту: Закон, и одговарајућим подзаконским актима.

Сертификационо тело МО и ВС издаје квалификоване електронске сертификате корисника у складу са документима:

- ETSI EN 319 412-1 V1.1.0 (2015-12) „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".
- ETSI EN 319 412-2 V2.0.15 (2015-06) „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".
- 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".

Сертификационо тело МО и ВС је одговорно за пружање комплетних услуга сертификације, које укључују следеће услуге, и то:

- Омогућавање извршавања сервиса за регистрацију корисника.
- Формирање асиметричног пара кључева за кориснике и придруженог квалификованог електронског сертификата за потребе креирања и верификације квалификованог електронског потписа и печата.
- Дистрибуцију приватног кључа и квалификованог електронског сертификата регистрационом ауторитету прописан Законом и пратећом регулативом.
- Омогућавање процедуре опозива квалификованих електронских сертификата и
- Обезбеђивање информације о статусу квалификованих електронских сертификата, а у случају појављивања сертификата у CRL и информације о разлогу појављивања.

Сертификационо тело МО и ВС персонализује средство за формирање квалификованог електронског потписа и печата корисницима (еИД картицу/електронска картица за печат и придружени PIN код за употребу средства), као и њихову безбедну дистрибуцију до регистрационог тела МО и ВС.

Сертификационо тело МО и ВС утврђује Општа правила пружања услуге сертификације (у даљем тексту: Општа правила) у складу са Законом.

Општи услови пружања услуга уграђују се у документа:

1. Политика пружања квалификованих услуга од поверења Сертификационог тела МО и ВС

2. Практична правила за пружање квалификоване услуге издавања квалификованих електронских сертификата за квалификовани електронски потпис/печат – овај документ.

Политика пружања квалификованих услуга од поверења Сертификационог тела МО и ВС (у даљем тексту: Политика) и Практична правила за пружање квалификоване услуге издавања квалификованих електронских сертификата за квалификовани електронски потпис/печат (у даљем тексту: Практична правила) у смислу Сертификационог тела МО и ВС су јавно доступна документа. Политика дефинише предмет рада Сертификационог тела, док Практична правила дефинишу процесе и начин њиховог коришћења при формирању и управљању квалификованим електронским сертификатима.

Политика 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.

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

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

Општи услови пружања услуга Сертификационог тела МО и ВС су у складу са документима:
- RFC 3647 „Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework" и
- ETSI EN 319 401 V2.3.1 (2021-05) „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
- ETSI EN 319 411-1 V1.3.1 (2021-05) „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements"
- ETSI EN 319 411-2 V2.5.1 (2023-10) „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates"

Сертификационо тело МО и ВС утврђује и Посебна интерна правила рада сертификационих тела и заштите система сертификације (у даљем тексту: Посебна правила) у којима су садржани и процедурално описани поступци и мере који се примењују приликом издавања и руковања квалификованим електронским сертификатима. Посебна правила су документи који нису јавно доступни и представљају пословну тајну Сертификационог тела.

Посебна 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;

- поступку израде резервне копије базе података и процедура целокупног система;
- поступцима и радњама 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 за пружање квалификоване услуге издавања квалификованих електронских сертификата за квалификовани електронски потпис припадницима МО и ВС на електронском идентификационом документу, као и за квалификовани електронски печат на smart картицама.

Сертификационо тело МО и ВС издаје квалификоване електронске сертификате за проверу квалификованог електронског потписа/печата.

Идентификациони подаци Сертификационог тела МО и ВС су:

Сертификационо тело МО и ВС
Центар за примењену математику и електронику
Војска Србије
Војводе Степе 445
11000 Београд
Србија

Овај документ се идентификује на следећи начин:

- Назив: Практична правила за пружање квалификоване услуге издавања квалификованих електронских сертификата за квалификовани електронски потпис/печат
- Верзија: 2.0
- OID: 1.3.6.1.4.1.42922.1.2.1.1
- Интернет адреса на којој је документ објављен: http://www.ca.vs.rs/sr/dokumenta/dokumenta-ca-mo-i-vs

1.3. Учесници у PKI систему МО и ВС

У овом поглављу су дате основне информације о учесницима у оквиру инфраструктуре јавних кључева (PKI- Public Key Infrastructure) у МО и ВС.

Носилац PKI инфраструктуре у МО и ВС је Управа за телекомуникације и информатику (Ј-6) ГШ ВС.

1.3.1. Сертификационо тело МО и ВС

Послове Сертификационог тела МО и ВС обавља организациона целина Војске Србије у оквиру Центра за примењену математику и електронику (ЦПМЕ) која издаје квалификоване електронске сертификате за потребе МО и ВС. Сертификационо тело МО и ВС је одговорно за публикацију ових Практичних правила у циљу подршке издавању квалификованих електронских сертификата.

У циљу објављивања информација које се односе на опозване квалификоване електронске сертификате, неопходно је да се изврши одговарајућа публикација листе опозваних сертификата (CRL – Certificate Revocation List). Сертификационо тело МО и ВС периодично објављује такву листу у складу са условима дефинисаним у овом документу. Поред публиковања статуса сертификата преко листе опозваних сертификата Сертификационо тело МО и ВС публикује ове информације и преко OCSP сервиса само у локалној рачунарској мрежи МО и ВС.

Сертификационо тело МО и ВС представља хијерархијску PKI структуру за издавање квалификованих електронских сертификата. Сертификационо тело МО и ВС има три Root Сертификациона тела МО и ВС и девет Intermediate Сертификационих тела, и то:

- **MO VS Root** Сертификационо тело је старо RSA коренско самопотписано сертификационо тело које само публикује CRL листу на Root нивоу, са следећим подређеним сертификационим телима:
  - **MO VS UzK CA 4** је RSA подређено Сертификационо тело које издаје квалификовани електронски сертификат:
    - запосленима у МО и ВС за потребе верификације квалификованог електронског потписа,
    - ученицима и студентима војних школа за потребе верификације квалификованог електронског потписа.

  и публикује своју CRL листу опозваних сертификата корисника.
  - **MO VS UzK CA** и **MO VS UzK CA 3** су RSA подређена Сертификациона тела која само публикују своје CRL листе опозваних сертификата корисника.
- **MO VS Root CA EC** је ECC коренско самопотписано Сертификационо тело које публикује CRL листу на Root нивоу, са следећим подређеним сертификационим телима:
  - **MO VS UzK CA EC** је ECC подређено Сертификационо тело које издаје квалификовани електронски сертификат:
    - запосленима у МО и ВС за потребе верификације квалификованог електронског потписа на идентификационим документима,
    - ученицима и студентима војних школа за потребе верификације квалификованог електронског потписа на идентификационим документима,
    - ОЈ МО и ВС за потребе верификације квалификованог електронског печата.
  - **MO VS TSA CA EC** је ECC подређено Сертификационо тело које издаје квалификовани електронски сертификат јединици за издавање временског жига (TSU - Time Stamping Unit).
- **MO VS Root CA RSA** је RSA коренско самопотписано Сертификационо тело које публикује CRL листу на Root нивоу, са следећим подређеним сертификационим телима:
  - **MO VS FSOVO CA RSA** је RSA подређено сертификационо тело које издаје електронски сертификат за аутентификацију и шифровање на војним здравственим легитимацијама.
  - **MO VS IT Resursi CA RSA** је RSA подређено Сертификационо тело које издаје SSL електронски сертификат за IT ресурсе.
  - **MO VS Interni resursi CA RSA** је RSA подређено Сертификационо тело које издаје електронски сертификат за аутентификацију запосленима у Сертификационом телу МО и ВС.
  - **MO VS * CA RSA** је RSA подређено Сертификационо тело које издаје електронски сертификат за потребе *.

* - познато само носиоцу PKI инфраструктуре у МО и ВС.
Квалификовани електронски сертификат МО и ВС корисника се генерише на основу валидног захтева за издавањем квалификованог електронског сертификата који се формира на основу података о МО и ВС кориснику који се узимају у процесу регистрације корисника. Учесници од интереса за ова Практична правила у читавој PKI инфраструктури МО и ВС који имају одговарајуће обавезе су: Сертификационо тело МО и ВС, регистрационо тело МО и ВС, корисници МО и ВС и потенцијалне треће стране.

Обавезе Сертификационог тела МО и ВС

Сертификационо тело МО и ВС гарантује да ће спроводити све процедуре дефинисане овим Практичним правилима. Сертификационо тело МО и ВС користи Политику пружања услуге издавање квалификованих електронских сертификата и Практична правила за пружање услуге издавања квалификованих електронских сертификата у циљу да корисници морају спроводити легалне услове коришћења издатих квалификованих електронских сертификата.

До нивоа специфицираног у одговарајућим поглављима Политике и овог Практичног правила, Сертификационо тело МО и ВС се обавезује на:

- Пуну сагласност са Политиком и овим Практичним правилима, као и свим одговарајућим додацима у тренутку када се публикују.
- Регуларно и периодично ажурирање Политике и овог Практичног правила, као и њихово јавно публиковање.
- Објављивање контакт детаља сертификационог ауторитета.
- Обезбеђивање услуга сертификације у складу са Законом, Правилником и осталим подзаконским актима,
- Обезбеђивање инфраструктуре Сертификационог тела и пружања сертификационих услуга.
- Обезбеђивање сигурних механизама који укључују механизам генерисања и заштите кључева..
- Обезбеђивање хитног обавештавања у случају компромитације сопственог приватног кључа.
- Издавање квалификованих електронских сертификата у складу са Политиком и овим Практичним правилима, као и испуњавање сопствених преузетих обавеза.
- Обавештавање регистрационог тела МО и ВС да су генерисани квалификовани електронски сертификати корисника на основу захтева и дистрибуција еИД у коме су квалификовани електронски сертификати.
- Обавештавање регистрационог тела МО и ВС уколико Сертификационо тело МО и ВС није способно да изврши валидацију захтева за добијање квалификованог електронског сертификата у складу са са Политиком и овим Практичним правилима.
- Након пријема валидног захтева од стране регистрационог тела МО и ВС Сертификационо тело МО и ВС издаје квалификовани електронски сертификат у складу са Политиком и овим Практичним правилима.
- Опозивање квалификованог електронског сертификата који је издат у складу са Политиком и овим Практичним правилима након пријема валидног захтева за опозив квалификованог електронског сертификата од регистрационог тела МО и ВС.

- Објављивање електронског сертификата сертификационих тела у складу са условима дефинисаним у Политици и у овим Практичним правилима.
- Обезбеђивање подршке корисницима и потенцијалним трећим странама као што је описано у Политици и у овим Практичним правилима.
- Обнављање сертификата сертификационог тела у складу са Политиком и овим Практичним правилима.
- Обавештавање трећих страна о статусу сертификата путем публиковања CRL листа на online репозиторијуму.
- Регуларно и периодично објављивање листе опозваних сертификата у складу са Политиком и овим Практичним правилима која је увек доступна свим заинтересованим странама.
- Достављања копије Политике и ових Практичних правила, као и осталих примењивих докумената по захтеву неке од страна.

Сертификационо тело МО и ВС потврђује да, осим горе наведених, нема других обавеза по овим Практичних правила и обавеза које проистичу из Закона.

Одговорности Сертификационог тела МО и ВС

- Сертификационо тело МО и ВС је одговорно за извршавање горе наведених обавеза у обиму који одређује законска регулатива Републике Србије.
- Сертификационо тело МО и ВС није одговорно за заштиту приватних кључева корисника намењених за креирање квалификованог електронског потписа/печата након уручења еИД или електронске картице печата регистрационом телу МО и ВС.
- Сертификационо тело МО и ВС није одговорно за неодговарајућу проверу валидности сертификата од стране која се поуздаје у квалификовани електронски сертификат издат од стране Сертификационог тела МО и ВС.
- Сертификационо тело МО и ВС није одговорно за могућу злоупотребу квалификованог електронског сертификата која је настала услед неиспуњавања обавеза корисника или треће стране која се поуздаје у квалификовани електронски сертификат издат од стране Сертификационог тела МО и ВС.
- Сертификационо тело МО и ВС није одговорно за неизвршавање својих обавеза које је последица ванредне ситуације или више силе.

1.3.2. Регистрациона тела МО и ВС

Захтев за издавањем квалификованог електронског сертификата за кориснике МО и ВС се формира посредством захтева за издавањем еИД и захтева за електронском картицом печата. Захтеви за издавањем еИД прикупљају се у Управи за кадрове МО. Управа за кадрове и остала службена лица која овласти Управа за кадрове МО су Регистрациона тела (RA – Registration Authority) за издавање квалификованог електронског сертификата за верификацију квалификованог електронског потписа. Захтеви за издавањем печата прикупљају се у Управи за организацију Сектора за људске ресурсе МО. Управа за организацију је Регистрационо тело (RA – Registration Authority) за издавање квалификованог електронског сертификата за потребе верификације квалификованог електронског печата.

