ПОЛИТИКА И ПРАКТИЧНА ПРАВИЛА ПРУЖАЊА УСЛУГА СЕРТИФИКАЦИОНОГ ТЕЛА КАНЦЕЛАРИЈЕ ЗА ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ И ЕЛЕКТРОНСКУ УПРАВУ

(Certification Policy and Practice Statement - CPPS)

- Услуга управљања квалификованим средством за креирање електронског печата на даљину

Верзија: 1.0

НАПОМЕНА: Документ садржи и дефиницију општих услова и релевантних политика, укључујући и политику информационе безбедности

Историја промена

Верзија	Датум	Разлог промене
1.0	21. новембар 2024.	Иницијална верзија

Садржај

1. УВОД

Канцеларија за информационе технологије и електронску управу (у даљем тексту: ITE), као посебна организација надлежна за пројектовање, усклађивање, развој и функционисање система електронске управе у Републици Србији и потребне инфраструктуре и ресурса информационо-комуникационих технологија, обезбеђује услове за електронско управно поступање и електронско комуницирање органа у Републици Србији.

Електронска идентификација и услуге од поверења предуслов су развијене електронске управе. У складу са својим надлежностима и улогом у систему државне управе, како би унапредила доступност и поузданост електронске управе, ITE је успоставила неопходне сервисе и пружалац је услуга електронске идентификације и квалификованих услуга од поверења.

ITE је изградила инфраструктуру јавних криптографских кључева (*Public Key Infrastructure - PKI*) и у улози сертификационог тела (у даљем тексту: ITE CA), уписана је у Регистар пружалаца квалификованих услуга од поверења за услугу управљања квалификованим средством за креирање електронског печата (у даљем тексту: еПечат).

Правни оквир за обављање послова који се односе на услугу еПечат чине Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС“, бр. 94/17 и 52/21) у даљем тексту: Закон) и подзаконска акта донета на основу Закона, а услуга се пружа у складу са одговарајућим међународним стандардима и препорукама, односно другим стандардима, документима и препорукама, које се односе на услуге електронске идентификације и услуге од поверења.

Осим овог документа, ITE CA утврђује и примењује и интерна правила рада и заштите система пружања услуга која представљају пословну тајну ITE CA.

1.1. Основне претпоставке

ITE CA користи у својој инфраструктури за издавање квалификованог сертификата за електронски печат хијерархију више *CA* (*Certification Authority*) сервера. Инфраструктуру ITE CA чине два сертификациона тела:
- „*EID RS CA Root* “, као *Root* сертификационо тело,
- „*EID RS eSeal*“, као подређено (*subordinate*) сертификационо тело.

„*EID RS CA Root*“ сервер ради као *Root* сертификационо тело на основу сертификата издатог самом себи (*self-signed certificate*) у процесу генерисања приватног криптографског кључа апликације сертификационог тела (*Root Key Generation Ceremony*). „*EID RS CA Root*“ сервер издаје сертификате подређеним сертификационим телима која су део инфраструктуре ITE CA.

„*EID RS eSeal*“ као подређено (*subordinate*) сертификационо тело издаје квалификоване сертификате за електронски печат корисницима услуге. Ближе одређење корисника дато је у делу 1.3.3 овог документа.

Функционисање хијерархијске инфраструктуре у потпуности је у складу са овим документом који садржи правила која су обавезујућа за све учеснике.

Електронски сертификати су стандардни сертификати *X*.509 верзије 3 који су намењени за валидацију квалификованог електронског печата.

Корисници еПечата ITE CA поседују један пар криптографских кључева (јавни и приватни кључ). Приватни криптографски кључ користи се за квалификовано електронско печатирање, а јавни криптографски кључ користи се за валидацију квалификованог електронског печата.

Структура овог документа је у складу са стандардима RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“ и ETSI EN 319 411-2 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates“.

1.2. Назив документа и идентификација

Овај документ носи назив „Политика и практична правила пружања услуга Сертификационог тела Канцеларије за информационе технологије и електронску управу“ (у даљем тексту: Политика и практична правила ITE CA), као што је означено на почетној страни документа.

Документ се идентификује бројем и датумом објављивања и важећу верзију је могуће преузети са веб презентације ITE CA, на адреси https://cloud.eid.gov.rs/ca/.

1.3. Учесници у PKI систему

Учесници у PKI систему су:
- Сертификационо тело (*Certification Authority - CA*);
- регистрациона тела;
- корисници;
- поуздајуће стране (трећа лица);
- остали учесници.

1.3.1. Сертификациона тела

ITE CA, обухвата два сертификациона тела (*Certification Authority - CA*):
- *EID RS CA Root*, као *Root* сертификационо тело,
- *EID RS eSeal*, као подређено сертификационо тело.

1.3.2. Регистрациона тела

Регистрациона тела за сертификационо тело обављају проверу идентитета. Централно регистрационо тело које ради у седишту ITE CA овлашћено је за одобравање и прослеђивање података за издавање квалификованих сертификата и захтева за промену статуса сертификата према апликацији сертификационог тела. Локације регистрационих тела јавно се објављују на веб презентацији ITE CA.

1.3.3. Корисници

Корисници услуге еПечат су органи, у складу са дефиницијом органа из члана 1 Закона о електронској управи[1], односно, државни органи и организације, органи и организације покрајинске аутономије, органи и организације јединица локалне самоуправе, установе, јавна предузећа, посебни органи преко којих се остварује регулаторна функција и правна и физичка лица којима су поверена јавна овлашћења.

Физичка лица у улози овлашћених службених лица корисника обављају послове у вези са коришћењем еПечата корисника за потребе корисника.

Корисник квалификованог сертификата за валидацију временских жигова је Канцеларија за информационе технологије и електронску управу.

