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

ПОЛИТИКА ЦЕРТИФИКАЦИЈЕ

ЦЕРТИФИКАЦИОНОГ ТИЈЕЛА МИНИСТАРСТВА ЗА НАУЧНОТЕХНОЛОШКИ РАЗВОЈ, ВИСОКО ОБРАЗОВАЊЕ И ИНФОРМАЦИОНО ДРУШТВО РЕПУБЛИКЕ СРПСКЕ

(CP – *Certificate Policy*)

(*1.3.6.1.4.26614.20.0.1.)*

Верзија 1.0

Бања Лука, април 2020. године

Садржај

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 (на енглеском језику: *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 (на енглеском језику: *Certification Policy*, у даљем тексту: ЦП) ЦА МНРВОИД и Практична правила пружања услуга цертификације ЦА МНРВОИД (на енглеском језику: *Certificate Practice Statement*, у даљем тексту: Практична правила или 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 (на енглеском језику: *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 (*subordinate*) цертификационо тијело, које издаје цертификате крајњим корисницима.

MNRVOID CA Root сервер ради као *Root* цертификационо тијело на основу цертификата издатог самом себи (на енглеском језику: *self-signed certificate*) у процесу генерисања приватног криптографског кључа апликације цертификационог тијела (на енглеском језику: *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 (*subordinate*) цертификационо тијело издаје квалификоване цертификате за електронски потпис физичким лицима и квалификоване цертификате за електронски печат правним лицима.

Опсег овог документа су услуге од повјерења које пружа ЦА МНРВОИД, а које се односе на издавање и управљање животним циклусом квалификованих 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*.

ЦА МНРВОИД издаје квалификоване електронске цертификате x.509 верзија 3 за потребе реализације функција аутентификације, шифровања и квалификованог електронског потписа или печата на паметној картици која задовољава одговарајуће безбједоносне стандарде и која је посебно визуелно персонализована паметна картица (у даљем тексту: еСрпска паметна картица).

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 – еСрпска паметну картицу. ЦА МНРВОИД обезбјеђује и придружени пин код за активацију ове паметне картице.

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.

1.2 Назив докумената и идентификациони подаци

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

Идентификациона ознака докумената (на енглеском језику: *Object Identifier – ОИД*) је: 1.3.6.1.4.26614.20.0.1.

Важећа верзија документа се објављује на интернет страници ЦА МНРВОИД и на интернет страници http://ca.vladars.net/policy/.

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:

- Цертификационо тијело (на енглеском језику: *Certification Authority*, у даљем тексту: ЦА),

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

- Регистрационо тијело (на енглеском језику: *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) чију улогу обавља Агенција за посредничке, информатичке и финансијске услуге Републике Српске (у даљем тексту: АПИФ),
- корисници услуге цертификације,
- треће стране и
- остали учесници.

Цертификациона тијела из опсега овог документа су *MNRVOID CA Root* и *MNRVOID CA 1*.

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

MNRVOID CA 1 као подређено (*subordinate*) цертификационо тијело издаје квалификоване цертификате корисницима ЦА МНРВОИД.

У сједишту ЦА МНРВОИД се налази Централно регистрационо тијело, док су локална регистрациона тијела овлашћене организационе јединице АПИФ-а. Листа доступних локалних регистрационих тијела се објвљује на интернет страници ЦА МНРВОИД.

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.

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.

Остали 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.

1.4 Употреба цертификата

MNRVOID CA Root цертификат је самопотписани цертификат, а његов приватни криптографски кључ се користи за потписивање цертификата подређеног *MNRVOID CA 1* и потписивање листе опозваних цертификата коју издаје *MNRVOID CA Root.*

MNRVOID CA 1 цертификат је цертификат подређеног цертификационог тијела које издаје квалификоване електронске цертификате крајњим корисницима, издавање регистара

опозваних цертификата и издавање цертификата за потписивање ОЦСП (на енглеском језику - *Online Certificate Status Protocol* – сервис за *on-line* провјеру статуса цертификата) одговора.

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

1.5.1 **Организација управљања документом**

Документ Политика 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, као и са веб адресе http://ca.vladars.net/policy/.

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

Управљачко тијело ЦА МНРВОИД (енг. *Policy Management Authorithy*, у даљем тексту: ПМА) усклађује форму и садржај овог документа са евентуалним промјенама насталим у процесу издавања квалификованих цертификата.

ПМА ЦА МНРВОИД такође редовно процјењује усклађеност документа ЦП са важећим законским и подзаконским актима Републике Српске, као и са међународним стандардима и регулативом.

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

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
ХСМ	енг. *Hardware Security Module* - Хардверски криптографски модул
ЈИБ	Јединствени идентификациони број правног лица
ЈМБ	Јединствени матични број физичког лица
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
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 1: Скраћенице које се користе у овом документу

2 Објављивање и локација података о цертификацији

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.

