РЕПУБЛИКА СРПСКА
ВЛАДА
МИНИСТАРСТВО ЗА НАУЧНОТЕХНОЛОШКИ РАЗВОЈ, ВИСОКО ОБРАЗОВАЊЕ И ИНФОРМАЦИОНО ДРУШТВО

ПРАКТИЧНА ПРАВИЛА ПРУЖАЊА УСЛУГА ЦЕРТИФИКАЦИЈЕ ЦЕРТИФИКАЦИОНОГ ТИЈЕЛА МИНИСТАРСТВА ЗА НАУЧНОТЕХНОЛОШКИ РАЗВОЈ, ВИСОКО ОБРАЗОВАЊЕ И ИНФОРМАЦИОНО ДРУШТВО РЕПУБЛИКЕ СРПСКЕ

(CPS – *Certificate Practice Statement*)

(1.3.6.1.4.26614.20.1.1)

Верзија 1.0

Бања Лука, април 2020. године

Садржај

1 Увод 9
1.1 Преглед 9
1.2 Назив докумената и идентификациони подаци 10
1.3 Учесници ПКИ система 11
1.3.1 Цертификационо тијело МНРВОИД 11
1.3.1.1 Управљачко тијело 11
1.3.1.2 Цертификационо тијело 12
1.3.2 Регистрационо тијело 12
1.3.3 Корисници услуга 13
1.3.4 Треће стране 14
1.3.5 Остали учесници 14
1.4 Употреба цертификата 14
1.4.1 Подручје примјене 14
1.4.1.1 Подручје примјене *MNRVOID CA Root* цертификата 14
1.4.1.2 Подручје примјене *MNRVOID CA 1* цертификата 15
1.4.2 Недозвољена примјена 15
1.5 Политика администрирања документа 15
1.5.1 Организација управљања документом 15
1.5.2 Лица за контакт 15
1.5.3 Лица одређена за усклађивање докумената са праксом издавања цертификата . 16
1.5.4 Процедуре за одобрење Практичних правила 16
1.6 Дефиниције и скраћенице 16
2 Објављивање и локација података о цертификацији 20
2.1 Локација за објављивање података о цертификацији 20
2.2 Објављивање података о цертификацији 20
2.3 Учесталост објављивања података о цертификацији 20
2.4 Контрола приступа подацима о цертификацији 21
3 Идентификација и аутентификација 21
3.1 Називи 21
3.1.1 Типови имена 21
3.1.2 Номенклатура имена 21
3.1.3 Анонимност или псеудоними корисника 22
3.1.4 Правила за тумачење различитих врста имена 22

3.1.4.1 Имена цертификационих тијела 22
3.1.4.2 Имена крајњих корисника услуга цертификације 22
3.1.5 Јединственост имена 23
3.1.6 Признавање, аутентификација и улога заштитног знака 24
3.2 Иницијална провјера идентитета 24
3.2.1 Метода доказивања посједовања приватног кључа 24
3.2.2 Потврда идентитета правног лица 24
3.2.2.1 Потврда идентитета подносиоца код електронског подношења захтјева 26
3.2.3 Потврда идентитета физичког лица 26
3.2.4 Информације о кориснику које се не провјеравају 27
3.2.5 Валидација ауторитета 27
3.2.6 Критеријуми за интероперабилност 27
3.3 Идентификација и аутентикација захтјева за обнављање кључева 27
3.3.1 Идентификација и аутентикација за рутинско обнављање кључева 27
3.3.2 Идентификација и аутентикација за обнављање кључева након опозива 27
3.4 Идентификација и аутентикација захтјева за суспензију или опозив цертификата 27
4 Оперативни захтјеви у вези животног циклуса цертификата 29
4.1 Подношење захтјева за издавање цертификата 29
4.1.1 Ко може да поднесе захтјев за издавање цертификата? 29
4.1.2 Процес достављања захтјева за издавање цертификата и одговорности 29
4.2 Обрада захтјева за издавање цертификата 30
4.2.1 Идентификација и потврђивање аутентичности подносиоца захтјева 30
4.2.2 Потврђивање или одбијање захтјева за издавање цертификата 31
4.2.3 Потребно вријеме за обраду захтјева за издавање цертификата 31
4.3 Издавање цертификата 31
4.3.1 Активности током процеса издавања цертификата 31
4.3.2 Обавјештење подносиоца захтјева о издатом цертификату 32
4.4 Прихватање цертификата 32
4.4.1 Спровођење процеса прихватања цертификата 32
4.4.2 Објављивање цертификата од стране СА тијела 32
4.4.3 Обавјештење других ентитета о издатом цертификату 32
4.5 Коришћење цертификата и асиметричног пара кључа 32
4.5.1 Коришћење приватног кључа и цертификата од стране корисника 33
4.5.2 Коришћење јавног кључа и цертификата од стране трећих страна 33
4.6 Обнављање цертификата 33
4.6.1 Услови за обнављање цертификата 33

4.6.2 Ко може захтијевати обнављање цертификата 33
4.6.3 Обрада захтјева за обнављањем цертификата 33
4.6.4 Обавјештење корисника да му је издат обновљени цертификат 33
4.6.5 Спровођење процеса прихватања обновљеног цертификата 33
4.6.6 Објављивање обновљеног цертификата од стране СА 33
4.6.7 Обавјештење других ентитета од стране СА о обнови датог цертификата 33
4.7 Генерисање новог пара кључева и цертификата корисника 34
4.7.1 Услови за генерисање новог пара кључева и цертификата 34
4.7.2 Ко може захтијевати нови цертификат са новим јавним кључем 34
4.7.3 Обрада захтјева за новим паром кључева и цертификатом 34
4.7.4 Обавјештење корисника да му је издат нови цертификат 34
4.7.5 Спровођење процеса прихватања новог цертификата 34
4.7.6 Објављивање новог цертификата од стране СА 34
4.7.7 Обавјештење других ентитета од стране СА о издавању новог цертификата 34
4.8 Измјена података у цертификату 34
4.8.1 Услови за измјену података у цертификату 34
4.8.2 Ко може захтијевати измјену података у цертификату 34
4.8.3 Обрађивање захтјева за измјену података у цертификату 34
4.8.4 Обавјештење корисника о измјени података у цертификату 34
4.8.5 Спровођење процеса прихватања новог цертификата са измијењеним подацима 35
4.8.6 Објављивање новог цертификата са измијењеним подацима 35
4.8.7 Обавјештење других корисника од стране ЦА о издавању новог цертификата са измијењеним подацима 35
4.9 Опозив и суспензија цертификата 35
4.9.1 Околности за опозив цертификата 35
4.9.2 Ко може захтијевати опозив цертификата? 35
4.9.3 Процедура захтјева за опозив цертификата 36
4.9.4 Период чекања захтјева за опозивом цертификата 36
4.9.5 Вријеме за које СА мора да процесира захтјев за опозивом цертификата 36
4.9.6 Захтјеви за треће стране у вези провјере статуса цертификата 37
4.9.7 Фреквенција издавања ЦР листе 37
4.9.8 Максимално кашњење у издавању ЦР листе 37
4.9.9 Расположивост *on-line* провјере статуса цертификата 37
4.9.10 Захтјеви за *on-line* провјеру статуса цертификата 37
4.9.11 Друге форме регистра опозвних цертифиакта 37

4.9.12 Специјални захтјеви у односу на компромитацију приватног кључа 37
4.9.13 Околности за суспензију цертификата 37
4.9.14 Ко може захтијевати суспензију цертификата? 37
4.9.15 Процедура захтјева за суспензијом цертификата и рактивацијом 38
4.9.16 Ограничење на трајање суспензије 39
4.10. Сервиси провјере статуса цертификата 39
4.10.1. Оперативне карактеристике 39
4.10.2. Расположивост сервиса 39
4.10.3. Додатне карактеристике 39
4.11. Престанак коришћења цертификата 39
4.12. Чување и реконструкција приватног кључа корисника 39
4.12.1 Политика и пракса чувања и реконструкције приватног кључа 39
4.12.2. Енкапсулација сесијског кључа и политика и пракса за реконструкцију 40
5 Управне, оперативне и физичке безбједносне контроле 40
5.1 Контрола физичке заштите 40
5.1.1 Локација и конструкција сајта 40
5.1.2 Физички приступ 40
5.1.3 Електрично напајање и климатизација 41
5.1.4 Изложеност поплавама и временским непогодама 41
5.1.5 Превенција и заштита од пожара 41
5.1.6 Медијуми за чување података 41
5.1.7 Одлагање непотребног материјала 41
5.1.8 Чување резервних копија 41
5.2 Контроле процедура 41
5.2.1 Улоге од повјерења 42
5.2.2 Број особа које се захтјевају по сваком задатку 42
5.2.3 Идентификација и аутентикација за сваку улогу 42
5.2.4 Улоге које захтјевају раздвајање дужности 42
5.3 Кадровске безбједносне контроле 42
5.3.1 Квалификације и искуство 42
5.3.2 Процедура провјере биографије 42
5.3.3 Захтјеви за обученошћу 43
5.3.4 Фреквенција и захтјеви за поновну обуку 43
5.3.5 Фреквенција и секвенца ротације послова 43
5.3.6 Казнене мјере за неовлашћене активности 43
5.3.7 Захтјеви за спољне сараднике 43

5.3.8 Документација која се доставља запосленима 43
5.4 Процедуре безбједносних провјера логова - ревизија 43
5.4.1 Типови забиљежених догађаја 43
5.4.2 Фреквенција процесирања логова 44
5.4.3 Период чувања *audit* логова 44
5.4.4 Заштита *audit* логова 44
5.4.5 Процедуре backup-а *audit* логова 44
5.4.6 Систем сакупљања *audit* логова 44
5.4.7 Обавјештавање субјекта који је проузроковао догађај 44
5.4.8 Оцјена рањивости система 44
5.5 Архивирање записа - логова 44
5.5.1 Типови архивираних записа 44
5.5.2 Период чувања архиве 44
5.5.3 Заштита архиве 45
5.5.4 Процедура *backup-а* архиве 45
5.5.5 Захтјеви за *timestamping* записима 45
5.5.6 Систем сакупљања записа 45
5.5.7 Процедуре за добијање и верификацију информација из архиве 45
5.6 Измјена кључева 45
5.7 Компромитација и опоравак у случају катастрофе 46
5.7.1 Процедуре за поступање у инцидентним и компромитујућим ситуацијама 46
5.7.2 Рачунарски ресурси, софтвер или подаци који су оштећени 46
5.7.3 Процедуре које се спроводе код компромитације приватног кључа ЦА 46
5.7.4 Могућности континуитета пословања након катастрофе 46
5.8 Завршетак рада ЦА МНРВОИД 46
6 Техничке безбједносне контроле 47
6.1 Генерисање и инсталација асиметричног пара кључева 47
6.1.1 Генерисање асиметричног пара кључева 47
6.1.2 Испорука приватног кључа кориснику 48
6.1.3 Достава јавног кључа до издаваоца цертификата 48
6.1.4 Достава јавног кључа издаваоца цертификата трећим странама 48
6.1.5 Дужине кључева 48
6.1.6 Генерисање криптографских параметара и провјера квалитета 49
6.1.7 Могуће „*Key Usage*" опције 49
6.2 Заштита приватног кључа и контрола криптографског хардверског модула 49
6.2.1 Стандарди и контроле криптографског хардверског модула 50

6.2.1.1 Стандарди и контроле криптографског модула за кориснике 50
6.2.1.2 Персонализација 52
6.2.2 *k* од *n* дистрибуција одговорности контроле приватног кључа 52
6.2.3 Безбједно чување приватног кључа 53
6.2.4 Backup приватног кључа 53
6.2.5 Архивирање приватног кључа 53
6.2.6 Трансфер приватног кључа на хардверски криптографски модул 53
6.2.7 Чување приватног кључа на хардверском криптографском модулу 53
6.2.8 Метода активације приватног кључа 53
6.2.9 Метода деактивирања приватног кључа 54
6.2.10 Метода уништења приватног кључа 54
6.2.11 Оцјењивање криптографских модула 54
6.3 Други аспекти управљања паром кључева 54
6.3.1 Архивирање јавног кључа 54
6.3.2 Периоди важења цертификата и приватног кључа 54
6.4 Активациони подаци 54
6.4.1 Генерисање и инсталација активационих података 55
6.4.2 Заштита активационих података 55
6.4.3 Други видови активационих података. 55
6.5 Безбједносне контроле рачунарског система 55
6.5.1 Специфични захтјеви за безбједност рачунарског система 55
6.5.2 Рангирање безбједности рачунара 55
6.6 Животни циклус техничких безбједносних контрола 55
6.6.1 Контроле развоја система 55
6.6.2 Контроле управљања безбједношћу 55
6.6.3 Животни циклус безбједносних контрола 56
6.7 Мрежне безбједносне контроле 56
6.8 Временски жиг 56
7 Профили цертификата и ЦР листа 56
7.1 Профили цертификата 56
7.1.1 Број верзије 56
7.1.2 Екстензије у цертификату 56
7.1.2.1 Општи профил цертификата 57
7.1.2.2 Профил *MNRVOID CA Root* цертификата 57
7.1.2.3 Профил *MNRVOID CA Subordinate* цертификата 57
7.1.2.4 Профил цертификата корисника 58

7.1.3 Објектни идентификатори алгоритама 60
7.1.4 Форме имена 60
7.1.5 Ограничења имена 60
7.1.6 Објектни идентификатор политике цертификације 61
7.1.7 Коришћење „*Policy Constraints*“ екстензије 61
7.1.8 Синтакса и семантика „*Policy Qualifier*“-са 61
7.1.9 Семантика процесирања критичне екстензије „*Certificate Policies*“ 61
7.2 Профил ЦР листе 61
7.2.1 Број верзије 62
7.2.2 CRL и CRL *entry* екстензије 62
7.3 ОЦСП профил 62
8 Провјера сагласности и друга оцјењивања 63
8.1 Фреквенција или услови оцјењивања 63
8.2 Идентитет/квалификације процјењивача 63
8.3 Однос оцјењивача према оцјењиваном ентитету 64
8.4 Теме покривене у процесу оцјењивања 64
8.5 Активности предузете као резултат утврђених недостатака 64
8.6 Комуникација резултата 64
9 Остали пословни и правни аспекти 65
9.1 Цијене 65
9.1.1 Цијене издавања цертификата 65
9.1.2 Цијена приступа цертификатима 65
9.1.3 Цијена приступа информацијама о статусу цертификата 66
9.1.4 Цијене за друге сервисе 66
9.1.5 Политика поврата новца 66
9.2 Финансијска одговорност 66
9.2.1 Покривање осигурања 66
9.2.2 Друга добра 66
9.2.3 Осигурање или гаранцијско покривање за крајње кориснике 66
9.3 Повјерљивост пословних информација 66
9.3.1 Опсег повјерљивих информација 67
9.3.2 Информације које нису у опсегу повјерљивих информација 67
9.3.3 Одговорност за заштиту повјерљивих информација 67
9.4 Приватност и заштита личних података 67
9.4.1 План приватности 67
9.4.2 Информације које се третирају као приватне 67

9.4.3 Информације које се не сматрају приватним 67
9.4.4 Одговорност за заштиту приватних информација 67
9.4.5 Обавјештење и сагласност на коришћење тајних података о личности 67
9.4.6 Откривање информација сходно правним и административним процесима 68
9.4.7 Друге околности за откривање информација 68
9.5 Права интелектуалног власништва 68
9.6 Права и обавезе 68
9.6.1 ЦА права и обавезе 68
9.6.2 Корисничка права и обавезе 69
9.6.3 Права и обавезе трећих страна 70
9.6.4 Права и обавезе других учесника 70
9.7 Непризнавање права 70
9.8 Ограничења одговорности 71
9.9 Одштете 72
9.10 Ступање на снагу и период важења ових Практичних правила 72
9.10.1 Ступање на снагу 72
9.10.2 Престанак важења 72
9.10.3 Ефекат завршетка и поновног рада 72
9.11 Појединачна обавјештења и комуникација са учесницима 72
9.12 Исправке 72
9.12.1 Процедуре за исправку 72
9.12.2 Механизам и период обавјештавања 72
9.12.3 Услови промјене објектног идентификатора (ОИД) 73
9.13 Процедуре рјешавања спорова 73
9.14 Закон који се поштује 73
9.15 Сагласност са примјенљивим законима 73
9.16 Остале одредбе 73
9.16.1 Комплетан уговор 73
9.16.2 Пренос права 73
9.16.3 Клаузула о ваљаности 74
9.16.4 Спровођење адвокатских накнада и одрицање од права 74
9.16.5 Виша сила 74
9.17 Друге одредбе 74
10 Референце 74

1 Увод

На основу закона којима се регулише организација система републичке управе Републике Српске, Министарство за научнотехнолошки развој, високо образовање и информационо друштво Републике Српске (у даљем тексту: МНРВОИД) врши стручне послове који су у вези са дигиталним идентитетима правних и физичких лица из Републике Српске, електронским представљањем и потписивањем. У складу са овим, МНРВОИД је успоставило инфраструктуру јавног кључа (енг. *Public Key Infrastructure* - у даљем тексту ПКИ) и на подручју Републике Српске је присутно као квалификовано цертификационо тијело које пружа услуге издавања квалификованих електронских цертификата, под именом цертификационо тијело Министарства за научнотехнолошки развој, високо образовање и информационо друштво Републике Српске (у даљем тексту: ЦА МНРВОИД, односно скраћеница MNRVOID CA када се користи као назив цертификационог тијела у техничком систему ПКИ).

ЦА МНРВОИД издаје квалификоване електронске цертификате у складу са законским и подзаконским актима којима се уређује област електронског потписа и других услуга повјерења у Републици Српској.

Политика цертификације (енг. *Certification Policy*, у даљем тексту: ЦП) ЦА МНРВОИД и Практична правила пружања услуга цертификације ЦА МНРВОИД (енг. *Certificate Practice Statement*, у даљем тексту: ЦПС) су јавно доступни документи који се објављују на страници цертификационог тијела.

Поред ових докумената, ЦА МНРВОИД прописује и интерна правила рада ЦА МНРВОИД као и заштиту система цертификације. Интерна правила рада представљају пословну тајну и као таква нису јавно доступна.

ЦА МНРВОИД Републике Српске издаје квалификоване електронске цертификате у складу са одговарајућим међународним стандардима и препорукама, а чија примјена је предвиђена законским и подзаконским актима којима се уређује област електронског потписа и других услуга повјерења Републике Српске.

1.1 Преглед

ЦА МНРВОИД у својој ПКИ инфраструктури за издавање квалификованих цертификата користи хијерархију више цертификационих тијела (енг. *Certification Authority,* у даљем тексту: ЦА).

Инфраструктуру ЦА МНРВОИД чине два цертификациона тијела:

- *MNRVOID CA Root*, као *Root,* самопотписано цертификационо тијело,
- *MNRVOID CA 1*, као подређено (енг. *subordinate*) цертификационо тијело, које издаје цертификате крајњим корисницима.

MNRVOID CA Root сервер ради као Root цертификационо тијело на основу цертификата издатог самом себи (енг. *self-signed certificate*) у процесу генерисања приватног криптографског кључа апликације цертификационог тијела (енг. *Root Key Generation Ceremony*). *MNRVOID CA*

Root сервер издаје цертификате подређеним цертификационим тијелима која су дио MNRVOID CA инфраструктуре.

MNRVOID CA 1 сервер као подређено (енг. *subordinate*) цертификационо тијело издаје квалификоване цертификате за електронски потпис физичким лицима и квалификоване цертификате за електронски печат правним лицима.

Функционисање хијерархијске инфраструктуре у потпуности је у складу са Политиком цертификације и овим Практичним правилима која су обавезујућа за ЦА МНРВОИД, лица којима је ЦА МНРВОИД издало квалификоване цертификате и трећа лица која се поуздају у цертификат издат од стране ЦА МНРВОИД.