1.3.4. Поуздајуће стране

Поуздајуће стране, односно трећа лица су физичка лица (појединци) и/или правна лица која прихватају сертификате и верификују електронски печат одређених електронских докумената која су потписана од стране корисника ITE CA, као и која врше валидацију сертификата издатих од стране ITE CA.

Поуздајуће стране обавезне су да провере статус квалификованог сертификата на основу регистра опозваних сертификата ITE CA пре него што прихвате информације које су наведене у сертификату.

Регистар опозваних сертификата ажурира се на дневном нивоу. Поуздајуће стране проверавају најновије расположиве информације о опозваности да би имале комплетну и правовремену информацију о опозивању сертификата.

Ни под којим условима се не треба ослањати на пружени податак о опозваности сертификата дуже од максималног рока важења примљеног одговора (*CRL*) који садржи податак о опозваности.

1.3.5. Остали учесници

Остали учесници су правна лица која, на неки начин, доприносе или учествују у обезбеђивању квалитета рада ITE CA: осигуравајуће друштво, произвођачи и дистрибутери опреме и софтвера.

1.4. Употреба сертификата

1.4.1. Подручје примене

Квалификовани сертификати и припадајући приватни криптографски кључеви користе се за квалификовано електронско печатирање.

Приватни криптографски кључеви који су придружени квалификованим сертификатима користе се у процесу квалификованог електронског печатирања електронског документа, који се може користити у општењу органа и општењу органа и странака, у правним пословима и другим правним радњама, као и у управном, судском и другом

[1] Закон о електронској управи („Службени гласник РС“ бр. 27/2018)

поступку пред државним органом, ако је законом којим се утврђује тај поступак, прописана употреба квалификованог електронског печата.

Квалификовани сертификати потврђују везу између јавног криптографског кључа корисника и идентитета корисника који је извршио квалификовано електронско печатирање електронског документа.

1.4.2. Недозвољене примене

Свака друга употреба квалификованог сертификата која није дефинисана овим документом и није у сагласности са одредбама закона којим се уређује електронски печат и другим документима који регулишу ову област, није дозвољена.

1.5. Политика администрирања документа

1.5.1. Организација управљања документом

Документ Политика и практична правила ITE CA креира и ажурира ITE CA:

Канцеларија за информационе технологије и електронску управу
ITE CA
Немањина 11
11000 Београд
Телефон +381 11 7358 400
Адреса електронске поште: kancelarija@ite.gov.rs
Адреса веб презентације: https://ite.gov.rs

Важећа верзија документа може да се преузме са веб презентације ITE CA на адреси https://cloud.eid.gov.rs/ca/.

1.5.2. Лица за контакт

Лица за контакт ITE CA су руководилац организационе целине надлежне за пружање услуга од поверења у ITE CA, запослени који обављају послове техничке подршке и други запослени овлашћени за давање информација у вези са применом Политике и практичних правила ITE CA и других аката ITE CA.

Контакт адресе лица из става 1. ове тачке објављене су на званичној веб презентацији ITE CA.

1.5.3. Лица одређена за усклађивање документа са праксом издавања сертификата

Управна структура ITE CA усклађује форму и садржај Политике и практичних правила ITE CA са евентуалним променама насталим у пракси издавања квалификованих сертификата.

Такође, управна структура ITE CA редовно процењује усклађеност Политике и практичних правила ITE CA са важећим законима.

1.5.4. Процедуре за одобрење документа Политика и практична правила ITE CA

Измене или допуне документа Политика и практична правила ITE CA врше се у складу са прописима, општим актима и другим актима која регулишу ову област, те зато могу бити предмет давања одобрења надлежног државног органа. Предлог измена и/или допуна документа Политика и практична правила ITE CA сачињава организациона јединица надлежна за стандарде дигитализације, а правно - техничку редакцију врши организациона јединица надлежна за правне послове. Директор Канцеларије за информационе технологије и електронску управу доноси измене и/или допуне тог акта, уз претходну верификацију директора две поменуте организационе јединице, који својим парафима потврђују/одобравају предлог тог акта.

1.6. Дефиниције и скраћенице

Поједини изрази који се користе у овом документу имају следеће значење:

1) **апликација сертификационог тела** - апликација на серверима ITE CA која генерише и потписује квалификоване сертификате и регистре опозваних сертификата, што се ради у хардверском криптографском модулу;
2) **електронски дневник** - електронска форма записа о спроведеним активностима;
3) **електронски документ** - скуп података састављен од слова, бројева, симбола, графичких, звучних и видео материјала, у електронском облику;
4) **компромитовање приватног криптографског кључа -** нарушавање безбедности којом се приватни криптографски кључ излаже могућем неовлашћеном приступу, као што су неовлашћено откривање, мењање или коришћење;
5) **корисник -** орган који користи квалификовани сертификат издат од стране ITE CA и чији се подаци налазе у сертификату;
6) **квалификовани електронски печат** - електронски печат којим се поуздано гарантује идентитет печатиоца, интегритет електронских докумената, и онемогућава накнадно порицање одговорности за њихов садржај, и који испуњава услове утврђене законом;
7) **квалификовани електронски сертификат -** електронски сертификат који је издат од стране сертификационог тела за издавање квалификованих сертификата и садржи податке предвиђене законом;
8) **подаци за креирање квалификованог електронског печата** - подаци за креирање електронског печата су јединствени подаци које користи печатилац за креирање електронског печата и који су логички повезани са одговарајућим подацима за валидацију електронског печата;
9) **подаци за валидацију квалификованог електронског печата** - подаци за валидацију електронског печата су подаци на основу којих се проверава да ли електронски печат одговара подацима који су печатирани;
10) **приватни криптографски кључ апликације сертификационог тела** - приватни криптографски кључ генерисан приликом иницијализације апликације сертификационог тела који служи за потписивање издатих квалификованих сертификата и регистара опозваних сертификата, што се ради у хардверском криптографском модулу;

11) **регистар опозваних сертификата** (*Certificate Revocation List - CRL*) - листа у коју се уписују серијски бројеви и други подаци свих опозваних сертификата које је издало сертификационо тело;
12) **сертификационо тело** - правно лице које издаје квалификоване сертификате;
13) **квалификовано средство за креирање квалификованих печата** - средство за креирање електронског печата је техничко средство (софтвер односно хардвер) које се користи за креирање електронског печата уз коришћење података за креирање електронског печата;
14) **средства за валидацију квалификованог печата** - одговарајућа техничка средства (софтвер и хардвер) која служе за валидацију квалификованог печата, уз коришћење података за валидацију електронског печата;
15) **запослени -** лице у радном односу или по другом основу ангажовано у ITE CA.

