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

ПОЛИТИКА СЕРТИФИКАЦИЈЕ СЕРТИФИКАЦИОНОГ ТЕЛА МО И ВС

за издавање квалификованих електронских сертификата

(CP - Certificate Policy)

(верзија 1.0)

OID CP документа: 1.3.6.1.4.1.42922.1.1.1.1

Београд, септембар 2014. године

Садржај

1. Увод и преглед основних претпоставки

Сертификационо тело Министарства одбране и Војске Србије (у наставку: Сертификационо тело МО и ВС) издаје квалификоване електронске сертификате. Сертификационо тело МО и ВС квалификоване електронске сертификате потписује користећи свој приватни кључ и асиметрични криптографски алгоритам.

У тако формираним електронским сертификатима, Сертификационо тело МО и ВС се идентификује као издавач квалификованог електронског сертификата у складу са Законом о електронском потпису и одговарајућим подзаконским актима.

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

- ETSI ESI TS 101 862 „Qualified Certificate Profile".
- RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".
- RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- ETSI TS 102 280 „X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons" и
- са обавезним садржајем дефинисаним у члану 17. Закона о електронском потпису (у даљем тексту - Закон).

1.1. Преглед основних претпоставки

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.
- Дистрибуцију приватног кључа и квалификованог електронског сертификата регистрационом ауторитету на основу Уредбе о војној легитимацији и Директиви о начину рада и поступању приликом издавања војне легитимације
- Омогућавање процедуре опозива квалификованих електронских сертификата и
- обезбеђивање информације о статусу квалификованих електронских сертификата.

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

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

Општа правила сертификације Сертификационог тела МО и ВС уграђују се у документа:

1. Политика сертификације - CP (Certificate Policy) – овај документ.
2. Практична правила рада Сертификационог тела МО и ВС за издавање квалификоаних електронских сертификата, CPS (Certification Practices Statement) (у даљем тексту: Практична правила).

Политика сертификације и Практична правила у смислу Сертификационог тела МО и ВС су јавно доступна документа. Политика сертификације дефинише предмет рада сертификационог тела, док Практична правила дефинишу процесе и начин њиховог коришћења при формирању и управљању квалификованим електронским сертификатима.

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

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

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

Општа правила функционисања 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 TS 101 456 „Policy Requirements for Certification Authorities Issuing 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 детаљно 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 интерна правила садрже детаљне одредбе о:

- систему физичке контроле приступа у поједине просторије сертификационог тела;
- систему логичке контроле приступа рачунарским ресурсима сертификационог тела;
- систему за чување приватног кључа сертификационог тела;
- систему дистрибуиране одговорности при активацији приватног кључа сертификационог тела;
- 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 Политику сертификације (у даљем тексту CP – Certificate Policy) Сертификационог тела МО и ВС које издаје квалификоване електронске сертификате припадницима МО и ВС на електронском идентификационом документу.

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

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

Јединствено име (Dname – issuer):
CN=MOVSRootCA
O=Ministarstvo odbrane i Vojska Srbije
L=Beograd
C=RS

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 (J-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 ове политике сертификације у циљу подршке издавању квалификованих електронских сертификата. У том смислу, ова Политика сертификације, као и придружени документ Практична правила, представљају одговарајућу политику и практична правила која се примењују при издавању квалификованих електронских сертификата.

У циљу објављивања информација које се односе на опозване квалификоване електронске сертификате, неопходно је да се изврши одговарајуће публиковање листе опозваних сертификата (CRL – Certificate Revocation List). Сертификационо тело МО и ВС периодично објављује такву листу у складу са условима дефинисаним у овом документу.

Сертификационо тело МО и ВС представља хијерархијску PKI структуру за издавање квалификованих електронских сертификата. Сертификационо тело МО и ВС има једно Root Сертификационо тело и једно Intermediate Сертификационо тело тело (MO VS UzK CA тело).