Регистрациона тела МО и ВС:

- Спроводе све кораке у процедури идентификације корисника што је дефинисано важећим законским документима и општим правилима сертификације Сертификационог тела МО и ВС.
- Уносе податке о кориснику и формирају захтев за издавање еИД.
- Иницирају процес којим се започиње процедура за издавање документа, у току којег се креирају криптографски кључеви и сертификати корисника.
- Преузимају електронска идентификациона документа.
- Дистрибуирају квалификовани електронски сертификат (електронске паметне картице које су физички носиоци електронског сертификата) до крајњих корисника.

Регистрациона тела МО и ВС делују у складу са законским прописима, процедурама и општим правилима сертификације Сертификационог тела МО и ВС. Не постоји ограничење у смислу броја регистрационих тела која могу бити придружена PKI инфраструктури.

Обавезе регистрационог тела МО и ВС

Регистрационо тело МО и ВС се обавезује на:

- Припремање потребних података за издавање квалификованих електронских сертификата у складу са Политиком и овим Практичним правилима.
- Извршавање свих активности на верификацији и провери аутентичности подносиоца захтева у складу са Уредбом о војној легитимацији („Службени војни лист“ 25/15 и 21/21), Директивом о начину и поступку издавања, коришћења, враћања, поништавања и начину вођења евиденције о издатим војним, кадетским и ученичким легитимацијама и идентификационим картицама („Службени војни лист“ 10/16 и 01/03), Правилника о печатима Војске Србије („Службени војни лист“ 20/25), Политиком и овим Практичним правилима.
- Достављање захтева до Сертификационог тела МО и ВС у електронски потписаној поруци (захтев за издавањем квалификованог електронског сертификата), у складу са процедурама које су описане у Политици и овим Практичним правилима.
- Записивање свих активности преко апликације регистрационог тела.
- Пријем, верификацију и прослеђивање ка Сертификационом телу МО и ВС свих захтева за опозивом, суспензијом и активацијом издатих сертификата у складу са процедурама Сертификационог тела МО и ВС, Политиком и овим Практичним правилима.
- Поступање у складу са Уредбом о војној легитимацији и Директивом о начину и поступку издавања, коришћења, враћања, поништавања и начину вођења евиденције о издатим војним, кадетским и ученичким легитимацијама и идентификационим картицама и Правилником о печатима Војске Србије.

Регистрационо тело МО и ВС је одговорно за извршавање горе наведених обавеза.

1.3.3. Корисници МО и ВС

Корисници представљају кориснике сертификационих услуга Сертификационог тела МО и ВС. То су запослена лица у МО и ВС, ученици, студенти Универзитета одбране и ОЈ МО и ВС (за печат).

Корисници су стране које:

- Подносе захтев за добијање квалификованог електронског сертификата,

- Идентификовани су као власници квалификованог електронског сертификата у самом сертификату,
- Поседују приватни кључ који одговара јавном кључу који је наведен у корисниковом квалификованом електронском сертификату.

Обавезе корисника квалификованих електронских сертификата

Сем ако није другачије дефинисано у Политици и овим Практичним правилима, корисници сертификационих услуга Сертификационог тела МО и ВС су одговорни за:

- Поседовање одговарајућих знања и, ако је неопходно, похађање одговарајуће обуке за коришћење квалификованих електронских сертификата и сертификационих услуга.
- Поштовање Политике и Практичних правила публикованих од стране Сертификационог тела МО и ВС.
- Обезбеђивање тачних и прецизних информација у њиховој комуникацији са Сертификационим телом МО и ВС и/или регистрационим телом МО и ВС.
- Упознавање, разумевање и сагласност са свим ставовима и условима у Политици и овим Практичним правилима, као и другим документима који су објављени на репозиторијуму Сертификационог тела МО и ВС.
- Нарушавања интегритета и произвођења неисправним квалификованог електронског сертификата издатог од стране Сертификационог тела МО и ВС.
- Коришћење квалификованог електронског сертификата само у сврхе дефинисане у складу са Политиком и овим Практичним правилима, као и важећим законским документима.
- Обавештавање регистрационог тела МО и ВС о било којим променама информација које су раније достављене.
- Прекид коришћења издатог квалификованог електронског сертификата уколико је било која информација у квалификованом електронском сертификату постала невалидна.
- Прекид коришћења квалификованог електронског сертификата издатог од Сертификационог тела МО и ВС уколико сам квалификовани електронски сертификат постане невалидан.
- 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.
- Уздржавање од достављања до Сертификационог тела МО и ВС, или било ког директоријума Сертификационог тела МО и ВС, било каквог материјала који садржи ставове који угрожавају било који закон или било које право било које стране.
- Подношење захтева за опозив квалификованог електронског сертификата у случају да постоји догађај који материјално утиче на интегритет издатог квалификованог електронског сертификата издатог од стране Сертификационог тела МО и ВС.
- Пријављивање сваке могуће злоупотребе свог приватног кључа и захтевање да се квалификовани електронски сертификат опозове у том случају.

1.3.4. Треће стране

Треће стране могу бити ентитети, као на пример физичка лица (појединци) и/или правна лица (компаније), која прихватају квалификоване електронске сертификате и верификују квалификовани електронски потпис/печат одређених електронских докумената која су потписана/печаћена од стране корисника Сертификационог тела МО и ВС, као и која врше валидацију квалификованог електронског сертификата издатог од стране Сертификационог тела МО и ВС.

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

У циљу провере валидности примењеног квалификованог електронског сертификата, треће стране морају увек да провере статус опозваности датог сертификата у оквиру листе опозваних сертификата издате од стране Сертификационог тела МО и ВС пре него што прихвате информације које су наведене у сертификату.

Обавезе трећих страна

Страна која се ослања на сертификат издат од Сертификационог тела МО и ВС обавезна је да:

- Поседује одговарајућа знања о коришћењу електронских сертификата и других технологија везаних за услуге сертификације.
- Се упозна са Политиком и овим Практичним правилима у вези наведених услова који важе за треће стране.
- Поштује и спроводи одредбе из Политике и ових Практичних правила када поступа са квалификованим електронским сертификатом издатим од Сертификационог тела МО и ВС.
- Верификује издати квалификовани електронски сертификат Сертификационог тела МО и ВС применом: провере валидности квалификованог електронског сертификата, провере Сертификационог тела које је издало квалификовани електронски сертификат, провере електронског потписа квалификованог електронског сертификата и провере статуса датог квалификованог електронског сертификата у важећој CRL листи, а у складу са процедуром валидације сертификата и комплетног ланца сертификата.
- Верује у издати квалификовани електронски сертификат Сертификационог тела МО и ВС само уколико се све информације које се односе на такав квалификовани електронски сертификат могу верификовати као коректне и ажурне.
- Разумно ослони и поуздa на квалификовани електронски сертификат издат од Сертификационог тела МО и ВС у складу са одговарајућим околностима.

1.3.5. Други учесници

Ово поглавље није применљиво у оквиру ових Практичних правила.

1.4. Коришћење сертификата издатих од стране Сертификационог тела МО и ВС

У овом поглављу се дефинише коришћење квалификованих електронских сертификата издатих од стране Сертификационог тела МО и ВС.

1.4.1. Прихватљиво коришћење квалификованих електронских сертификата

Квалификовани електронски сертификати које изда Сертификационо тело МО и ВС се користе у акредитованим апликацијама МО и ВС у којима се спроводи верификација електронског потписа/печата.

1.4.2. Забрањено коришћење квалификованих електронских сертификата

Забрањено је коришћење квалификованог електронског сертификата за сврхе које не одговарају садржају поља употребе сертификата (KeyUsage).

1.5. Администрација Практичних правила за пружање услуге издавања квалификованих електронских сертификата

У овом поглављу су описане активности у вези администрације ових Практичних правила.

1.5.1. Организација администрирања Практичних правила

Сертификационог тела МО и ВС је одговорно за прописну администрацију ових Практичних правила, и то у смислу периодичног прегледа и ажурирања, као и ванредних промена одговарајућих одредби које проистичу из евентуалних промена у законској регулативи или одговарајућа сазнања о критичним слабостима и другим техничким карактеристикама примењених криптографских алгоритама и дужина кључева.

Сертификационо тело МО и ВС најмање једном у току календарске године врши преглед ових Практичних правила.

1.5.2. Контакт особа

Особа у Сертификационом телу МО и ВС, одговорна за Практична правила за пружање услуге издавања квалификованих електронских сертификата је:

пуковник др Радомир Продановић, дипл. инж.
Email: radomir.prodanovic@cpme.uti.vs - РАМКО
radomir.prodanovic@vs.rs - Интернет

1.5.3. Особа која одређује погодност Практичних правила за пружање услуге издавања квалификованих електронских сертификата

Погодност Практичних правила за пружање услуге издавања квалификованих електронских сертификата Сертификационог тела МО и ВС одређује Управа за телекомуникације и информатику (J-6) ГШ ВС као носилац PKI инфраструктуре у МО и ВС.

1.5.4. Процедура одобравања Практичних правила за пружање услуге издавања квалификованих електронских сертификата

Након извршене ревизије и измена, Практична правила се достављају Управи за телекомуникације и информатику (J-6) ГШ ВС која је надлежна за одобравање документа.

1.6. Дефиниције и скраћенице

У овом документу поједини изрази имају следеће значење:

1.6.1. Дефиниције

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

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

Политика пружања квалификованих услуга од поверења Сертификационог тела МО и ВС – 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.

Практична правила за пружање квалификоване услуге издавања квалификованих електронских сертификата за квалификовани електронски потпис/печат – Јавна Практична правила и процедуре које сертификационо тело примењује у процедури издавања сертификата.

Пружалац квалификоване услуге од поверења – је правно лице или физичко лице у својству регистрованог субјекта које пружа једну или више квалификованих услуга од поверења.

Сертификационо тело – издавач сертификата – У контексту одређеног сертификата, Сертификационо тело – издавач 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 налазе публикована Практична правила 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 – је скуп података састављен од слова, бројева, симбола, графичких, звучних и видео материјала, у електронском облику.

Електронски потпис – скуп података у електронском облику који су придружени или логички повезани са другим (потписаним) подацима у електронским облику тако да се електронским потписом потврђује интегритет тих података и идентитет 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 у складу са Законом.

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

Средства за формирање електронског потписа/печата – 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/печата – средства за формирање електронског потписа која испуњавају додатне услове утврђене Законом.

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

Средства за проверу електронског потписа/печата – 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/печата – средства за проверу електронског потписа која испуњавају додатне услове утврђене Законом.

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.

Корисник – правно лице, предузетник, државни орган, орган територијалне аутономије, орган локалне самоуправе или физичко лице коме се издаје електронски сертификат.

Сертификационо тело - правно лице које издаје електронске сертификате у складу са одредбама Закона.

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 аудит-а.

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

Идентификација – процес утврђивања идентитета појединца или организације. У контексту PKI система, аутентикација се односи на два процеса:

- Утврђивање да дато име појединца или организације одговара реалном идентитету појединца или организације и
- Утврђивање да је појединац или организација који се пријављује за одређени сервис под датим именом у ствари баш тај (под тим именом) појединац или организација.

Ауторизација – процедура утврђивања права које неки индентификовани 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.

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) – Листа издата и електронски потписана од стране CA која укључује серијске бројеве опозваних сертификата, као и време опозива. Таква листа се мора користити од стране трећих страна увек када треба проверити валидност сертификата и/или верификацију електронског потписа.

Серијски број сертификата – 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 – 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 информације постаје недоступан неовлашћеним лицима (шифрат).

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 информацију, 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 (којим се обезбеђује: аутентичност, интегритет и непорецивост трансакција) и дигиталне енвелопе (којим се обезбеђује чување симетричног кључа у шифрованом облику). 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.

Hash алгоритми – једносмерни криптографски алгоритми помоћу којих се врши криптографска трансформација информације произвољне величине у hash вредност фиксне величине (160, 224, 256, 374, 512 битова (или више)).

Идентификатор објекта – 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.

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 физичких токена, као на пример смарт картица.

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

1.6.2. Скраћенице

Скраћенице на енглеском језику:

CA – Certification Authority

CEN- European Committee Standardization

CRL – Certificate Revocation List

CSR – Certificate Service Request

CWA- CEN Workshop Agreement

EAL- Evaluation Assurance Level

ETSI – European Telecommunication Standardization Institute

OID – Object Identifier

OCSP – Online Certificate Status Protocol

PKI – Public Key Infrastructure

RA – Registration Authority

RFC – Request For Comments

Скраћенице на српском језику:

еИД - електронски идентификациони документ

Сертификационо тело МО и ВС - Сертификационо тело Министарства одбране и Војске Србије

МО – Министарство Одбране

ВС – Војска Србије

УзК – Управа за Кадрове

УО – Управа за организацију

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 Сертификационог тела МО и ВС.