Списак скраћеница које се помињу у документу приказан је у оквиру Табеле 1.

Табела 1. Списак скраћеница

Скраћеница	**Објашњење**
AES (Advanced Encryption Standard)	Алгоритам симетричне криптографије намењен за шифровање
CA (Certification Authority)	Сертификационо тело
CPPS (Certification Policy and Practice Statement)	Политика и практична правила пружања услуга сертификационог тела
CRL (Certificate Revocation List)	Регистар опозваних сертификата
EAL (Evaluation Assurance Level)	Тестирани ниво сигурности (постоји седам нивоа сигурности и то од *EAL*1 до *EAL7*)
FIPS (Federal Information Processing Standards)	Стандард захтеваног нивоа сигурности за криптографске модуле (*Security Requirements for Cryptographic Modules*) - постоји четири нивоа
HSM (Hardware Security Module)	Хардверски криптографски модул за операције са приватним криптографским кључем
OID (Object Identifier)	Идентификатор објекта
PKI (Public Key Infrastructure)	Инфраструктура јавних криптографских кључева
RFC (Request for Comments)	Документа која дефинишу интернет стандарде и препоруке.
QSCD (Qualified Signature / Seal Creation Device)	Квалификовано средство за креирање електронских потписа / печата (HSM уређај)
X.509	Стандард за електронске сертификате, описан у документу *RFC* 5280
UTC (Coordinated Universal Time)	Координисано универзално време
ETSI (European Telecommunications Standards Institute)	Европски институт за стандарде из области телекомуникација
IPS	Систем за превенцију упада

(Intrusion Prevention System)	
NTP *(Network Time Protocol)*	Протокол мрежног времена
PED key	Електронски програмиран уређај са USB интерфејсом за приступ рачунарском систему чија је сврха да чува генерисани тајни податак за приступ HSM уређајима.

2. ОБЈАВЉИВАЊЕ И ЛОКАЦИЈА ПОДАТАКА О СЕРТИФИКАЦИЈИ

2.1. Локација за објављивање података о сертификацији

ITE CA објављује податке и сву документацију која се односи на издавање квалификованих сертификата на веб страни https://cloud.eid.gov.rs/ca/. Веб страна је јавно доступна, као и документација која се на њој налази.

2.2. Објављивање података о сертификацији

ITE CA објављује на својој веб презентацији:
- Политику и практична правила ITE CA, као документ који садржи и опште услове пружања услуга,
- корисничка упутства,
- сертификате *CA* сервера
- регистар опозваних сертификата,
- законску регулативу из подручја пружања услуга од поверења и електронске идентификације,
- друга акта и обавештења.

Објављивање докумената по одобрењу обавља овлашћени запослени задужен за управљање садржајем веб презентације.

Обавештења корисницима, информације о законским актима и друге информације објављују се пре почетка примене законских аката у ITE CA. Сертификати ITE CA и припадајуће информације објављују се после њиховог издавања.

Објављивање корисничких упутстава и образаца за кориснике на веб презентацији одобрава ITE CA. Објављивање ових докумената обавља се без претходне најаве, а старије верзије докумената се уклањају.

2.3. Учесталост објављивања података о сертификацији

ITE CA ажурира објављене податке следећом динамиком:
- регистар опозваних сертификата објављује на свака 24 сата,
- све остале податке и документе објављује после евентуалних измена које су усвојене и одобрене од стране ITE CA или надлежног органа.

2.4. Контрола приступа подацима о раду ITE CA

Документи и информације објављени на веб презентацији ITE CA су бесплатни и јавно доступни.

ITE CA има успостављене логичке и физичке сигурносне мере у циљу спречавања неауторизованог додавања, брисања или промене, као и заштите интегритета и аутентичности. Приступ објављеним документима и информацијама је ограничен на могућност читања.

Право додавања, промене и брисања података на веб презентацији ITE CA имају само овлашћени запослени у ITE CA.

3. ИДЕНТИФИКАЦИЈА И АУТЕНТИКАЦИЈА

3.1. Одређивање имена

3.1.1. Врсте имена

У квалификованим електронским сертификатима које издаје ITE CA, име сертификационог тела које издаје сертификате, поље *Issuer* и име корисника сертификата, поље *Subject*, су јединствена имена (*Distinguished Name - DN*).