У поменутој архитектури:

- MO VS Root Сертификационо тело– је главно самопотписано сертификационо тело које издаје сертификате Intermediate сертификационим телима и публикује CRL листу на Root нивоу.
- Intermediate Сертификационо тело (MO VS UzK CA тело) – је 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.

МО VS UzK CA тело публикује своју листу опозваних сертификата корисника.

1.3.2. Регистрациона тела МО и ВС

Захтеви за издавањем квалификованог електронског сертификата за кориснике МО и ВС се формирају посредством захтева за издавањем еИД. 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).

Регистрациона тела МО и ВС:
- Спроводи 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 (идентификациона документа која 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.

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 и студенти Универзитета одбране.

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.

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 одређених електронских докумената која су потписана од стране корисника Сертификационог тела МО и ВС, као и која врше валидацију квалификованог електронског сертификата издатих од стране Сертификационог тела МО и ВС.

Верификација квалификованог електронског потписа 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.

1.3.5. Други учесници

Ово поглавље није примењиво у оквиру ове СР.

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 квалификованог електронског сертификата

Квалификовани електронски сертификат Сертификационог тела МО и ВС се користи у дефинисаним и одобреним апликацијама које је одобрио носилац PKI инфраструктуре у МО и ВС, а у којима се спроводи верификација електронског потписа.

1.4.2. Забрањено коришћење квалификованог електронског сертификата

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

1.5. Администрација Политике сертификације Сертификационог тела МО и ВС

У овом поглављу су описане активности у вези администрације ове СР.

1.5.1. Организација администрирања Политике сертификације

Сертификационо тело МО и ВС је одговорно за прописну администрацију ове СР, и то у смислу периодичног прегледа и ажурирања, као и ванредних промена одговарајућих одредби које проистичу из евентуалних промена у законској регулативи или техничким карактеристикама примењених криптографских алгоритама и дужина кључева.

1.5.2. Контакт особа

Контакт особа у Сертификационом телу МО и ВС за СР документ је:

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

1.5.3. Особа која одређује погодност CP документа

Погодност CP документа 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 CP документа

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

1.6. Дефиниције и скраћенице

1.6.1. Дефиниције

У овом документу поједини изрази имају следеће значење:

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

Сертификат сертификационог тела – Сертификат за дато сертификационо тело издат (електронски потписан) од стране другог сертификационог тела или самопотписан (уколико се ради о Root сертификационом телу).

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

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

Сертификационо тело – издавач сертификата (Issuing CA) – У контексту одређеног сертификата, сертификационо тело – издавач сертификата је оно сертификационо тело које је издало (електронски потписало) сертификат.

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

Регистрационо тело (RA) – Ентитет који је одговоран за идентификацију и аутентикацију корисника/власника сертификата, као и креирање захтева за издавање сертификата, али који не издаје и не потписује сертификат (тј. RA врши одговарајуће послове (идентификацију корисника) и у том смислу је делегирано од CA). Често се и термин LRA (Local Registration Authority) користи у истом контексту.

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

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

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

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

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

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

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

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

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

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

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

Корисник – физичко лице запослено у МО и ВС и физичко лице које користи војно здравствено осигурање, а коме се издаје електронски сертификат.

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

Захтев за сертификат - Захтев послат од стране регистрационог тела који захтева сертификат 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 праћења активности у Систему.

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, идентификација се односи на два процеса:

- Утврђивање да дато име појединца или организације одговара реалном идентитету појединца или организације
- 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 аутентиковани корисник има за коришћење одговарајуће апликације или сервиса.

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

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

Листа опозваних сертификата (CRL – Certificate Revocation List) – Листа издата и електронски потписана од стране CA која укључује серијске бројеве опозваних сертификата, време када је опозив извршен и разлог опозива. Таква листа се мора користити од стране трећих страна увек када треба проверити валидност сертификата и/или верификацију електронског потписа.

Серијски број сертификата (Sertificate Serial Number)– 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.

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).

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

Криптографија – наука о заштити тајности информација.