Квалификовани цертификати су стандардни цертификати x.509 верзије 3 који су намијењени за валидацију квалификованог електронског потписа или печата.

Корисници квалификованих цертификата ЦА МНРВОИД посједују један пар криптографских кључева - јавни и приватни кључ. Приватни криптографски кључ се користи за квалификовано електронско потписивање или печатирање, а јавни криптографски кључ се користи за валидацију квалификованог електронског потписа или печата.

ЦА МНРВОИД обезбјеђује средство за формирање електронског потписа или печата корисницима - паметна картица која задовољава одговарајуће безјбедоносне стандарде и која је посебно визуелно персонализована паметна картица (у даљем тексту: еСрпска паметна картица). ЦА МНРВОИД обезбјеђује и придружени активациони код (пин код) за активацију ове паметне картице.

ЦА МНРВОИД утврђује и интерна правила рада цертификационог тијела и заштите система цертификације (у даљем тексту: Интерна правила) којима се осигурава исправно провођење заштитних и безбједносних мјера у систему цертификцаије. Интерна правила су приватни документи и представљају пословну тајну цертификационог тијела.

Практична правила ЦА МНРВОИД представљају документ који описује поступке које примјењује ЦА МНРВОИД приликом издавања квалификованог електронског цертификата, употребе квалификованог електронског цертификата од стране крајњег корисника и опозива квалификованог електронског цертификата. Документ је структурисан по RFC 3647[1], односно међународно прихваћеном обрасцу ETSI EN 319 411-2 - *Policy Requirements for Certification Authorities Issuing Qualified Certificates*.

1.2 Назив докумената и идентификациони подаци

Овај документ носи назив ,,Практична правила пружања услуга цертификације Цертификационог тијела Министарства за научнотехнолошки развој, високо образовање и информационо друштво Републике Српске".

ЦА МНРВОИД издаје квалификоване електронске цертификате за потребе реализације функција аутентификације, шифровања и квалификованог електронског потписа на паметној еСрпска картици.

Идентификациона ознака документа (енг. *Object Identifier* – ОИД) је: 1.3.6.1.4.26614.20.1.1.

[1] RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

Идентификационе ознаке докумената Политике цертификације Цертификационог тијела Министарства за научнотехнолошки развој, високо образовање и информационо друштво и Практична правила ЦА МНРВОИД су приказане у табели испод.

ОИД		Објашњење
1.3.6.1.4.1.26614.		Јединствен идентификациони број који је додијељен Влади Републике Српске од стране IANA
1.3.6.1.4.1.26614.20		Јединствени идентификациони број који је додијељен ЦА МНРВОИД од стране Владе Републике Српске
1.3.6.1.4.1.26614.20.x	x=0	Јединствени идентификациони број додијељен од стране ЦА МНРВОИД за документ Политика цертификације
	x=1	Јединствени идентификациони број додијељен од стране ЦА МНРВОИД за документ Практична правила
1.3.6.1.4.1.26614.20.x.y	y –	актуелна верзија документа

Табела 1: OID и њихова значења унутар ЦА МНРВОИД

1.3 Учесници ПКИ система

У овом поглављу дате су основне информације о учесницима у оквиру ПКИ система ЦА МНРВОИД.

Учесници ПКИ система ЦА МНРВОИД су:

- ЦА,
- Регистрационо тијело (енг. *Registration Authority*, у даљем тексту: РА) које се састоји од централног регистрационог тијела при ЦА МНРВОИД (у даљем тексту: централно РА) и локалног регистрационог тијела (у даљем тексту: локално РА),
- корисници услуге цертификације,
- треће стране и
- остали учесници.

1.3.1 **Цертификационо тијело МНРВОИД**

Структура ЦА МНРВОИД састоји се од:

- Управљачког тијела ЦА МНРВОИД (енг. *Policy Management Authorithy*, у даљем тексту: ПМА)
- ЦА, и
- РА.

1.3.1.1 Управљачко тијело

Управљачког тијело ЦА МНРВОИД - ПМА је тијело у оквиру ЦА МНРВОИД, које је одговорно за администрирање, разматрање, припрему, усвајање и спровођење одлука које се односе на рад ЦА МНРВОИД.

ПМА врши интерни надзор над радом ЦА, РА тијела и осталих учесника у пословном процесу.

1.3.1.2 Цертификационо тијело

ЦА МНРВОИД обухвата два цертификациона тијела, и то:

- *MNRVOID CA Root*, као *Root* цертификационо тијело,
- *MNRVOID CA 1*, као подређено цертификационо тијело.

1.3.2 **Регистрационо тијело**

РА ЦА МНРВОИД састоји се од:

- Централног РА које се налази у сједишту ЦА МНРВОИД и које је задужено за одобравање и прослеђивање података за издавање квалификованих електронских цертификата и захтјева за суспензију или опозив цертификата (у даљем тексту: захтјев за промјену статуса цертификата),
- Локалног РА које је доступно на удаљеним локацијама, а које чине организационе јединице Агенције за посредничке, информатичке и финансијске услуге (у даљем тесту: АПИФ) на територији Републике Српске. Листа доступних локалних РА објављује се и ажурира на интернет страници ЦА МНРВОИД. Пословнице локалног регистрационог тијела овлашћене су за провјеравање идентитета корисника, провјеру тачности и правилности поднесених захтјева и доказа о извршеној уплати накнаде за издавање квалификованих електронских цертификата, као и за прослеђивање исправно попуњених захтјева за издавање квалификованих електронских цертификата према централном регистрационом тијелу и других одговарајућих докумената.

У поступцима обраде захтјева корисника ЦА МНРВОИД, на основу захтјева физичког лица из Републике Српске, Босне и Херцеговине за издавање квалификованог електронског потписа или захтјева овлаштеног лица из Републике Српске, Босне и Херцеговине за подношење захтјева за издавање квалификованог електронског печата за правна лица, користе се подаци из евиденција грађана Републике Српске, Босне и Херцеговине, а који се воде у складу са важећим законским и подзаконским актима којима се регулише област полиције и унутрашњих послова Републике Српске, Босне и Херцеговине. Ови подаци обухватају личне податке и фотографију подносиоца захтјева. Подаци о лицима из Републике Српске, Босне и Херцеговине преузимају се електронским путем од надлежног тијела за вођење датих евиденција, уз обавезно потписану сагласност за обраду личних података подносиоца захтјева.

У поступцима обраде захтјева корисника, на основу захтјева овлаштеног лица за подношење захтјева за издавање кавлификованог електронског цертификата за правна лица - електронског печата, користе се подаци из регистра пословних субјеката Републике Српске, а који се води у складу са законом којим се регулише област вођења регистара пословних субјеката Републике Српске. Надлежно тијело за вођење овог регистра у Републици Српској према важећем пропису је АПИФ.

Обавезе локалног регистрационог тијела - АПИФ су:

- Пријем захтјева за издавање квалификованих цертификата ЦА МНРВОИД у складу са Политиком цертификације и овим Практичним правилима;
- Провјера исправности попуњеног захтјева за издавање квалификованог цертификата ЦА МНРВОИД;

- Провјера идентитета лица које подноси захтјев за издавање квалификованих цертификата ЦА МНРВОИД;
- Провјера доказа о извршеној уплати накнаде за издавање квалификованих цертификата ЦА МНРВОИД;
- Преузимање исправно попуњеног и потписаног захтјева и сагласности за обраду личних података подносиоца захтјева;
- Достављање писаног захтјева за издавање квалификованих цертификата ЦА МНРВОИД и друге пратеће документације;
- Обавјештавање подносиоца захтјева о издатом квалификованом цертификату ЦА МНРВОИД те његово уручивање подносиоцу захтјева уз обавезну провјеру идентитета подносиоца захтјева код уручивања, као и уручивање обавијести о одбијању захтјева за издавање квалификованиог цертификата подносиоцу захтјева.

1.3.3 **Корисници услуга**

Корисници услуга ЦА МНРВОИД су физичка и правна лица која су склапањем уговора са ЦА МНРВОИД као тијелом које пружа услуге повјерења преузела уговорне обавезе корисника.

Корисници услуга ЦА МНРВОИД могу бити:

- физичка лица и
- правна лица.

У категорији правних лица као корисника услуга ЦА МНРВОИД могу се наћи лица различитих правних форми у складу с прописима Републике Српске као што су предузећа, самостални предузетници, органи јавне управе и др.

Обавезе корисника су да:

- поштују Политику цертификације и Практична правила ЦА МНРВОИД;
- посједују одговарајућа знања за коришћење квалификованих електронских цертификата;
- пруже тачне и прецизне информације РА;
- користе цертификате ЦА МНРВОИД у складу са Политиком цертификације и Практичним правилима ЦА МНРВОИД, као и важећим законским и подзаконским актима којима се уређује област електронског потписа, других услуга повјерења, електронског документа и електронског пословања Републике Српске и Босне и Херцеговине.
- обавијесте локално РА или ЦА МНРВОИД о било којим промјенама података који су достављени код подношења захтјева за издавање квалификованих цертификата, у складу са Политиком цертификације и Практичним правилима ЦА МНРВОИД, као и важећим законским и подзаконским актима којима се уређује област електронског потписа и других услуга повјерења Републике Српске;
- престану користити цертификат ЦА МНРВОИД уколико је било која информација у цертификату постала неважећа или нетачна;
- користе само један квалификовани цертификат за квалификовани електронски потпис у датом тренутку;

- захтијевају промјену статуса издатог квалификованог цертификата: суспензију или опозив у случају догађаја који утиче на интегритет издатог цертификата или уколико сумњају на злоупотребу приватног кључа.

1.3.4 **Треће стране**

Трећа лица су лица која прихватају квалификоване електронске цертификате ЦА МНРВОИД и верификују квалификовани електронски потпис електронских докумената која су потписана од стране корисника ЦА МНРВОИД цертификата.

Трећа лица су обавезна провјерити статус цертификата у регистру опозваних цертификата (на енглеском језику - *Certificate Revocation List* - у даљем тексту: *ЦР листа*), при чему је ЦА МНРВОИД одговорно за редовно ажурирање ЦР листе.

ЦР листа се ажурира на дневном нивоу. Трећа лица провјеравају расположиве листе опозваних цертификата, како би имали увид у опозване и суспендоване цертификате. Трећа лица ни под којим условима не треба да се ослањају на ЦР листе након истека важења исте.

1.3.5 **Остали учесници**

Остала учесници су друга лица која на било који начин учествују у раду ЦА МНРВОИД, као што су произвођачи и дистрибутери опреме и софтвера за ЦА МНРВОИД.

Остали учесници су сва лица која приступају регистру опозваних цертификата и интернет страници ЦА МНРВОИД. Сви они који приступају датим ресурсима ЦА МНРВОИД су сагласни са одредбама Политике цертификације, као и са одредбама ових Практичних правила, те другим важећим одредбама који се тичу коришћења услуга ЦА МНРВОИД.

ЦА МНРВОИД редовно ажурира садржаје у циљу осигурања да стране које приступају датим ресурсима добијају поуздане, ажурне и тачне информације.

ЦА МНРВОИД, међутим, не може прихватити било какву одговорност која је ван ограничења дефинисаних у Политици цертификације и овим документом.

1.4 Употреба цертификата

У овом поглављу се дефинише прихватљиво коришћење квалификованих електронских цертификата издатих од стране ЦА МНРВОИД.

1.4.1 **Подручје примјене**

Квалификовани цертификати и припадајући приватни кључеви користе се за:

- квалификовано електронско потписивање или квалификовано електронско печатирање, и
- аутентификацију корисника.

1.4.1.1 Подручје примјене *MNRVOID CA Root* цертификата

MNRVOID CA Root цертификат је самопотписани цертификат, а његов приватни криптографски кључ се користи за:

- потписивање цертификата подређеног *MNRVOID CA 1*,
- потписивање листе опозваних цертификата коју издаје *MNRVOID CA Root*

1.4.1.2 Подручје примјене *MNRVOID CA 1* цертификата

MNRVOID CA 1 цертификат је цертификат подређеног цертификационог тијела које издаје квалификоване електронске цертификате крајњим корисницима. Приватни криптографски кључ *MNRVOID CA 1* цертификата се користи за:

- потписивање цертификата крајњих корисника које издаје *MNRVOID CA 1*,
- потписивање ЦР листа које издаје *MNRVOID CA 1*.

1.4.2 Недозвољена примјена

Није дозвољена употреба квалификованог електронског цертификата ако није дефинисана овим документом и ако није у сагласности са законским и подзаконским актима којима се уређује област електронског потписа и других услуга повјерења Републике Српске.

1.5 Политика администрирања документа

У окивиру овог поглавља се налазе описани начини управљања израдом овог документа, као и контакт особе задужене за примјену документа.

1.5.1 Организација управљања документом

Документ Практична правила пружања услуга цертификације ЦА МНРВОИД креира и ажурира ЦА МНРВОИД:

Министарство за научнотехнолошки развој, високо образовање и информационо друштво Републике Српксе

Трг Републике Српске 1

78000 Бања Лука

Тел: 051/339-744

Факс: 051/338-856

Електронска пошта: ca@mnrvoid.vladars.net

Интернет страница МНРВОИД: https://www.vladars.net/sr-SP-Cyrl/Vlada/Ministarstva/mnk/Pages/default.aspx

Интернет страница ЦА МНРВОИД: https://www.vladars.net/sr-SP-Cyrl/Vlada/Ministarstva/mnk/Pages/default.aspx

Важећа верзија документа може се преузети са интернет странице ЦА МНРВОИД http://ca.vladars.net/policy/.

Промјене садржаја документа обављају се путем интерних приједлога и захтјева за усклађивањем са законском регулативом и другим мјеродавним нормама.

1.5.2 Лица за контакт

Лица за контакт су запослени у ЦА МНРВОИД који су овлашћени за пружање информација у вези овог документа, пословних процеса ЦА МНРВОИД, као и комуникације са корисницима. Контакт информације запослених у ЦА МНРВОИД могу се видјети на интернет страници ЦА МНРВОИД, како је наведено у 1.5.1.

1.5.3 **Лица одређена за усклађивање докумената са праксом издавања цертификата**

ПМА ЦА МНРВОИД усклађује форму и садржај овог документа са евентуалним промјенама насталим у процесу издавања квалификованих цертификата.

ПМА ЦА МНРВОИД такође редовно и ванредно, односно по потреби процјењује усклађеност Практичних правила са важећим законским и подзаконским актима Републике Српске, као и са међународним стандардима и регулативом.

1.5.4 **Процедуре за одобрење Практичних правила**

Документ Практична правила се редовно периодично прегледа и по потреби ажурира. Интерном процедуром се дефинише период прегледа Практичних правила, а који не може бити дужи од једне године. Практична правила се могу ажурирати и чешће него једном годишње уколико се десе промјене у интерним процедурама, законској регулативи или дође до промјене у примјењеним криптографским алгоритмима и дужинама криптографских кључева.

Процедура у случају ажурирања, корекције или креирања нове верзије документа овог документа је сљедећа:

- ЦА креира нову верзију документа Практична правила у складу са законском регулативом и измјењеним пословним процесима ЦА МНРВОИД,
- ЦА подноси нову верзију документа ПМА на разматрање, усклађивање и одобравање,
- ПМА одобрава нову верзију документа Практична правила или га упућује ЦА на додатне корекције и усклађивање,
- ЦА МНРВОИД објављује ажурирану верзију документа Практична правила.

1.6 Дефиниције и скраћенице

Поједини изрази који се користе у овим Практичним правилима имају сљедеће значење:

Цертификационо тијело - правно лице, орган јавне управе или самостални предузетник у Републици Српској који је регистрован и који издаје електронске цертификате или пружа друге услуге повјерења које су у вези са електронским потписима у складу с законским и подзаконским актима којима се регулише област електронског потписа и других услуга повјерења у Републици Српској.

Електронски документ - једнообразно повезан цјеловит скуп података који су електронски обликовани (израђени помоћу рачунара и других електронских уређаја), послани, примљени или сачувани на електронском, магнетном, оптичком или другом медију и који садржи особине којима се утврђује аутор, утврђује вјеродостојност садржаја, те доказује вријеме када је документ сачињен.

Електронски потпис – скуп података у електронском облику који су придружени или су логички повезани са другим подацима у електронском облику и који служе за идентификацију потписника и аутентичност потписаног електронског документа.

Квалификовани електронски потпис – потпис којим се поуздано гарантује идентитет потписника и који испуњава услове прописане у складу законским и подзаконским актима

којима се регулише област електронског потписа и других услуга повјерења у у Републици Српској.

Електронски печат - скуп података у електронском облику који су придружени или су логички повезани са другим подацима у електронском облику и који обезбјеђују аутентичност и цјеловитост тих података.

Квалификовани електронски печат – електронски печат који је креиран помоћу средства за израду квалификованог електронског печата и који се заснива на квалификованом цертификату за електронски печат.

Електронски цертификат за електронски потпис - потврда у електронском облику која повезује податке за верификацију електронског потписа са неким лицем и потврђује идентитет тог лица.

Електронски цертификат за електронски печат - потврда у електронском облику која повезује податке за верификацију електронског печата са правним лицем, односно самосталним предузетником и органом јавне управе и потврђује назив тог правног лица, односно самосталног предузетника и органа јавне управе.

Квалификовани електронски цертификат за електронски потпис – потврда коју је издало Цертификационо тијело и која испуњава услове прописане законским и подзаконским актима којима се регулише област електронског потписа и других услуга повјерења у Републици Српској.

Квалификовани електронски цертификат за електронски печат – потврда коју је издало Цертификационо тијело и који испуњава услове прописане законским и подзаконским актима којима се регулише област електронског потписа и других услуга повјерења у Републици Српској.

Корисник – правно лице, односно самостални предузетник, орган јавне управе или физичко лице које користи услуге цертификационог тијела.

Правно лице – пословни субјект, односно самостални предузетник или орган јавне управе.

Потписник – лице које посједује средство за израду електронског потписа, а које потписује у своје име или у име правног лица, односно самосталног предузетника или органа јавне управе.

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

Средство за израду електронског потписа – одговарајућа рачунарска опрема и рачунарски програм које потписник користи при изради електронског потписа.

Средство за израду квалификованог електронског потписа – одговарајућа рачунарска опрема и рачунарски програм које потписник користи при изради електронског потписа и који испуњавају услове прописане законским и подзаконским актима којима се регулише област електронског потписа и других услуга повјерења у Републици Српској.

Подаци за верификацију електронског потписа – подаци, као што су кодови или јавни криптографски кључеви, који се користе ради провјере валидности електронског потписа.

Средство за верификацију електронског потписа – одговарајућа рачунарска опрема и рачунарски програм који се користе за провјеру података за верификацију потписа.

Идентификација - поступак провјере идентитета корисника у поступку подношења захтјева за издавање, суспензију или опозив квалификованог електронског цертификата.

Аутентикација - електронски поступак провјере и потврђивања идентитета власника цертификата.

Цертификација - поступак издавања квалификованих електронских цертификата.

Пар кључева асиметричног криптографског алгоритма – два јединствено повезана криптографска кључа, од којих је један јавни кључ, а други приватни кључ.

Јавни кључ - јавно познат кључ из корисничког пара кључева.

Приватни кључ - кључ из корисничког пара кључева који је познат само кориснику.

У табели испод су дате скраћенице које се користе у овом документу, као и њихово значење.