2.1. Репозиторијуми

Сертификационо тело МО и ВС публикује информације у вези електронских сертификата које издаје на online репозиторијумима који су организовани на одређеним Web серверу.

Сертификационо тело МО и ВС има online репозиторијум докумената у којима објављују информације о практичним правилима и процедурама рада, укључујући Политику као и ово Практично правило.

Сертификационо тело МО и ВС објављује податке и сву документацију која се односи на пружање квалификованих услуга од поверења на својој интернет страници: http://www.ca.vs.rs/sr/pki. Интернет страница је јавно доступна

Сертификационо тело МО и ВС задржава право да учини расположивим и публикује информације у вези сопствених политика и процедура рада путем било ког погодног начина.

Стране у комуникацији (укључујући кориснике и треће стране) које приступају репозиторијуму Сертификационог тела МО и ВС у потпуности су сагласне са одредбама Политике и ових Практичних правила, као и са било којим другим условима коришћења које је Сертификационо тело МО и ВС учинио доступним.

Сертификационо тело МО и ВС чини све у својој моћи у циљу осигурања да стране које приступају његовом репозиторијуму добијају поуздане, ажурне и тачне информације. Сертификационо тело МО и ВС, међутим, не може прихватити било какву одговорност која је ван ограничења дефинисаних у Политици и овим Практичним правилима.

2.2. Публиковање информација о сертификатима

Сертификационо тело МО и ВС публикује информације о сертификатима на претходно поменутим репозиторијумима, и то:

- Сертификате коренских и подређених сертификационих тела МО и ВС
- Информације о статусима опозваности сертификата (CRL).
- Основне документе рада Сертификационог тела МО и ВС (Политика, ова Практична правила, итд.).

Сертификационо тело МО и ВС не публикује јавно било какве информације из квалификованих електронских сертификата корисника и не публикује јавно квалификоване електронске сертификате корисника.

Из разлога њихове осетљивости и пословне тајне, Сертификационо тело МО и ВС неће публиковати Посебна правила рада.

2.3. Време и фреквенција публиковања

Сертификационо тело МО и ВС публикује информације о статусу опозваности издатих сертификата (CRL листе и OCSP само за кориснике у локалној рачунарској мрежи МО и ВС)), као што је назначено и прецизирано у овим Практичним правилима (наслов 4.9.7).

2.4. Контроле приступа репозиторијумима

За потребе Сертификационог тела МО и ВС Центар за командно информационе системе (ЦКИСИП) одржава расположивим приступ до јавног репозиторијума са сврхом омогућавања:

- Добављање сертификата Root и Intermediate Сертификационих тела,
- Добаваљања CRL листе Сертификационог тела МО и ВС у циљу валидације сертификата издатог од стране Сертификационог тела МО и ВС.
- Добављања Политика и Практичних правила.

Сертификационо тело МО и ВС може ограничити или забранити приступ одређеним услугама, одређеним директоријумима, итд.

3. Идентификација и аутентификација корисника

Сертификационо тело МО и ВС одржава документована Практична правила и процедуре у циљу аутентикације и утврђивања идентитета и/или других атрибута подносиоца захтева/крајњих корисника квалификованог електронског сертификата Сертификационог тела МО и ВС.

Регистрационо тело детаљније прописује и одржава процедуре за аутентикацију, утврђивање идентитета и друге атрибуте подносиоца захтева за квалификованим електронским сертификатом.

Аутентикација и утврђивање идентитета се извршавају пре издавања квалификованог електронског сертификата и извршава је регистрационо тело МО и ВС.

Сертификационо тело МО и ВС користи потврђене процедуре у циљу прихватања захтева регистрационог тела МО и ВС преко кога ентитети желе да постану чланови PKI хијерархије.

Сертификационо тело МО и ВС аутентификује захтеве страна које желе да опозову квалификовани електронски сертификат у складу са овом Политиком.

Сертификационог тела МО и ВС одржава одговарајуће процедуре у циљу одређивања Практичних правила за додељивање имена.

3.1. Називи

3.1.1. Типови имена

У циљу идентификације корисника, Сертификационо тело МО и ВС спроводи одговарајућа правила додељивања имена којима се корисници на једнозначан начин разликују у систему.

3.1.2. Потреба да имена буду са реалним значењем

Када се подносе захтев за квалификованим електронским сертификатом име подносиоца захтева мора бити у потпуности реално и са одговарајућим значењем. Сертификационо тело МО и ВС издаје квалификовани електронски сертификат подносиоцима захтева који достављају документоване захтеве преко регистрационог тела МО и ВС који садрже име, а које се може верификовати.

3.1.3. Анонимност корисника

Сертификационо тело МО и ВС не издаје анонимне квалификоване електронске сертификате корисницима нити издаје анонимним корисницима квалификоване електронске сертификате.

3.1.4. Правила за интерпретацију различитих форми имена

Ово поглавље није применљиво у оквиру ових Практичних правила.

3.1.5. Јединственост имена

Имена придружена корисницима квалификованих електронских сертификата за потпис су јединствена у домену Сертификационог тела МО и ВС. Име корисника квалификованог електронског сертификата за потпис се увек користи заједно са јединственим идентификационим бројем корисника које се уписује у Dname поље корисника. Као јединствени идентификациони број корисника користи се ЈМБГ (Јединствени Матични Број Грађана) или јединствени број из базе података Сертификационог тела МО и ВС.

Имена придружена корисницима квалификованих електронских сертификата за печат су јединствена у домену Сертификационог тела МО и ВС. Име корисника квалификованог електронског сертификата за печат се увек користи заједно са јединственим идентификационим бројем корисника које се уписује у Dname поље корисника. Као јединствени идентификациони број корисника користи се јединствени број из базе података Сертификационог тела МО и ВС.

3.1.6. Препознавање, аутентикација и улога робних марки („trandemarks“)

Сертификационо тело МО и ВС не прихвата “trademark” ознаке, логое или друге графичке или текстуалне материјале који су заштићени од копирања, а предложени за укључење у квалификоване електронске сертификате које издаје.

3.2. Иницијална провера идентитета

У циљу реализације процедуре идентификације и аутентикације за иницијалну корисникову регистрацију регистрационо тело МО и ВС спроводи све потребне кораке провере података корисника, укључујући консултовање одговарајућих база података.

3.2.1. Метода доказивања поседовања приватног кључа

Ово поглавље није применљиво у оквиру ових Практичних правила зато што не постоји удаљено слање захтева за израдом квалификованог електронског сертификата од стране корисника.

3.2.2. Аутентикација идентитета организације

Сертификационо тело МО и ВС издаје квалификовани електронски сертификат за потпис на еИД запосленима у МО и ВС, ученицима и кадетима који имају потписан Уговор о школовању. Регистрационо тело МО и ВС врши проверу да ли су лица којима се издаје еИД запослена у МО и ВС и да ли имају уговор о школовању са МО и ВС.

Сертификационо тело МО и ВС издаје квалификовани електронски сертификат за печат на електронској картици за печат организационим јединицама МО и ВС. Регистрационо тело МО и ВС врши проверу да ли организационе јединице постоје у МО и ВС и да ли имају право на печат.

3.2.3. Аутентикација идентитета појединца

У циљу идентификације и аутентикације индивидуалног корисника који подноси захтев за квалификовани електронски сертификат, регистрационо тело МО и ВС може применити кораке који укључују, али нису ограничени на:

- Проверу докумената као што су идентификационе картице, пасош, возачка дозвола.
- Утврђивање идентитета која се базира на достављеној и постојећој документацији.
- Захтев да се појединац физички појави у регистрационом телу МО и ВС у одговарајућој фази пре него што се изда квалификовани електронски сертификат.

3.2.4. Информације корисника које се не верификују

Ово поглавље није применљиво у оквиру ових Практичних правила.

3.2.5. Валидација ауторитета

Ово поглавље није применљиво у оквиру ових Практичних правила.

3.2.6. Критеријуми за интероперабилност

Ово поглавље није применљиво у оквиру ових Практичних правила.

3.3. Идентификација и аутентикација захтева за обнављање кључева

Ово поглавље није применљиво у оквиру ових Практичних правила.

3.3.1. Идентификација и аутентикација за рутинско обнављање кључева

Ово поглавље није применљиво у оквиру ових Практичних правила.

3.3.2. Идентификација и аутентикација за обнављање кључева након опозива

Ово поглавље није применљиво у оквиру ових Практичних правила.

3.4. Идентификација и аутентикација захтева за опозив или суспензију сертификата

У циљу спровођења процедура идентификације и аутентикације захтева за опозивом или суспензијом квалификованог електронског сертификата, Сертификационо тело МО и ВС захтева коришћење online аутентикационог механизма (аутентикација путем електронског сертификата) преко Web комуникације до самог Сертификационог тела МО и ВС, односно аутентикацију на апликацију регистрационог тела преко које се врши опозив (суспензија) квалификованог електронског сертификата.

Примери безбедног достављања захтева за опозивом или суспензијом су дигитално потписани захтеви од стране регистрационог тела МО и ВС или овлашћених лица Сертификационог тела МО и ВС.

4. Оперативни захтеви у вези животног циклуса квалификованог електронског сертификата

За све кориснике постоји стална обавеза да информишу регистрационо тело МО и ВС о свим променама у информацијама које су објављене у квалификованом електронском сертификату за читав период важности таквог сертификата.

4.1. Подношење захтева за добијање квалификованог електронског сертификата

4.1.1. Ко може да достави захтев за издавање квалификованог електронског сертификата?

Корисници подносе захтев за издавање еИД, а тим и аутоматски захтев за добијање квалификованог електронског сертификата за потпис сходно: Уредби о војној легитимацији и Директиви о начину и поступку издавања, коришћења, враћања, поништавања и начину вођења евиденције о издатим војним, кадетским и ученичким легитимацијама и идентификационим картицама.

Корисници имају одговорност да доставе поуздане и тачне информације у својим захтевима за издавање еИД.

Корисници (ОЈ МО и ВС) подносе захтев за издавање електронске картице за печат, а тиме аутоматски добијају квалификовани електронски сертификат за печат сходно Правилнику о печатима Војске Србије.

Корисници захтев подносе регистрационом телу МО и ВС.

Захтев 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 квалификованог електронског сертификата (enrollment) и одговорности

Корисник захтев за издавањем квалификованог електронског сертификата за потпис подноси кроз Захтев за издавањем еИД, односно кроз захтев за издавање војне легитимације (идентификационе картице, ученичке легитимације, кадетске легитимације).

Податке о кориснику његова организација може доставити регистрационом телу МО и ВС у облику XML фајла електронским путем.

Оператери регистрационог ауторитета МО и ВС за еИД се пријављују на web страну апликације за рад регистрационог тела помоћу службеног еИД, и уносе све неопходне податке о кориснику за генерисање квалификованог електронског сертификата :

- Име,
- Презиме,
- ЈМБГ,
- Назив организације и организационе јединице у оквиру организације којој корисник припада,

- Седиште организације (назив града),
- Email адресу корисника у наведеној организацији.

Корисник захтев за издавањем квалификованог електронског сертификата за печат подноси кроз Захтев за издавањем електронског печата, односно кроз захтев за издавање електронске картице за печат.

Оператери регистрационог ауторитета МО и ВС за електронски печат (Управа за организацију) се пријављују на web страну апликације за рад регистрационог тела помоћу службеног еИД, и уносе све неопходне податке о организационој јединици МО и ВС за генерисање квалификованог електронског сертификата за печат:

- Назив организације и организационе јединице у оквиру организације којој корисник припада,
- Седиште организације (назив града),

Подаци се могу прилагодити сходно типу корисника на кога се односе. Ови подаци се прослеђују Сертификационом телу МО и ВС заштићеном комуникацијом на начин прописан Интерним правилима.

4.2. Процесирање захтева за добијање квалификованог електронског сертификата

4.2.1. Извршавање функције идентификације и аутентикације корисника

Након пријема захтева за издавање еИД или електронског печата, а тиме и захтева за добијање квалификованог електронског сертификата за датог корисника, регистрационо тело МО и ВС врши дефинисану идентификациону и аутентикациону процедуру у циљу валидације захтева корисника и захтева за издавање еИД.