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

Криптографски кључ – тајна и случајна информација одговарајуће дужине у битовима која се користи у криптографским алгоритмима, у процедурама шифровања и дешифровања.

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

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

Идентификатор објекта (Object identifier) – Секвенца целобројних 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 публиковани основни документи рада CA, као и евентуалне друге информације које се односе на пружање сертификационих услуга од стране датог CA.

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

Кориснички уговор – Уговор између трећих страна и CA у циљу обезбеђења сертификационих услуга.

1.6.2. Скраћенице

У овом наслову описане су скраћенице које се користе у овом документу.

Скраћенице на енглеском језику:

CA – Certification Authority

CEN- European Committee Standardization

CP – Certificate Policy

CPS – Certificate Practices Statement

CRL – Certificate Revocation List

CSR – Certificate Service Request

CWA- CEN Workshop Agreement

EAL- Evaluation Assurance Level

ETSI – European Telecommunication Standardization Institute

FIPS – Federal Information Processing Standard

OID – Object IDentifier

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

2. Одговорности за публиковање и репозиторијуме

Ово поглавље се односи на све 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 одређеном Web или LDAP серверу.

Сертификационо тело МО и ВС има online репозиторијум докумената у којима објављују информације о практичним правилима и процедурама рада, укључујући CPS као и ову CP.

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.

2.2. Публиковање информација о сертификатима

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

- Сертификате Сертификационог тела МО и ВС (Root сертификат и сертификат Интермедиате сертификационог тела МО VS UzK CA),
- Информације о статусима опозваности сертификата (CRL).

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

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), као што је назначено и прецизирано у овој политици (наслов 4.1) и CPS документу.

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 сертификационог тела,
- Добаваљања CRL листе Сертификационог тела МО и ВС у циљу валидације сертификата издатог од стране Сертификационог тела МО и ВС.
- Добављања Политике сертификације и Практичних правила.

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

3. Идентификација и аутентикација 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 који издаје Сертификационог тела МО и ВС. Аутентикација и утврђивање идентитета се извршавају пре издавања квалификованог електронског сертификата.

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

Сертификационо тело МО и ВС аутентикује захтеве страна које желе да опозову сертификате у складу са овом политиком.

Сертификационо тело МО и ВС одржава одговарајуће процедуре у циљу одређивања практичних правила за додељивање имена.

3.1. Називи

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

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

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

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

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.

У циљу идентификације и аутентикације индивидуалног корисника који подноси захтев за издавање квалификованог електронског сертификата, 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 који се базира на достављеној документацији.
- Захтев да се појединац физички појави у регистрационом телу МО и ВС у одговарајућој фази пре него што се изда квалификовани електронски сертификат.

3.3. Идентификација и аутентикација захтева за обнављање кључева

Ово поглавље није применљиво у оквиру ове СР.

3.4. Идентификација и аутентикација захтева за опозив 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.

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

4. Оперативни захтеви у вези животног циклуса 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

Корисници подносе захтев за издавање еИД, а тим и аутоматски захтев за добијање квалификованог електронског сертификата сходно: Уредби о војној легитимацији, Директиви о начину рада и поступању приликом издавања војне легитимације. Корисници захтев подносе регистрационом телу МО и ВС.

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

4.2. Процесирање захтева за добијање квалификованог електронског сертификата

Након пријема захтева за издавање еИД, 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 провере захтева корисника и захтева за издавање еИД.

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

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 одобреног захтева.

4.3. Издавање квалификованог електронског сертификата

Након што регистрационо тело МО и ВС достави валидан захтев за издавањем еИД, Сертификационо тело МО и ВС спроводи процес издавања квалификованог електронског сертификата који се састоји од:

- Генерисање и чување асиметричног пара кључева на SSCD уређају (смарт картица, односно еИД) и квалификованог електронског сертификата за верификацију квалификованог електронског потписа и њихов упис у еИД током процеса електронске персонализације.

Ова процедура се детаљно описује у CPS документу.