Скраћеница	Значење скраћенице
МНРВОИД	Министарство за научнотехнолошки развој, високо образовање и информационо друштво Републике Српске
ЦА	енг. *Certification Authority* - Цертификационо тијело
ЦА МНРВОИД	Цертификационо тијело Министарства за научнотехнолошки развој, високо образовање и информационо друштво Републике Српске
РА	енг. *Registration Authority* - Регистрационо тијело
Централно РА	Централно регистрационо тијело
Локално РА	Локално регистрационо тијело
АПИФ	Агенција за посредничке, информатичке и финансијске услуге Републике Српске
ПМА	енг. *Policy Management Authorithy* - Управљачко тијело ЦА МНРВОИД
ЦП	енг. *Certification Policy* - Политика цертификације
ЦПС	енг. *Certificate Practice Statement* - Практична правила пружања услуга цертификације
ЦР листа	енг. *Certificate Revocation List* - Регистар опозваних цертификата
ДН	енг.*Distinguished Name* - Јединствено име
ОИД	енг. *Object Identifier* - Јединствени идентификациони број објекта
ПКИ	енг. *Public Key Infrastructure* - Инфраструктура јавних кључева
ЦДП	енг. *CRL Distribution Point* - Линк за локацију опозваних цертификата
ХСМ	енг. *Hardware Security Module* - Хардверски криптографски модул
АИА	енг. *Authority Information Access* - Линк за локацију

	цертификата цертификционог тијела
ЈИБ	Јединствени идентификациони број правног лица
ЈМБ	Јединствени матични број физичког лица
МБ	Матични број - јединствена идентификациона нумеричка ознака субјекта уписа у Регистру привредних субјеката у Републици Српској
Паметна картица	Мини-рачунар, који у себи садржи меморију, процесор и интерфејс за приступ подацима на тој картици и напајање
Паметна еСрпска картица	Визуелно персонализована паметна картица према дизајну ЦА МНРВОИД
УРЛ	Интернет локација
Audit логовања	Испис података о електронском приступу појединим компонентама ПКИ система у сврху праћења и контроле приступа запослених
Backup	Архива
MNRVOID CA Root	Самопотписано цертификационо тијело
MNRVOID CA 1	Подређено (*subordinate)* цертификационо тијело
SSCD	енг. *Secure Signature Creation Device* – софтвер или харвдер који омогућава генерисање електронског потписа, а који је у складу са спецификацијама Анекса II Директиве 910/2014.
ОЦСП	енг. *Online Certificate Status Protokol* - Сервис за *on-line* провјеру статуса цертификата
Hash алгоритам	Математички алгоритам који омогућава мапирање података произвољне величине (енг. *message*) у одговарајући низ фиксне величине (енг. *hash, hash value*)
Key Usage екстензије	Екстензије које дефинишу намјену одређеног цертификата
Enhanced Key Usage екстензије	Екстензије које указују на једну или више намјена јавног кључа, поред или умјесто основних намјена дефинисаних у *Key Usage* екстензији

Табела 2: Скраћенице које се користе у овом документу

2 Објављивање и локација података о цертификацији

У оквиру овог поглавља се налазе описане локације за објављивање података везаних за цертификацију.

2.1 Локација за објављивање података о цертификацији

ЦА МНРВОИД објављује податке и сву документацију која се односи на издавање квалификованих електронских цертификата на интернет страници: https://www.vladars.net/sr-SP-Cyrl/Vlada/Ministarstva/mnk/ca/Pages/default.aspx која је јавно доступна као и наведени подаци и документација.

Јавно доступна документација и информације о ЦА МНРВОИД налазе се на интернет страници: https://www.vladars.net/sr-SP-Cyrl/Vlada/Ministarstva/mnk/ca/Pages/default.aspx Регистар суспендованих и опозваних цертификата - ЦР листа ЦА МНРВОИД налази се на интернет страници http://root.ca.vladars.net/cdp/ као и на секундарној интернет страници http://sub.ca.vladars.net/cdp/. Наведене интернет странице су уписане у Линк за локацију опозваних цертификата (енг. CRL Distribution Point – у даљем тексту: ЦДП) сваког крајњег корисника.

Цертификати *MNRVOID Root CA* и *MNRVOID CA 1* могу се преузети и са интернет странице http://ca.vladars.net/aia/.

Регистар суспендованих и опозваних цертификата - ЦР листа ЦА МНРВОИД налази се и на интернет страници http://ca.vladars.net/cdp/

2.2 Објављивање података о цертификацији

ЦА МНРВОИД објављује на својој интернет страници сљедеће податке:

- важеће законске и подзаконске акте којима се уређује област електронског потписа и других услуга повјерења, електронског документа и електронског пословања у Републици Српској, Босни и Херцеговини;
- Политику цертификације ЦА МНРВОИД,
- Практична правила пружања услуга цертификације ЦА МНРВОИД,
- обрасце уговора за пружање услуга цертификације,
- обрасце захтјева за коришћење услуга цертификације, суспензије и опозива издатих цертификата
- корисничка упутства,
- цертификате *MNRVOID Root CA* и *MNRVOID CA 1*,
- регистар опозваних цертификата,
- цјеновник о висини накнада за услуге електронске цертификације,
- друга акта и обавјештења.

2.3 Учесталост објављивања података о цертификацији

ЦА МНРВОИД ажурира објављене податке сљедећом динамиком:

- ЦР листу: регистре суспендованих или опозваних цертификата која се објављује на свака 24 сата. У случају опозива или суспензије цертификата, ажурирани регистар опозваних цертификата се одмах објављује.
- промјене на постојећим документима објављују се у најкраћем року послије настале промјене,
- додатни документи објављују се у најкраћем року по одобравању и усвајању.

2.4 Контрола приступа подацима о цертификацији

Подаци који су објављени на званичној интернет страници ЦА МНРВОИД су јавно доступни. Приступ је ограничен на могућност читања.

ЦА МНРВОИД има успостављане логичке и физичке мјере безбједности за заштиту података на интернет страници од неовлаштеног брисања, додавања или промјена.

Приступ ЦА МНРВОИД интернет страници и подацима је бесплатан, али ЦА МНРВОИД задржава право да врши наплату одређених електронских сервиса који су доступни на интернет страници ЦА МНРВОИД.

3 Идентификација и аутентификација

У оквиру овог поглавља су дефинисани критеријуми на основу којих се врши идентификација и аутентикација корисника у поступку подношења захтјева за издавање, суспензију или опозив квалификованог електронског цертификата, тако што се дефинишу називи, иницијална провјера идентитета корисника и слично. Поступке идентификације и потврђивања идентитета корисника проводи мрежа локалних регистрационих тијела.

3.1 Називи

Називима се дефинишу типови имена, номенклатура имена, те критеријуми за анонимност и псеудониме корисника.

3.1.1 **Типови имена**

У квалификованим електронским цертификатима које издаје ЦА МНРВОИД имена корисника цертификата као и име цертификационог тијела које издаје цертификате су јединствена имена (на енглеском језику: *Distinguished Name*, у даљем тексту: ДН).

3.1.2 **Номенклатура имена**

ЦА МНРВОИД користи номенклатуту имена која гарантије јединственост имена у свом ПКИ систему. Јединственост имена се постиже кориштењем комбинације имена и презимена корисника и јединственог матичног броја(у даљем тексту: ЈМБ) за физичка лица, односно употребом имена правног лица и јединственог идентификационог броја (у даљем тексту: ЈИБ) за правна лица.

ЦА МНРВОИД користи екстензију *Subject Alternative Name* у које може да се унесе адреса електронске поште корисника цертификата.

3.1.3 Анонимност или псеудоними корисника

Корисници не могу да буду анонимни и не могу да користе псеудониме. ЦА МНРВОИД ће одбити сваки захтјев за издавање квалификованог електронског потписа унутар ког корисник жели да буде аноним или жели да користи псеудоним.

3.1.4 Правила за тумачење различитих врста имена

У квалификованим електронским цертификатима, имена корисника су вјерно представљена латиничним словима српског језика, при чему:

- име и презиме физичког лица мора бити наведено као у личној карти лица;
- скраћени и пуни назив правног лица мора бити наведено као и у службеним регистрима.

3.1.4.1 Имена цертификационих тијела

Структура имена *MNRVOID CA Root* приказана је у наредној табели.

Атрибут	Вриједност
Име *CA* сервера (CN) =	*MNRVOID CA Root*
Организација (O) =	Ministarstvo za naučnotehnološki razvoj visoko obrazovanje i informaciono društvo
Идентификатор организације(2.5.4.97) =	VATBA-440166068003
Мјесто (L) =	Banja Luka
Ентитет (S) =	Republika Srpska
Ознака државе (C) =	BA

Табела 3: Структура имена MNRVOID Root CA

Структура имена *MNRVOID CA 1* приказана је у наредној табели.

Атрибут	Вриједност
Име CA сервера (CN) =	*MNRVOID CA 1*
Организација (O) =	Ministarstvo za naučnotehnološki razvoj visoko obrazovanje i informaciono društvo
Идентификатор организације (2.5.4.97) =	VATBA-440166068003
Мјесто (L) =	Banja Luka
Ентитет (S) =	Republika Srpska
Ознака државе (C) =	BA

Табела 4: Структура имена MNRVOID CA 1

3.1.4.2 Имена крајњих корисника услуга цертификације

Структура имена крајњих корисника (поље *Subject*) услуга цертификације је приказана је у наредним табелама.

Структура имена крајњих корисника квалификованог електронског потписа - физичког лица приказана је у наредној табели:

Атрибут	Вриједност
Јединствено име (CN) =	Ime Prezime
Име (G) =	Ime
Презиме (SN) =	Prezime
Серијски број (SERIALNUMBER) =	PNOBA-JMB (Jedinstveni matični broj)
Организација/правно лице (O) =	FIZIČKO LICE

Мјесто (L) =	Општина/Grad
Ознака државе (C) =	BA

Табела 5: Структура имена крајњег корисника - физичко лице

Структура имена крајњих корисника цертификата за аутентикацију и енкрипцију - физичког лица приказана је у наредној табели:

Атрибут	Вриједност
Јединствено име (CN) =	Ime Prezime ENCR
Име (G) =	Ime
Презиме (SN) =	Prezime
Серијски број (SERIALNUMBER) =	PNOBA-JMB (Jedinstveni matični broj)
Организација/правно лице (O) =	FIZIČKO LICE
Мјесто (L) =	Opština/Grad
Ознака државе (C) =	BA

Табела 6: Структура имена крајњег корисника - физичко лице

Структура имена крајњих корисника квалификованог електронског печата - правног лица приказана је у наредној табели:

Атрибут	Вриједност
Јединствено име (CN) =	Skraćeno ime pravnog lica
Организација/правно лице (O) =	PRAVNO LICE
Организациона јединица (O) =	Pun naziv pravnog lica
Идентификатор организације (2.5.4.97) =	VATBA-JIB
Мјесто (L) =	Opština/ grad sjedišta
Ознака државе (C) =	BA

Табела 7: Структура имена крајњег корисника аутора електронског печата - правно лице

Структура имена крајњих корисника цертификата за аутентикацију и енкрипцију - правног лица приказана је у наредној табели:

Атрибут	Вриједност
Јединствено име (CN) =	Skraćeno ime pravnog lica ENCR
Организација/правно лице (O) =	PRAVNO LICE
Организациона јединица (O) =	Pun naziv pravnog lica
Идентификатор организације (2.5.4.97) =	VATBA-JIB
Мјесто (L) =	Opština/ grad sjedišta
Ознака државе (C) =	BA

Табела 8: Структура имена крајњег корисника аутора електронског печата - правно лице

3.1.5 **Јединственост имена**

ЦА МНРВОИД гарантује јединственост имена у свом ПКИ систему.

У оквиру поља „Subject“, јединственост имена се постиже употребом имена и презимена и ЈМБ - атрибут серијски број у цертификату за физичка лица (SERIALNUMBER), односно употребом имена правног лица и ЈИБ правног лица - атрибут Идентификатор организације (2.5.4.97) у цертификату за правна лица.

3.1.6 **Признавање, аутентификација и улога заштитног знака**

Имена којима би се кршила интелектуална или ауторска права других нису дозвољена. Цертификационо тијело МНРВОИД није обавезно да верификује да ли је коришћење таквих имена законито. Корисник је дужана да обезбједи законито коришћење одабраног имена односно корисник је дужан да се идентификује идентификационим документом којим се поуздано може утврдити идентит корисника.

3.2 Иницијална провјера идентитета

Провјера идентитета подносиоца захтјева за издавање квалификованог електронског цертификата ЦА МНРВОИД врши се на основу увида у личну карту физички присутног подносиоца захтјева, односно овлаштеног лица те упоређивањем података наведених у личној карти подносиоца захтјева с подацима наведеним у захтјеву подносиоца за издавање квалификованог електронског цертификата ЦА МНРВОИД.

3.2.1 **Метода доказивања посједовања приватног кључа**

Ово поглавље није примјенљиво у оквиру овог документа зато што не постоји креирање кључева изван самог ЦА тијела:

- за квалификовани електронски цертификат за потребе аутентификације/шифровања приватни кључ се креира у сигурном окружењу ЦА тијела (користећи ХСМ) ,
- за квалификовани електронски цертификат за верификацију квалификованог електронског цертификата приватни кључ се генерише на самој паметној картици.

Подносилац захтјева за издавање квалификованог електронског цертификата ЦА МНРВОИД постаје власник приватних кључева тек након преузимања персонализоване паметне еСрпска картице.

3.2.2 **Потврда идентитета правног лица**

Иницијална идентификација и потврђивање идентитета овлаштеног лица које представља правно лице се проводи поступком непосредне идентификације.

Иницијална идентификација и потврђивање идентитета лица које има пуномоћ овлаштеног лица да у његово име поднесе захтјев за издавање квалификованог електронског печата, такође се проводи поступком непосредне идентификације.

Иницијалну идентификацију и потврђивање идентитета овлаштеног лица које представља правно лице, односно лица које има пуномоћ овлаштеног лица проводи мрежа локалних регистрационих тијела.

У својству овлаштеног лица које представља правно лице које подноси захтјев за издавање, суспензију или опозив квалификованог електронског печата ЦА МНРВОИД може да буде само једно физичко лице и то:

- уколико правно лице има неколико овлаштених представника/заступника који имају неограничен обим овлаштења (без ограничења овлаштења), било који од њих може поднијети захтјев за издавање, суспензију или опозив квалификованог електронског цертификата за електронски печат;

- уколико правно лице има неколико овлаштених представника/заступника који имају различит обим овлаштења, само представника/заступник који има неограничено овлаштење (без ограничења овлаштења) може поднијети захтјев за издавање, суспензију или опозив квалификованог електронског печата ЦА МНРВОИД;
- овлаштени пуномоћник - лице које има пуномоћ од овлаштеног представника/заступника да поднесе само захтјев за издавање квалификованог електронског печата ЦА МНРВОИД.

Провјера идентитета овлаштеног подносиоца захтјева за издавање, суспензију или опозив квалификованог електронског печата ЦА МНРВОИД врши се на основу увида у личну карту овлаштеног подносиоца захтјева, те упоређивањем података наведених у личној карти овлаштеног подносиоца захтјева с подацима наведеним у захтјеву овлаштеног подносиоца захтјева.

За потребе иницијалне идентификације и потврђивања идентитета правног лица, ЦА МНРВОИД и локално РА прикупљају податке о правном лицу, као и податке о овлаштеном представнику/заступнику правног лица, односно податке о овлаштеном пуномоћнику, према обрасцу захтјева за издавање квалификованог електронског печата ЦА МНРВОИД који је доступан на интернет страници ЦА МНРВОИД.

Подаци о правном лицу обухватају податке који се налазе у регистру пословних субјеката Републике Српске, и то: Пословно име, Скраћено пословно име, Матични број (МБ), ЈИБ, Сједиште, Адреса, Поштански број мјеста сједишта, Телефон, Телефакс, Адреса електронске поште. Уколико се у Регистру пословних субјеката Републике Српске не налази податак о Поштанском броју мјеста сједишта, Телефону, Телефаксу и Адреси електронске поште, дати подаци се прикупљају, али не провјеравају.

За потребе иницијалне идентификације и потврђивање идентитета физичког лица - овлаштеног представника/заступника правног лица, односно овлаштеног пуномоћника, ЦА МНРВОИД, посредством мреже локалног регистрационог тијела, прикупља податке о наведеним лицима према обрасцу који је доступан на интернет страници ЦА МНРВОИД. Ови подаци укључују: Презиме, Име, Пол, Датум рођења, ЈМБ; као и податке о о важећој личној карти: Серијски број, Вриједи до, Надлежни орган.

ЦА МНРВОИД, кроз електронску размјену података са тијелом надлежним за вођење личних података о грађанима Републике Српске, Босне и Херцеговине, прибавља наведене личне податке о подносиоцу захтјева за издавање, суспензију или опозив квалификованог електронског печата - овлаштеном представнику/заступнику правног лица, односно овлаштеном пуномоћнику, као и фотографију датог лица.

ЦА МНРВОИД, посредством мреже локалног РА, прикупља, али не провјерава сљедеће податке о овлаштеном представнику/заступнику правног лица, односно овлаштеном пуномоћнику: Контакт телефон и Адреса електронске поште.

Након провјере података попуњеног захтјева за издавање, суспензију или опозив квалификованог електронског печата ЦА МНРВОИД у односу на податке наведене у личној карти овлаштеног подносиоца захтјева - овлаштеног представника/заступника правног лица, односно овлаштеног пуномоћника, службеник локалног РА врши визуелну провјеру идентитета овлаштеног подносиоца захтјева. Провјера се врши на основу важеће личне карте,

односно да ли постоји подударност присутног подносиоца захтјева са фотографијом у предоченој личној карти.

У случају подношења захтјева за издавање квалификованог електронског печата од стране овлаштеног пуномоћника, службеник локалног РА врши провјеру истовјетности података о представнику/заступнику који су наведени у захтјева за издавање квалификованог електронског печата са подацима о овлаштеном лицу у регистру пословних субјеката Републике Српске, као и истовјетност података о овлаштеном пуномоћнику који су наведени у овјереној пуномоћи са подацима у предоченој личној карти пуномоћника.

3.2.2.1 Потврда идентитета подносиоца код електронског подношења захтјева

Идентитет овлаштеног представника/заступника правног лица, у случају подношења захтјева за издавање или суспензију квалификованог електоронског печата електонским путем, потврђује се посредно - односно квалификованим електонским потписом овлаштеног представника/заступника којим је захтјев потписан.

3.2.3 Потврда идентитета физичког лица

Иницијална идентификација и потврђивање идентитета физичког лица се проводи поступком непосредне идентификације.

Провјера идентитета подносиоца захтјева за издавање, суспензију или опозив квалификованог електронског потписа ЦА МНРВОИД врши се на основу увида у личну карту подносиоца захтјева, те упоређивањем података наведених у личној карти подносиоца захтјева с подацима наведеним у захтјеву подносиоца за издавање квалификованог електронског потписа ЦА МНРВОИД.

Иницијалну идентификацију и потврђивање идентитета физичког лица - подносиоца захтјева за издавање квалификованог електронског потписа проводи мрежа локалних РА.

За потребе иницијалне идентификације и потврђивање идентитета физичког лица, ЦА МНРВОИД, посредством мреже локалног РА, прикупља податке о физичком лицу према обрасцу који је доступан на интернет страници ЦА МНРВОИД. Ови подаци укључују: Презиме, Име, Пол, Датум рођења, ЈМБ; као и податке о о важећој личној карти: Серијски број, Вриједи до, Надлежни орган.

ЦА МНРВОИД, кроз електронску размјену података са тијелом надлежним за вођење личних података о грађанима Републике Српске, Босне и Херцеговине, прибавља наведене личне податке о подносиоцу захтјева за издавање квалификованог електронског потписа, као и фотографију датог лица.

ЦА МНРВОИД, посредством мреже локалног РА, прикупља, али не провјерава сљедеће податке: Контакт телефон, Поштански број мјеста пребивалишта и Адреса електронске поште.

Након провјере података попуњеног захтјева за издавање квалификованог електронског потписа ЦА МНРВОИД у односу на податке наведене у личној карти подносиоца захтјева, службеник локалног регистрационог тијела врши визуелну провјеру идентитета подносиоца захтјева. Провјера се врши на основу важеће личне карте, односно да ли постоји подударност присутног подносиоца захтјева са фотографијом у предоченој личној карти.