4.2.2. Потврђивање или одбијање апликације за добијање квалификованог електронског сертификата корисника

Регистрационо тело МО и ВС потврђује или одбија кориснички захтев за добијање квалификованог електронског сертификат корисника у зависности да ли је захтев потпун и исправан.

Сертификационо тело МО и ВС потврђује или одбија електронски захтев за издавање квалификованог електронског сертификата у зависности од тога да ли је захтев потпун и исправан.

Након потврђивања захтева за издавање квалификованог електронског сертификата прослеђује се захтев на обраду.

4.2.3. Потребно време за процесирање апликације корисника

Сертификационо тело МО и ВС мора да изврши све аутентикационе активности и процесира захтев за издавање квалификованог електронског сертификата у оквиру најкраћег временског периода од добијања валидног захтева.

4.3. Издавање квалификованих електронских сертификата

4.3.1. Активности Сертификационог тела МО и ВС током процеса издавања квалификованог електронског сертификата

Након доставе валидног електронског захтева корисника за издавањем квалификованог електронског сертификата, Сертификационо тело МО и ВС спроводи процес издавања квалификованог електронског сертификата који се састоји од следећих активности:

- Процедура верификације електронског потписа/печата на достављеном захтеву за издавање сертификата,
- Генерисање и чување асиметричног пара кључева на SSCD уређају (електронска картица) и квалификованог електронског сертификата за верификацију квалификованог електронског потписа и њихов упис у еИД или електронску картицу за печат током процеса електронске персонализације.

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

- Корисник који је поднео захтев за издавање квалификованог електронског сертификата позитивно је идентификован и његов идентитет је потврђен.
- Подаци који су наведени у пријави су истинити.
- Корисник не поседује валидан квалификовани електронски сертификат за који се пријавио.

4.3.2. Обавештење корисника од стране СА о издатом квалификованом електронском сертификату

Квалификовани електронски сертификат уписан је на еИД корисника који Сертификационо тело МО и ВС доставља регистрационом телу МО и ВС.

Регистрационо тело доставља еИД или електронску картицу за печат кориснику, а тиме и квалификовани електронски сертификат.

4.4. Прихватање квалификованог електронског сертификата

4.4.1. Спровођење процеса прихватања квалификованог електронског сертификата

Издати квалификовани електронски сертификат од стране Сертификационог тела МО и ВС се сматра прихваћеним од стране корисника самим чином преузимања еИД (електронске картице за печат).

Иницирање генерисања квалификованог електронског сертификата је потврђено од стране администратора регистрационог тела МО и ВС, а само генерисање квалификованог електронског сертификата је потврђено од стране оператера Сертификационог тела МО и ВС у поступку електронске персонализације.

Било која примедба на издати квалификовани електронски сертификат мора бити експлицитно достављена регистрационом телу МО и ВС. Регистрационо тело МО и ВС је у обавези да извести Сертификационо тело МО и ВС о примедбама на издати квалификовани електронски сертификат.

Потврда о одбијању преузимања еИД због нетачних података у квалификованом електронском сертификату мора такође бити достављена на претходно описан начин.

4.4.2. Објављивање квалификованог електронског сертификата од стране Сертификационог тела МО и ВС

Сертификационо тело МО и ВС јавно не објављује квалификоване електронске сертификате корисника.

4.4.3. Обавештење других ентитета о издатом сертификату

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.5. Коришћење квалификованог електронског сертификата и асиметричног пара кључа

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

4.5.1. Коришћење приватног кључа и квалификованог електронског сертификата од стране корисника

Корисник се обавезује да ће користити приватни кључ и изгенерисани квалификовани електронски сертификат од стране Сертификационог тела МО и ВС само у предвиђеним апликацијама које обезбеди и одобри носилац PKI инфраструктуре у МО и ВС, као и у складу са дефинисаним начином коришћења кључа у самом квалификованом електронском сертификату (Key Usage и Enhanced Key Usage екстензије).

Корисник може користити свој приватни кључ само након прихватања одговарајућег квалификованог електронског сертификата.

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

4.5.2. Коришћење јавног кључа и квалификованог електронског сертификата од стране трећих страна

Трећа страна је обавезна да прихвати квалификовани електронски сертификат издат од Сертификационог тела МО и ВС само у оним апликацијама које су дефинисане и одобрене од стране носиоца PKI инфраструктуре у МО и ВС, као и са предвиђеним начином коришћења квалификованог електронског сертификата дефинисаним у самом сертификату.

Трећа страна је обавезна да прописно и успешно примењује операцију јавног кључа који екстрахује из издатог квалификованог електронског сертификата и одговорна је да спроводи проверу статуса опозваности датог квалификованог електронског сертификата коришћењем метода који је дефинисан у Политици пружања услуге издавања квалификованих електронских сертификата и Практичним правилима за пружање услуге издавања квалификованих електронских сертификата.

4.6. Обнављање квалификованог електронског сертификата

4.6.1. Услови за обнављање квалификованог електронског сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.6.2. Ко може захтевати обнављање квалификованог електронског сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.6.3. Процесирање захтева за обнављањем квалификованог електронског сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.6.4. Обавештење корисника да му је издат обновљени квалификовани електронски сертификат

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.6.5. Спровођење процеса прихватања обновљеног сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.6.6. Објављивање обновљеног квалификованог електронског сертификата од стране CA

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.6.7. Обавештење других ентитета од стране CA о обнови датог квалификованог електронског сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.7. Генерисање новог пара кључева и квалификованог електронског сертификата корисника

4.7.1. Услови за генерисање новог пара кључева и квалификованог електронског сертификата

Услови за генерисање новог пара кључева корисника су:

- Квалификовани електронски сертификат датог корисника је истекао или
- Квалификовани електронски сертификат датог корисника је опозван, а корисник има право да накнадно затражи добијање новог квалификованог електронског сертификата, под условима дефинисаним у Политици и овом документу.

4.7.2. Ко може захтевати нови квалификовани електронски сертификат са новим јавним кључем

Сви корисници МО и ВС који испуњавају услове из тачке 4.7.1.

4.7.3. Процесирање захтева за новим паром кључева и квалификованим електронским сертификатом

У случају да је квалификовани електронски сертификат истекао, и уколико се жели добити нови квалификовани електронски сертификат, мора се поднети захтев за издавање новог еИД (електронске картице за печат) који је исти као и сваки нови захтев за добијање квалификованог електронског сертификата. У том случају, увек се генерише нови пар асиметричних кључева.

Такође, уколико је квалификовани електронски сертификат корисника опозван, а разлог за опозив је компромитација кључа, корисник може добити нови квалификовани електронски сертификат само на основу генерисаног новог пара асиметричних кључева и путем процедуре која је идентична достављању првобитног захтева за издавање новог квалификованог електронског сертификата, односно еИД (електронске картице за печат).

Након достављања захтева за издавањем новог квалификованог електронског сертификата (еИД или електронске картице за печат), даља процедура је у потпуности идентична као и процедура за добијање првог квалификованог електронског сертификата.

4.7.4. Обавештење корисника да му је издат нови квалификовани електронски сертификат

Ова процедура је идентична процедури издавања првог квалификованог електронског сертификата, односно издавању еИД или електронске картице за печат.

4.7.5. Спровођење процеса прихватања новог квалификованог електронског сертификата

Ова процедура је идентична процедури прихватања првог квалификованог електронског сертификата.

4.7.6. Објављивање новог квалификованог електронског сертификата од стране Сертификационог тела МО и ВС

Сертификационо тело МО и ВС јавно не објављује квалификоване електронске сертификате корисника.

4.7.7. Обавештење других ентитета од стране СА о издавању новог сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.8. Модификације квалификованог електронског сертификата корисника

4.8.1. Услови за модификацију квалификованог електронског сертификата корисника

Модификација квалификованог електронског сертификата за потпис се врши на основу одговарајућег захтева у следећој ситуацији:

- када је дошло до промене података у пољу Subject Alternative Name (алтернативно име корисника).

Ово није примењиво за електронски печат у оквиру ових Практичних правила.

4.8.2. Ко може захтевати модификацију квалификованог електронског сертификата

Модификацију квалификованог електронског сертификата може захтевати корисник електронског сертификата или овлашћена лица у оквиру регистрационог тела МО и ВС.

Ово није примењиво за електронски печат у оквиру ових Практичних правила.

4.8.3. Процесирање захтева за модификацијом квалификованог електронског сертификата

При пријему захтева за модификацију података корисника квалификованог електронског сертификата, овлашћено лице регистрационог тела МО и ВС, уз присуство корисника квалификованог електронског сертификата, врши модификацију података, извршену модификацију потписује својим приватним кључем и документ са квалификованим електронским сертификатом враћа кориснику.

Ово није примењиво за електронски печат у оквиру ових Практичних правила.

4.8.4. Обавештење корисника да му је издат нови модификовани квалификовани електронски сертификат

Током спровођења процеса модификације података квалификованог електронског сертификата, корисник квалификованог електронског сертификата мора бити присутан, те није потребно накнадно обавештавање о извршењу ове акције.

Ово није примењиво за електронски печат у оквиру ових Практичних правила.

4.8.5. Спровођење процеса прихватања новог модификованог квалификованог електронског сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.8.6. Објављивање новог модификованог квалификованог електронског сертификата од стране СА

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.8.7. Обавештење других ентитета од стране СА о издавању новог модификованог квалификованог електронског сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.9. Опозив, суспензија и реактивација квалификованог електронског сертификата

4.9.1. Услови за опозив квалификованог електронског сертификата корисника

Након одговарајућег захтева, Сертификационо тело МО и ВС врши опозив издатог квалификованог електронског сертификата у случају:

- Губитка, крађе, модификације, неауторизованог објављивања или неке друге компромитације приватног кључа корисника квалификованог електронског сертификата.
- Да је субјект квалификованог електронског сертификата нарушио материјалне обавезе које су дефинисане Политиком или у овом Практичним правилима.
- Да извршење одговарајућих обавеза лица која су наведена у Политици 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 информација које се садрже у квалификованом електронском сертификату корисника.
- Да се организациона јединица МО и ВС угасила или преформирала.

4.9.2. Ко може захтевати опозив квалификованог електронског сертификата

Опозив квалификованог електронског сертификата датог корисника може захтевати сам корисник, овлашћени службеник регистрационог тела МО и ВС или Сертификационог тела МО и ВС. Другим речима, захтев за опозивом квалификованог електронског сертификата може да поднесе власник квалификованог електронског сертификата, након прописне аутентикације, или одговарајући службеник Сертификационог тела МО и ВС или регистрационог тела МО и ВС уз доказ да је испуњен један од услова за опозив сертификата, наведен у 4.9.1.

4.9.3. Процедура захтева за опозивом квалификованог електронског сертификата

Ако се деси неки од горе поменутих догађаја, корисник мора што пре да контактира службеника регистрационог тела МО и ВС у циљу достављања захтева за опозивом квалификованог електронског сертификата. Поменути контакт може бити online или путем других канала комуникације.

Сертификационо тело МО и ВС опозива квалификовани електронски сертификат одмах након верификације идентитета стране која је захтевала опозив (службеник регистрационог тела МО и ВС) и потврдом да је захтев поднет у складу са процедуром захтеваном у Политици и у овом документу.

Верификација идентитета може бити извршена на основу информационих елемената који су садржани у идентификационим подацима које је корисник доставио регистрационом телу МО и ВС у оквиру процедуре за подношења захтева за еИД (електронску картицу за печат). Након испуњења поменутих услова, службеник регистрационог тела МО и ВС електронски преко апликације регистрационог тела подноси захтев за опозив сертификата, потом Сертификационо тело МО и ВС извршава промптну активност у циљу опозива квалификованог електронског сертификата.

Операција опозива сертификата подразумева следеће акције:

1. Упис серијског броја квалификованог електронског сертификата корисника у листу опозваних сертификата.
2. Промену стања квалификованог електронског сертификата корисника на *Опозван*.

4.9.4. Grace период захтева за опозив квалификованог електронског сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.9.5. Време за које CA мора да процесира захтев за опозив квалификованог електронског сертификата

Сертификационо тело МО и ВС опозива квалификовани електронски сертификат одмах након што добије захтев за опозивом од регистрационог тела МО и ВС.

4.9.6. Захтеви за треће стране у вези провере статуса квалификованог електронског сертификата

Треће стране морају проверити статус квалификованог електронског сертификата на који желе да се ослоне провером важеће CRL (CRL – Certificate Revocation List).

Треће стране морају бити у сагласности са Политиком, а посебно са обавезама трећих страна публикованим у Политици или овом документу.

4.9.7. Фреквенција издавања CRL листе

Листа опозваних сертификата Сертификационог тела МО и ВС које издаје квалификоване електронске сертификате ажурира се на свака 24 сата радним даном, а када после радног дана наступају нерадни дани ажурира се следећег радног дана. Листа опозваних сертификата за Root Сертификационо тела МО и ВС ажурира се на 12 месеци.