4.4. Прихватање сертификата

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

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 у поступку електронске персонализације.

Било која примедба на издати квалификовани електронски сертификата 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. Регистрационо тело МО и ВС је у обавези да покрене нову процедуру за издавање квалификованог електронског сертификата са тачним подацима.

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, и то:

- Корисник се обавезује да ће користити приватни кључ и квалификовани електронски сертификат издат 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, суспензије или опозива издатог сертификата.
- Трећа страна је обавезна да прихвати и користи квалификовани електронски сертификат издат од стране 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 сертификата коришћењем метода који је дефинисан у CP и CPS документима Сертификационог тела МО и ВС.

4.6. Обнављање квалификованог електронског сертификата

Ово поглавље није применљиво у оквиру ове CP.

4.7. Генерисање новог пара кључева и квалификованог електронског сертификата корисника

У случају да је квалификовани електронски сертификат истекао, и уколико се жели добити нови квалификовани електронски сертификат, мора се поднети захтев за издавање новог квалификованог електронског сертификата 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.

Након достављања захтева за издавањем новог квалификованог електронског сертификата, даља процедура је у потпуности идентична као и процедура за добијање првог квалификованог електронског сертификата.

4.8. Модификације квалификованог електронског сертификата корисника

Модификација квалификованог електронског сертификата је могућа и врши се у следећим ситуацијама:

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

Модификацију врши овлашћено лице из регистрационог тела МО и ВС и наведену промену електронски потписује својим приватним кључем.

4.9. Суспензија и опозив квалификованог електронског сертификата

Квалификовани електронски сертификат се суспендује у следећим ситуацијама:

- Суспензију квалификованог електронског сертификата захтева власник или одговарајуће лице из Сертификационог тела МО и ВС или регистрационог тела МО и ВС.
- 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, а на основу примљеног захтева од регистрационог тела МО и ВС, Сертификационо тело МО и ВС врши суспензију издатих квалификованих електронских 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 може захтевати активацију свог квалификованог електронског сертификата преко регистрационог тела, односно у случају да је еИД нађен корисник може захтевати реактивацију квалификованог електронског сертификата који је био привремено суспендован.

Квалификовани електронски сертификат се реактивира у следећим ситуацијама:

- Ако активирање квалификованог електронског сертификата захтева власник или одговарајуће лице из Сертификационог тела МО и ВС или регистрационог тела 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.

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 овом CP или у CPS документу.
- Да извршење одговарајућих обавеза лица која су наведена у овој CP касни или је спречено услед природне катастрофе, рачунарског или комуникационог отказа, или услед другог узрока који излази ван контроле датог лица, и као резултат, информације о другом лицу су материјално угрожене или компромитоване.
- Да се десила промена одређених информација која се садрже у квалификованом електронском сертификату власника.

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 овој CP, као и у CPS 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. Након испуњења поменутих услова, службеник регистрационог тела МО и ВС електронски (апликација регистрационог тела - ЦИС) подноси захтев за опозив сертификата, потом Сертификационо тело МО и ВС извршава промптну активност у циљу опозива квалификованог електронског сертификата.

Листа опозваних сертификата (CRL – Certificate Revocation List) за Intermediate Сертификациона тела МО и ВС 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.

Сертификационо тело МО и ВС публикује све опозване и суспендоване квалификоване електронске сертификате у својој CRL листи.

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

Треће стране морају бити у сагласности са Сертификационо тело МО и ВС политиком, а посебно са обавезама трећих страна које произилазе из публикованих CP и CPS докумената

4.10. Сервиси провере статуса квалификованих електронских сертификата

За проверу статуса користе се CRL листе публиковане на online репозиторијуму Сертификационог тела МО и ВС, а које корисници или треће стране могу слободно преузети.

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 CP и CPS.
- 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.
- Сертификационо тело МО и ВС је престало са пружањем услуга сертификације.

4.12. Чување и реконструкција приватног кључа корисника

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

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.