Табела 2. Структура имена *Root* сертификационог тела „*EID RS CA Root*“ у квалификованим сертификатима

Име *CA* сервера (CN) =	*EID RS CA Root*
Организација (O) =	Kancelarija za informacione tehnologije i elektronsku upravu
Идентификатор организације (OI) =	VATRS-110177886
Место (L) =	*Beograd*
Ознака државе (C) =	*RS*

Табела 3. Структура имена подређеног сертификационог тела „*EID RS eSeal*“ у квалификованим сертификатима

Име *CA* сервера (CN) =	*EID RS eSeal*
Организација (O) =	Kancelarija za informacione tehnologije i elektronsku upravu
Идентификатор организације (OI) =	VATRS-110177886
Место (L) =	*Beograd*
Ознака државе (C) =	*RS*

Табела 4. Структура имена корисника квалификованог сертификата за електронски печат

Јединствено име (CN) =	*Naziv organa* (Назив органа ћириличним или латиничним).
Серијски број	*CA:RS-JIK* (Јединствени идентификатор

(SERIALNUMBER) =	корисника).
Организација (O) =	Naziv organa
Идентификатор организације (2.5.4.97) =	MB:RS-MB (Матични број органа).
Место (L) =	Седиште органа
Идентификатор организације (2.5.4.97) =	VATRS-PIB (Порески идентификациони број (ПИБ) органа).
Ознака државе (C) =	*RS*

Табела 5. Структура имена корисника квалификованог сертификата за електронски печат који се користи за валидацију временских жигова

Јединствено име (CN) =	*Naziv jedinice (Назив јединице за формирање временских жигова).*
Серијски број (SERIALNUMBER) =	*CA:RS-JIK* (Јединствени идентификатор корисника).
Организација (O) =	Naziv organa
Идентификатор организације (2.5.4.97) =	MB:RS-MB (Матични број органа).
Место (L) =	Седиште органа
Идентификатор организације (2.5.4.97) =	VATRS-PIB (Порески идентификациони број (ПИБ) број органа).
Ознака државе (C) =	*RS*

3.1.2. Смисленост имена

Имена и називи у атрибутима поља *Subject* која идентификују корисника су смислени.

Подаци о кориснику који се уписују у поље *Subject* наводе се онако како су дефинисани прописом, односно регистровани у надлежном регистру или евиденцији.

Садржај поља сертификата *Subject Alternative Name* може бити адреса е-поште која не мора бити смислена.

3.1.3. Анонимност или псеудоними корисника

Корисници не могу да буду анонимни.

Корисници не могу користити псеудониме. ITE CA ће одбити захтев за анонимношћу и коришћењем псеудонима.

ITE CA одбија било који захтев за анонимношћу и коришћење псеудонима.

3.1.4. Правила за тумачење различитих врста имена

У квалификованим сертификатима су имена корисника верно представљена латиничким или ћириличким словима српског језика.

Коришћење специјалних знакова у именима корисника није дозвољено, изузев цртице (-) и астериска односно звездице (*).

3.1.5. Јединственост имена

ITE CA гарантује јединственост имена у свом домену. ITE CA додељује сваком кориснику јединствено име (*Distinguished Name - DN*), које се уписује у поље *Subject* квалификованог сертификата.

3.1.6. Признавање, аутентикација и улога заштитног знака

Није применљиво.

3.2. Почетна провера идентитета

Почетна провера тачности идентитета је део поступка подношења захтева за пружање услуге. Проверу свих података захтева пружалац услуге спроводи поређењем са достављеним или самостално прибављеним документима и подацима из меродавног и надлежног извора односно регистра или евиденције у електронском облику, у складу са важећим позитивно-правним прописима.

3.2.1. Метод доказивања поседа приватног кључа

Приватни криптографски кључ корисника генерише се у ITE CA на квалификованом средству за креирање електронских печата (HSM уређај).
HSM уређај смештен је у ITE CA. По издавању сертификата заједно са припадајућим приватним криптографским кључем, корисник га користи кроз свој информациони систем (систем корисника), путем веб сервиса.

Испред HSM уређаја је апликативни слој (у даљем тексту: апликација еПечат), и веб сервис који омогућава кориснику приступ еПечату. **Приступ приватном кључу корисника на HSM уређају је заштићен ПИН-ом који поставља сам корисник, односно овлашћено лице корисника**. ПИН за приступ кључу корисника се чува у криптованом облику и познат је искључиво кориснику.

Повезивање система корисника и апликације еПечат је заштићено серверским сертификатом (SSL) и корисничким именом и лозинком. Корисничко име и лозинка се користе за добијање привременог веб токена који је неопходан за аутентикацију сваког позива еПечат сервиса.
Приликом сваког захтева за печатирање, систем корисника мора као параметар да проследи ПИН за приступ кључу како би ауторизовао печатирање. ПИН за приступ кључу се апликацији еПечат прослеђује у криптованом облику.

3.2.2. Аутентикација идентитета правног лица

Квалификовани сертификат за електронски печат (еПечат) се може издати само органу, а захтев подноси физичко лице у улози овлашћеног лица органа.

Пре провере података о органу, регистрационо тело проверава идентитет подносиоца захтева и овлашћење тог физичког лица да у име органа поднесе захтев.

Да би се проверила ваљаност имена и других података о органу, подносилац захтева мора, уз попуњен образац захтева, доставити односно ставити на располагање службена документа и податке о органу, укључујући пун назив, матични број, порески идентификациони број, адресу седишта (улица и број, град), и друге тражене податке.
Пружалац услуге може обављати додатне провере података о кориснику увидом у одговарајућа документа и регистре и евиденције у електронском облику.

3.2.3. Аутентикација идентитета физичког лица

Квалификовани сертификат за електронски печат (еПечат) се може издати само органу, а захтев подноси физичко лице у улози овлашћеног лица органа.

Аутентикација идентитета подносиоца захтева обавља се на основу важеће личне карте или путне исправе и акта органа који доказује овлашћење лица да у име органа поднесе захтев.

Када се провера идентитета обавља на локацији регистрационог тела, обавља се на основу физичке идентификације и непосредног увида у личну карту или путну исправу и акт органа односно доказ о овлашћењу подносиоца захтева.

У електронској процедури подношења захтева, аутентикација идентитета обавља се квалификованим електронским сертификатом са личне карте подносиоца захтева и акта односно доказа о овлашћењу подносиоца захтева у електронском облику.

3.2.4. Непроверени подаци о кориснику

Сви подаци о кориснику које захтевају прописи морају да буду проверени.