4.9.8. Максимално кашњење у издавању CRL листе

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.9.9. Расположивост процедуре online провере статуса квалификованог електронског сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.9.10. Захтеви online провере статуса квалификованог електронског сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.9.11. Расположивост других форми објављивања статуса квалификованог електронског сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.9.12. Специјални захтеви у односу на компромитацију приватног кључа

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.9.13. Услови за суспензију квалификованог електронског сертификата

Квалификовани електронски сертификат се суспендује у следећим ситуацијама:

- Суспензију квалификованог електронског сертификата захтева корисник или одговарајуће лице из Сертификационог тела МО и ВС или регистрационог тела МО и ВС.
- Корисник је прекршио одговарајућа правила коришћења квалификованог електронског сертификата.
- Суспензију квалификованог електронског сертификата захтева надлежни орган за заштиту података или неки други виши орган који има оправдане сумње да квалификовани електронски сертификат садржи неисправне податке или да се приватни кључ који одговара јавном кључу из квалификованог електронског сертификата може користити без сагласности власника квалификованог електронског сертификата.
- Суспензију квалификованог електронског сертификата захтева суд, тужилац или институције које врше криминалну истрагу да би спречили даљу или потенцијалну злоупотребу.
- У случају губитка еИД (електронске картице за печат), а на основу примљеног захтева од регистрационог тела МО и ВС, Сертификационо тело МО и ВС врши суспензију издатих квалификованих електронских сертификата. Захтев у овом случају доставља регистрационо тело МО и ВС оператер одговарајућом електронски потписаном поруком.

4.9.14. Ко може захтевати суспензију квалификованог електронског сертификата

Суспензију квалификованог електронског сертификата датог корисника може захтевати сам корисник, надлежни орган за заштиту података, овлашћени службеник регистрационог тела МО и ВС, Сертификационо тело МО и ВС, суд, тужилац или институције које врше криминалну истрагу.

4.9.15. Процедура захтева за суспензијом квалификованог електронског сертификата

Захтев за суспензијом квалификованог електронског сертификата сертификационом телу доставa оператер регистрационог тела МО и ВС преко апликације регистрационог ауторитета кроз одговарајућу електронско потписану поруку.

Лица и институције из тачке 4.9.14 подносе захтев за суспензијом квалификованог електронског сертификата захтев у писаној форми регистрационом телу МО и ВС. Регистрационо тело МО и ВС установљава валидност захтева и утврђује идентитет подносиоца захтева. Уколико је захтев валидан врши суспензију.

Операција суспензије сертификата је идентична опозиву с тим што се стање сертификата поставља на *Суспендован*.

4.9.16. Ограничење периода суспензије квалификованог електронског сертификата

Суспензија квалификованог електронског сертификата траје онолико дуго колико трају и услови због којих је суспензија и захтевана. Када ови услови престану да важе, корисник, односно подносилац захтева за опозивом квалификованог електронског сертификата, може захтевати реактивацију квалификованог електронског сертификата.

У случају да је еИД или електронска картица за печат нађен корисник може захтевати реактивацију квалификованог електронског сертификата који је био привремено суспендован.

Сертификационо тело МО и ВС публикује серијске бројеве свих опозваних и суспендованих квалификованих електронских сертификата у својој CRL листи и преко OCSP сервиса само у локалној рачунарској мрежи МО и ВС.

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

Квалификовани електронски сертификат се реактивира у следећим ситуацијама:

- Ако активирање квалификованог електронског сертификата захтева корисник или одговарајуће лице из Сертификационог тела МО и ВС или регистрационог тела МО и ВС на основу чијег је захтева извршена суспензија.
- Ако активирање квалификованог електронског сертификата захтева надлежни орган за заштиту података или неки други виши орган на основу чијег захтева је извршена суспензија.
- Ако активирање квалификованог електронског сертификата захтева суд, тужилац или институција која врши криминалну истрагу на основу чијег захтева је извршена суспензија,

под условом да се не нарушавају правила функционисања Сертификационог тела МО и ВС и безбедност система.

Операцију активирања квалификованог електронског сертификата из стања суспендован може да врши оператер регистрационог тела МО и ВС или одређена лица из Сертификационог тела МО и ВС. Она подразумева следеће акције:

1. Брисање серијског броја квалификованог електронског сертификата корисника из листе опозваних сертификата.
2. Промену стања квалификованог електронског сертификата корисника у LDAP-у на валидан и брисање истог из CRL.

4.10. Сервиси провере статуса сертификата

4.10.1. Оперативне карактеристике

Листа опозваних сертификата Сертификационог тела које издаје квалификоване електронске сертификате ажурира се на свака 24 сата радним даном, а када после радног дана наступају нерадни дани ажурира се следећег радног дана. Листа опозваних сертификата за Root Сертификационо тело МО и ВС ажурира се на 12 месеци.

Информација о статусу опозваности сертификата коришћењем OCSP сервиса доступна је у реалном времену само у локалној рачунарској мрежи МО и ВС.

4.10.2. Расположивост сервиса

Сервис за суспензију или опозив расположив је 24 сата 365 дана. Репозиторијум, односно локација на којој се налази CRL расположива је 24 сата 365 дана. OCSP сервис расположив је 24 сата 365 дана.

4.10.3. Опциона обележја

Ово поглавље није применљиво у оквиру ових Практичних правила.

4.11. Престанак коришћења квалификованог електронског сертификата

Након престанка коришћења квалификованог електронског сертификата издатог од стране Сертификационог тела МО и ВС, дати квалификовани електронски сертификат мора бити опозван.

Престанак коришћења квалификованог електронског сертификата може бити из следећих разлога:

- Уколико корисник није користио квалификовани електронски сертификат у складу са правилима дефинисаним у Политици и Практичним правилима.
- Престанак радног односа по било ком основу.
- У случају губитка права која проистичу из положаја и радног места (суспензија, дисциплински поступак, судски поступак, ...).
- У случају смрти корисника квалификованог електронског сертификата.
- У случају гашења или преформирања организационе јединице МО и ВС.
- Сертификационо тело МО и ВС 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

Приватни кључ корисника којим се врши квалификовани електронски потпис или печат се нигде не чува изузев на смарт картици корисника (еИД, електронска картица за печат).

Реконструкција приватног кључа није применљива у оквиру ових Практичних правила.

4.12.2. Енкапсулација сесијског кључа и политика и пракса за реконструкцију

Ово поглавље није примењиво у оквиру ових Практичних правила.

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 Сертификационог тела МО и ВС као подршка у циљу реализације функција генерисања кључева, аутентикације субјеката, издавања квалификованог електронског сертификата, опозива квалификованог електронског сертификата, audit-а и архивирања.

Ове не-техничке безбедносне контроле су критичне за поверење у квалификоване електронске сертификате издате од стране Сертификационог тела МО и ВС пошто недостатак безбедности може компромитовати оперативни рад Сертификационог тела МО и ВС резултујући на пример у креирању квалификованих електронских сертификата и CRL са погрешним информацијама или компромитацијом приватног кључа Сертификационог тела МО и ВС.

5.1. Физичке безбедносне контроле

Сертификационо тело МО и ВС имплементира одговарајуће механизме физичке контроле у својим просторијама.

5.1.1. Локација и конструкција сајта

Сертификационог тело МО и ВС се налази у просторијама Центра за примењену математику и електронику у Београду.

Безбедне просторије Сертификационог тела МО и ВС су лоциране у простору који одговара потребама извршења операција високе безбедности. Постоје означене зоне са физичком контролом приступа и закључане канцеларије са одговарајућим касама.

5.1.2. Физички приступ

Приступ просторијама Сертификационог тела МО и ВС је омогућен само овлашћеном особљу.

Физички приступ је ограничен имплементацијом одговарајућих механизама контроле приступа из једне у другу зону безбедности, као и у зону високе безбедности. У том смислу, операције Сертификационог тела МО и ВС су лоциране у оквиру безбедне рачунарске собе (Фарадејев кавез), која је подржана физичким надгледањем.

5.1.3. Електрично напајање и климатизација

Сва опрема Сертификационог тела МО и ВС је прикључена на јединице за непрекидно напајање.

Температура и влажност ваздуха се у просторијама одржава у оквиру унапред специфицираног опсега помоћу клима уређаја.

Напајање се извршава са редудансом високог нивоа.

5.1.4. Изложеност поплавама и временским непогодама

Унутар просторија Сертификационог тела МО и ВС нема водоводних инсталација.

Просторије Сертификационог тела МО и ВС су заштићене од поплава.

5.1.5. Превенција и заштита од пожара

Превенција и заштита од пожара су имплементиране.

Просторије Сертификационог тела МО и ВС су опремљене детекторима дима и противпожарним апаратима.

5.1.6. Медијуми за чување података

Медијуми се чувају на безбедан начин. Backup медијуми се чувају на одвојеној локацији која је физички обезбеђена.

5.1.7. Одлагање смећа

Изношење смећа се контролише.

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

5.1.8. Одлагање резервних копија

Ово поглавље није применљиво у оквиру ових Практичних правила.

5.2. Процедуралне контроле

Сертификационо тело МО и ВС иницира 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/печат и PKI системе.

Сваки запослени у Сертификационом телу МО и ВС 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 који обављају послове у Сертификационом телу МО и ВС, а 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 Сертификационом телу МО и ВС, између осталих, су:

- Администратор безбедности,
- Систем администратори и

- Оператери.

ЦПМЕ у коме се налази организациона јединица која ради послове Сертификационог тела МО и ВС иницира преко надлежних органа безбедоносну проверу свих запослених који су кандидати за поверљиве улоге у циљу стицања увида у њихову поверљивост.

5.2.2. Број особа које се захтевају по сваком задатку

За поједине задатке може се захтевати да буду извршавани од стране више од једног запосленог.

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 Сертификационог тела МО и ВС дефинисано је које улоге/дужности могу бити комбиноване од стране једног запосленог, а које то не смеју.

Тамо где се захтева вишеструка контрола примењује се процедура где је потребно да најмање m од n поверљивих запослених у Сертификационом телу МО и ВС искажу своја подељена знања у циљу омогућавања извршења безбедносно осетљивих операција.

5.3. Кадровске безбедносне контроле

5.3.1. Квалификација и искуство

Од надлежних органа захтева се извршење неопходних активности у циљу провере биографије, квалификација, као и неопходног искуства у циљу реализације у оквиру контекста компетенције специфичног посла. Такве провере биографије типично укључују:

- Проверу да ли је лице правоснажно осуђивано;
- Погрешне презентације информација од стране кандидата;
- Одговарајуће референце.

За рад у Сертификационом телу МО и ВС су неопходни стручњаци који су технолошки и професионално компетентни и који имају потребна знања из криптографије, електронског потписа, PKI система, смарт картица, HSM-ова, итд..

5.3.2. Процедура провере биографије

Преко надлежног органа захтева се реализација одговарајуће 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

Спроводи се и обезбеђује обука за лица која раде послове Сертификационог тела, а у циљу реализације функција пословања Сертификационог тела МО и ВС.

5.3.4. Фреквенција и захтеви за поновну обуку

Периодично ажурирање обуке се врши 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 Практичних правила.

5.3.6. Казнене мере за неовлашћене активности

Постоје одговарајуће мере које се спроводе према лицима која обављају послове у Сертификационом телу: за неовлашћене активности, неовлашћено коришћење ауторитета, као и неовлашћено коришћење система у циљу спровођења санкција за одређено непословно и ризично понашање, које може бити различито у зависности од различитих околности.

5.3.7. Документација која се доставља запосленима

Запосленима је доступна сва документација која се односи на Сертификационо тело МО и ВС, а за потребе иницијалне обуке, дообуке или за друге сврхе.

5.4. Процедуре безбедносних провера логова auditing

Сертификационо тело МО и ВС има систем за логовање догађаја и систем за праћење догађаја. Ови системи су имплементирани за сврху одржавања безбедног окружења. У том смислу, Сертификационо тело МО и ВС имплементира контроле наведене у наредном тексту.

5.4.1. Типови забележених догађаја

Сертификационо тело МО и ВС 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

Сертификационог тела МО и ВС чува аудит логове (дневничке записе) у реалном времену, који се касније процесирају и архивирају на седмичном нивоу.

5.4.3. Период чувања аудит логова

Сертификационо тело МО и ВС процесира и архивира аудит логове на седмичном нивоу, који се трајно чувају.

5.4.4. Заштита аудит логова

Аудит логови се могу видети само од стране ауторизованог особља.