5.1. Физичке безбедносне контроле

Сертификационо тело МО и ВС имплементира физичке контроле у својим просторијама укључујући следеће:

- 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.
- 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 су лоциране у оквиру безбедне рачунарске собе која се надгледа техничким средствима и одговорним лицима.
- Напајање се извршава са редундансом високог нивоа.
- Просторије Сертификационог тела МО и ВС су заштићене од поплава.
- Механизам за дојаву пожара.
- Медијуми се чувају на безбедан начин. Backup медијуми се такође чувају на одвојеној локацији која је физички обезбеђена.
- Изношење смећа се контролише.

5.2. Процедуралне контроле

Сертификационо тело МО и ВС иницира кадровску и управну праксу која обезбеђује разумну сигурност у поверљивост и компетенцију запослених.

Сваки запослени који обавља послове Сертификационог тела 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.

Сви запослени који обављају послове Сертификационог тела 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,
- оператери.

ЦПМЕ у коме се налази организациона целина која обавља 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.

Тамо где се захтева вишеструка контрола примењује се процедура m од m<=n, 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

Надлежни органи врше неопходне активности провере биографије, квалификација, као и неопходног искуства запослених који обављају послове у Сертификационом телу МО и ВС, а у циљу реализације провере компетенције специфичног посла. Такве провере биографије типично укључују:

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

5.3.2. Процедура провере биографије

Надлежни органа врши релевантне проверу запослених и потенцијалних сарадника по процедури надлежног органа Министарства одбране.

5.3.3. Захтеви за обученошћу

За лица која обављају послове у Сертификационом телу МО и ВС обезбеђује се обуку у циљу реализације функција пословања Сертификационог тела МО и ВС.

5.3.4. Поновна обука

Периодично понављање и проширивање обуке може такође бити извршено у циљу успоставе континуитета и ажурности знања запослених, као и одговарајућих процедура.

5.3.5. Ротација послова

Ово поглавље није применљиво у оквиру ове СР.

5.3.6. Казнене мере у односу на запослене

Постоје одговарајуће мере које се спроводи према лицима која обављају послове Сертификационог тела МО и ВС: 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. Контроле независних уговарача

Независни уговарачи су субјекти који морају да поштују процедуре заштите приватности и услова поверљивости као и лица која обављају послове у Сертификационом телу МО и ВС. Незавини уговарачи су потенцијални сарадници и подлежу процедурама провере од стране надлежног органа Министарства одбране.

5.3.8. Документација за иницијалну обуку и поновну обуку

Припадницима који обављају послове у Сертификационом телу МО и ВС доступна је сва документација која се односи на иницијалну обуку, поновну обуку или дообуку.

5.4. Процедуре безбедносних провера

Процедуре контроле логова укључују: логовање догађаја и система за логовање. Ове продуре су имплементиране за сврху одржавања безбедног окружења.

У том смислу, Сертификационо тело МО и ВС имплементира следеће контроле:

- Сертификационо тело МО и ВС записује догађаје који укључују, али нису ограничени на операције везане за животни циклус сертификата, као и захтеве достављене систему.
- Сертификационо тело МО и ВС чува контролисане дневничке записе у реалном времену.
- Дневнички записи се могу видети само од стране ауторизованог особља – администратора система.
- Сертификационо тело МО и ВС имплементира процедуре backup-а дневничких записа.

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

Сертификационо тело МО и ВС реализује с времена на време процену рањивости система на основу дневничких заиса.

5.5. Архивирање записа

Опште политике чувања записа Сертификационог тела МО и ВС укључују следеће:

- Типови записа – Сертификационо тело МО и ВС чува на безбедан начин записе о издатим квалификованим електронским сертификатима, подацима из дневничких записа, информацијама о апликацијама за издавање сертификата.
- Период чувања – Сертификационо тело МО и ВС чува на безбедан начин поменуте записе о електронским сертификатима Сертификационог тела МО и ВС за период који је назначен у CPS документу Сертификационог тела МО и ВС, а што је усклађено са Законом.
- Заштита архиве – услови за заштиту архиве укључују:
  - Записе које само систем администратори (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.
- Процедуру backup-а архиве.
- Захтеве за процедуром чувања барем две одвојене копије архиве које су под контролом две различите особе.
- Процедуре у циљу добијања и верификације архивских информација – У циљу добијања и верификације архивских информација, Сертификационо 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.