3.2.4 **Информације о кориснику које се не провјеравају**

ЦА МНРВОИД прикупља, али не провјерава сљедеће податке о подносиоцима захтјева: Телефон, Поштански број мјеста пребивалишта и Адреса електронске поште, односно податке о Телефону, Поштанском броју мјеста сједишта, Телефаксу и Адреси електронске поште правног лица.

За тачност информација о наведеним подацима одговорност сноси подносилац захтјева, односно потписник у случају физичког лица, односно у случају правног лица овлаштени представник/ заступник правног лица или његов пуномоћник.

3.2.5 Валидација ауторитета

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

3.2.6 Критеријуми за интероперабилност

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

3.3 Идентификација и аутентикација захтјева за обнављање кључева

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

3.3.1 **Идентификација и аутентикација за рутинско обнављање кључева**

Ово поглавље није примјенљиво у оквиру ових Практичних правила. Захтјев за рутинско обнављање кључева се извршава издавањем новог квалификованог цертификата.

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

Ово поглавље није примјенљиво у оквиру ових Практичних правила. Захтјев за обнављање кључева се извршава издавањем новог квалификованог цертификата.

3.4 Идентификација и аутентикација захтјева за суспензију или опозив цертификата

У циљу провођења процедура идентификације и аутентикације захтјева за суспензију или опозив цертификата корисника, дефинисано је да корисници - власници квалификованих електронских цертификата МНРВОИД, захтјев за промјену статуса цертификата: суспензију или опозив могу поднијети на један од три начина:

- Електронским путем,
- Писаним путем, и
- Телефонским путем.

Образац захтјева за суспензију или опозив квалификованог електронског цертификата, подаци о званичној адреси електронске поште и контакт телефону налазе се на интернет страници ЦА МНРВОИД.

Власник - корисник квалификованог електронског потписа, захтјев за суспензију електронског потписа може поднијети електронски тако што електронски потписан захтјев шаље на званичну адресу електронске поште ЦА МНРВОИД.

Власник - корисник квалификованог електронског печата, захтјев за суспензију квалификованог електронског потписа може поднијети електронски тако што електронски потписан захтјев од стране овлаштеног заступника/ представника правног лица и овјерен квалификованим електронским печатом датог правног лица шаљу на званичну адресу електронске поште ЦА МНРВОИД. Електронски начин подношења захтјева за суспензију електронског цертификата дозвољен је само у ситуацијама када не постоји сумња у губитак или компромитованост приватног кључа квалификованог електронског цертификата.

Власник - корисник квалификованих електронских цертификата ЦА МНРВОИД, захтјев за суспензију или опозив квалификованог електронског потписа, може поднијети лично у просторијама ЦА МНРВОИД. Идентификација подносиоца захтјева за суспензију или опозив квалификованог електронског потписа врши се поступком непосредне идентификације, на начин који је описан у дијелу 3.2.3. Идентификација овлашћеног заступника/ представника правног лица код подношења захтјева за суспензију или опозив квалификованог електронског печата врши се поступком непосредне идентификације, на начин који је описан у дијелу 3.2.2.

Власник - корисник квалификованог електронског цертификата ЦА МНРВОИД, захтјев за суспензију или опозив квалификованог електронског потписа, може поднијети телефонским путем на званични телефонски број ЦА МНРВОИД. Корисник - власник квалификованог електронског цертификата представља се својим именом и презименом и изговара тајну ријеч за промјену статуса (суспензију или опозив), коју је дефинисао приликом закључења уговора о пружању услуга цертификације са ЦА МНРВОИД. Овлаштени службеник ЦА МНРВОИД провјерава да ли се изговорена тајна ријеч подудара са тајном ријечи која се налази у уговору са датим корисником.

ЦА МНРВОИД задржава право прибављања додатних информација и провјере оправданости захтјева за суспензију или опозив електронског цертификата у циљу отклањања потенцијалних ризика. Комуникација се у том случају успоставља лично или телефонским путем, на основу контакт података о кориснику - подносиоцу захтјева за промјену статуса и тајне ријечи дефинисане у уговору о пружању услуга цертификације између корисника и ЦА МНРВОИД.

4 Оперативни захтјеви у вези животног циклуса цертификата

Корисници имају сталну обавезу да информишу ЦА МНРВОИД о свим промјенама у информацијама које су објављене у цертификату током периода важења квалификованог електронског цертификата.

4.1 Подношење захтјева за издавање цертификата

У оквиру овог поглавља је дефинисано ко и на који начин може поднијети захтјев за издавање цертификата.

4.1.1 **Ко може да поднесе захтјев за издавање цертификата?**

ЦА МНРВОИД захтјева лично подношење захтјева за издавање квалификованог електронског цертификата, у просторијама локалног РА. Овлашћеним подносиоцима захтјева за издавање квалификованог електронског печата - власницима квалификованих електронских потписа, с обзиром да су претходно прошли процедуру личне идентификације код издавања квалификованог електронског потписа, ЦА МНРВОИД омогућава електронски начин подношења захтјева за издавање квалификованог електронског печата.

Захтјев за издавање квалификованог електронског потписа ЦА МНРВОИД могу да поднесу сви грађани Републике Српске, Босне и Херцеговине који имају важећу личну карту Босне и Херцеговине, издату од стране надлежног тијела.

Захтјев за издавање квалификованог електронског потписа подноси физичко лице, док захтјев за издавање квалификованог електронског печата ЦА МНРВОИД могу да поднесу сва правна лица, самостални предузетници и органи јавне управе који су регистровани у Републици Српској.

Захтјев за издавање квалификованог електронског печата подноси правно лице, односно његов овлаштени представник/заступник или пуномоћник овлаштеног представника/заступника.

Захтјев за издавање квалификованог електронског печата правним лицима може се поднијети и електронским путем, уколико је захтјев за издавање квалификованог електронског печата потписан квалификованим електронским потписом овлаштеног представника/заступника. Образац захтјева налази се на интернет страници ЦА МНРВОИД. Електронски потписан захтјев за издавање квалификованог електронског печата шаље се на дефинисане адресе за електронску кореспонденцију локалном РА и ЦА МНРВОИД.

4.1.2 **Процес достављања захтјева за издавање цертификата и одговорности**

Локално РА тијело, након извршене провјере правилности и потпуности поднесеног захтјева за издавање квалификованог електронског цертификата, као и извршене провјере идентитета подносиоца захтјева и доказа о уплаћеној накнади за издавање квалификованог

електронског цертификата, подносиоцу захтјева за квалификовани електронскои цертификат нуди закључење уговора о пружању услуга цертификације.

Уговор о пружању услуга цертификације је уговор који подносилац захтјева за квалификовани електронски цертификат закључује са ЦА МНРВОИД, посредством локалног РА. Подносилац захтјева за квалификовани електронски цертификат потписује три (3) примјерка уговора о пружању услуга цертификације. Приликом својеручног потписивања овог уговора, подносилац захтјева за квалификовани електронски цертификат је обавезан да, у за то предиђеном мјесту у уговору, упише тајну ријеч, чија је функција кориштења исте код упућивања захтјева за промјену статуса (опозив или суспензија) цертификата телефонским путем, а у сврху потврђивања идентитета корисника – власника квалификованог електронског цертификата.

Локално РА, попуњен и потписан образац захтјева, уговоре о пружању услуга цертификације и пратеће документе доставља ЦА МНРВОИД. Достављање образаца захтјева и пратећих докумената за издавање квалификованог електронског цертификата врши се службеним путем, посредством властите мреже локалног РА за достављање докумената.

4.2 Обрада захтјева за издавање цертификата

У оквиру овог поглавља су дефинисане радње које обавља локално и централно регистрационо тијело по пријему захтјева за издавање квалификованог цертификата.

4.2.1 **Идентификација и потврђивање аутентичности подносиоца захтјева**

ЦА МНРВОИД захтјева лично подношење захтјева за издавање квалификованог електронског цертификата, у просторијама локалног РА. Овлашћеним подносиоцима захтјева за издавање квалификованог електронског печата - власницима квалификованих електронских потписа, с обзиром да су претходно прошли процедуру личне идентификације код издавања квалификованог електронског потписа, ЦА МНРВОИД омогућава електронски начин подношења захтјева за издавање квалификованог електронског печата.

Након пријема захтјева за издавање квалификованог цертификата, овлаштени службеник локалног РА провјерава и утврђује испуњеност сљедећих услова:

- правилности и потпуности захтјева;
- идентитет подносиоца захтјева и
- доказ о уплаћеној накнади.

Уколико захтјев није тачно и у потпуности попуњен и потписан од стране подносиоца издавање квалификованог електронског цертификата, овлаштени службеник локалног РА одбацује такав захтјев те подносиоца захтјева упућује на исправно и потпуно попуњавање и потписивање захтјева.

Идентификација подносиоца захтјева за издавање квалификованог електронског потписа врши се поступком непосредне идентификације, на начин који је описан у дијелу 3.2.3. Идентификација подносиоца захтјева за издавање квалификованог електронског печата врши се поступком непосредне идентификације, на начин који је описан у дијелу 3.2.2.

Начин доказивања извршене уплате накнаде за издавање квалификовног електронског цертификата, ЦА МНРВОИД утврђује и објављује на својој интернет страници, у дијелу који се

односи на утврђивање инструкције за уплату накнаде за издавање квалификвоаног електронског цертификата.

4.2.2 **Потврђивање или одбијање захтјева за издавање цертификата**

ЦА МНРВОИД издаје квалификовани електронски цертификат уколико су испуњени сљедећи услови:

- потврђен је идентитет подносиоца захтјева;
- подносилац захтјева је лично поднио идентификациону документацију;
- сви подаци и документација о подносиоцу захтјева су успјешно примљени и провјерени;
- сви подаци наведени у захтјеву сматрају се одговарајућим и комплетним.

Уколико корисник не испуњава горе наведене услове или на било који начин повриједи одредбе ових практичних правила, ЦА МНРВОИД ће одбити захтјев за издавање квалификованог електронског цертификата и о томе, посредством РА, доставити кориснику писану обавијест о одбијању захтјева за издавање квалификованог електронског цертификата.

4.2.3 **Потребно вријеме за обраду захтјева за издавање цертификата**

ЦА МНРВОИД врши обраду захтјева након пријема потпуног захтјева за издавање квалификованог електронског цертификата, без одлагања.

Попуњене захтјеве за издавање квалификованог електронског цертификата локално РА доставља службеним путем, кроз властиту мрежу достављања докумената, у складу с редовном динамиком достављања докумената локалног РА.

4.3 Издавање цертификата

У овом поглављу су дефинисане активности које обавља ЦА МНРВОИД током поступка издавања квалификованих електронских цертификата, као и обавезе везане за обавјештавање корисника.

4.3.1 **Активности током процеса издавања цертификата**

Након пријема потпуног захтјева за издавање квалификованог електронског цертификата, ЦА МНРВОИД спроводи процес издавања одговарајућих цертификата који се састоји од:

- генерисања асиметричног пара кључева и квалификованог цертификата за аутентикацију/шифровање;
- генерисања асиметричног пара кључева и квалификованог цертификата за електронски потпис или печат;
- упис асиметричног пара кључева и квалификованог цертификата за аутентикацију/шифровање на паметну еСрпска картицу током процеса електронске персонализације паметне картице,
- упис асиметричног пара кључева и квалификованог цертификата за електронски потпис или печат на паметну еСрпска картицу током процеса електронске персонализације паметне картице као и
- визуелне персонализације паметне еСрпска картице.

4.3.2 **Обавјештење подносиоца захтјева о издатом цертификату**

Квалификовани електронски цертификати се генеришу у оквиру ЦА МНРВОИД и уписују на *SSCD - Secure Signature Creation Device* - паметну еСрпска картицу која се уручује лично кориснику у пословним јединицама локалног регистрационог тијела, заједно са потписаним и овјереним уговором о пружању услуга цертификације.

Локално РА, по пријему паметне еСрпска картице у својим пословним јединицама, обавјештава подносиоце захтјева за издавање квалификованог електронског цертификата о могућности преузимања цертификата и закљученог уговора о пружању услуга цертификације. Локално РА, подносиоце захтјева о могућности преузимања цертификата обавјештава путем контакт података наведених у обрасцу поднесеном обрасцу - адреса електронске поште или контакт телефон.

Локално РА уручиће писану обавијест о одбијању захтјева за издавање квалификованог електронског цертификата у својим пословним јединицама, након пријема такве обавијести од стране ЦА МНРВОИД. Локално РА, подносиоце захтјева о могућности преузимања обавијести о одбијању захтјева, обавјештава путем контакт података наведених у поднесеном обрасцу - адреса електронске поште или контакт телефон.

4.4 Прихватање цертификата

У оквиру овог поглавља су дефинисани поступци провођења процеса прихватања цертификата, објављивање цертификата и обавјештење других лица о издатим цертификатима.

4.4.1 **Спровођење процеса прихватања цертификата**

Квалификовани електронски цертификат издат од стране ЦА МНРВОИД сматра се прихваћеним од стране корисника након протока петнаест (15) дана од дана његовог преузимања уколико корисник не пријави да постоје било какве неправилности у издатом цертификату.

С друге стране, уколико се накнадно утврди да у квалификованом цертификату постоје погрешни подаци, корисник је дужан да се обрати ЦА МНРВОИД или локалном РА ради издавања новог квалификованог цертификата.

4.4.2 **Објављивање цертификата од стране СА тијела**

Поглавље није примјењиво у оквиру ових Практичних правила.

4.4.3 **Обавјештење других ентитета о издатом цертификату**

Поглавље није примјењиво у оквиру ових Практичних правила.

4.5 Коришћење цертификата и асиметричног пара кључа

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

4.5.1 **Коришћење приватног кључа и цертификата од стране корисника**

Корисник се обавезује да ће користити приватни кључ и креирани квалификовани цертификат од стране ЦА МНРВОИД у складу са дефинисаним начином коришћења кључа у самом цертификату (на енглеском језику: *Key Usage* и *Enhanced Key Usage* екстензије).

Коришћење приватног кључа и цертификата представља дио корисниковог уговора са ЦА МНРВОИД. У том смислу, корисник може користити свој приватни кључ само након прихватања одговарајућег цертификата.

Корисник престаје да користи свој приватни кључ након истицања периода валидности или опозива издатог цертификата.

4.5.2 **Коришћење јавног кључа и цертификата од стране трећих страна**

Трећа страна је обавезна да прихвата издате квалификоване цертификате ЦА МНРВОИД само уколико се користе у складу са предвиђеним начином коришћења цертификата дефинисаним у самом цертификату. Трећа страна је обавезна да користи јавни кључ и цертификат за валидацију квалификованог потписа или печата и одговорна је да спроводи провјеру статуса опозваности датог цертификата коришћењем метода који је дефинисан у документима Политика цертификације и овим Практичним правилима.

4.6 Обнављање цертификата

Обнова квалификованог цертификата се не врши. Цијели процес се извршава издавањем новог квалификованог цертификата.

4.6.1 **Услови за обнављање цертификата**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.6.2 **Ко може захтијевати обнављање цертификата**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.6.3 **Обрада захтјева за обнављањем цертификата**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.6.4 **Обавјештење корисника да му је издат обновљени цертификат**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.6.5 **Спровођење процеса прихватања обновљеног цертификата**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.6.6 **Објављивање обновљеног цертификата од стране СА**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.6.7 **Обавјештење других ентитета од стране СА о обнови датог цертификата**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.7 Генерисање новог пара кључева и цертификата корисника

Нови асиметрични парови приватних кључева и квалификованих цертификата издају са на новој паметној еСрпска картици.

4.7.1 **Услови за генерисање новог пара кључева и цертификата**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.7.2 **Ко може захтијевати нови цертификат са новим јавним кључем**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.7.3 **Обрада захтјева за новим паром кључева и цертификатом**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.7.4 **Обавјештење корисника да му је издат нови цертификат**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.7.5 **Спровођење процеса прихватања новог цертификата**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.7.6 **Објављивање новог цертификата од стране СА**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.7.7 **Обавјештење других ентитета од стране СА о издавању новог цертификата**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.8 Измјена података у цертификату

У оквиру овог поглавља описани су услови везани за измјену података у цертификату. Измјена податка у квалификованом цертификату се не врши. Читав процес се извршава издавањем новог квалификованог цертификата.

4.8.1 **Услови за измјену података у цертификату**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.8.2 **Ко може захтијевати измјену података у цертификату**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.8.3 **Обрађивање захтјева за измјену података у цертификату**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.8.4 **Обавјештење корисника о измјени података у цертификату**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.8.5 **Спровођење процеса прихватања новог цертификата са измијењеним подацима**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.8.6 **Објављивање новог цертификата са измијењеним подацима**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.8.7 **Обавјештење других корисника од стране ЦА о издавању новог цертификата са измијењеним подацима**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.9 Опозив и суспензија цертификата

У оквиру овог поглавља дефинисане су процедуре везане за престанак важења и повлачење цертификата.

4.9.1 **Околности за опозив цертификата**

Након упућивања захтјева за промјену статуса - опозив квалификованог електронског цертификата од стране корисника цертификата или другог надлежног органа у складу са законом, ЦА МНРВОИД врши опозив издатог електронског цертификата у случају губитка, крађе, модификације, неауторизованог објављивања или неке друге компромитације приватног кључа корисника цертификата, као и у случају промјене одређених информација које су садржане у цертификату датог лица, губитка правне способности или смрти корисника цертификата.

Према прописима којима се регулише област електронског потписа и других услуга повјерења у Републици Српској, издати цертификат се опозива истеком рока на који је издат, односно на дан престанка важења, на захтјев корисника, на службени захтјев суда, на захтјев ЦА МНРВОИД у случајевима неиспуњавања техничких услова, односно ако се при употреби електронског цертификата не поступа на прописан начин.

4.9.2 **Ко може захтијевати опозив цертификата?**

Опозив квалификованог електронског цертификата може захтијевати сам корисник или овлашћени службеник ЦА МНРВОИД. Другим ријечима, захтјев за опозивом цертификата може да поднесе власник цертификата, након прописне идентификације и аутентикације, или:

- надлежни орган за заштиту података или неки други надлежни орган који има оправдане сумње да цертификат садржи неисправне податке или да се приватни кључ који одговара јавном кључу из цертификата може користити без сагласности власника, а на сонову службеног захтјева датих органа;
- суд, тужилац или институције које врше криминалистичку истрагу да би спријечили даља кривична дјела, а на основу службеног захтјева датих органа;
- надлежне институције за вођење евиденције о губитку правне способности корисника, као и надлежне инстиуције за утврђивање смрти корисника;

- ЦА МНРВОИД истеком рока на који је издат цертификат, односно на дан престанка важења цертификата,као и у случајевима неиспуњавања техничких услова, односно ако се при употреби електронског цертификата не поступа на прописан начин

Према прописима којима се регулише област електронског потписа и других услуга повјерења у Републици Српској, ЦА МНРВОИД је обавезан да изврши опозив цертификата, најкасније у року од 24 часа, корисницима који су то изричито затражили; за које је утврђена нетачност или непотпуност података у евиденцији цертификата; као и за кориснике за које је примљена службена обавијест о губитку пословне способности или за које је примљена службена обавијест о смрти.

4.9.3 **Процедура захтјева за опозив цертификата**

Ако се деси неки од догађаја наведених у условима за опозив цертификата наведених у дијелу 4.9.1 и 4.9.2, корисник мора да без одлагања посјети ЦА МНРВОИД у сврху подношења захтјева за опозив електронског цертификата.

У случају немогућности брзе посјете ЦА МНРВОИД, а имајући у виду значај брзог реаговања код захтјева за промјену статуса - опозив квалификованог електронског цертификата подноси се телефонским путем на званични телефонски број ЦА МНРВОИД. Корисник - власник квалификованог електронског цертификата представља се својим именом и презименом, те изговара тајну ријеч за промјену статуса коју је дефинисао приликом закључења уговора о услугама цертификације са ЦА МНРВОИД. Овлаштени службеник ЦА МНРВОИД провјерава да ли се изговорена тајна ријеч подудара са тајном ријечи која се налази у уговору о пружању услуга цертификације са датим корисником - подносиоцем захтјева за опозив квалификованог електронског цертификата.