5.4.5. Процедуре backup-а аудит логова

Сертификационо тело МО и ВС имплементира процедуре backup-а аудит логова.

5.4.6. Систем сакупљања аудит логова

Сертификационог тело МО и ВС сакупља и чува аудит логове у реалном времену.

5.4.7. Обавештење субјекта који је проузроковао догађај

У случају аларма или инцидентног догађаја, обавештава се администратор безбедности Сертификационог тела МО и ВС.

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

5.4.8. Оцена рањивости система

Сертификационо тело МО и ВС реализује с времена на време, а најмање једном годишње, процену рањивости система.

5.5. Архивирање записа/логова

Опште политике чувања записа Сертификационог тела МО и ВС укључују одредбе наведене у наставку текста.

5.5.1. Типови архивираних записа

Сертификационо тело МО и ВС на безбедан начин чува записе о издатим квалификованим електронским сертификатима, auditing подацима, информације о апликацијама за издавање сертификата, као и документацију о самим апликацијама за издавање сертификата.

5.5.2. Период чувања архиве

Сертификационог тела МО и ВС чува на безбедан начин поменуте записе о квалификованим електронским сертификатима за период који је назначен у Закону и одговарајућем подзаконском акту.

5.5.3. Заштита архиве

Услови за заштиту архиве укључују:

- Записе које само систем аудитори (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

Сертификационо тело МО и ВС спроводи одговарајућу процедуру backup-а архиве.

Сертификационо тело МО и ВС реализује захтеве за процедуром чувања барем две одвојене копије архиве које су под контролом две различите особе.

5.5.5. Захтеви за timestamping записа

Ово поглавље није применљиво у оквиру ових Практичних правила.

5.5.6. Систем сакупљања записа

Сертификационо тело МО и ВС спроводи одговарајући систем сакупљања записа/логова који се архивирају.

5.5.7. Процедуре за добијање и верификацију информација из архиве

У оквиру Сертификационог тела МО и ВС, дефинисане су процедуре у циљу добијања и верификације архивских информација.

У циљу добијања и верификације архивских информација, Сертификационо тело МО и ВС и регистрационо тело МО и ВС одржава записе под јасном хијерархијском контролом и са јасним описом посла. Сертификационо тело МО и ВС чува записе у електронској или папирној форми.

Сертификационо тело МО и ВС може захтевати од 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 Сертификационо тело МО и ВС сматра одговарајућом.

Сертификационо тело МО и ВС може да измени начин чувања записа ако је то евентуално потребно да буде у сагласности са одговарајућом акредитацијом и супервизорном шемом коју спроводи Надлежни орган за акредитацију у супервизију PKI система у Републици Србији.

5.6. Измена кључева

У случају истека или опозива електронског сертификата Сертификационог тела у складу са условима дефинисаним у овом документу Сертификационо тело МО и ВС врши генерисање новог пара кључева и електронског сертификата Сертификационог тела МО и ВС

Сертификационо тело МО и ВС омогућује дистрибуирање свог електронског сертификата свим корисницима и заинтересованим странама, као и у случају првог генерисаног електронског сертификата.

У случају истека или опозива квалификованог електронског сертификата корисника врши се генерисање новог пара кључева и квалификованог електронског сертификата и његова дистрибуција кориснику као и у случају првог генерисаног квалификованог електронског сертификата у складу са процедуром описаном у Политици и у овом документу.

5.7. Компромитација и опоравак у случају катастрофе

5.7.1. Процедуре за поступање у инцидентним и компромитујућим ситуацијама

У Посебним правилима рада, Сертификационо тело МО и ВС документује процедуре које треба извршити при решавању инцидената, као и извештавања у вези са евентуалном компромитацијом кључева Сертификационог тела МО и ВС.

5.7.2. Рачунарски ресурси, софтвер или подаци који су оштећени

У Посебним правилима рада, Сертификационо тело МО и ВС документује процедуре опоравка које се користе уколико су рачунарски ресурси, софтвер, и/или подаци неисправни или се сумња да су неисправни.

5.7.3. Процедуре које се спроводе код компромитације приватног кључа корисника

Сертификационо тело МО и ВС тежи да поново успостави безбедно окружење у корацима који укључују, али нису ограничени само на, опозив неисправних, или се сумња да су неисправни, сертификата одговарајућих ентитета. Након тога, Сертификационо тело МО и ВС може поново издати нови квалификовани електронски сертификат датом ентитету.

5.7.4. Могућности континуитета пословања након катастрофе

Сертификационо тело МО и ВС у случају природне или друге катастрофе имплементира мере које омогућавају континуиран рад сервиса у ограниченом обиму. Наставак пословања ће обезбедити сходно насталој ситуацији.

5.8. Завршетак рада Сертификационог тела МО и ВС

Пре него што прекине своје активности пружања сертификационих услуга, Сертификационо тело МО и ВС:

- Обезбеђује својим корисницима који имају валидне квалификоване електронске сертификате обавештење о намери да престане са пружањем сертификационе услуге, тј. да престане да извршава активности у својству Сертификационог тела.

- На основу захтева регистрационог тела МО и ВС опозива све квалификоване електронске сертификате који су још увек валидни (тј. оне који нису опозвани или им није истекао рок важности) након обавештења, а без захтева за сагласношћу корисника.
- Регистрационо тело МО и ВС благовремено обавештава о опозиву квалификованог електронског сертификата све кориснике на које се то односи.
- Чини разумне мере у циљу заштите записа које чува у складу са Политиком и овим Практичних правила.

Уколико је то могуће, обезбеђује одговарајуће мере за обезбеђење сукцесије у смислу поновног издавана квалификованог електронског сертификата од стране другог Сертификационог тела које је sukcesor – настављач издавања квалификованог електронског сертификата датог Сертификационог тела – и које поштује исту Политику, као и иста Практична правила.

6. Техничке безбедносне контроле

Ово поглавље дефинише техничке безбедносне мере које примењује Сертификационо тело МО и ВС у циљу заштите криптографских кључева и активационих података (као на пример PIN-ови, лозинке, итд.).

Безбедносно управљање кључевима Сертификационог тела МО и ВС 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 Сертификационог тела МО и ВС да се безбедно извршавају функције генерисања кључева, аутентикације корисника, регистрације корисника, издавања квалификованог електронског сертификата, опозива квалификованог електронског сертификата, auditinga 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

Сертификационо тело МО и ВС 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. Сертификационо тело МО и ВС имплементира и документује процедуре генерисања кључева у складу са Политиком и овим Практичним правилима.

Сертификационо тело МО и ВС примењује јавне, међународне стандарде у вези безбедних и поузданих система.

Сертификационо тело МО и ВС генерише следеће асиметричне парове кључева:

- За потребе Root Сертификационог тела МО и ВС – асиметрични пар кључева се генерише на хардверском безбедносном модулу (HSM – Hardware Security Module).
- За потребе Intermediate Сертификационог тела МО и ВС – асиметрични пар кључева се генерише на хардверском безбедносном модулу.
- За потребе корисника – за електронски потпис/печат – овај асиметрични пар кључева се генерише на електронској картици корисника (SSCD уређају) и никада га не напушта.

Сертификационо тело МО и ВС користи безбедан процес генерисања свог Root приватног кључа у складу са документованом процедуром.

Приватни кључ Root Сертификационог тела МО и ВС се користи за електронско потписивање: електронских сертификата Сертификационог тела МО и ВС (пре свега за издавање електронског сертификата Intermediate Сертификационог тела МО и ВС) и листе

опозваних електронских сертификата. Друге сврхе коришћења приватног кључа Root Сертификационог тела МО и ВС су забрањене.

6.1.2. Испорука приватног кључа кориснику

Сертификационо тело МО и ВС испоручује приватни кључ кориснику на електронској картици корисника (SSCD уређају), односно на електронском идентификационом документу и електронској картици за печат.

6.1.3. Достава јавног кључа до издавача сертификата

Корисник не генерише пар асиметричних криптографских кључева, а тиме и не доставља јавни кључ до издавача сертификата. Јавни кључ се генерише у поступку персонализације еИД или електронске картице за печат.

Достављање захтева за издавање квалификованог електронског сертификата крајњег корисника у PKCS#10 формату врши оператер регистрационог тела МО и ВС који пре слања захтева врши проверу идентитета подносиоца захтева и истинитост података из припремљеног захтева.

Оператер регистрационог тела МО и ВС електронски потписује захтев на бази свог приватног кључа који се налази на службеном електронском идентификационом документу и припрема поруку коју шаље Сертификационом телу МО и ВС.

6.1.4. Достава јавног кључа издаваоца сертификата трећим странама

Сертификационо тело МО и ВС може да доставља своје јавне кључеве Root Сертификационог тела МО и ВС и Intermediate Сертификационог тела МО и ВС, у облику X.509v3 сертификата путем репозиторијума коме могу да приступају треће стране.

6.1.5. Дужине кључева

За потребе свог RSA приватног кључа Root Сертификационог тела МО и ВС и одговарајуће потписивање, Сертификационо тело МО и ВС користи SHA256/RSA комбинацију hash и асиметричног алгоритма, при чему се користи дужина кључа од 4096 бита и период валидности сертификата од 20 година.

За потребе својих ECC Root приватних кључева и одговарајуће потписивање, Сертификационо тело МО и ВС користи SECP521R1 алгоритам и SHA512withECDSA hash, при чему се се користи дужина кључа од 521 бита и период валидности сертификата од 20 година.

За потребе приватног кључа RSA подређених сертификационих тела и одговарајућег алгоритма за квалификовано електронско потписивање, Сертификационо тело МО и ВС користи SHA256/RSA, комбинацију hash и асиметричног алгоритма са дужином кључа од 3072 бита и периодом валидности сертификата од 10 година.

За потребе приватног кључа ECC подређених сертификационих тела и одговарајућег алгоритма за квалификовано електронско потписивање, Сертификационо тело МО и ВС

користи SECP521R1 алгоритам и SHA384withECDSA hash, са дужином кључа од 384 бита и периодом валидности сертификата од 10 година.

Сертификационо тело МО и ВС ће извршити 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 криптографске алгоритме или уколико законодавац другачије наложи.

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 хардверским криптографским уређајима, и то:

- HSM – за кључеве Сертификационог тела МО и ВС и
- еИД и електронска картица за печат (SSCD уређај) - за кључеве корисника за потребе квалификованог електронског потписа и печата, респективно.

Квалитет начина генерисања поменутих криптографских параметара искључиво зависи од квалитета хардверског генератора случајних бројева на HSM-овима и SSCD уређаја.

6.1.7. Могуће „Key Usage" опције

У електронским сертификатима Root Сертификационог тела МО и ВС и Intermediate Сертификационог тела МО и ВС, као и квалификованим електронским сертификатима (кориснички сертификати) издатим од стране Сертификационог тела МО и ВС користе се следеће вредности у екстензији „Key Usage“:

Електронски сертификат Root Сертификационог тела МО и ВС:

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

Електронски сертификат Intermediate Сертификационог тела МО и ВС:

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

Квалификовани електронски сертификат за квалификовани електронски потпис/печат корисника:

- Digital Signature, Non-Repudiation

6.2. Заштита приватног кључа и контрола криптографског хардверског модула

Сертификационо тело МО и ВС користи одговарајуће криптографске уређаје у циљу реализације задатака управљања и заштите кључева Сертификационог тела МО и ВС. Поменути криптографски уређаји су познати под именом Хардверски криптографски модули (Hardware Security Module - HSM).

6.2.1. Стандарди и контроле криптографског хардверског модула

Генерисање приватног кључа Сертификационог тела МО и ВС се дешава у оквиру безбедног криптографског уређаја који задовољава одговарајуће захтеве у складу са међународним стандардом Common Criteria EAL4+ (CWA 14169). Овај стандард гарантује, између осталог да је било који покушај нарушавања интегритета уређаја или криптографске меморије истовремено детектован, и да приватни кључеви не могу да напусте уређај.

HSM уређаји не смеју да напуштају просторије Сертификационог тела МО и ВС изузев ретких прилика унапред дефинисаних премештања и пресељења. Сертификационо тело МО и ВС чува записе у вези свих тих премештања или пресељења.

6.2.2. k од n дистрибуција одговорности контроле приватног кључа

Процедура чувања приватног кључа Сертификационог тела МО и ВС захтева вишеструке контроле од стране, на одговарајући начин ауторизованог особља. Ауторизација процедуре чувања кључева и ауторизација одговарајућег особља мора бити извршена од стране више од једног члана управне структуре.

У процедури дељења тајни Сертификационо тело МО и ВС користи вишеструке ауторизоване носиоце у циљу да заштити и побољша поверљивост приватних кључева и обезбеди одговарајућу процедуру опоравка кључа.