Регистрационо тело МО и ВС чува на безбедан начин документацију о самим пријавама за издавање квалификованих електронскох сертификата.

5.6. Измена кључева

Сертификационо тело МО и ВС поседује процедуру, описану у CPS документу, која се спроводи у случају истека сертификата сертификационог тела или опозива сертификата сертификационог тела у складу са условима дефинисаним у овој CP.

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

5.7. Компромитација и опоравак у случају катастрофе

У Посебним интерним 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.

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

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

Сертификационо тело МО и ВС у случају природне или друге катастрофе имплементира мере које омогућавају континуиран рад сервиса у ограниченом обиму.

5.8. Завршетак рада Сертификационог тела МО и ВС

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

- Обавештава своје кориснике који имају важеће квалификоване електронске сертификате о намери да престане са пружањем сертификационе услуге, тј. да престане да извршава активности у својству Сертификационог тела МО и ВС.

- На основу захтева регистрационог тела МО и ВС опозива све квалификоване електронске сертификате који су још увек важећи (тј. оне који нису опозвани или им је истекао рок важности) након обавештења, а без захтева за сагласношћу корисника.
- Регистрационо тело благовремено обавештава о опозиву сертификата све кориснике на које се то односи.
- Чини разумне мере у циљу заштите записа које чува у складу са овом СР.
- Уколико је то могуће, обезбеђује одговарајуће мере обезбеђења сукцесије у смислу поновног издавана квалификованих електронских сертификата од стране другог сертификационог тела које је сукцесор – настављач издавања сертификата – и које поштује исти СР документ.

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 је критично у циљу осигурања да су сви кључеви и активациони подаци заштићени и да се користе искључиво на дозвољен начин од стране ауторизованих особа.

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 квалификованих електронских сертификата, опозива квалификованих електронских 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

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 овом СР. Сертификационо тело МО и ВС примењује јавне, интернационалне и Европске стандарде прописане Законом у вези безбедних и поузданих система.

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

Приватни Root кључ Сертификационог тела МО и ВС се користи за електронско потписивање сертификата Сертификационог тела МО и ВС (пре свега за издавање сертификата Intermediate сертификационог тела) и листе опозваних сертификата. Друге сврхе коришћења приватног кључа Root Сертификационог тела МО и ВС су забрањене.

За потребе свог Root приватног кључа и одговарајуће потписивање, Сертификационо тело МО и ВС користи SHA256/RSA, комбинацију hash и асиметричног алгоритма, при чему се карактеристике кључа могу постављати конфигурабилно, али се користи дужина кључа од 4096 бита, период валидности приватног кључа Root CA од 10 година, и период валидности сертификата од 20 година.

За потребе приватног кључа Intermediate сертификационог тела и одговарајућег алгоритма за квалификовано електронско потписивање, Сертификационо тело МО и ВС користи SHA256/RSA, комбинацију hash и асиметричног алгоритма са препорученом дужином кључа од 3072 бита, периодом валидности приватног кључа сертификационог тела од 5 година, 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.

6.2. Заштита приватног кључа

Сертификационо тело МО и ВС користи одговарајуће криптографске уређаје у циљу реализације задатака управљања кључевима сертификационог тела. Поменути криптографски уређаји су познати под именом Хардверски безбедносни модули (HSM - Hardware Security Modules).

Генерисање приватног кључа Сертификационог тела МО и ВС се дешава у оквиру безбедног криптографског уређаја који задовољава одговарајуће захтеве у складу са међународним стандардима FIPS 140-2 L3 или Common Criteria EAL4+стандардом (CWA 14169). Ови стандарди гарантују, између осталог да је било који покушај нарушавања интегритета уређаја или криптографске меморије истовремено детектован, и да приватни кључеви не могу да напусте уређај.