ЦА МНРВОИД опозива цертификат одмах након верификације идентитета стране која је захтјевала опозив. Верификација идентитета може бити извршена на основу информационих елемената који су садржани у идентификационим подацима које је корисник доставио код подношења захтјева за издавање цертификата или код подношења захтјева за промјену статуса цертификата. Након испуњења поменутих услова, ЦА МНРВОИД предузима хитну активност у циљу опозива цертификата.

Операцију опозива корисничких цертификата врши овлаштени службеник ЦА МНРВОИД. Опозив квалификованог електронског цертификата подразумјева одобравање захтјева за опозив цертификата и упис серијског броја цертификата корисника у листу опозваних цертификата - ЦР листу.

4.9.4 **Период чекања захтјева за опозивом цертификата**

Након подношења захтјева за опозив квалификованог цертификата, ЦА МНРВОИД ће приступити обради захтјева за опозив цертификата, без одлагања.

4.9.5 **Вријеме за које СА мора да процесира захтјев за опозивом цертификата**

ЦА МНРВОИД извршава опозив квалификованог цертификата одмах по пријему захтјева за опозив цертификата, а након спроведене идентификације подносиоица захтјева.

4.9.6 **Захтјеви за треће стране у вези провјере статуса цертификата**

Током рада са квалификованим цертификатима које је издало ЦА МНРВОИД, треће стране имају обавезу да провјеравају опозваност цертификата.

4.9.7 **Фреквенција издавања ЦР листе**

Листа опозваних цертификата - ЦР листа подређеног цертификационог тијела MNRVOID CA 1 ажурира се са сваким опозивом квалификованог електронског цертификата крајњег корисника, односно најмање на сваких 24 сата.

Листа опозваних цертификата цертификационог тијела MNRVOID CA Root редовно се објављује на сваких шест мјесеци и приликом опозивања подређеног цертификационог тијела.

4.9.8 **Максимално кашњење у издавању ЦР листе**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.9.9 **Расположивост *on-line* провјере статуса цертификата**

ЦА МНРВОИД има реализован ОЦСП (на енглеском језику - *Online Certificate Status Protocol)* – сервис за *on-line* провјеру статуса цертификата.

4.9.10 **Захтјеви за *on-line* провјеру статуса цертификата**

Корисници и треће стране дужни су да провјере статус квалификованог цертификата на основу јавно доступног регистра опозваних цертификата или ОЦСП сервис ЦА МНРВОИД.

4.9.11 **Друге форме регистра опозвних цертифиакта**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.9.12 **Специјални захтјеви у односу на компромитацију приватног кључа**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

4.9.13 **Околности за суспензију цертификата**

Квалификовани електронски цертификат се суспендује у сљедећим ситуацијама:

- ако суспензију цертификата захтијева корисник - власник цертификата;
- ако суспензију цертификата захтијева надлежни орган за заштиту података или неки други надлежни орган који има оправдане сумње да цертификат садржи неисправне податке или да се приватни кључ који одговара јавном кључу из цертификата може користити без сагласности власника;
- ако суспензију цертификата захтијева суд, тужилац или институције које врше криминалну истрагу да би спријечили даље злочине.

4.9.14 **Ко може захтијевати суспензију цертификата?**

Суспензију цертификата може захтијевати сам корисник, суд, тужилац, институције које врше криминалну истрагу да би спријечиле даља кривична дјела, као и други надлежни органи који у складу с законом имају овлашћење да траже суспензију квалификованог електронског цертификата.

4.9.15 **Процедура захтјева за суспензијом цертификата и рактивацијом**

4.9.15.1 Процедура захтјева за суспензијом цертификата

Захтјев за суспензијом цертификата може бити упућен на један од три начина:

- електронским путем (уколико не постоји сумња у губитак или компромитованост цертификата),
- писаним путем, и
- телефонским путем.

Процес идентификације и аутентикације захтјева за суспензију или опозив цертификата за сваки наведени начин подношења захтјева за суспензију детаљно је описан у дијелу 3.4.

Поступак суспензије цертификата је идентичан опозиву с тим што се у случају суспензије цертификата, датом цертификату у систему ЦА МНРВОИД додјељује статус суспендован, а који оставља могућност да се цертификат послије одређеног времена поново активира.

Након успјешно поднесеног захтјева за суспензију квалификованог цертификата - промјену статуса цертификата, ЦА МНРВОИД објављује серијске бројеве свих опозваних и суспендованих цертификата у својој ЦР листи.

За вријеме суспензије, или након опозива цертификата, период оперативног рада датог цертификата се истовремено сматра завршеним.

4.9.15.2 Процедура захтјева за реактивацију цертификата

Суспензија цертификата траје онолико дуго колико трају и разлози због којих се захтијева суспензија цертификата ЦА МНРВОИД. Када ови услови престану да важе, корисник може захтијевати реактивацију свог цертификата.

Захтјев за реактивацију суспендованог захтјева подноси се лично, на образцу ЦА МНРВОИД за промјену статуса квалификованог електронског цертификата, у просторијама ЦА МНРВОИД.

Процес идентификације и аутентикације захтјева за промјену статуса квалификованог електронског цертификата за лично подношење детаљно је описан у дијелу 3.4.

ЦА МНРВОИД задржава право прибављања додатних информација и провјере оправданости захтјева за реактивацију цертификата у циљу отклањања потенцијалних ризика.

Квалификовани електронски цертификат се реактивира након позитивне процјене оправданости захтјева за промјену статуса квалификованог статуса - реактивацију упућеног од стране подносиоца захтјева, и то:

- ако активирање цертификата захтијева власник цертификата, односно овлаштено лице које је и поднијело захтјев за суспензију;
- ако активирање цертификата захтијева надлежни орган за заштиту података или неки други надлежни орган на основу чијег захтјева је извршена суспензија;
- ако активирање цертификата захтијева суд, тужилац или други надлежни орган у скалду са законом на основу чијег захтијева је извршена суспензија.

Операцију активирања цертификата из статуса суспендован врши овлаштени службеник ЦА МНРВОИД. Она подразумјева брисање серијског броја цертификата корисника из ЦР листе.

4.9.16 **Ограничење на трајање суспензије**

Нема ограничења у времену трајања суспензије квалификованог цертификата.

4.10. Сервиси провјере статуса цертификата

У оквиру овог поглавља су дефинисани сервиси везани за статус провјере цертификата

4.10.1. Оперативне карактеристике

ЦА МНРВОИД објављује све опозване и суспендоване цертификате у својој ЦР листи. Листу опозваних цертификата ЦА МНРВОИД редовно ажурира на сваких 24 сата, уколико у међувремену није било опозива корисничких цертификата.

Такође, ЦА МНРВОИД подржава *on-line* провјеру статуса цертификата путем *ОЦСП* протокола.

4.10.2. Расположивост сервиса

Треће стране, у циљу провјере статуса цертифиакта на који се желе ослонити, морају користити електронске ресурсе које Цертификационо тијело МНРВОИД чини расположивим путем регистра опозваних цертификата и *on-line* протокола за провјеру статуса цертификата.

4.10.3. Додатне карактеристике

Ово поглавље није примјенљиво у оквиру Практичних правила.

4.11. Престанак коришћења цертификата

Након престанка коришћења цертификата издатог од стране ЦА МНРВОИД, цертификат мора бити опозван.

Престанак коришћења цертификата може бити из сљедећих разлога:

- корисник жели да прекине коришћење услуга ЦА МНРВОИД;
- ЦА МНРВОИД је престало са пружањем услуга цертификације.

4.12. Чување и реконструкција приватног кључа корисника

У оквиру овог поглавља се налазе процедуре чувања и реконструкције приватног кључа корисника

4.12.1 Политика и пракса чувања и реконструкције приватног кључа

ЦА МНРВОИД обезбјеђује услове за генерисање вишеструких парова асиметричних кључева за кориснике.

Први пар кључева и први цертификат служе за аутентикацију корисника и за шифровање симетричних кључева путем процедуре дигиталне коверте и логовање паметним картицама на *Windows* домен за датог корисника.

Други пар кључева и други цертификат служе за електронско потписивање квалификованим електронским потписом.

Приватни кључ корисника којим се врши квалификовани електронски потпис се нигдје не чува изузев на еСрпска паметној картици корисника.

4.12.2. Енкапсулација сесијског кључа и политика и пракса за реконструкцију

Ово поглавље није примјенљиво у оквиру оквиру Практичних правила.

5 Управне, оперативне и физичке безбједносне контроле

Ово поглавље описује друге безбједносне контроле које не спадају директно у техничке контроле, а које се користе од стране ЦА МНРВОИД као подршка у циљу реализације функције генерисања кључева, аутентикације субјеката, издавања цертификата, опозива цертификата, ревизије и архивирања.

Ове безбједносне контроле су од суштинској значаја за обезбјеђење повјерења у цертификате које издаје ЦА МНРВОИД обзиром да недостатак безбједносних контрола може компромитовати оперативни рад ЦА МНРВОИД доводећи до нпр. креирања цертификата и ЦР листе са погрешним информацијама или компромитације приватног кључа ЦА МНРВОИД.

5.1 Контрола физичке заштите

ЦА МНРВОИД имплементира одговарајуће механизме физичке контроле у својим просторијама.

5.1.1 **Локација и конструкција сајта**

Просторије ЦА МНРВОИД се налази у Административном центру Владе Републике Српске, у просторијама МНРВОИД, у Бањој Луци,Трг Републике Српске 1.

Просторије ЦА МНРВОИД су осигуране, безбједне просторије лоциране у простору који одговара потребама извршења операција високе безбједности.

5.1.2 **Физички приступ**

Приступ просторијама ЦА МНРВОИД је омогућен само овлашћеном особљу ЦА МНРВОИД.

Физички приступ је ограничен имплементацијом одговарајућих механизама контроле приступа из једне у другу зону безбједности, као и у зону високе безбједности. Физички прелазак из зоне у зону може бити изведен само коришћењем безконтактних картица овлашћеног особља ЦА МНРВОИД, а на основу којих се остварује контрола приступа. Хардверска и програмска опрема ЦА МНРВОИД се налази у сервер сали, на централној локацији Владе Републике Српске. Сва правила физичке контроле ЦА МНРВОИД усклађена су са постојећом инфраструктуром и праксама физичке контроле у Административном центру Владе Републике Српске, као и са праксом обезбјеђења сервер сале, дата центра Владе Републике Српске. Ове праксе се односе на локацију и конструкцију просторије; контролу физичког приступа; напајање и климатизацију; заштиту од поплаве, воде; заштиту од пожара;

чување и смјештање података; уништавање непотребних материјала; похрањивање података на резервну локацију.

5.1.3 **Електрично напајање и климатизација**

Сва опрема ЦА МНРВОИД је прикључена на јединице за непрекидно напајање.

Температура и влажност ваздуха се у просторијама одржава у оквиру унапријед дефинисаних интервала помоћу клима уређаја.

Напајање и вентилација се извршавају са редундансом високог нивоа.

5.1.4 **Изложеност поплавама и временским непогодама**

Унутар просторија ЦА МНРВОИД нема водоводних инсталација. Просторије ЦА МНРВОИД су удаљене од ријечних и других водених токова.

5.1.5 **Превенција и заштита од пожара**

Превенција и заштита од пожара су имплементиране у складу са праксама које се примјењују у дата центру Владе Републике Српске.

5.1.6 **Медијуми за чување података**

Медијуми се чувају на безбједан начин. Медији са подацима се чувају у оквиру система ЦА МНРВОИД као и на резервном медијуму који се користи као Backup.

5.1.7 **Одлагање непотребног материјала**

Непотребан папирни материјал се уништава тако што се пропушта кроз машине за сјечење папирног отпада. Електронски медијуми се прије одлагања морају физички/механички уништити. Поступак уништавања непотребног материјала се одвија под надзором запослених у ЦА МНРВОИД.

5.1.8 **Чување резервних копија**

ЦА МНРВОИД користи систем похрањивања података тако да се копије програмске опреме и шифрованих база цертификационог тијела редовно обнављају и чувају.

5.2 Контроле процедура

ЦА МНРВОИД спроводи кадровску и управну праксу која обезбјеђује разумну сигурност у повјерљивост и компетенцију запослених, као и задовољавајуће перформансе у вези са њиховим дужностима у обављању послова који се односе на пружање услуга повјерења и ПКИ системе.

Сваки запослени ЦА МНРВОИД потписује изјаву да ће се придржавати правне регулативе у вези заштите (личних) података, као и да ће задовољити све постављене захтјеве у вези са повјерљивошћу.

5.2.1 **Улоге од повјерења**

Сви запослени у ЦА МНРВОИД који извршавају операције повезане са управљањем електронским кључевима, као и било које друге операције које материјално утичу на такве операције, сматрају се дужностима од повјерења.

ЦА МНРВОИД спроводи иницијално истраживање свих запослених који су кандидати за обављање повјерљивих улога у циљу разумног покушаја стицања увида у њихову повјерљивост и компетенције.

5.2.2 **Број особа које се захтјевају по сваком задатку**

Тамо гдје се захтијева дуална контрола, потребно је да најмање два повјерљива запослена ЦА МНРВОИД искажу њихова подијељена знања у циљу омогућавања извршења текућих операција. Другим ријечима, у оквиру ЦА МНРВОИД, ниједну осетљиву операцију не може извршити само један запослени.

5.2.3 **Идентификација и аутентикација за сваку улогу**

Свака улога запослених у оквиру ЦА МНРВОИД дефинише одговарајуће захтјеве у погледу идентификације и аутентикације корисника.

5.2.4 **Улоге које захтјевају раздвајање дужности**

У оквиру ЦА МНРВОИД дефинисано је које улоге/дужности могу бити комбиноване од стране једног запосленог, а које то не смију.

5.3 Кадровске безбједносне контроле

У оквиру овог поглавља су дефинисане кадровске контроле.

5.3.1 **Квалификације и искуство**

ЦА МНРВОИД извршава неопходне активности у циљу провјере захтијеване биографије запослених, квалификација, као и неопходног искуства у циљу адекватног обављања радних обавеза.

Запослени у ЦА МНРВОИД не смију бити осуђени за кривично дјело, у складу с прописима којима се регулише област и услови за запошљавање у систему јавне управе Републике Српске. Провјере биографије укључују провјере да ли постоји претходне пресуде за кривична дјела, погрешне презентације информација од стране кандидата, те да ли запослени посједују потребно радно искуство.

За рад у ЦА МНРВОИД су неопходни стручњаци који су технолошки и професионално компетентни и који имају потребна знања из криптографије, електронског потписа, ПКИ система, паметних картица, заштите личних података и др.

5.3.2 **Процедура провјере биографије**

ЦА МНРВОИД реализује релевантне провјере запослених на бази статусних извештаја који су издати од стране компетентних ауторитета, изјава трећих страна или изјава самих запослених.

5.3.3 **Захтјеви за обученошћу**

ЦА МНРВОИД обезбјеђује обуку за своје запослене у циљу реализације функција пословања ЦА МНРВОИД. Такође, ЦА МНРВОИД ће у складу с потребама, организовати и обуке за запослене у локалном РА.

5.3.4 **Фреквенција и захтјеви за поновну обуку**

Периодична додатна обука мора бити извршена у циљу успоставе континуитета и ажурности знања запослених, као и одговарајућих процедура.

5.3.5 **Фреквенција и секвенца ротације послова**

На основу прописа којима се регулише област рада, радних односа и услови запошљавања у републичкој управи у Републици Српској, врши се запошљавање нових сарадника.

5.3.6 **Казнене мјере за неовлашћене активности**

Дисциплинске и казнене мјере за неовлашћене активности запослених спроводиће се у складу с важећим прописима којима се регулише област рада, радних односа и запошљавања у републичкој управи у Републици Српској.

У складу с потребама, ЦА МНРВОИД утврђиваће одговарајуће мјере за идентификовање неовлашћених активности, неовлашћено коришћење ауторитета, као и неовлашћено коришћење система у циљу спровођења одговарајућих санкција за одређено непословно и ризично понашање, у складу с законом којим се дефинише дата област у Републици Српској.

5.3.7 **Захтјеви за спољне сараднике**

Спољни сарадници подлијежу политици и процедури заштите приватности и услова повјерљивости као и запослени у ЦА МНРВОИД.

5.3.8 **Документација која се доставља запосленима**

ЦА МНРВОИД чини доступном сву документацију запосленима која се односи на рад и контролу рада ЦА МНРВОИД, обуке и др.

5.4 Процедуре безбједносних провјера логова - ревизија

Процедуре a*udit* логовања укључују чување информација о догађајима унутар ПКИ система и ревизију система и имплементиране су за сврху одржавања безбједног окружења. У том смислу, ЦА МНРВОИД имплементира контроле наведене у наредном тексту.

5.4.1 **Типови забиљежених догађаја**

ЦА МНРВОИД записује догађаје који укључују, али нису ограничени на операције везане за животни циклус цертификата, покушаје приступа систему, као и захтјеве достављене систему.

5.4.2 **Фреквенција процесирања логова**

ЦА МНРВОИД чува *audit* логове у реалном времену, који се касније процесирају на дневном нивоу и архивирају на седмичном нивоу.

5.4.3 **Период чувања *audit* логова**

ЦА МНРВОИД процесира и архивира *audit* логове на седмичном нивоу, који се трајно чувају.

5.4.4 **Заштита *audit* логова**

Audit логови се могу видјети само од стране ауторизованог особља.

5.4.5 **Процедуре backup-а *audit* логова**

ЦА МНРВОИД имплементира процедуре *backup-a audit* логова.

5.4.6 **Систем сакупљања *audit* логова**

ЦА МНРВОИД сакупља и чува *audit* логове у реалном времену.

5.4.7 **Обавјештавање субјекта који је проузроковао догађај**

У случају аларма или инцидентног догађаја, обавјештава се администратор система, администратор безбједности и руководилац ЦА МНРВОИД. Субјекат који је проузроковао одређени догађај се не обавјештава.

5.4.8 **Оцјена рањивости система**

ЦА МНРВОИД врши процјену рањивости система у склопу свакодневних активности које се проведе на систему и анализом ризика, те прегледом електронских записа са система и ручних евиденција.

ЦА МНРВОИД може ангажовати спољне сараднике за повремену процјену рањивости система.

5.5 Архивирање записа - логова

Захтјеви за чувањем записа који се примењују на ЦА МНРВОИД укључују одредбе наведене у наставку текста.

5.5.1 **Типови архивираних записа**

ЦА МНРВОИД на безбједан начин чува записе ЦА МНРВОИД о издатим квалификованим електронским цертификатима, информације о апликацијама за издавање цертификата, као и документацију о самим апликацијама за издавање цертификата.

5.5.2 **Период чувања архиве**

ЦА МНРВОИД чува на безбједан начин записе ЦА МНРВОИД о квалификованим електронским цертификатима у роковима који су одређени законским и подзаконским актима којима се уређује област електронског потписа и других услуга повјерења Републике Српске.

5.5.3 **Заштита архиве**

Услови за заштиту архиве укључују:

- записе које само запослени којима су додијељена овлашћења 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; као и
- заштиту очувања карактеристика медија на којима се архива чува, као нпр. реализација захтјева да се подаци периодично мигрирају на нове медијуме и др.

5.5.4 **Процедура *backup-a* архиве**

ЦА МНРВОИД спроводи одговарајућу процедуру *backup-a* архиве.

ЦА МНРВОИД реализује захтјеве за процедуром чувања барем двије одвојене копије архиве које су под контролом двије различите особе.