Приватни кључ Сертификационог тела МО и ВС се користи под условима дефинисаним у оквиру **k** од **n** контроле од стране више запослених са поверљивим улогама.

Носиоци дељених тајни (n носилаца) Сертификационог тела МО и ВС имају задатак да активирају и деактивирају приватни кључ. Након активације приватног кључ он постаје активиран у дефинисаном времену.

Носилац дељене тајне је лично упознат са креирањем, поновним креирањем и дистрибуцијом тајне на његовог следећег члана ланца поверљивости.

Носилац дељене тајне може примити дељену тајну на физичком медијуму који је одобрен за коришћење од Сертификационог тела МО и ВС. Сертификационо тело МО и ВС чува записе у вези дистрибуције дељене тајне.

6.2.3. Безбедно чување приватног кључа

Сертификационо тело МО и ВС користи безбедни криптографски уређај да чува своје приватне кључеве у складу са захтевима исказаним у стандарду Common Criteria EAL4+(CWA 14169).

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

6.2.4. Backup приватног кључа

Приватни кључеви Сертификационог тела МО и ВС backup-ује се у складу са процедуром дефинисаном у интерним правилима рада Сертификационог тела МО и ВС. У процедури backup-а, користе се процедуре backup-а кључа које су подржане од стране датог HSM уређаја.

Заштићене копије приватног кључа Сертификационог тела МО и ВС се чувају на екстерној меморији (флеш меморија, ЦД, ...), на сигурном месту и у шифрованом облику.

6.2.5. Архивирање приватног кључа

Backup-ован приватни кључ Сертификационог тела МО и ВС се архивира према процедури описаној у Посебним интерним правилима рада Сертификационог тела МО и ВС.

6.2.6. Трансфер приватног кључа на хардверски криптографски модул

Процедура безбедног експортовања приватног кључа Сертификационог тела МО и ВС у циљу backup-а, као и процедура безбедног импорта архивираног приватног кључа на HSM су описане у Посебним интерним правилима рада Сертификационог тела МО и ВС.

6.2.7. Чување приватног кључа на хардверском криптографском модулу

Када се приватни кључ Сертификационог тела МО и ВС налази и користи на HSM уређају, он се чува у шифрованом облику у меморији HSM уређаја.

6.2.8. Метода активације приватног кључа

Оператер са посебним овлашћењима има задатак да активира приватни кључ. Приватни кључ је активан у дефинисаном периоду времена.

Сваком коришћењу приватног кључа Сертификационог тела МО и ВС претходи уношење тајног податка од стране оператера и коришћење његове службене смарт картице.

6.2.9. Метода деактивирања приватног кључа

Оператер са посебним овлашћењима има задатак да деактивира приватни кључ.

6.2.10. Метода уништења приватног кључа

Приватни кључ Сертификационог тела МО и ВС се не обнавља.

Приватни кључ Сертификационог тела МО и ВС ће бити уништен на крају свог животног циклуса.

Приватни кључеви Сертификационог тела МО и ВС се уништавају на крају њиховог животног века у циљу гаранције да они неће никада бити поново активирани и коришћени.

Приватни кључеви Сертификационог тела МО и ВС и његови дељени делови се уништавају на начин који онемогућава њихову реконструкцију.

Процес уништавања кључева је документован у Посебним интерним правилима рада и одговарајући записи се архивирају.

Након генерисања новог асиметричног пара кључева и новог сертификата Сертификационог тела МО и ВС, претходни приватни кључ се брише из HSM-а, а резервне копије се уништавају на најсигурнији могући начин (дефинисан у Посебним интерним правилима).

Приватни кључеви корисника на електронском идентификационом документу уништавају се бушењем контактног микроконтролера.

6.2.11. Рангирање криптографских хардверских модула

Ово поглавље није применљиво у оквиру ових Практичних правила.

6.3. Други аспекти управљања паром кључева

6.3.1. Архивирање јавног кључа

Сертификационо тело МО и ВС архивира свој сопствени јавни кључ.

6.3.2. Периоди валидности сертификата и приватног кључа

Сертификационо тело МО и ВС издаје корисничке квалификоване електронске сертификате за периодом коришћења као што је назначено у самим квалификованим електронским сертификатима.

Период важења квалификованих електронских сертификата на електронским идентификационим документима са чипом се поклапа са периодом валидности самог еИД (5 година).

Време валидности приватног кључа Root Сертификационог тела МО и ВС је 10 година, док је сам Root сертификат Сертификационог тела МО и ВС валидан 20 година.

Време валидности приватног кључа Intermediate Сертификационог тела МО и ВС је 5 година – док је сам сертификат Intermediate Сертификационог тела МО и ВС валидан 10 година.

6.4. Активациони подаци

6.4.1. Генерисање и инсталација активационих података

Сертификационо тело МО и ВС безбедно процесира активационе податке придружене приватним кључевима Сертификационог тела МО и ВС, као и свим другим приватним кључевима у датом PKI систему.

6.4.2. Други аспекти у вези активационих података

Ово поглавље није применљиво у оквиру ових Практичних правила.

6.5. Безбедносне контроле рачунара

6.5.1. Специфични захтеви за безбедност рачунара

Сертификационо тело МО и ВС имплементира специфичне безбедносне контроле над рачунарима који се користе у оквиру датог PKI система.

Рачунари који се користе у оквиру Сертификационог тела МО и ВС 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 Сертификационог тела МО и ВС није дозвољен. Сертификационо тела МО и ВС могу стартовати само овлашћене особе која поседују одговарајућу смарт картицу и њој придружен PIN.

6.5.2. Рангирање безбедности рачунара

Ово поглавље није применљиво у оквиру ових Практичних правила.

6.6. Животни циклус техничких безбедносних контрола

6.6.1. Контроле развоја система

Сертификационо тело МО и ВС реализује периодичне развојне управљачке контроле.

6.6.2. Контроле управљања безбедношћу

Сертификационо тело МО и ВС реализује периодичне безбедносне управљачке контроле.

6.6.3. Животни циклус безбедносних контрола

Ово поглавље није применљиво у оквиру ових Практичних правила.

6.7. Мрежне безбедносне контроле

Сертификационо тело МО и ВС одржава и примењује висок ниво система мрежне безбедности, укључујући примену firewall уређаја.

6.8 Временски печат

Ово поглавље није применљиво у оквиру ових Практичних правила.

7. Профили сертификата и CRL листа

Ово поглавље специфицира формате сертификата и CRL листа које издаје Сертификационо тело МО и ВС, а у циљу омогућавања животног циклуса квалификованог електронског сертификата.

7.1. Профили сертификата

Сертификационо тело МО и ВС издаје следеће врсте сертификата:

- Сертификате Root Сертификационих тела МО и ВС
- Сертификате Intermediate Сертификационих тела МО и
- Квалификовани електронски сертификат за кориснике:
  - запослене у МО и ВС,
  - ученике и студенте војних школа и
  - организационе јединице МО и ВС.

7.1.1. Број верзије

Сертификационо тело МО и ВС 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 Сертификационог тела МО и ВС су наведени у наставку.

Општи профил сертификата

У следећој табели приказан је општи профил електронских сертификата Сертификационог тела МО и ВС:

Име профила	Општи профил	
Период валидности сертификата	1 – 20 година	
Basic Constraints Екстензија	End Entity | CA, Path length=x	
Чување кључева	Смарт картица | HSM	
Заједничке екстензије	Authority Key Identifier Subject Key Identifier Authority Information Access CRL Distribution Point	
Дужина кључева	RSA -4096, 3072; ECC – 521, 384	
Key Usage екстензија – могуће вредности	Digital Signature Non-Repudiation Key Encipherment	Certificate Signing CRL Signing
Enhanced Key Usage Екстензија – могуће вредности	Client Authentication Server Authentication Email Protection	

	Microsoft Smart Card Logon
QC (Qualified Certificate) статемент екстензија	OID екстензије (1.3.6.1.5.5.7.1.3) са стандардним вредностима

Детаљан приказ сертификата дат је у документима „Преглед профила сертификата за Root и подчињена RSA CA тела МО и ВС“ и „Преглед профила сертификата за Root и потчињена ECC CA тела МО и ВС“.

Профил сертификата Root Сертификационог тела МО и ВС

У следећој табели приказан је профил електронског сертификата Root Сертификационог тела МО и ВС:

Име профила	Root CA
Период валидности цертификата	20 година
Екстензија основних ограничења	CA
Чување кључева	HSM
Заједничке екстензије	Subject Key Identifier
Применљива дужина кључева	RSA – 4096; ECC - 521
Екстензија коришћења кључа	Certificate Signing Off-Line CRL signing CRL Signing CRL Distribution Point

Детаљан приказ сертификата дат је у документима „Преглед профила сертификата за Root и подчињена RSA CA тела МО и ВС“ и „Преглед профила сертификата за Root и потчињена ECC CA тела МО и ВС“.

Профил сертификата Intermediate Сертификационог тела МО и ВС

У следећој табели приказан је профил сертификата Intermediate Сертификационог тела МО и ВС:

Име профила	Intermediate CA
Период валидности цертификата	10 година
Екстензија основних ограничења	CA
Чување кључева	HSM
Заједничке екстензије	Authority Key Identifier Subject Key Identifier Authority Information Access CRL Distribution Point
Применљива дужина кључева	RSA – 3072; ECC - 384

Екстензија коришћења кључа	Certificate Signing Off-Line CRL signing CRL Signing

Детаљан приказ сертификата дат је у документима „Преглед профила сертификата за Root и подчињена RSA CA тела МО и ВС“ и „Преглед профила сертификата за Root и потчињена ECC CA тела МО и ВС“.

Профил сертификата крајњих корисника намењен за квалификовани електронски потпис и печат

Профил сертификата за квалификовани електронски потпис и печат намењен је за крајње кориснике МО и ВС.

Профил сертификата за квалификовано електронско потписивање/печаћење треба да послужи као шаблон за генерисање сертификата за потребе верификације квалификованог електронског потписа/печата.

У следећој табели приказан је профил сертификата за потребе верификације квалификованог електронског потписа/печата.

Име профила	**Сертификати крајњих корисника**
Период валидности цертификата	5 година
Екстензија основних ограничења	End Entity
Чување кључева	Смарт картица - SSCD
Заједничке екстензије	Authority Key Identifier Subject Key Identifier Authority Information Access CRL Distribution Point
Применљива дужина кључева	RSA – 3072, 2048; ECC - 384
Екстензија коришћења кључа	Digital Signature Non-Repudiation
Екстензија напредног коришћења кључа	Email Protection (1.3.6.1.5.5.7.3.4)
QC (Qualified Certificate) статемент екстензија	OID екстензије (1.3.6.1.5.5.7.1.3) са стандардним вредностима укључујући SSCD екстензију

Детаљан приказ сертификата дат је у документима „Преглед профила сертификата за Root и подчињена RSA CA тела МО и ВС“ и „Преглед профила сертификата за Root и потчињена ECC CA тела МО и ВС“.

7.1.3. Објектни идентификатори алгоритама

Сертификационо тело МО и ВС у сертификатима које издаје користи комбинацију алгоритама:

- **SHA256/RSA** са OID-ом: **1.2.840.113549.1.1.11**
- **SHA384withECDSA** са OID-ом: **1.2.840.10045.4.3.3**

Међутим, Сертификационо тело МО и ВС подржава имплементацију било којих комбинација hash и асиметричног криптографског алгоритма.

7.1.4. Форме имена

За потребе профила квалификованог електронског сертификата корисника, обавезно је унети следеће податке:

- За сертификат за електронски потпис (физичка лица):
  - Име и презиме.
  - Назив организације у којој корисник ради.
  - ЈМБГ корисника или .
- За сертификат за електронски печат (организационе јединице):
  - Назив организационе јединице
  - Шифра организационе јединице.

За потребе профила квалификованог електронског сертификата, ови подаци се могу прилагодити сходно типу корисника на кога се односе.

На овај начин, у DN пољу изгенерисаног квалификованог електронског сертификата од стране Сертификационог тела МО и ВС за датог корисника је следећи садржај:

- CN = вредност дефинисана у следећем поглављу,
- O = Организација,
- C = Земља у којој организација има седиште.

7.1.5. Ограничења имена

Ограничења која се односе на имена корисника у квалификованим електронским сертификатима проистичу из подзаконског акта Закона, а користиће се све до прилагођавања условима из Правилника о условима које морају да испуњавају квалификовани електронски сертификати ("Службени гласник РС", број 34/18 и 26/18).
У наставку су наведена поменута ограничења.