Хардверски и софтверски механизми који штите приватне кључеве сертификационог тела су документовани у Посебним интерним правилима рада.

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.

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

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.

Сертификационо тело МО и ВС користи безбедни криптографски уређај да чува своје приватне кључеве у складу са међународним захтевима исказаним у FIPS 140-2 L3 или Common Criteria EAL4+ стандарду (CWA 14169).

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.

Сертификационо тело МО и ВС приватни кључ чува у складу са процедуром дефинисаном у CPS документу.

Сертификационо тело МО и ВС користи процедуру дељења тајни имањем вишеструких ауторизованих носиоца 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.

Сертификационо тело МО и ВС приватне кључеве уништава 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 његове дељени делови се уништавају на начин који онемогућава њихову реконструкцију.

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

6.3. Други аспекти управљања паром кључева

Сертификационо тело МО и ВС архивира свој сопствени јавни кључ.

Сертификационо тело МО и ВС издаје квалификоване електронске сертификате корисницима са периодом коришћења као што је назначено у квалификованом електронском сертификату.

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

6.4. Активациони подаци

Сертификационо тело МО и ВС безбедно процесира активационе податке придружене приватним кључевима сертификационог тела, као и свим другим приватним кључевима у датом PKI систему (Intermediate сертификациона тела, корисници).

6.5. Безбедносне контроле рачунара

Сертификационо тело МО и ВС имплементира безбедносне котроле над рачунарима који се користе у сертификационом телу, а у оквиру датог PKI система.

6.6. Животни циклус техничких безбедносних контрола

Сертификационо тело МО и ВС реализује периодичне развојне и безбедносно управљачке контроле.

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 ове СР.

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:

- Сертификат Root Сертификационог тела МО и ВС.
- Сертификат Intermediate Сертификационог тела МО и ВС (сертификат MO VS UzK CA).
- Квалификовани електронски сертификат за кориснике:
  - запослене у МО и ВС,
  - ученике и студенте војних школа.

7.1.1. Општи профил сертификата

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

Име профила	**Општи профил**	
Период валидности сертификата	1 – 20 година	
Екстензија основних ограничења	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	4096, 3072, 2048	
Екстензија коришћења кључа – могуће вредности	Digital Signature Non-Repudiation Key Encipherment	Certificate Signing CRL Signing
Екстензија напредног коришћења кључа – 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	

7.1.2. Профил сертификата Root Сертификационог тела МО и ВС

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

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

7.1.3. Профил сертификата Intermediate Сертификационих тела МО и ВС

Профил сертификата Intermediate Сертификационог тела МО и ВС:

Име профила	MO i VS 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	3072
Екстензија коришћења кључа	Certificate Signing Off-Line CRL signing CRL Signing

7.1.5. Профили сертификата крајњих корисника намењен за квалификовани електронски потпис

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

Профил сертификата за квалификовано електронско потписивање треба да послужи као шаблон за генерисање сертификата за квалификовани електронски потпис.

У следећој табели приказан је профил сертификата за квалификовани електронски потпис:

Име профила	VS Potpisivanje
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	2048
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

7.2. Профил CRL листе

У складу са IETF PKIX RFC 2459, 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:

Верзија	[Version 2]	
Издавалац	CountryName=RS, OrganizationName=Ministarstvo odbrane i Vojska Srbije, commonName= * Location=Beograd	
Датум издавања	[Date of Issuance]	
Датум наредног издавања	[Date of Issuance + 25 hours]	
Идентификатор алгоритма потписивања	Sha256RSA	
Идентификатор кључа потписника		
Број листе	Redni broj CRL liste	
Опозвани сертификати	CRL Entries	
	Sertificate Serial Number	Date and Time of Revocation
	[Sertificate Serial Number]	[Date and Time of Revocation]

* commonName сертификационог тела које је генерисало CRL

7.3. OCSP профил

Ово поглавље није примењиво у оквиру ове СР.