3.2.5. Провера тачности података

Подносилац захтева доставља, односно ставља на располагање, ажурне податке о кориснику односно важећа акта и податке о органу.
Пружалац услуге може извршити проверу података о кориснику у одговарајућем регистру односно евиденцији у електронском облику.
Сви подаци о кориснику које треба уписати у квалификовани сертификат морају да буду исправни и идентични подацима који су достављени у обрасцу захтева.

3.2.6. Критеријуми за међусобну сарадњу

ITE CA не предвиђа унакрсно сертификовање.

3.3. Идентификација и аутентикација захтева за обновом кључа

3.3.1. Идентификација и аутентикација захтева за рутинском обновом кључа

ITE CA не дозвољава обнову кључа. По истеку рока важења, корисник може доставити нови захтев за издавање квалификованог сертификата за електронски печат по процедури која је описана у овом документу.

3.3.2. Идентификација и аутентикација захтева за заменом кључа после опозива

ITE CA не дозвољава замену кључа после опозива. По опозиву, корисник може доставити нови захтев за издавање квалификованог сертификата за електронски печат по процедуру која је описана у овом документу.

3.4. Идентификација и аутентикација захтева за опозивом

Идентификација и аутентикација захтева за опозив обавља се на основу важеће личне карте или путне исправе подносиоца захтева и акта органа који доказује овлашћење лица да у име органа поднесе захтев.

Када се захтев за промену статуса сертификата подноси на локацији регистрационог тела, идентификација и аутентикација се обављају на основу физичке идентификације и непосредног увида у личну карту или путну исправу и акт органа односно доказ о овлашћењу подносиоца захтева.

У електронској процедури подношења захтева, идентификација и аутентикација захтева се обављају квалификованим електронским сертификатом са личне карте подносиоца захтева и акта односно доказа о овлашћењу подносиоца захтева у електронском облику.

4. ОПЕРАТИВНИ ЗАХТЕВИ У ПРОЦЕСУ ИЗДАВАЊА СЕРТИФИКАТА

4.1. Подношење захтева за издавање сертификата

4.1.1. Ко може да поднесе захтев за издавање сертификата

Захтев може да поднесе орган односно физичко лице овлашћено да у име органа поднесе захтев за издавање квалификованог сертификата за електронски печат.

4.1.2. Услови за издавање сертификата

За издавање квалификованог сертификата за електронски печат корисник је дужан да:
- достави попуњен образац захтева и све податке и документацију потребну за обраду и одобрење захтева и закључење уговора,
- испуни захтеве који се односе на проверу идентитета и овлашћења подносиоца захтева,
- упозна се са општим условима пружања услуге и релевантним политикама и практичним правилима пружаоца услуге и сагласност изрази потписивањем уговора о пружању услуге,
- обезбеди присуство овлашћених лица корисника церемонији генерисања кључева како би поставили ПИН-а за приступ приватном кључу корисника.

Документација за издавање квалификованог сертификата садржи податке на основу којих ITE CA може да ступи у контакт са корисником.

Корисник закључује са ITE CA уговор о пружању услуге који садржи и опште услове.

Коришћење услуге се уговара на период од пет година и везује се за датум издавања сертификата. Под датумом издавања сертификата сматра се датум када је он креиран у ITE CA и уписан на средство за креирање квалификованог електронског печата.

4.2. Обрада захтева за издавање сертификата

4.2.1. Обављање функција идентификације и потврђивања аутентичности

ITE CA идентификује подносиоца захтева на основу важеће личне карте или путне исправе и акта органа односно доказа о овлашћењу да у име корисника поднесе захтев за издавање квалификованог сертификата за електронски печат.

Када се провера идентитета обавља на локацији регистрационог тела, обавља се на основу физичке идентификације и непосредног увида у важећу личну карту или путну исправу и доказе о овлашћењу подносиоца захтева.

У електронској процедури подношења захтева, аутентикација идентитета обавља се квалификованим електронским сертификатом са личне карте подносиоца захтева и доказа о овлашћењу подносиоца захтева у електронском облику.

Проверу свих података захтева пружалац услуге спроводи поређењем са достављеним или самостално прибављеним документима и подацима из меродавног и надлежног извора односно регистра или евиденције у електронском облику, у складу са важећим позитивно-правним прописима.

4.2.2. Одобрење или одбијање захтева за издавање сертификата

ITE CA ће одобрити захтев за издавање квалификованог електронског сертификата, уколико су испуњени следећи услови:
- подносилац захтева је обезбедио доказе о свом идентитету и овлашћењу да у име корисника поднесе захтев,
- захтевана документација је успешно примљена и проверена,
- сви подаци захтева и пратећа документација сматрају се одговарајућим и комплетним.

Ако подносилац захтева не испуни услове из става 1. ове тачке или ако на било који начин повреди одредбе ових практичних правила, ITE CA ће одбити захтев за издавање квалификованог електронског сертификата.

4.2.3. Време обраде захтева за издавање сертификата

ITE CA врши обраду захтева одмах после приспећа захтева, тако да обрада може да траје најдуже 30 дана од дана пријема захтева, уколико је документација комплетна.

Ако подносилац захтева не комплетира документацију за издавање сертификата у року од 90 дана од дана подношења захтева, сматра се да је одустао од захтева за издавање сертификата.

4.3. Издавање сертификата

4.3.1. Активности током издавања сертификата

Издавање квалификованог електронског сертификата, врши се на следећи начин:

- овлашћено лице корисника доставља попуњен образац захтева за издавање квалификованог електронског сертификата за електронски печат заједно са пратећом документацијом на локацију регистрационог тела или путем електронског сервиса за подношење захтева,
- регистрационо тело проверава захтев корисника, прихвата или одбија захтев, и о одлуци обавештава корисника,
- у случају прихватања захтева, корисник и пружалац услуге договарају термин церемоније генерисања криптографских кључева и закључују уговор о издавању и коришћењу квалификованог електронског сертификата који садржи и опште услове,
- на церемонији генерисања криптографских кључева корисника корисник поставља ПИН за приступ свом приватном кључу (ПИН за приступ кључу),
- генерише се кориснички приватни криптографски кључ у квалификованом средству за креирање електронских печата у сертификационом телу. Уједно се генерише и јавни кључ.