2.2 Објављивање података о цертификацији

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/.

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

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,
- 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 успостављене 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

3.1 Називи

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

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).

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.

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

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 наведен као и у службеним регистрима.

ЦА МНРВОИД гарантује јединственост имена у свом ПКИ систему. Јединственост имена се гарантује употребом комбинације 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.

Имена којима би се кршила интелектуална или ауторска права других нису дозвољена. ЦА МНРВОИД није обавезно да верификује да ли је кориштење таквих имена законито. Корисник је дужан да обезбиједи законито кориштење одабраног имена односно корисник је

дужан да се идентификује идентификационим документом којим се поуздано може утврдити идентитет корисника.

3.2 Иницијална провјера идентитета

Провјера идентитета подносиоца захтјева за издавање, суспензију или опозив 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.

Поступак идентификације корисника детаљније је описан у Практичним правилима.

3.3 Идентификација и аутентикација захтјева за обнављање кључева

Захтјев за обнављање кључева се извршава издавањем новог квалификованог цертификата.

3.4 Идентификација и аутентикација захтјева за суспензију или опозив цертификата

Корисник цертификата захтјева суспензију или опозив квалификованог цертификата у складу са поступком описаним у документу Практична правила.

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

Захтјев може да поднесе физичко или правно лице које испуњава услове наведене у документу Практична правила.

4.2 Обрада захтјева за издавање цертификата

ЦА МНРВОИД идентификује корисника и одобрава захтјев за издавање квалификованог цертификата уколико су испуњени услови прописани у документу Практична правила. ЦА МНРВОИД може да одбије захтјев уколико нису испуњени услови прописани у документу Практична правила.

4.3 Издавање цертификата

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

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.

Квалификовани електронски цертификати се генеришу у оквиру ЦА МНРВОИД и уписују на SSCD (на енглеском језику: *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.

Поступци у вези пријема и провјере захтјева за издавање квалификованог електронског цертификата, обавјештавање корисника о издатом цертификату од стране ЦА тијела, као и поступак уручивања цертификата детаљно су описани у документу ЦПС.

4.4 Прихватање цертификата

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

4.5 Коришћење цертификата и асиметричног пара кључа

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).

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

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 овом документу и Практичним правилима.

4.6 Обнова цертификата

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

4.7 Генерисање новог пара кључева и цертификата корисника

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

4.8 Измјена података у цертификату

Измјена података у квалификованом цертификату се не врши. Читав процес се извршава издавањем новог квалификованог цертификата.

4.9 Опозив и суспензија цертификата

Опозив и суспензија цертификата су регулисани документом ЦПС.

4.10 Сервиси провјере статуса цертификата

ЦА МНРВОИД објављује све опозване и суспендоване цертификате у својој ЦР листи.

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

4.11 Престанак кориштења цертификата

Након престанка кориштења 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

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 паметних картица на *Windows* домен за датог корисника.

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

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.

5 Управне, оперативне и физичке безбједносне контроле

5.1 Физичке безбједносне контроле

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.

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

Физички приступ је ограничен имплементацијом одговарајућих механизама контроле, коришћењем бесконтактних картица овлаштеног 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.

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.

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

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

5.2 Процедуралне контроле

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.

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.

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 осјетљиву операцију не може извршити само један запослени.

5.3 Кадровске безбједносне контроле

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

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.

5.4 Процедуре безбједносних провјера логова - ревизија

Процедуре *audit* логовања укључују чување информација о догађајима унутар ПКИ система и ревизију система и имплементиране су за сврху одржавања безбиједног окружења.

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

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

Audit логови се могу видјети само од стране ауторизованог особља.

У случају аларма или инцидентног догађаја, обавјештава се администратор система, администратор безбједности и руководиоц ЦА МНРВОИД. Субјекат који је проузроковао одређени *audit* догађај се не обавјештава о самој *audit* активности.

5.5 Архивирање записа - логова

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. Ти записи се чувају у роковима који су одређени законским и подзаконским актима којима се уређује област електронског потписа и других услуга повјерења Републике Српске.

5.6 Измјена кључева

ЦА МНРВОИД посједује процедуру, која се спроводи у случају истека електронских цертификата ЦА МНРВОИД или опозива цертификата ЦА МНРВОИД. 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

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

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

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

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;
- благовремено обавјештава о опозиву цертификата ЦА МНРВОИД све кориснике на које се то односи;
- повлачи све издате цертификате корисника након обавјештења, а без неопходне сагласности корисника;
- чини разумне мјере у циљу заштите записа које чува у складу са документима ЦП и ЦПС;
- 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 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.

6.1 Генерисање и инсталација асиметричног пара кључева

У овом поглављу су дефинисане процедуре везане за асиметрични пар кључева.