8. Провера сагласности са Политиком сертификације

Сертификационо тело МО и ВС врши периодичну проверу сагласности својих политика, укључујући и ову СР. Рад Сертификационог тела МО и ВС је такође у сагласности са најважнијим међународним и Европским стандардима у овој области, као и са Европском директивом 1999/93/ЕС о електронским потписима.

У домену издавања квалификованих електронских серификата, Сертификационо тело МО и ВС ради у оквиру ограничења дефинисаним у оквиру Закона о електронском потпису Републике Србије, као и одговарајућим подзаконским актима.

Сертификационо тело МО и ВС спроводи редовне интерне анализе усклађености пословања са овом СР, као и са CPS документом. Интерне анализе спроводе одговарајући запослени ВС са датим задужењима.

9. Други пословни и правни аспекти

9.1. Цене

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

9.2. Финансијска одговорност

Ово поглавље није применљиво у оквиру ове СР.

9.3. Поверљивост пословних информација

Ово поглавље није применљиво у оквиру ове СР.

9.4. Приватност и заштита персоналних информација

Сертификационо тело МО и ВС се придржава правила заштите приватности персоналних података и правила поверљивости како је прописано у CPS документу, као и у одговарајућој законској регулативи.

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

- 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 уздржавати од њиховог коришћења и објављивања трећим странама.

9.5. Права интелектуалног власништва

Сертификационо тело МО и ВС поседује и задржава сва права интелектуалног власништва придружена својим базама података, Web сајтовима, 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 и ову СР.

9.6. Представљање и гаранције

Ово поглавље није применљиво у оквиру ове СР.

9.7. Непризнавање гаранције

Ово поглавље није применљиво у оквиру ове СР.

9.8. Ограничења одговорности

Сертификационо тело МО и ВС не прихвата било какву другу одговорност осим оне која је експлицитно дефинисана у овом документу.

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

9.9. Одштете

Ово поглавље није применљиво у оквиру ове СР.

9.10. Период важности и крај валидности Политике сертификације

Ово поглавље није применљиво у оквиру ове СР.

9.11. Појединачна обавештења и комуникација са учесницима

Ово поглавље није применљиво у оквиру ове СР.

9.12. Исправке

Ово поглавље није применљиво у оквиру ове СР.

9.13. Процедуре решавања спорова

Сви спорови који се односе на ову СР ће се решавати арбитражом. Ако се спор не реши у оквиру десет (10) дана након иницијалног обавештења сходно правилима СР, стране у спору достављају спор на арбитражу. Арбитража се састоји од 3 арбитра, свака страна предлаже по једног, док трећег предлажу заједно обе стране у спору. Место за арбитражу је Београд, Србија, а арбитри одређују све трошкове арбитраже.

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

9.14. Закон који се поштује

Ова СР је издата у потпуности у складу са одговарајућом законском регулативом Републике Србије, и то пре свега са Законом о електронском потпису и одговарајућим подзаконским

актима. Све правне ствари које се односе на Сертификационо тело МО и ВС и/или који се односе на 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 ове СР.

9.16. Разне одредбе

Ово поглавље није применљиво у оквиру ове СР.

9.17. Друге одредбе

Ово поглавље није применљиво у оквиру ове СР.

10. Историја документа

Верзија	Датум	Опис промена
1.0	29.11.2013.	Потписана верзија

11. Референце

- Закон о електронском потпису, Службени Гласник Републике Србије, бр. 135/2004
- Правилник о ближим условима за издавање електронских сертификата, Службени Гласник Републике Србије, бр. 48/2005
- RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework
- RFC 5280 – Request For Comments 5280, Internet X.509 Public Key Infrastructure / Certificate and CRL Profile
- Практична правила Сертификационог тела Министарства одбране и Војске Србије за издавање квалификованих електронских сертификата

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