4.3.2. Обавештавање корисника о издавању сертификата

ITE CA обавештава корисника о издавању сертификата непосредно након генерисања криптографских кључева. Обавештење и подаци о издатом сертификату достављају се и на адресу електронске поште корисника која је наведена у обрасцу захтева.

4.4. Преузимање сертификата

4.4.1. Поступак преузимања сертификата

Електронски сертификат са припадајућим приватним криптографским кључем је смештен у квалификованом средству за креирање електронских печата (HSM уређај) у ITE CA. Корисник не преузима сертификат већ га користи кроз свој информациони систем (систем корисника), путем веб сервиса.

4.4.2. Објављивање сертификата

Квалификовани сертификат се не објављује јавно од стране ITE CA.

4.4.3. Обавештење о издавању сертификата трећих лица

Трећа лица се не обавештавају о издавању квалификованог сертификата.

4.5. Коришћење пара криптографских кључева и сертификата

4.5.1. Коришћење приватног кључа корисника и сертификата корисника

Приватни криптографски кључ корисника користи се за креирање квалификованог печата, а квалификовани сертификат за валидацију квалификованог печата.

4.5.2. Коришћење јавног кључа и сертификата од стране трећег лица

Трећа страна користи јавни кључ и квалификовани сертификат за валидацију квалификованог печата.

4.6. Обнова сертификата

Обнова квалификованог сертификата се не врши. Цео процес се извршава издавањем новог квалификованог сертификата.

4.6.1. Околности за обнову сертификата

Не врши се.

4.6.2. Ко може да захтева обнову сертификата

Не врши се.

4.6.3. Обрада захтева за обнову сертификата

Не врши се.

4.6.4. Обавештење корисника о обнови сертификата

Не врши се.

4.6.5. Поступак прихватања обавештења о обнови сертификата

Не врши се.

4.6.6. Објављивање сертификата код кога је извршена обнова

Не врши се.

4.6.7. Обавештавање трећих лица о издавању сертификата

Не врши се.

4.7. Замена јавног кључа у сертификату

Замена јавног кључа у квалификованом сертификату се не врши.

4.7.1. Околности за замену јавног кључа у сертификату

Не врши се.

4.7.2. Ко може да захтева замену јавног кључа у сертификату

Не врши се.

4.7.3. Обрада захтева за замену јавног кључа у сертификату

Не врши се.

4.7.4. Обавештење корисника о замени јавног кључа у сертификату

Не врши се.

4.7.5. Поступак прихватања обавештења о замени јавног кључа у сертификату

Не врши се.

4.7.6. Објављивање сертификата код кога је извршена замена јавног кључа

Не врши се.

4.7.7. Обавештење трећих лица о издавању сертификата

Не врши се.

4.8. Промена података у сертификату

Промена података у квалификованом сертификату се не врши.

4.8.1. Околности за промену података у сертификату

Не врши се.

4.8.2. Ко може да захтева промену података у сертификату

Не врши се.

4.8.3. Обрада захтева за промену података у сертификату

Не врши се.

4.8.4. Обавештење корисника о промени података у сертификату

Не врши се.

4.8.5. Поступак прихватања обавештења о промени података у сертификату

Не врши се.

4.8.6. Објављивање сертификата код кога је извршена промена података

Не врши се.

4.8.7. Обавештење трећих лица о издавању сертификата

Не врши се.

4.9. Опозив и суспензија сертификата

4.9.1. Околности опозива сертификата

ITE CA дужно је да опозове квалификовани сертификат за електронски печат из следећих разлога:
- оштећења или злоупотребе техничких средстава (хардвера или софтвера) или приватног криптографског кључа, односно компромитовања или сумње у компромитовање приватног криптографског кључа,
- промене података у сертификату, које захтевају издавање новог сертификата,
- неиспуњавања обавеза корисника сертификата одређених овом Политиком и практичним правилима ITE CA и уговором,
- накнадног утврђивања да подаци које је доставио корисник при идентификацији нису тачни,
- уколико опозив квалификованог сертификата захтева корисник сертификата,
- уколико корисник квалификованог сертификата изгуби пословну способност,
- уколико се промене околности које битно утичу на важење сертификата,
- из других разлога који су утврђени законом и другим прописима који регулишу ову област.

4.9.2. Ко може да захтева опозив сертификата

Опозив квалификованог сертификата може да захтева:
- корисник квалификованог сертификата,
- ITE CA,
- надлежни државни орган на основу закона.

4.9.3. Процедуре за опозив сертификата

4.9.3.1. Опозив сертификата услед компромитовања приватног криптографског кључа

Корисник односно овлашћено лице корисника доставља захтев за опозив квалификованог сертификата услед компромитовања приватног криптографског кључа лично, на локацији регистрационог тела, или електронским путем.

ITE CA може да се одлучи за опозив квалификованог сертификата и без захтева корисника, уколико установи да је дошло до компромитовања приватног криптографског кључа.

После опозива квалификованог сертификата, корисник може да захтева издавање новог квалификованог сертификата.

4.9.3.2. Опозив сертификата услед промене података у сертификату

Опозив квалификованог електронског сертификата услед промене података у сертификату, врши се на исти начин како је одређено у тачки 4.9.3.1.

ITE CA може да се одлучи за опозив квалификованог сертификата и без захтева корисника, уколико процени да је дошло до промене података у сертификату, које захтевају издавање новог квалификованог сертификата.

После опозива квалификованог сертификата, корисник може да захтева издавање новог квалификованог сертификата.