5.5.5 **Захтјеви за *timestamping* записима**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

5.5.6 **Систем сакупљања записа**

ЦА МНРВОИД спроводи одговарајући систем сакупљања записа-логова који се архивирају.

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

У оквиру ЦА МНРВОИД, дефинисане су процедуре у циљу добијања и верификације архивских информација.

У циљу добијања и верификације архивских информација, ЦА МНРВОИД одржава записе под јасном хијерархијском контролом и са јасним описом посла. ЦА МНРВОИД чува записе у електронској и/или папирној форми.

ЦА МНРВОИД може захтијевати од свог локалног РА или корисника да доставе одговарајућа документа у циљу подршке овог захтјева. Ови записи могу бити чувани у електронској, папирној и у било којој другој форми за коју ЦА МНРВОИД сматра да је одговарајућа, за шта постоји информатичка подршка.

ЦА МНРВОИД може да измјени начин чувања записа ако је то евентуално потребно у циљу усклађивања с одговарајућим прописом или стандардом коју спроводи надлежни орган за акредитацију и супервизију ПКИ система у Републици Српској, Босни и Херцеговини.

5.6 Измјена кључева

ЦА МНРВОИД посједује процедуру, детаљно описану у овом документу, која се спроводи у случају истека електронских цертификата ЦА МНРВОИД или опозива цертификата ЦА МНРВОИД у складу са условима дефинисаним у овом документи и Политици цертификације. У оба случаја, врши се генерисање новог пара кључева ЦА МНРВОИД и дистрибуција електронских цертификата свим корисницима, као и у случају првог генерисаног цертификата ЦА МНРВОИД.

5.7 Компромитација и опоравак у случају катастрофе

У оквиру овог поглавља се дефинишу процедуре у случају катастрофе.

5.7.1 **Процедуре за поступање у инцидентним и компромитујућим ситуацијама**

ЦА МНРВОИД документује процедуре које треба извршити приликом рјешавања инцидената, као и за потребе извјештавања у вези са евентуалном компромитацијом кључева ЦА МНРВОИД.

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

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

5.7.3 **Процедуре које се спроводе код компромитације приватног кључа ЦА**

ЦА МНРВОИД тежи да поново успостави безбједно окружење у корацима који укључују, али нису ограничени само на опозив неисправних цертификата ЦА тијела. Након тога, ЦА МНРВОИД може поново издати нови цертификат одговрајућем ЦА тијелу.

5.7.4 **Могућности континуитета пословања након катастрофе**

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

5.8 Завршетак рада ЦА МНРВОИД

Прије него што прекине своје активности пружања услуга повјерења ЦА МНРВОИД:

- обавјештава кориснике - власнике важећих цертификата (цертификати који нису опозвани и којима није истекао рок важења) о намјери да престане са пружањем услуга повјерења;
- повлачи све издате цертификате корисника након обавјештења, а без неопходне сагласности корисника;
- благовремено обавјештава о опозиву цертификата ЦА МНРВОИД све кориснике на које се то односи;
- чини разумне мјере у циљу заштите записа које чува у складу са Политиком цертификације и овим Практичним правилима;
- уколико је то могуће, обезбјеђује одговарајуће мјере обезбјеђења сукцесије у смислу поновног издавања цертификата од стране другог ЦА тијела које је насљедник - сукцесор услуге издавања цертификата ЦА МНРВОИД - и које поштује исте или еквивалентне политике цертификације и практична правила ЦА МНРВОИД.

6 Техничке безбједносне контроле

Ово поглавље дефинише техничке безбједносне мјере које примјењује ЦА МНРВОИД у циљу заштите криптографских кључева и активационих података (као на примјер активациони код - пин, лозинке, итд.). Безбједносно управљање кључевима је критично у циљу осигурања да су сви кључеви и активациони подаци заштићени и да се користе искључиво од стране ауторизованих запослених.

Такође, дефинисане су и друге техничке безбједносне контроле које се користе од стране ЦА МНРВОИД у циљу безбједног извршавања функције генерисања кључева, аутентикације корисника, регистрације корисника, издавања цертификата, опозива цертификата, ревизије и архивирања. Техничке контроле укључују животни циклус безбједносних контрола, као и оперативне безбједносне контроле.

У овом поглављу се такође дефинишу техничке безбједносне контроле над РА, корисницима и другим учесницима.

6.1 Генерисање и инсталација асиметричног пара кључева

У овом поглављу су дефинисане процедуре везане за асиметрични пар кључева

6.1.1 **Генерисање асиметричног пара кључева**

ЦА МНРВОИД безбједно генерише и штити своје сопствене приватне кључеве, коришћењем безбједних и поузданих система и примјењује неопходне превентивне мјере у циљу спрјечавања компромитације или неауторизованог коришћења. ЦА МНРВОИД имплементира и документује процедуре генерисања кључева у складу са Политиком цертификације и овим документом. ЦА МНРВОИД примјењује јавне, интернационалне и европске стандарде у вези безбједних и поузданих система.

ЦА МНРВОИД генерише сљедеће асиметричне парове кључева:

- за потребе *MNRVOID CA 1* (*subordinate* у *MNRVOID CA* ПКИ хијерархији) - асиметрични пар кључева се генерише на хардверском безбједносном модулу (не енглеском језику: *Hardware Security Module*, у даљем тексту: ХСМ);
- за потребе корисника- аутентикација/шифровање (дигиталних енвелопа) - овај асиметрични пар кључева се генерише у оквиру система *MNRVOID CA* и приватни кључ, заједно са цертификатом, се уписује на паметну еСрпска картицу корисника током процеса персонализације електронског цертификата;
- за потребе корисника - квалификовани електронски потпис - овај асиметрични пар кључева се генерише на паметној еСрпска картици корисника и никада не напушта паметну картицу. Генерисање се врши у току процеса доперсонализације паметне картице приликом уручења електронског идентификационог документа.

ЦА МНРВОИД користи безбједан процес генерисања свог *MNRVOID CA Root* приватног кључа у складу са документованом процедуром. ЦА МНРВОИД дистрибуира дијељене тајне за своје приватне кључеве. ЦА МНРВОИД је власник приватних кључева и посједује ауторитет да пренесе одговарајуће дијељене тајне на ауторизоване носиоце дијељених тајни.

Приватни кључ *MNRVOID CA Root* се користи за електронско потписивање ЦА МНРВОИД цертификата (издавање *subordinate* цертификата *MNRVOID CA 1*), ЦР листе суспендованих и опозваних цертификата, као и евентуалних акредитованих *Root*-потписаних ентитета (ЦА трећих страна). Друге сврхе коришћења приватног кључа *MNRVOID CA Root* су забрањене.

6.1.2 **Испорука приватног кључа кориснику**

ЦА МНРВОИД испоручује два приватна кључа кориснику на паметној еСрпска картици (један генерисан у оквиру самог система ЦА МНРВОИД, а други генерисан на самој паметној картици).

6.1.3 **Достава јавног кључа до издаваоца цертификата**

Оба квалификована цертификата и јавни кључ корисника, као дио асиметричног пара кључева се доставља до ЦА МНРВОИД кроз персонализациони софтвер у оквиру самог ЦА МНРВОИД (приликом припреме података за персонализацију еСрпска паметне картице) и то у облику захтјева за издавање цертификата у PKCS#10 формату.

6.1.4 **Достава јавног кључа издаваоца цертификата трећим странама**

ЦА МНРВОИД чини доступним своје јавне кључеве *MNRVOID CA* Root и *subordinate MNRVOID CA 1*, у облику X.509v3 цертификата тако што их објављује на интернет страници ЦА МНРВОИД, којој могу да приступају сви корисници и треће стране. Такође, ЦА МНРВОИД објављује *MNRVOID CA* Root и *MNRVOID CA 1* на интернет адреси која је доступна у екстензији *Authority Information Access* свих цертификата које издаје ЦА МНРВОИД.

6.1.5 **Дужине кључева**

За потребе свог *MNRVOID CA* Root приватног кључа и одговарајуће потписивање, *MNRVOID CA Root* користи *SHA-512/RSA* комбинацију *hash* и асиметричног алгоритма са дужином кључа од 4096 бита и периодом валидности цертификата од 20 година.

За своје *subordinate MNRVOID CA 1* приватни кључ и одговарајући алгоритам за електронско потписивање, *MNRVOID CA 1* користи *SHA-512/RSA* комбинацију *hash* и асиметричног алгоритма са дужином кључа од 4096 бита, као и период валидности цертификата од 20 година.

ЦА МНРВОИД издаје корисницима цертификате са *SHA-512/RSA* комбинацијом *hash* и асиметричног алгоритма са дужином кључева од 2048 бита.

ЦА МНРВОИД задржава право на измјену горе наведених комбинација алгоритама и дужина кључева уколико се у криптографској теорији и пракси покажу слабости наведених алгоритама и свјетска криптографска јавност препоручи поузданије алгоритме, као и у случајевима дефинисања нових стандарда за hash и асиметричне алгоритме.

6.1.6 **Генерисање криптографских параметара и провјера квалитета**

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

- ХСМ - за асиметричне кључеве ЦА и за први пар асиметричних кључева за кориснике – за дигиталну енвелопу, и
- Паметна картица - за кључеве корисника за потребе квалификованог електронског потписа и печата.

Квалитет начина генерисања поменутих криптографских параметара искључиво зависи од квалитета хардверског генератора случајних бројева на ХСМ-овима и паметним картицама коришћеним у MNRVOID CA.

С обзиром да су и ХСМ-ови и паметне картице цертификоване по стандарду FIPS 140-2 Level 3, квалитет генерисаних криптографских параметара је загарантован.

6.1.7 **Могуће „*Key Usage*" опције**

У електронским цертификатима (*Root* и *Subordinate MNRVOID CA* цертификати) издатим од стране ЦА МНРВОИД и квалификованим електронским цертификатима (кориснички цертификати) издатим од стране ЦА МНРВОИД користе се сљедеће вриједности у екстензији „*Key Usage*“:

- Цертификат *MNRVOID CA Root: Certificate Signing, Off-Line CRL Signing, CRL Signing*
- Цертификат *MNRVOID CA 1: Certificate Signing, Off-Line CRL Signing, CRL Signing*
- Цертификат за аутентикацију корисника и дигиталну енвелопу: *Digital Signature*, *Key Encipherment*.
- Квалификовани цертификат за квалификовани електронски потпис или печат корисника: *Digital Signature, Non-Repudiation.*

6.2 Заштита приватног кључа и контрола криптографског хардверског модула

ЦА МНРВОИД користи одговарајуће криптографске уређаје у циљу реализације задатака управљања и заштите кључева ЦА МНРВОИД. Поменути криптографски уређаји су познати под именом хардверски безбједносни модули - раније поменути ХСМ.

6.2.1 **Стандарди и контроле криптографског хардверског модула**

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

ХСМ уређаји не смију да напуштају ЦА МНРВОИД просторије изузев одређених прилика унапријед дефинисаних премјештања и пресељења. ЦА МНРВОИД чува записе у вези свих тих премјештања или пресељења.

У случају да одговарајући ХСМ захтјева одржавање или поправку, која се не може извршити у оквиру ЦА МНРВОИД просторија, они се онда безбједно преносе до њиховог произвођача уз поштовање свих неопходних безбједносних мјера, детаљно описаних у овом ЦПС документу.

6.2.1.1 Стандарди и контроле криптографског модула за кориснике

ПКИ систем ЦА МНРВОИД користи паметне еСрпска картице "*MultiAppId v4.0.1*" компаније "*Thales*" које задовољавају сљедеће спецификације прописане Политиком цертификације:

- Оперативни систем
  - Минимум *Global Platform* 2.2.1 стандард
  - Минимум *Javacard* 3.0.4
  - *PACE support: privacy protection with explicit user consent*
  - Комуникациони интерфејс:
    - *Fully compliant with ISO/IEC 7816-3 – contact interface*
    - *ISO/IEC 14443 - 3, 4 – contactless interface*
    - *Support of Extended Length APDU (Tx 32/64kB – Rx 1kB/32kB) in T=1 or T=CL*
- Инсталиране апликације
  - Апликације везане за електронску идентификацију
    - У складу са ICAO Doc 9303 седмо издање: *Passive & Active Authentication, Basic Access Control, Supplemental Access Control (SAC)*
      - У складу са регулативом број 2252/2004 –TR-03110 v2.10/2.21- PART1 (EU-EAC)
  - *IAS Classic V4.4*
    - Аплети да подржавају минималне стандарде везане за ПКИ и могућност лаке интеграције у ПКИ инфраструктури:
      - *Biometry Match-On-Card capabilities*
      - *PKCS#1 (RSA Cryptography standard)*
      - *PKCS#15 (Cryptographic Token Information Format Standard)*
      - *Qualified Signature and Seal Creation Device under eIDAS regulation EU 910/2014*
  - Могућност похране биометријских података
    - *Secure and convenient offline user authentication through fingerprints*
      - *ISO/IEC 19794-2 Finger Minutiae Compact-Size Card formats*

- *ISO/IEC 7816-4 and 7816-11*
- *Anti yes-card mechanism based on RSA 2048 digital signature*

- Криптографија
  - Криптографски алгоритми: 3DES (ECB, CBC), RSA up to 4096 bits, AES (128, 192, 256), ECC up to 521 bits, SHA1 and SHA2 (224, 256, 384, 512)
  - *AIS31 random generator*
  - *On board Key Generation (RSA up to 4096 bits and Elliptic curve up to 521 bits)*
- *Common criteria* цертификација као у табели:

Protection Profile	***Nickname***	***Applicable***	***Assurance level***
ANSSI-PP-2010-03M01	PP-SUN+PACE	*Javacard Platform with PACE option*	EAL5+
BSI-CC-PP-0055	PP-BAC	*eMRTD*	EAL4+
PP-BSI-0068-V2-2011-MA-01	PP-SAC		EAL5+
PP-BSI-0056-V1-2012	PP-BAC+EACv1		
PP-BSI-0056-V2-2012-MA-02	PP-SAC+EACv1		
PP-BSI-0059-SSCD-P2	PP-SSCD (CORE)	*Compliant with EN 419211 part 2 to part 6 Qualified Digital Signature using: PIN of Match-On-Card*	EAL5+
BSI-PP-0075-SSCD-P3	PP-SSCD (CORE)		
BSI-PP-0071-2012	PP-SSCD (EXT)		
BSI-PP-0072-2012	PP-SSCD (EXT)		
BSI-PP-0076-2012	PP-SSCD (EXT)		

- Чип
  - *SLE78C(L)FX400(V)PH DUAL chip from Infineon*
  - *High frequency CPU clock*
  - Дуал интерфејс – контактни и безконтактни (*fees applicable for VHBR*)
  - *16-bit CPU with "Integrity Guard"©*
  - *SOLID FLASH™90nm technology*
  - *400 Kbytes Non Volatile Memory (Flash technology)*
  - Minimum 500,000 *write/erase cycles*
  - *Data retention for minimum 25 years at 25°C*
  - *Common Criteria EAL6+ certified*
- Усклађеност са стандардима
  - Физичке карактеристике и методе тестирања
    - ISO/IEC 7810 (*Identification cards – Physical characteristics*)
    - ISO/IEC 10373 (*Identification cards – Test methods*) *Parts*: 1/3/6
  - Контантни интерфејс
    - ISO/IEC 7816 (*Identification cards – Integrated circuit cards) Parts*: 3/4/5/6/8/9/11/15
  - Безконтактни интерфејс
    - ISO/IEC 14443 (*Identification cards – Contactless integrated circuit(s) cards – Proximity integrated circuit(s) cards) Parts: 1/2/3/4*

- Физичка заштита и дизајн

Карактеристика	Вриједност
Трајност картице	Минимално 6 година
Материјал	Поликарбонат, УВ неактиван
Димензије	8.55 x 5.4 cm (у складу са ISO 7810 стандардом)
Дебљина	0,78 мм (у складу са ИСО 7810/7816 стандардом)
Боје	Предња страна: минимално 5 боја, Задња страна: минимално 5 боја
Елементи заштите	ОВД елемент, заштита у зони слике, на начин да је могуће преко њега вршити персонализацију димензија приближно 20мм x 25 мм
	Микротекст
	Мотиви видљиви под УВ свјетлом таласне дужине λ1
	Shadow image (индент)
	Мотив који се може провјеравати ИР свјетлом (невидљив при дјеловању ИР свјетла)
	Мотив штампан оптички варијабилном бојом (ОВИ) - опционо
	Серијски број картице
Радно окружење	Температурни опсег: од -25^{0}Ц до +70^{0}Ц (пик до 85^{0}Ц) Влажност: 10% - 90%
Чип и интерфејс	Дуал интерфејс

Табела 9: Техничке карактеристике паметне еСрпска картице

Одговарајући минидрајвер, "PKCS#11" библиотека и упутства за коришћење ће бити доступни корисницима за бесплатно преузимање на посебном дијелу интернет странице ЦА МНРВОИД.

6.2.1.2 Персонализација

Персонализација паметних еСрпска картица се обавља у просторијама које имају мјере заштите дефинисане у поглављу 5. Управне, оперативне и безбједоносне контроле.

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

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

Процедура дијељених тајни ЦА МНРВОИД користи вишеструке ауторизоване носиоце у циљу да заштити и побољша повјерљивост приватних кључева и обезбједи одговарајућу процедуру опоравка кључа.

Приватни кључ ЦА МНРВОИД се користи под условима дефинисаним у оквиру ***k*** од ***n*** контроле од стране више запослених са повјерљивим улогама.

Прије него што носилац дијељене тајне прихвати дијељену тајну он мора лично да се упозна са креирањем, поновним креирањем и дистрибуцијом тајне на његовог сљедећег члана ланца повјерљивости.

Носилац дијељене тајне може примити дијељену тајну на физичком медијуму, као што је одређени хардверски криптографски модул (на примјер паметна картица) који је одобрен за

коришћење од стране ЦА МНРВОИД. ЦА МНРВОИД чува писане записе у вези дистрибуције дијељене тајне.

ЦА МНРВОИД документује сопствену дистрибуцију дијељених тајни за активацију свог приватног кључа и има могућност да измјени начин дистрибуције физичког медијума у случају да носиоци физичких медијума захтијевају да буду замијењени у њиховим улогама као носиоци физичког медијума.

6.2.3 **Безбједно чување приватног кључа**

ЦА МНРВОИД користи безбједни криптографски уређај да чува своје приватне кључеве у складу са захтјевима исказаним у стандарду FIPS 140-2 L3.

Процедура чувања приватног кључа ЦА МНРВОИД захтјева вишеструке контроле од стране, на одговарајући начин ауторизованог особља са повјерљивим ролама. Ауторизација процедуре чувања кључева и ауторизација одговарајућег особља мора бити извршена од стране више од једног члана управне структуре.

Хардверски и софтверски механизми који штите приватне кључеве ЦА МНРВОИД су документовани у Интерним правилима рада ЦА МНРВОИД.

6.2.4 **Backup приватног кључа**

ЦА МНРВОИД приватни кључ се *backup*-ује у складу са процедуром дефинисаном у Интерним правилима рада ЦА МНРВОИД. У процедури *backup*-а користе се процедуре *backup*-а кључа које су подржане од стране датог ХСМ уређаја.

Копије приватног кључа ЦА МНРВОИД се чувају на екстерној меморији (*flash* меморија, CD и др.) на сигурном мјесту у шифрованом облику.

6.2.5 **Архивирање приватног кључа**

Backup-ован приватни кључ ЦА МНРВОИД се архивира према процедури описаној у Интерним правилима рада ЦА МНРВОИД.

6.2.6 **Трансфер приватног кључа на хардверски криптографски модул**

Процедура безбједног експортовања приватног кључа ЦА МНРВОИД у циљу *backup*-а, као и процедура безбједног импорта архивираног приватног кључа на ХСМ су описане у посебним Интерним правилима рада ЦА МНРВОИД.