ЦА МНРВОИД безбједно генерише и штити своје сопствене приватне кључеве, коришћењем безбједних и поузданих система и примјењује неопходне превентивне мјере у циљу спријечавања компромитације или неауторизованог коришћења.

ЦА МНРВОИД испоручује два приватна кључа кориснику на паметној картици.

ЦА МНРВОИД доставља своје јавне кључеве *MNRVOID CA* Root и *subordinate MNRVOID CA 1,* у облику X.509 верзија 3 цертификата путем свог електронског репозиторијума доступног на интернет страници ЦА МНРВОИД.

За потребе свог *MNRVOID CA* Root и *subordinate MNRVOID CA 1* приватног кључа и одговарајуће потписивање, ЦА МНРВОИД користи SHA-512/RSA комбинацију *hash* и асиметричног алгоритма са дужином кључа од 4096 бита и периодом 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.

У електронским цертификатима 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 (на енеглеском језику: *Hardware Security Module*, у даљем тексту: ХСМ)

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.

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.

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

Backup ЦА МНРВОИД приватног кључа се врши у складу са процедуром дефинисаном у Интерним правилима рада ЦА МНРВОИД. Копије приватног кључа ЦА МНРВОИД се чувају на екстерној меморији у шифрованом облику. Процедуре безбједног експортовања приватног кључа ЦА МНРВОИД у циљу *backup*-а и безбједног импорта архивираног приватног кључа на ХСМ су описане у посебним Интерним правилима рада ЦА МНРВОИД.

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

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. 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.

ЦА МНРВОИД за генерисање цертификата за кориснике користи паметне еСрпска картице “MultiAppId v4.0.1” компаније “Thales”. Персонализација паметних еСрпска картица се

обавља у просторијама које имају мјере заштите дефинисане у поглављу 5. Управне, оперативне и безбједоносне контроле.

6.3 Други аспекти управљања паром кључева

ЦА МНРВОИД архивира свој сопствени јавни кључ.

ЦА МНРВОИД издаје корисничке цертификате за периодом коришћења како је назначено у самим цертификатима. Вријеме валидности цертификата *MNRVOID CA Root* је 20 година. Вријеме валидности *MNRVOID CA 1* цертификата је 20 година.

6.4 Активациони подаци

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

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 (ПИН кодове/лозинке) за приступ приватним криптографским кључевима који се налазе на средству за креирање квалификованог потписа.

6.5 Безбједносне контроле рачунара

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.

6.6 Животни циклус техничких безбједносних контрола

ЦА МНРВОИД реализује периодичне развојне и безбједносне управљачке контроле.

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,
- Квалификоване електронске цертификате за физичка и правна лица.

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

ЦА МНРВОИД објављује у оквиру документа ЦПС профиле цертификата које користи за све типове цертификата које издаје.

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.

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

ЦА МНРВОИД прихвата периодичну провјеру сагласности својих политика цертификације, укључујући ову Политику цертификације, 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 документом ЦПС. Интерне провјере проводи ПМА тијело, односно запослени са додијељеним овлашћењима за интерни надзор.

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 документима ЦП и ЦПС, 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 интерне 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.

9 Остали пословни и правни аспекти

9.1 Цијене

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

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

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.

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.

Финансијска одговорност корисника је дефинисана документом ЦПС.

9.3 Повјерљивост пословних информација

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

9.4 Приватност и заштита личних података

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

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

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.

ЦА МНРВОИД је одговорно за заштиту приватности корисникових информација.

ЦА МНРВОИД за потребе пружања услуга цертификације користи тајне податке о личности само уз потписану корисникову сагласност на захтјеву за издавање цертификата.

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 процесуирање 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.

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 и докумената ЦП и ЦПС.

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 ЦПС и ову Политику цертификације.

9.6 Права и обавезе

ЦА МНРВОИД гарантује пружање услуге цертификације, у складу са Политиком цертификације 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.

Права и обавезе свих учесника у ПКИ систему МНРВОИД су регулисани документом ЦПС.

9.7 Непризнавање гаранције

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 документима ЦП и ЦПС.

9.9 Одштете

Ово поглавље није примјенљиво у оквиру овог документа.

9.10 Ступање на снагу и период важења ове Политике цертификације

Политика цертификације ступа на снагу по усвајању од стране управљачке структуре ЦА МНРВОИД.

Тренутна верзија Политике цертификације је на снази до објављивања нове верзије.

9.11 Појединачна обавјештења и комуникација са учесницима

ЦА МНРВОИД дистрибуира актуелну верзију Политике цертификације 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 документом и Практичним правилима.

9.12 Исправке

ЦА МНРВОИД ће уградити извршити неопходне измјене на својим важећим документима у случајевима промјене регулативе и процедуре рада.

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 Политика цертификације издата је 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

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 овог документа.