4.9.3.3. Опозив сертификата услед неиспуњења обавеза корисника

У случају да корисник не испуњава своје обавезе, ITE CA спроводи процедуру опозива квалификованог сертификата корисника:
1) опозива квалификовани сертификат корисника,
2) обавештава корисника о опозиву квалификованог сертификата електронском поштом.

После опозива квалификованог сертификата, корисник може да захтева издавање новог квалификованог сертификата.

4.9.4. Време од пријаве до опозива сертификата

После подношења захтева за опозив квалификованог сертификата од стране корисника, ITE CA ће приступити обради захтева за опозив сертификата, без одлагања.

4.9.5. Временски рок у коме сертификационо тело спроводи захтев за опозив сертификата

ITE CA извршава опозив квалификованог сертификата одмах по пријему захтева за опозив сертификата, а после спроведене идентификације.

4.9.6. Захтев за проверу опозваности сертификата од стране поуздајућих страна

Током рада са квалификованим сертификатима издатим од стране ITE CA, поуздајуће стране имају обавезу да проверавају опозваност сертификата. Уколико поуздајућа страна у датом тренутку не може да прибави информацију о опозваности сертификата, она не сме да се поузда у такав сертификат.

4.9.7. Учесталост објављивања регистра опозваних сертификата

Регистар опозваних сертификата подређеног (*subordinate*) сертификационог тела редовно се објављује на свака 24 сата.

Регистар опозваних сертификата *Root* сертификационог тела редовно се објављује на сваких 12 месеци и приликом опозива подређеног (*subordinate*) сертификационог тела.

4.9.8. Максимално кашњење у објављивању регистра опозваних сертификата

У случају да пре редовне објаве, дође до опозива или суспензије квалификованог сертификата, ITE CA може да објави нови регистар опозваних сертификата и пре истека рока важности регистра опозваних сертификата.

4.9.9. Расположивост *on-line* провере опозваности/статуса сертификата

Регистар опозваних сертификата је стално доступан за *on-line* проверу опозваности квалификованих сертификата.

4.9.10. Захтеви за *on-line* проверу опозваности сертификата

Корисници и поуздајуће стране дужни су да провере статус квалификованог сертификата на основу јавно доступног регистра опозваних сертификата.

4.9.11. Друге форме регистра опозваних сертификата

Није примењиво.

4.9.12. Посебни захтеви у случају компромитовања кључа

Ако корисник зна или сумња у компромитацију његовог приватног кључа дужан је да одмах престане са његовим коришћењем и поднесе захтев за опозив квалификованог сертификата.

4.9.13. Околности суспензије и прекида суспензије сертификата

Није примењиво.

4.9.14. Ко може да захтева суспензију и прекид суспензије сертификата

Није примењиво.

4.9.15. Процедуре за суспензију и прекид суспензије сертификата

Није примењиво.

4.9.16. Ограничење периода на који се сертификат суспендује

Није примењиво.

4.10. Услуге о статусу сертификата

4.10.1. Оперативне карактеристике

ITE CA пружа услугу провере статуса/опозваности квалификованог сертификата посредством регистра опозваних сертификата.

4.10.2. Доступност услуге

Регистар опозваних сертификата је доступан по моделу 24/7. У случају настанка околности које су изван контроле ITE CA или услед утицаја више силе услуга ће бити доступна у складу са планом континуитета пословања.

4.10.3. Додатне карактеристике

У регистру опозваних сертификата поред података о серијском броју, датуму и времену опозива квалификованог сертификата уписан је и разлог опозива сертификата.

4.11. Престанак коришћења сертификата

Корисник престаје са коришћењем квалификованог сертификата после:
- истека рока важности квалификованог сертификата,
- извршеног опозива квалификованог сертификата.

4.12. Откривање и обнова приватног кључа корисника

4.12.1. Политика откривања и обнове приватног кључа корисника

Не врши се.

4.12.2. Политика енкапсулације кључа сесије и обнове

Не врши се.

5. ТЕХНИЧКЕ КАРАКТЕРИСТИКЕ СИСТЕМА ЗА ИЗДАВАЊЕ еПЕЧАТА

Систем за издавање електронских сертификата ITE CA за квалификовано електронско печатирање се састоји од следећих компоненти:

- Софтвер CA тела са базом података је специјализован софтвер за подршку издавања електронских сертификата. Софтвер је сертификован према CWA 14167-1 што му омогућава да се користи за издавање квалификованих електронских сертификата.
- CRL компонента омогућава објављивање листе опозваних електронских сертификата. Приступ листи је омогућен преко https протокола.
- QSCD – Qualified Signature Creation Device је HSM – Hardware Security Module који је посебан хардверски уређај који се користи за издавање електронских сертификата тако што чува, штити и користи криптографске кључеве CA тела за потписивање свих захтева за издавање сертификата. Поседује FIPS 140-2 Level 3

и Common Criteria (EN 419221-5) сертификацију, као и eIDAS усклађеност за QSCD уређаје.

6. КОНТРОЛА ФИЗИЧКОГ ПРИСТУПА, ПРОЦЕДУРА И ОВЛАШЋЕНИХ ЛИЦА

Ово поглавље описује контролу физичког окружења, процедура и овлашћених лица, која је имплементирана у ITE CA да би се заштитило функционисање система.

6.1. Контрола физичког приступа

6.1.1. Локација и размештај просторија

Најважнија опрема ITE CA која служи за обављање делатности из овог документа, налази се у заштићеној просторији Државног дата центра, у објекту на централној локацији ITE CA.