6.2.7 **Чување приватног кључа на хардверском криптографском модулу**

Када се приватни кључ ЦА МНРВОИД налази и користи на ХСМ уређају, он се чува у шифрованом облику у меморији ХСМ уређаја.

6.2.8 **Метода активације приватног кључа**

Носиоци дијељених тајни ЦА МНРВОИД имају задатак да активирају и деактивирају приватни кључ ЦА МНРВОИД. Приватни кључ је тада активан у дефинисаном периоду времена.

6.2.9 **Метода деактивирања приватног кључа**

Носиоци дијељених тајни ЦА МНРВОИД имају задатак да активирају и деактивирају приватни кључ ЦА МНРВОИД. Приватни кључ је тада деактиван у дефинисаном периоду времена.

6.2.10 **Метода уништења приватног кључа**

Приватни кључ ЦА МНРВОИД се не обнавља. Приватни кључ ЦА МНРВОИД ће бити уништен на крају свог животног циклуса.

ЦА МНРВОИД приватни кључеви се уништавају на крају њиховог животног вијека у циљу гаранције да они неће никада бити поново активирани и коришћени.

Приватни кључеви ЦА МНРВОИД се уништавају тако што се исти обришу, као и брисањем њихових дијељених дијелова/тајни.

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

Након генерисања новог асиметричног пара кључева и новог цертификата ЦА МНРВОИД, претходни приватни кључ се брише из ХСМ, а *backup* копије се уништавају на најсигурнији могући начин.

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

6.2.11 **Оцјењивање криптографских модула**

Стандарди за криптографске модуле према којима може да се врши њихово оцјењивање, односно класификовање су FIPS и EAL, као што је наведено у тачкама 6.2.1 и 6.2.1.1.

6.3 Други аспекти управљања паром кључева

У оквиру овог поглавља су обрађени остали аспекти управљања паром кључева.

6.3.1 **Архивирање јавног кључа**

ЦА МНРВОИД архивира свој сопствени јавни кључ.

6.3.2 **Периоди важења цертификата и приватног кључа**

ЦА МНРВОИД издаје корисничке цертификате за периодом коришћења као што је назначено у самим цертификатима.

Временски период важности цертификата *MNRVOID CA Root* је 20 година.

Временски период важности *MNRVOID CA 1* цертификата је 20 година.

6.4 Активациони подаци

У оквиру овог поглавља су дефинисани активациони подаци.

6.4.1 **Генерисање и инсталација активационих података**

ЦА МНРВОИД безбједно процесира активационе податке придружене приватним кључевима ЦА МНРВОИД, као и свим другим приватним кључевима у датом ПКИ систему.

Активирање приватног кључа корисника се врши путем активационог податка који је генерисан случајним путем, послије чега се активациони податак доставља кориснику.

Активациони податак има четири нумеричка карактера.

Корисник има могућност промјене активационог податка.

6.4.2 **Заштита активационих података**

Запослени у ЦА МНРВОИД су дужни да чувају све лозинке и физичке медијуме са којима је могуће поновно активирање кључева цертификационог тијела.

Корисници су дужни да чувају активационе податке за приступ приватним криптографским кључевима који се налазе на квалификованом средству за креирање квалификованог потписа.

6.4.3 **Други видови активационих података.**

Ово поглавље није примјењиво у оквиру ових Практичних правила.

6.5 Безбједносне контроле рачунарског система

У оквиру овог поглавља су дефинисане начини безбједносних контрола рачунара.

6.5.1 **Специфични захтјеви за безбједност рачунарског система**

ЦА МНРВОИД имплементира специфичне безбједносне контроле над рачунарима који се користе у оквиру датог ПКИ система.

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

Неауторизован приступ рачунарима ЦА МНРВОИД није дозвољен.

6.5.2 **Рангирање безбједности рачунара**

Ово поглавље није примјењиво у оквиру ових Практичних правила.

6.6 Животни циклус техничких безбједносних контрола

У оквиру овог програма су дефинисане процедуре које се односе на поступке сталног праћења система безбједности и контролних механизама, те њиховог усавршавања.

6.6.1 **Контроле развоја система**

ЦА МНРВОИД реализује периодичне развојне управљачке контроле.

6.6.2 **Контроле управљања безбједношћу**

ЦА МНРВОИД реализује периодичне безбједносне управљачке контроле.

6.6.3 **Животни циклус безбједносних контрола**

Ово поглавље није примјењиво у оквиру ових Практичних правила.

6.7 Мрежне безбједносне контроле

MNRVOID CA одржава и примјењује висок ниво система мрежне безбједности, укључујући примјену *firewall* уређаја и система за превенцију и заштиту од напада.

6.8 Временски жиг

Ово поглавље није примјењиво у оквиру ових Практичних правила.

7 Профили цертификата и ЦР листа

Ово поглавље описује формате цертификата и ЦР листа које издаје ЦА МНРВОИД.

7.1 Профили цертификата

ЦА МНРВОИД издаје сљедеће врсте цертификата у оквиру *MNRVOID CA* ПКИ хијерархије:

- *MNRVOID CA Root,*
- *MNRVOID CA 1*,
- Квалификовани цертификати за физичка и правна лица.

ЦА МНРВОИД издаје квалификоване електронске цертификате физичким и правним на паметној - еСрпска картици (за аутентификацију/шифровање и за израду квалификованог електронског потписа или печата)

ЦА МНРВОИД објављује у оквиру ових Практичних правила профиле цертификата које користи за све типове цертификата које издаје.

7.1.1 **Број верзије**

ЦА МНРВОИД издаје цертификате у формату *X.509v3* тако да су сви издати електронски цертификати верзије 3.

7.1.2 **Екстензије у цертификату**

Профили цертификата који се издају од стране ЦА МНРВОИД су наведени у наставку.

7.1.2.1 Општи профил цертификата

Општи профил MNRVOID CA цертификата:

Категорија	Вриједност	
Име профила	X.509 верзија 3	
Период валидности цертификата	5 година - кориснички 20 година - *MNRVOID CA 1* 20 година - *MNRVOID CA Root*	
Екстензије основних ограничења	*End Entity|CA, Path length=none*	
Чување кључева	Паметна картица | ХСМ	
Заједничке екстензије	*Authority Key Identifier* *Subject Key Identifier* *Authority Information Access* *CRL Distribution Point*	
Дужина кључева	2048, 4096	
Key Usage екстензија - могуће вриједности	*Digital Signature* *Non-Repudiation* *Key Encipherment*	*Certificate Signing* *CRL Signing* *Off-line CRL Signing*
Enhanced Key Usage екстензија – могуће вриједности	*Client Authentication* *Smart Card Log-on*	
ОИД Политике	1.3.6.1.4.1.26614.20.0.1	
URL за политику цертификације	**http://ca.vladars.net/policy**	

Табела 10: Општи профил MNRVOID CA цертификата

7.1.2.2 Профил *MNRVOID CA Root* цертификата

Профил *MNRVOID CA Root* цертификата:

Категорија	Вриједност
Име профила	*MNRVOID CA Root*
Период валидности цертификата	20 година
Екстензија основних ограничења	*Subject Type=CA* *Path Length Constraint=None*
Чување кључева	*ХСМ*
Заједничке екстензије	*Authority Key Identifier* *Subject Key Identifier*
Примјенљива дужина кључева	*4096*
Екстензија коришћења кључа	*Certificate Signing,* *Off-line CRL Signing,* *CRL Signing*

Табела 11: Профил MNRVOID CA Root цертификата

7.1.2.3 Профил *MNRVOID CA Subordinate* цертификата

Профил *MNRVOID CA Subordinate* цертификата:

Категорија	Вриједност
Име профила	*MNRVOID CA 1*

Период валидности цертификата	20 година
Екстензија основних ограничења	*Subject Type=CA* *Path Length Constraint=0*
Чување кључева	*XCM*
Заједничке екстензије	*Authority Key Identifier* *Subject Key Identifier* *Authority Information Access* *CRL Distribution Point*
Применљива дужина кључева	*4096*
Екстензија коришћења кључа	*Certificate Signing* *Off-Line CRL signing* *CRL Signing*

Табела 12: Профил MNRVOID CA Subordinate цертификата

7.1.2.4 Профил цертификата корисника

У сљедеће двије табеле су приказани профили квалификованих цертификата за дигитални потпис и за аутентикацију које издаје ЦА МНРВОИД.

7.1.2.4.1 Квалификовани цертификат за аутентикацију/шифровање

Категорија	Вриједност
Име профила	Квалификовани цертификат за аутентикацију/шифровање
Период валидности цертификата	5 година
Екстензија основних ограничења	*Subject Type=End Entity* *Path Length Constraint=None*
Чување кључева	*Smart kartica – SSCD/QSCD|CA*
Заједничке екстензије	*Authority Key Identifier* *Subject Key Identifier* *CRL Distribution Point* *Authority Information Access* *Certificate Policies* *Subject Alternative Name*
Применљива дужина кључева	2048
Екстензија коришћења кључа	*Digital Signature* *Key Encipherement*
Екстензија напредног коришћења кључа	*Client Authentication* (1.3.6.1.5.5.7.3.2) *Smart Card Logon* (1.3.6.1.4.1.311.20.2.2)
Certificate Policy екстензија	Policy Identifier=1.3.6.1.4.1.26614.20.0.1
UserID ОИД	0.9.2342.19200300.100.1.1 = ENCR
ОИД Политике	1.3.6.1.4.1.26614.20.0.1
УРЛ за ЦП	http://ca.vladars.net/policy

Табела 13: Квалификовани цертификат за аутентикацију/шифровање

7.1.2.4.2 Квалификовани цертификат за квалификовани електронски потпис

Категорија	Вриједност
Име профила	Квалификовани цертификат за квалификовани електронски потпис
Период валидности цертификата	5 година
Екстензија основних ограничења	*End Entity*
Чување кључева	*Паметна картица – SSCD/QSCD*
Заједничке екстензије	*Authority Key Identifier* *Subject Key Identifier* *CRL Distribution Point* *Authority Information Access* *Certificate Policies*
Применљива дужина кључева	2048
Екстензија коришћења кључа	*Digital Signature* *Non-Repudiation*
QC (Qualified Certificate) statement ekstenzija	Policy Identifier=0.4.0.194112.1.2
Certificate Policy екстензија	Policy Identifier=0.4.0.194112.1.2
UserID ОИД	0.9.2342.19200300.100.1.1 = ENCR
ОИД Политике	1.3.6.1.4.1.26614.20.0.1
УРЛ за ЦПС	http://ca.vladars.net/policy

Табела 14: Квалификовани цертификат за квалификовани електронски потпис

7.1.2.4.3 Квалификовани цертификат за квалификовани електронски печат

Категорија	Вриједност
Име профила	Квалификовани цертификат за квалификовани електронски печат
Период валидности цертификата	5 година
Екстензија основних ограничења	*End Entity*
Чување кључева	*Паметна картица – SSCD/QSCD*
Заједничке екстензије	*Authority Key Identifier* *Subject Key Identifier* *CRL Distribution Point* *Authority Information Access* *Certificate Policies*
Применљива дужина кључева	2048
Екстензија коришћења кључа	*Digital Signature* *Non-Repudiation*
QC (Qualified Certificate) statement ekstenzija	*Policy Identifier*=0.4.0.194112.1.3
UserID ОИД	0.9.2342.19200300.100.1.1 = ENCR
Certificate Policy екстензија	Policy Identifier=0.4.0.194112.1.3
ОИД Политике	1.3.6.1.4.1.26614.20.0.1
УРЛ за ЦПС	http://ca.vladars.net/policy

Табела 15: Квалификовани цертификат за квалификовани електронски печат

7.1.3 **Објектни идентификатори алгоритама**

MNRVOID CA у цертификатима које издаје користи комбинацију алгоритама:

- SHA512RSA са OID-ом: 1.2.840.113549.1.1.13

Међутим, ЦА МНРВОИД ПКИ систем подржава имплементацију и других комбинација *hash* и асиметричног криптографског алгоритма.

7.1.4 **Форме имена**

У квалификованим електронским цертификатима које издаје ЦА МНРВОИД, име цертификационог тијела се наводи у пољу *Issuer* а име корисника се наводи у пољу *Subject*.

7.1.5 **Ограничења имена**

Ограничења која се односе на имена корисника у квалификованим електронским цертификатима проистичу из законских и подзаконских аката којима се уређује област електронског потписа и других услуга повјерења Републике Српске.

У наставку су наведена поменута ограничења.

- Поље „*Subject*" квалификованог електронског цертификата мора да има атрибут „*commonName*".
- У атрибут „*commonName*" квалификованог електронског цертификата за израду електронског потписа треба да је уписано пуно име и презиме потписника. Подаци се уписују сљедећим редом: име, размак, презиме. За атрибут „*CommonName*" треба користити UTF8String кодирање, тако да сва слова из имена и презимена буду вјерно представљена одговарајућим карактерима.
- У атрибут „*commonName*" квалификованог електронског цертификата за аутентикацију и енкрипцију треба да је уписано пуно име и презиме потписника и додатни текстуални податак који је одређен пољем *UserID* ОИД. Подаци се уписују сљедећим редом: име, размак, презиме, размак вриједност поља *UserID* ОИД. За атрибут „*CommonName*" треба користити UTF8String кодирање, тако да сва слова из имена и презимена буду вјерно представљена одговарајућим карактерима.
- У атрибут „*commonName*" квалификованог електронског цертификата за израду електронског печата треба да је уписан скраћени назив аутора квалификованог електронског печата. За атрибут „*commonName*" треба користити *UTF8String* кодирање, тако да сва слова из скраћеног имена правног лица буду вјерно представљена одговарајућим карактерима.
- Корисник потписује сагласност код подношења захтјева за издавање квалификованог електронског цертификата да ће електронски цертификат за израду електронског потписа садржати ЈМБ у сврху постизања јединствености имена.
- Цертификати који се користе у комуникацији између органа, комуникацији органа и странака, достављању и изради одлуке органа у електронском облику у управном, судском и другом поступку пред државним органом, треба да садрже ЈМБ. Цертификате који садрже ЈМБ, ЦА МНРВОИД не смије учинити јавно доступним.

7.1.6 Објектни идентификатор политике цертификације

У овом поглављу је дефинисана структура објектног идентификатора цертификације (у даљем тексту: ОИД) за потребе Политика цертификације и овог документа која се користи при издавању цертификата у оквиру ПКИ система ЦА МНРВОИД.

Формат структуре ОИД је сљедећи:

- 1.3.6.1.4.1.26614.а.б.ц

Број 1.3.6.1.4.1 представља општи префикс за *private-enterprize* број са странице: http://www.iana.org/assignments/smi-numbers, 26614 је *Private Enterprize Number (PEN)* додељен Влади Републике Српске.

Слова иза PEN-а имају сљедећа предложена значења:

а. Ознака институције

20 – МНРВОИД

б. Тип документа

0 – ЦП - *Certificate Policy*

1 – ЦПС - *Certificate Practice Statement*

ц. Верзија документа

1 – N Ознака верзије документа

7.1.7 Коришћење „*Policy Constraints*“ екстензије

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

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

ЦА МНРВОИД користи потпоље *Policy Qualifier Id=CPS* поља *Certificate Policy* цертификата корисника, у коме објављује адресу веб странице на којој се налазе ова Практична правила и друга акта ЦА МНРВОИД и потпоље *Policy Qualifier Id=User Notice* у коме је наведено да се ради о квалификованом електронском цертификату за потпис или печат.

7.1.9 Семантика процесирања критичне екстензије „*Certificate Policies*“

У цертификатима издатим од стране ЦА МНРВОИД, неопходно је да екстензија „*Certificate Policies*“ има сљедеће вриједности:

- одговарајући ОИД Политике цертификације по којој се издаје дати цертификат,
- веб адресу на којој се налазе ова Практична правила ради преузимања.

7.2 Профил ЦР листе

У складу са IETF PKIX RFC 2459, MNRVOID CA подржава издавање ЦР листе које су у сагласности са сљедећим условима:

- бројеви верзија су подржани за ЦР листе су верзије 2 (X.509v2),
- ЦР листа и ЦР екстензије су попуњене и њихова критичност је посебно назначена.

Профил ЦР листе ЦА МНРВОИД је приказан у сљедећој табели:

Атрибут	Вриједност	
Issuer Name	CN = *MNRVOID CA 1* O = Ministarstvo za naučnotehnološki razvoj visoko obrazovanje i informaciono društvo 2.5.4.97 = VATBA-440166068003 L = Banja Luka S = Republika Srpska C = BA	
Effective date	[*Date of Issuance*]	
Next Update	[*Date of Issuance* + 24 *hours*]	
Signature Algorithm	sha512RSA	
Signature Hash Algorithm	sha512	
CRL Number	Redni broj CRL liste	
Revocation List	*CRL Entries*	
	Serial number	*[Certificate Serial Number]*
	Revocation date	*[Date and Time of Revocation]*
	CRL Reason Code	*[Reason Code of Revocation]*

Табела 16: Профил ЦР листе ЦА МНРВОИД

7.2.1 Број верзије

ЦА МНРВОИД генерише и објављује ЦР листе верзије 2 (X.509v2).

7.2.2 CRL и CRL *entry* екстензије

ЦР листа која се издаје од стране ЦА МНРВОИД има сљедеће екстензије:

- *CRL Number* - редни број ЦР листе

ЦР entry екстензије листе су:

- серијски број суспендованог или опозваног цертификата,
- датум и вријеме суспензије или опозива,
- разлог суспензије или опозива.

7.3 ОЦСП профил

МНРВОИД ЦА омогућава електронску провјеру статуса квалификованог цертификата посредством ОЦСП протокола на интернет страници ЦА МНРВОИД. ОЦСП профил је у складу са документом RFC 6960: X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol* –ОЦСП.

8 Провјера сагласности и друга оцјењивања

У оквиру овог поглавља су дефинисани механизми оцјењивања и провјера.

8.1 Фреквенција или услови оцјењивања

Приликом уписа у евиденцију цертификационих тијела у Републици Српској, ЦА МНРВОИД је добио позитивну оцјену стручне Комисије коју је формирао надлежни орган за вођење ове евиденције у Републици Српској - МНРВОИД.

ЦА МНРВОИД прихвата периодичну провјеру сагласности својих политика цертификације, укључујући ова Практична правила, што укључује и надзор од стране надлежног органа за послове инспекцијског надзора у области електронског потписа и других услуга повјерења у Републици Српској.

Пословање ЦА МНРВОИД је усклађено са прописима којима се регулише област електронског потписа и других услуга повјерења у Републици Српској, које се континуирано усклађује са најважнијим међународним и стандардима Европске Уније у овој области.

У домену издавања квалификованих електронских цертификата, ЦА МНРВОИД ради у оквиру ограничења дефинисаним у законским и подзаконским актима којима се уређује област електронског потписа и других услуга повјерења Републике Српске.

8.2 Идентитет/квалификације процјењивача

Надзор над радом ЦА МНРВОИД врши надлежни орган за инспекцијски надзор у области електронског потписа и других услуга повјерења у Републици Српској - Републичка управа за инспекцијске послове Републике Српске.

Поред тога, ЦА МНРВОИД проводи редовне интерне провјере усклађености пословања са Политиком цертификације, као и са овим Практичним правилима. Интерне провјере проводи ПМА тијело, односно запослени са додијељеним овлашћењима за интерни надзор. ЦА МНРВОИД по потеби може ангажовати и спољне сараднике за процјену усклађености пословања са Практичним правилима.

Након испуњења утврђених услова за издавање квалификованих електронских цертификата према прописима којима се регулише област електронског потписа и других услуга повјерења у Републици Српској, надлежни орган за инспекцијски надзор у области електронског потписа и других услуга повјерења у Републици Српској - Републичка управа за инспекцијске послове Републике Српске врше редовни и ванредни надзор по потреби над радом ЦА МНРВОИД у складу с прописима Републике Српске.

8.3 Однос оцјењивача према оцјењиваном ентитету

Као што је наведено у тачки 8.2.