- Поље „subject" квалификованог електронског сертификата мора да има атрибут „commonName ".
- У атрибут „commonName" сертификата за електронски потпис треба да буде уписано пуно име и презиме потписника, јединствени идентификатор потписника унутар сертификационог тела и ЈМБГ или деперсо број из базе Сертификационог тела МО и ВС. Подаци се уписују следећим редом: име, размак, презиме, размак, јединствени идентификатор унутар сертификационог тела, цртица, јединствени идентификатор унутар регистрационог ауторитета и на крају цртица и „узк". За атрибут „commonName" треба користити UTF8String кодирање, тако да сва слова из имена и презимена буду верно представљена одговарајућим карактерима.
- У атрибут „commonName" сертификата за електронски печат треба да буде уписан пун назив организационе јединице, јединствени идентификатор потписника унутар сертификационог тела. Подаци се уписују следећим редом: назив организационе

јединице, размак, јединствени идентификатор унутар сертификационог тела. За атрибут „commonName“ треба користити UTF8String кодирање, тако да сва слова из назива организационе јединице буду верно представљена одговарајућим карактерима.

- Сертификационо тело МО и ВС 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 Политике и Практичних правила која се користи при издавању сертификата у оквиру PKI МО и ВС.

Формат структуре OID-а је следећи:

1.3.6.1.4.1.42922.10.а.б. (е.ф.).ц.д. (г.х.)

Број 1.3.6.1.4.1 представља општи префикс за private-enterprise број са сајта:

http://www.iana.org/assignments/smi-numbers,

42922 је Private Enterprize Number (PEN) додељен Министарству одбране и Војсци Србије.

10 – односи се на организацију Сертификационо тело МО и ВС

Слова иза Организације имају следећа предложена значења:

а. Тип објектног идентификатора
1–Документација
2– Сертификациона тела
3–TSP сервиси

б. Тип документа
1 – Политика пружања услуга од поверења (CP - Certificate Policy)
(е.ф.) – односи се на верзију CP
2 – Практична правила рада (CPS - Certificate Practice Statement)

ц. Подтип документа Практичних правила рада
1 – Практична правила рада за пружање квалификоване услуге издавања квалификованих електронских сертификата за квалификовани електронски потпис/печат
2 – Практична правила рада за пружање квалификоване услуге валидације електронских потписа/печата
3 – Практична правила рада за пружање квалификоване услуге издавања квалификованог електронског временског жига
(г.х.) – односи се на верзију Практичног правила
4 – Практична правила рада за пружање квалификоване услуге издавања квалификованих електронских сертификата за аутентикацију Web сајтова

7.2. Профил CRL листе

У складу са IETF RFC 5280, Сертификационо тело МО и ВС 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 CRL (Certificate Revocation List) листе је приказан у следећој табели:

<table>
<tr><td>Version</td><td colspan="2">[Version 2]</td></tr>
<tr><td>Issuer Name</td><td colspan="2">CountryName=RS,
OrganizationName=Ministarstvo odbrane i Vojska Srbije,
commonName= *
Location=Beograd</td></tr>
<tr><td>Effective date</td><td colspan="2">[Date of Issuance]</td></tr>
<tr><td>Next Update</td><td colspan="2">[Date of Issuance + 26 hours]</td></tr>
<tr><td>Signature Algorithm identifier</td><td colspan="2">RSA - Sha256RSA; ECC - SHA384withECDSA</td></tr>
<tr><td>Authority Key identifier</td><td colspan="2"></td></tr>
<tr><td>CRL Number</td><td colspan="2">Redni broj CRL liste</td></tr>
<tr><td rowspan="3">Revoked sertificates</td><td colspan="2">CRL Entries</td></tr>
<tr><td>Sertificate Serial Number</td><td>Date and Time of Revocation</td></tr>
<tr><td>[Sertificate Serial Number]</td><td>[Date and Time of Revocation]</td></tr>
</table>

* commonName сертификационог тела које је генерисало CRL

7.2.1. Број верзије

Сертификационо тело МО и ВС генерише и објављује CRL листе верзије 2 (X.509v2).

7.2.2. CRL и CRL entry екстензије

CRL листа која се издаје од стране Сертификационог тела МО и ВС 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

Профил одговора OCSP сервиса усаглашен је са документом IETF RFC 6960.

7.3.1. Број верзије

Профил одговора OCSP сервиса је у складу са верзијом 1 према документу IETF RFC 6960.

7.3.2. OCSP екстензије

OCSP сервис користи следеће екстензије:

- Nonce – Вредност Nonce из захтева за статус сертификата
- Extended Revoked Definition – Код разлога опозива сертификата (Reason code)

8. Провера сагласности и друга оцењивања

8.1. Фреквенција или услови оцењивања

Сертификационо тело МО и ВС прихвата периодичну проверу сагласности својих Политика, укључујући ова Практична правила.

Рад Сертификационог тела МО и ВС је такође у сагласности са најважнијим међународним и Европским стандардима у овој области, као и са Европском директивом eIDAS (electronic ID and Services) из 2017. године.

У домену издавања квалификованих електронских сертификата, Сертификационо тело МО и ВС ради у оквиру ограничења дефинисаним у оквиру Закона, као и одговарајућим подзаконским актима.

8.2. Идентитет/квалификације процењивача

Сертификационо тело МО и ВС спроводи редовне интерне провере усклађености пословања са Политиком, као и са овим Практичним правилима. Интерну проверу спроводе одговарајући запослени у Сертификационом телу МО и ВС са датим задужењима.

8.3. Однос оцењивача према оцењиваном ентитету

Ово поглавље није применљиво у оквиру ових Практичних правила.

8.4. Теме покривене у процесу оцењивања

У процесу оцењивања рада Сертификационог тела МО и ВС врши се провера сагласности оперативног рада Сертификационог тела МО и ВС са Политиком и овим Практичним правилима, као и са Посебним интерним правилима рада.

8.5. Активности предузете као резултат утврђених недостатака

Сертификационо тело МО и ВС треба да усклади свој оперативни рад у складу са евентуалним налазима добијеним након провере.

8.6. Комуникација резултата

Резултати провере могу бити расположиви носиоцу PKI инфраструктуре у МО и ВС.

9. Други пословни и правни аспекти

9.1. Цене

9.1.1. Цене издавања или обнове квалификованог електронског сертификата

Сертификационо тело МО и ВС не наплаћује коришћење издатих квалификованих електронских сертификата корисницима МО и ВС.

9.1.2. Цена приступа сертификатима

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.1.3. Цена приступа информацијама о статусу сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.1.4. Цене за друге сервисе

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.1.5. Политика повраћаја новца

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.2. Финансијска одговорност

9.2.1. Покривање осигурања

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.2.2. Друга добра

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.2.3. Осигурање или гаранцијско покривање за крајње кориснике

Корисник је дужан да обештети Сертификационо тело МО и ВС 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 Сертификационо тело МО и ВС могло 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 Сертификационо тело МО и ВС или било које лице које прима и односи се према добијеном квалификованом електронском 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 приватног кључа Root Сертификационог тела МО и ВС.
- Кршења било којих закона који су применљиви, укључујући оне који се односе на заштиту интелектуалних права, рачунарске вирусе, приступ рачунарским системима итд.

9.3. Поверљивост пословних информација

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.3.1. Опсег поверљивих информација

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.3.2. Информације које нису у опсегу поверљивих информација

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.3.3. Одговорност за заштиту поверљивих информација

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.4. Приватност и заштита персоналних информација

9.4.1. План приватности

Сертификационо тело МО и ВС се придржава правила заштите приватности персоналних података и правила поверљивости како је прописано у овим Практичним правилима, као и у одговарајућим законским документима.

9.4.2. Информације које се третирају као приватне

Сертификационо тело МО и ВС третира приватним све информације које се односе на кориснике квалификованог електронског сертификата.

9.4.3. Информације које се не сматрају приватним

Сертификационо тело МО и ВС не сматра приватним само оне информације корисника за које је дата 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

Сертификационо тело МО и ВС је договорно за заштиту приватности корисникових информација које су смештене у бази података Сертификационог тела МО и ВС.

Сертификационо тело МО и ВС неће публиковати нити објављивати информације корисника осим информација у квалификованом електронском сертификату, на и у електронском идентификационом документу.

9.4.5. Откривање информација сходно правним и административним процесима

Сертификационо тело МО и ВС не објављује, нити се захтева да објављује, било коју поверљиву информацију без индентификованог и потврђеног захтева од стране:

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

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 уздржати од њиховог коришћења и објављивања трећим странама.

9.4.6. Друге околности за откривање информација

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.5. Права интелектуалног власништва

Сертификационо тело МО и ВС поседује и задржава сва права интелектуалног власништва придружена његовим базама података, квалификованим електронским сертификатима које издаје, као и било којим другим публикацијама које на било који начин припадају или потичу од стране Сертификационог тела МО и ВС, укључујући Политику и ова Практична правила.

9.6. Представљање и гаранције

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.6.1. CA представљање и гаранције

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.6.2. RA представљање и гаранције

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.6.3. Корисничко представљање и гаранције

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.6.4. Представљање и гаранције трећих страна

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.6.5. Представљање и гаранције других учесника

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.7. Непризнавање гаранције

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.8. Ограничења одговорности

Сертификационо тело МО и ВС не прихвата било какву другу одговорност осим оне која је експлицитно дефинисана у Политици и у овим Практичним правилима.

Ни у ком случају (изузев злоупотребе или намере) Сертификационо тело МО и ВС није одговорно за:

- Било какав губитак података.
- Било коју индиректну или случајну штету која је проузрокована или је везана за коришћење, испоруку, лиценцу, перформансе квалификованог електронског сертификата или квалификованих електронских потписа/печата.
- Било коју трансакцију или услугу понуђену или у оквиру обухвата ових Практичних правила.
- Било коју другу штету изузев оних које потичу од оправданог ослањања на верификоване информације које се налазе у издатом квалификованом електронском сертификату.
- Било коју одговорност која се појавила у случају грешке у верификованим информацијама која је резултат грешке, злоупотребе или намере апликанта.
- Било какво коришћење квалификованих електронских сертификата у апликацијама, сервисима, порталима која нису одобрена од стране Управе за телекомуникације и информатику (Ј-6) ГШ ВС.

9.9. Одштете

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.10. Период важности и крај валидности Практичних правила за пружање услуге издавања квалификованих електронских сертификата

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.10.1. Важност

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.10.2. Крај валидности

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.10.3. Ефекат завршетка и поновног рада

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.11. Појединачна обавештења и комуникација са учесницима

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.12. Исправке

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.12.1. Процедуре за исправку

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.12.2. Механизам и период обавештавања

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.12.3. Услови промене објектног идентификатора (OID)

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.13. Процедуре решавања спорова

Сертификационо тело МО и ВС се реферише на арбитражу у циљу решавања свих спорова који се односе на Политику и ова Практична правила. Ако се спор не реши у оквиру десет (10) дана након иницијалног обавештења сходно правилима Политике и ових Практичних правила, 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, Република Србија, а арбитри одређују све трошкове арбитраже.

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

9.14. Закон који се поштује

Ова Практична правила су издата у потпуности у складу са одговарајућом законском регулативом Републике Србије, и то пре свега са Законом и одговарајућим подзаконским актима. Све правне ствари које се односе на Сертификационо тело МО и ВС и/или који се односе на квалификоване електронске сертификате издате од стране Сертификационог тела МО и ВС ће бити процесуиране од стране одговарајућег суда у Републици Србији.

9.15. Сагласност са применљивим законима

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.16. Разне одредбе

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.16.1. Комплетан уговор

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.16.2. Додељивање

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.16.3. Озбиљност

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.16.4. Спровођење правног поступка

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.16.5. Виша сила

Ово поглавље није применљиво у оквиру ових Практичних правила.

9.17. Друге одредбе

Ово поглавље није применљиво у оквиру ових Практичних правила.

10. Историја документа

Верзија	Датум	Опис промена
1.0	29.11.2013.	Потписана верзија
2.0	28.02.2023.	Усаглашавање са терминологијом у Закону, са стандардима и са новом хијерархијском структуром Сертификационог тела. Потписана верзија.
3.0	06.07.2026.	Усаглашавање са законском регулативом и новом структуром и хијерархијом сертификационих тела.

11. Референце

- Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, Службени Гласник Републике Србије, бр. 94/2017 и 52/ 2021

- Уредба о условима за пружање квалификованих услуга од поверења, Службени Гласник Републике Србије, бр. 37/18

- 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 пружања услуге издавања квалификованих електронских сертификата Министарства одбране и Војске Србије

12. Компаније и организације

[1] Војска Србије, http://www.vs.rs

[2] НетСеТ д.о.о, http://www.netset.rs

[3] IANA (Internet Assigned Numbers Authority), http://www.iana.org