8.4 Теме покривене у процесу оцјењивања

У процесу оцјењивања рада ЦА МНРВОИД, било екстерног од стране надлежног инспекцијског органа или интерног од стране интерних ревизора, врши се провјера усклађености оперативног рада ЦА МНРВОИД са Политиком цертификације и овим Практичним правилима, као и са интерним правилима рада.

8.5 Активности предузете као резултат утврђених недостатака

ЦА МНРВОИД треба да усклади свој оперативни рад у складу са евентуалним налазима екстерног или интерног надзора, односно супервизије или ревизије.

8.6 Комуникација резултата

Резултати екстерне или интерне ревизије представљају интерне документе ЦА МНРВОИД и као такви се не објављују јавно, осим ако није другачије наложено. По пријему резултата ревизије ЦА МНРВОИД ће у најкраћем року приступити отклањању евентуално пронађених недостатака.

9 Остали пословни и правни аспекти

У оквиру овог поглавља су дефинисани пословно-правни аспекти који се тичу рада и правила пружања услуга цертификације ЦА МНРВОИД.

9.1 Цијене

У оквиру овог поглавља су дефинисане цијене издавања цертификата

9.1.1 **Цијене издавања цертификата**

ЦА МНРВОИД наплаћује услугу издавања квалификованог електронског цертификата и друге услуге повјерења у складу са важећим цјеновником о висини накнада за услуге електронске цертификације ЦА МНРВОИД који се налази на интернет страници ЦА МНРВОИД.

ЦА МНРВОИД задржава права да мијења услове коришћења цертификата од стране корисника.

9.1.2 **Цијена приступа цертификатима**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

9.1.3 **Цијена приступа информацијама о статусу цертификата**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

9.1.4 **Цијене за друге сервисе**

ЦА МНРВОИД задржава право да наплаћује различите услуге у зависности од пружених услуга у сваком конкретном случају.

9.1.5 **Политика поврата новца**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

9.2 Финансијска одговорност

ЦА МНРВОИД, односно Република Српска, сноси финансијску одговорност за обављање своје делатности у складу са законским и подзаконским актима којима се уређује наведена област у Републици Српској.

9.2.1 **Покривање осигурања**

ЦА МНРВОИД је дужно да обезбиједи износ осигурања од ризика и одговорности за могућу штету насталу вршењем услуга издавања квалификованих електронских цертификата у складу са законским и подзаконским актима којима се уређује наведена област у Републици Српској.

9.2.2 **Друга добра**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

9.2.3 **Осигурање или гаранцијско покривање за крајње кориснике**

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

- давања лажног или погрешно презентованог податка достављеног од стране корисника или њихових заступника;
- било ког пропуста корисника да достави материјалну чињеницу да је погрешна презентација или пропуст учињен из немарности или са намјером да се превари ЦА МНРВОИД или било које лице које прима и односи се према добијеном цертификату;
- необезбјеђивања одговарајуће заштите корисниковог приватног кључа, некоришћења безбједног система како је захтјевано или неизвршења одговарајућих превентивних мера неопходних да се спречи компромитација, губитак, објављивање, модификација или неауторизовано коришћење корисниковог приватног кључа или напада на интегритет MNRVOID CA Root приватног кључа;
- кршења било којих закона који су примјенљиви, укључујући оне који се односе на заштиту интелектуалних права, вирусе, приступ рачунарским системима итд.

9.3 Повјерљивост пословних информација

Пословне информације се чувају у складу са законским и подзаконским актима којима се уређује наведена област у Републици Српској.

9.3.1 **Опсег повјерљивих информација**

Повјерљиве информације су све информације које ЦА МНРВОИД прикупи или генерише у току обављања својих оперативних послова.

9.3.2 **Информације које нису у опсегу повјерљивих информација**

Информације које се не сматрају као повјерљиве су сви подаци који се уграђују у садржај цертификата, регистар опозваних цертификата, те подаци и документи који су јавно обајвљени на веб страници ЦА МНРВОИД.

9.3.3 **Одговорност за заштиту повјерљивих информација**

Запослени у ЦА МНРВОИД и корисници су обавезни да чувају тајност пословних података уз примјену мјера које користе за заштиту својих тајних података и да их користе само за потребе због којих су и били прикупљени у односу на ова Практична правила. Запослени у ЦА МНРВОИД и корисници неће неовлаштено откривати повјерљиве информације, без претходног одобрења, које даје корисник или надлежни орган, у писаној форми.

9.4 Приватност и заштита личних података

У оквиру овог поглавља је дефинисана заштита личних података.

9.4.1 **План приватности**

ЦА МНРВОИД се придржава правила заштите приватности личних података и правила повјерљивости како је прописано у овим Практичним правилима, као и у одговарајућим законским и подзаконским актима којима се уређује област заштите приватности личних података и повјерљивости у Републици Српској.

9.4.2 **Информације које се третирају као приватне**

ЦА МНРВОИД третира личним информацијама све информације које се односе на кориснике цертификата.

9.4.3 **Информације које се не сматрају приватним**

ЦА МНРВОИД не сматра личним само оне информације корисника за које је сам корисник дао сагласност да се могу публиковати. Најчешће се то односи само на податке који се садрже у издатим квалификованим електронским цертификатима.

9.4.4 **Одговорност за заштиту приватних информација**

ЦА МНРВОИД је одговорно за заштиту приватности корисникових информација у складу са 9.3.3.

9.4.5 **Обавјештење и сагласност на коришћење тајних података о личности**

ЦА МНРВОИД за потребе пружања услуга цертификације користи тајне податке о личности само уз потписану корисникову сагласност на захтјеву за издавање цертификата. Сматра се да је корисник дао сагласност потписивањем захтјева за издавање цертификата као

и уговора о пружању услуга цертификације, те са тим прихватио услове пружања услга цертификације ЦА МНРВОИД.

9.4.6 **Откривање информација сходно правним и административним процесима**

ЦА МНРВОИД не објављује, нити се захтјева да објављује, било коју повјерљиву информацију без аутентикованог и потврђеног захтјева од:

- саме стране за коју се таква информација чува или
- надлежног суда.

ЦА МНРВОИД може наплатити одговарајућу административну цијену за процесирање оваквих објављивања.

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

9.4.7 **Друге околности за откривање информација**

ЦА МНРВОИД и његови партнери могу учинити расположивом специфичну политику приватности у циљу заштите личних података корисника који захтјева издавање цертификата од стране ЦА МНРВОИД путем интернет странице, ЦП и ових Практичних правила.

9.5 Права интелектуалног власништва

ЦА МНРВОИД посједује и задржава сва права интелектуалног власништва придружена његовим базама података, интернет страницама, електронским цертификатима које издаје, као и било којим другим публикацијама које на било који начин припадају или потичу од стране ЦА МНРВОИД, укључујући ЦП и ова Практична правила.

9.6 Права и обавезе

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

9.6.1 **ЦА права и обавезе**

ЦА МНРВОИД гарантује пружање услуге цертификације, у складу са овим Практичним правилима и другим актима ЦА МНРВОИД који су усклађени са законским и подзаконским актима којима се уређује област електронског потписа и других услуга повјерења у Републици Српској.

ЦА МНРВОИД има обавезу да:

- Прије успостављања уговорног односа са корисником цертификата, јавно информише корисника о релевантним условима коришћења цертификата;
- Изврши провјеру идентитета корисника цертификата који учествује у поступку издавања или промјене статуса цертификата, у зависности да ли се корисник идентификује као физичко или правно лице, као и провјеру тачности података у захтјеву за издавање односно промјену статуса цертификата;

- Подаци садржани у цертификату буду поуздани и тачни;
- Са корисником цертификата закључи уговор и исти чува десет година по престанку важења цертификата;
- Изда цертификат у складу са условима дефинисаним законом и подзаконским актима;
- Обезбједи да цертификат садржи све потребне податке, у складу са важећим законским и подзаконским актима, као и у складу са захтјевима стандарда који се примјењују у овој области;
- Унесе у податак основне податке о свом идентитету и идентитету корисника, као и јавни јавни криптографски кључ корисника цертификата који је пар његовом приватном криптографском кључу;
- Обезбједи видљив податак у цертификату о тачном датуму и времену издавања цертификата;
- Изврши или одбије да изврши захтјев за промјену статуса цертификата, у складу са условима дефинисаним законом;
- Води ажуран, тачан и безбједним мјерама заштићен регистар опозваних цертификата, који је јавно доступан;
- Обезбједи видљив податак у регистру опозваних цертификата о тачном датуму и времену опозива/суспензије цертификата;
- Врши контролу обављања дјелатности локалних регистрационих тијела;
- Обавља дјелатност у складу са важећим прописима која се уређује заштита личних података;
- извршава и све друге обавезе предвиђене важећим законским и подзаконским аката којима се уређује област електронског потписа и других услуга повјерења у Републици Српској, као и документима ЦП и овим Практичним правилима.

Локално РА, овлашћено од стране ЦА МНРВОИД за обављање послова регистрационог тијела има права и обавезе да:

- Провјери идентитет корисника у поступлу издавања квалификованог цертификата, као и да провјери тачност података у захтјеву са издавање квалификованог електронског цертификата;
- Прослиједеиподатке за издавање квалификованог електронског цертификата као и сву документацију централном РА;
- Извршава и све друге обавезе предвиђене документима ЦП и овим Практичним правилима.

ЦА МНРВОИД одговара за обавезе локалног РА.

9.6.2 **Корисничка права и обавезе**

ЦА МНРВОИД обезбјеђује поштовање свих права корисника, односно омогућава остваривање обавеза корисника, која су утврђена законским и подзаконским актима којима се уређује област електронског потписа и других услуга повјерења у Републици Српској и овим Практичним правилима.

Корисник је обавезан да:

- Пружи тачне и поуздане податке о свом идентитету, у зависности да ли се идентификује као физичко или правно лице, информације о адреси за физичко

лице, односно докаже својство овлаштеног представника/заступника у правном лицу, пружи тачне и поздане податке о правном лицу;
- У поступку провјере идентитета, корисник цертификата који подноси захтјев за физичко лице мора бити физички присутан, као и овлаштени представник/заступник у случају подношења захтјева за правно лице;
- Уколико правно лице подноси захтјев путем пуномоћника, онда пуномоћник мора бити физички присутан, како би се провјерио његов идентитет;
- Обавијести ЦА МНРВОИД о промјени података о идентитету и осталих података садржаних у цертификату, најкасније у року од 24 сата од настанка промјене;
- Прегледа податке садржане у цертификату и обавјести ЦА МНРВОИД о евентуалним грешкама, послије преузимања, а прије кориштења цертификата;
- Користи средство за креирање квалификованих потписа или печата које обезбјеђује ЦА МНРВОИД;
- Употребљава цертификат само за намјене одређене овим Практичним правилима;
- Чува приватникриптографски кључ и у тајности чува лозинку за приступ приватном криптографском кључу;
- У случају губитка, оштећења или злоупотребе техничких средстава (хардвера ли софтвера) или приватног криптографског кључа, односно компромитовања или сумње у компрпмитовање приватног криптографског кључа, без одлагања подесе захтјев за опозив или суспензију цертификата;
- извршава и све друге обавезе предвиђене важећим законским и подзаконским аката којима се уређује област електронског потписа и других услуга повјерења у Републици Српској, као и документима ЦП и овим Практичним правилима.

9.6.3 **Права и обавезе трећих страна**

Трећим странама гарантује се да ЦА МНРВОИД услуге цертификације пружа трећим лицима у складу са законом и подзаконским актима, овим Практичним правилима и интерним правилима рада ЦА МНРВОИД.

Обавезе трећих лица, прије него што се поуздају у квалификовани цертифиакт издат од стране ЦА МНРВОИД су:

- Да провјере статус квалификованог цертификата
- Да се не поуздају у неважећи цертификат (опозван, суспендован или истекао)
- Да се упознају са одговорностима и ограничењима одговорности ЦА МНРВОИД дефинисаним у овим Практичним правилима и другим актима објављеним на веб страници ЦА МНРВОИД.

9.6.4 **Права и обавезе других учесника**

Сваком кориснику гарантује се да ЦА МНРВОИД услуге цертификације пружа у складу са законским и другим подзаконским актима, овим Практичним правилима и другим општим актима и интерним правилима рада ЦА МНРВОИД.

9.7 Непризнавање права

ЦА МНРВОИД признаје права корисника која су у складу са важећом законском регулативом у Републици Српској и Босни и Херцеговини.

9.8 Ограничења одговорности

ЦА МНРВОИД не прихвата било какву другу одговорност осим оне која је експлицитно дефинисана у Политици цертификације и овим Практичниим правилима.

Осим у случају злоупотребе или стварне намјере, ЦА МНРВОИД није одговорно за:

- Било какав губитак профита;
- Било какав губитак података;
- Било коју индиректну или случајну штету која је проузрокована или је везана за коришћење, испоруку, лиценцу, перформансе цертификата или електронских потписа;
- Било коју трансакцију или услугу понуђену у оквиру ових Практичних правила;
- Било коју другу штету изузев оних које потичу од оправданог ослањања на верификоване информације које се налазе у издатом цертификату;
- Било коју одговорност која се појавила у случају грешке у верификованим информацијама која је резултат грешке, злоупотребе или намјере апликанта;
- Употребу цертификата супротно законским и подзаконским аката којима се уређује област електронског потписа и других услуга повјерења у Републици Српској, као и документима ЦП и овим Практичним правилима.
- Промјену сертификата на било који начин од стране корисника;
- Евентуалну злоупотребу техничких средстава (хардвер или софтвер) или приватног криптографског кључа код корисника, односно компромитовања приватног криптографског кључа код корисника;
- Нефункционисање или грешку у функционисању техничких средстава корисника или трећих лица, у ком случају ЦА МНРВОИД није у обавези да пружи техничку подршку у отклањању проблема насталог у функционисању техничких средстава.

ЦА МНРВОИД не одговара за штету која настане као посљедица околности, које су изван контроле ЦА МНРВОИД.

Корисник цертификата је одговоран за штету која настане у случају коришћења цертификата након истека рока важења цертификата, опозива или суспензије, као и у другим случајевима недозвољеног кориштења цертификата, укључујући и неиспуњење обавеза утврђених у 9.6.2 ових Практичних правила.

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

Корисник цертификата одговара за штету уколико са намјером, крајњом непажњом или из нехата обрише цертификат или криптографске кључеве са средства за креирање квалификованог електронског потписа или печата, као и када на било који начин оштети средство или перманентно блокира средство, тако да онемогући његово кориштење.

ЦА МНРВОИД може извршити деблокаду активационог податка корисника, уколико средство за креирање квалификованог електронског потписа није трајно блокирано.

Поступак деблокаде активационог податка корисника (пин кода) објављује се на интернет страници ЦА МНРВОИД. Накнада за услуге деблокаде активационог податка корисника плаћа се према важећем цјеновнику ЦА МНРВОИД.

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

9.9 Одштете

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

9.10 Ступање на снагу и период важења ових Практичних правила

9.10.1 **Ступање на снагу**

Практична правила ступају на снагу након њиховог усвајања од стране управљачке структуре ЦА МНРВОИД.

9.10.2 **Престанак важења**

Трајање Практичних правила није временски ограничено. Тренутна верзија документа је на снази до објављивања нове верзије.

9.10.3 **Ефекат завршетка и поновног рада**

Након престанка важења Практичних правила, као резултата објављивања нове верзије, цертификати ће се користити у складу са оним Практичним правилима која су била актуелна на дан издавања цертификата.

У случају промјена до нивоа када ово није могуће ЦА МНРВОИД ће обавијестити кориснике на начин дефинисан у 9.12.2 преко јавне веб странице дефинисане у 2.1.

У случају када долази до промјене неке секције овог документа која нема материјалне посљедице по корисника, остале секције документа могу остати на снази.

Такође зависно од промјена које у том случају претрпи овај документ управљачка структура ЦА МНРВОИД може иницирати креирање нове верзије овог документа.

9.11 Појединачна обавјештења и комуникација са учесницима

ЦА МНРВОИД дистрибуира актуелну верзију Практичних правила и текуће верзије свих јавних докумената преко веб странице дефинисане у 2.1.

ЦА МНРВОИД комуницира са корисницима путем електронске поште, поште и веб странице, осим ако није другачије одређено овим Практичним правилима.

9.12 Исправке

9.12.1 **Процедуре за исправку**

Запослени у ЦА МНРВОИД могу своје примједбе слати директно ПМА тијелу ЦА МНРВОИД у писаном облику или електронском поштом, на адресе дефинисане у секцији 1.5.2.

9.12.2 **Механизам и период обавјештавања**

ЦА МНРВОИД може одлучити да не обавјештава наручиоце и трећа лица у случају измјена са малим или никаквим утицајем. ЦА МНРВОИД ПМА у потпуности одлучује о томе да ли измјене имају било какав утицај на наручиоце и трећа лица, на сопствену одговорност.

Све измјене у Практичним правилима биће објављене на интернет страници дефинисаној у 2.1.

ЦА МНРВОИД ће обавјестити кориснике о промјенама које имају материјалног утицаја на њих, путем електронске поште и на јавној интернет страници дефинисаној у 2.1.

9.12.3 **Услови промјене објектног идентификатора (ОИД)**

ОИД Практичних правила ће бити промјењен у случају када промјене имају материјални утицај на наручиоце и трећа лица, тј. Нова верзија Практичних правила резултује новим ОИД.

9.13 Процедуре рјешавања спорова

У случају евентуалних спорова у примјени правила утврђених ЦП и овим Практичним правилима, уговорне стране ће спор рјешавати споразумно.

Уколико се споразум не постигне, за све евентуалне спорове надлежни су судови у Републици Српској.

9.14 Закон који се поштује

Ова Практична правила су издата у потпуности у складу са одговарајућим законским и подзаконским актима којима се уређује област електронског потписа и других услуга повјерења у Републици Српској.

За спорове који могу проистећи из рада ЦА МНРВОИД надлежни су судови у Републици Српској.

9.15 Сагласност са примјенљивим законима

Овај правилник је усаглашен са законским и подзаконским актима којима се регулише област електронског потписа и других услуга повјерења у Републици Српској.

9.16 Остале одредбе

9.16.1 **Комплетан уговор**

Ова Практична правила и уговор са наручиоцем, односно корисником обухватају све елементе који дефинишу однос између ЦА МНРВОИД и корисника цертификата.

9.16.2 **Пренос права**

Корисницима цертификата није дозвољено да права и обавезе који проистичу из ових Практичних правила и уговора у цјелости или парцијално пренесу на трећа лица по било ком основу.

ЦА МНРВОИД има право да уговор закључен са корисником, односно права и обавезе из тог уговора, у потпуности или дјелимично, без сагласности корисника, пренесе на друго регистровано цертификационо тијело у Републици Српској.

9.16.3 **Клаузула о ваљаности**

Неваљаност једног или више дијелова овог документа неће имати утицај на ваљаност осталих одредби, под условом да немају утицај на материјалне одредбе, односно немају утицај на повјерење у цертификат и употребу цертификата.

9.16.4 **Спровођење адвокатских накнада и одрицање од права**

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

9.16.5 **Виша сила**

Вишу силу представљу ванредне околности и непредвидљиве ситуације, као што су природне катастрофе, тероризам, недостатак напајања или прекид телекомуникационих веза, пожар, непредвидљиив инциденти као што су сајбер напади са циљем онемогућавања сервиса, Владине мјере, грешке у криптографским алгоритмима и слично.

ЦА МНРВОИД се ослобађа одговорности за било коју штету причињену кориснику, другом учеснику или трећем лицу, приликом пружања услуге цертификације, уколико је до штете дошло услијед разлога који су ван контроле ЦА МНРВОИД, односно услијед више силе.

9.17 Друге одредбе

Ово поглавље није примјенљиво у оквиру ових Практичних правила.

10 Референце

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 цертификације цертификационог тијела МНРВОИД