Контрола физичког приступа, надзора и заштите заштићене просторије имплементирана је у складу са стандардима заштите ITE CA, и то на следећи начин:
- приступ у заштићену просторију бележи се и уноси у дневник за приступ просторији, а исти се периодично прегледа,
- приступ без пратње ограничен је на лица која се налазе на листи за приступ,
- приступ са пратњом уз претходно одобрење овлашћеног лица ITE CA захтева се за сва лица која се не налазе на листи за приступ,
- приступ због одржавања система мора бити унапред најављен, осим у случају хитне интервенције,
- зидови су ојачане конструкције,
- браве, електронски системи заштите и системи противпожарне заштите одобрени су од стране организационог дела ITE CA, надлежног за безбедност и заштиту,
- простор и систем надгледани су 24 сата, 7 дана у недељи од стране овлашћених лица организационог дела ITE CA и заштићени су системом противпровалне заштите, односно сензорима који су повезани са централним уређајем за надзор просторија,
- заштићена просторија је обезбеђена од излива воде.

6.1.2. Контрола физичког приступа за појединце

ITE CA обезбеђује да је приступ систему сертификације ограничен искључиво на ауторизоване запослене.

Запослени ITE CA мора да се придржава следећих обавеза:
- извршава своје администраторске дужности у заштићеној просторији, у коју је улазак могућ искључиво уз идентификацију са бесконтактном картицом,
- штити лозинке које омогућавају приступ приватним криптографским кључевима,
- обезбеђује USB токене и PED уређаје за аутентикацију администратора и оператера и друге медије који садрже криптографске кључеве,
- штити резервне копије приватног кључа,
- одјављује се са свих апликација у случају да напушта рачунар, а рачунар остаје без надзора,
- после завршетка рада закључава металне ормане у којима се налазе сервери ITE CA.

Запослени који обавља послове пријема захтева за издавање квалификованог сертификата и захтева за промену статуса сертификата дужан је да се придржава следећих обавеза:
- извршава своје дужности у зони пријема,
- штити лозинке које омогућавају пријављивање на апликацију за пријем захтева за издавање квалификованог сертификата и пријем захтева за промену статуса сертификата,
- одјављује се са свих апликација у случају да напушта рачунар, а рачунар остаје без надзора.

6.1.3. Напајање и климатизација

ITE CA је опремљено:
- системом за непрекидни извор напајања електричном енергијом и стабилизацију напона за рачунарску и комуникациону опрему, који је повезан са агрегатом,
- независним системом за климатизацију који омогућава контролу температуре и влажности ваздуха унутар просторија ITE CA.

6.1.4. Заштита од поплаве

Унутар заштићене просторије на централној локацији ITE CA не постоји водоводна инсталација. ITE CA је предузело све техничке мере заштите од евентуалних поплава од водоводних инсталација у окружењу.

Зграда на централној локацији ITE CA, у којој се налази опрема која служи за обављање делатности из овог документа, удаљена је од речних и других водених токова.

6.1.5. Заштита од ватре

Просторије на централној локацији ITE CA, заштићене су системом за рано откривање и аутоматску дојаву пожара.

Заштићена просторија се посебно штити локалним системом за гашење пожара који није штетан за људе, рачунарску и комуникациону опрему.

6.1.6. Смештање медија

Сви рачунарски медији који садрже податке о пословима ITE CA, укључујући и медије са резервним копијама података, чувају се у државним дата центрима у Београду и Крагујевцу.

6.1.7. Одлагање непотребних података

Непотребна папирна документација и рачунарски медији за смештај података се комисијски секу на комадиће и физички уништавају у посебном одељењу за одлагање непотребних материјала.

Подаци са медија, као што су криптографски кључеви, подаци за активирање или електронски дневници, неповратно се бришу, у складу са политиком информационе безбедности и интерним правилима.

6.1.8. Смештај резервних копија података на удаљеној локацији

ITE CA користи безбедну удаљену локацију за смештај медија са подацима. Медији се смештају у Државни дата центар у Крагујевцу. Просторија у којој је смештена резервна копија података је под надзором овлашћених службених лица.

6.2. Контрола процедура

6.2.1. Поверљиве улоге овлашћених лица

Апликација сертификационог тела и апликација регистрационог тела користе поверљиве улоге, које се додељују овлашћеним лицима ITE CA у зависности од њихових дужности.

ITE CA гарантује, да послови из овог документа које обављају овлашћена лица ITE CA, могу да буду накнадно прегледани по активностима. Наиме, активности запослених на административним пословима, у зависности од врсте активности, уписују се у електронске дневнике или ручне евиденције.

6.2.1.1. Поверљиве улоге овлашћених лица сертификационог и регистрационог тела

Овлашћена лица ITE CA, у зависности од додељене улоге, могу да имају одређене налоге, и то:
- на серверима ITE CA,
- на хардверским криптографским модулима - *HSM* уређајима,
- на апликацији сертификационог тела,
- на *firewall*-овима и радној станици за администрирање *firewall*-ова.

Привилегије одређених налога на оперативним системима рачунара и налога у апликацијама, ограничавају приступ овлашћеним лицима ITE CA на радње које су им потребне у обављању њихових дужности и укључују следеће улоге:
- главног администратора безбедности - свеукупну одговорност за администрирање и имплементацију безбедносних функција и процедура, као и управљање активностима на додатном унапређењу послова генерисања, опозива и суспензије квалификованих сертификата,
- систем администраторе - ауторизовану одговорност за инсталацију, конфигурисање и одржавање безбедних система издаваоца квалификованих сертификата тела за регистрацију корисника, генерисање квалификованих сертификата, обезбеђење квалификованих средстава за креирање електронског печата за кориснике и управљање опозивом квалификованих сертификата,
- систем операторе - одговорност за рад безбедних система издаваоца сертификата у текућем раду на дневном нивоу и ауторизовану одговорност за имплементацију система за формирање резервних копија и процедуре опоравка,
- систем евидентичаре - ауторизовану одговорност за прегледање и одржавање архива и лог фајлова безбедних система издаваоца сертификата.

6.2.2. Потребан број овлашћених лица за оперативне послове

ITE CA има имплементирану вишеструку ауторизацију за оперативне послове наведене у овој тачки.

Две ауторизације потребне су да би се извршили следећи послови:
- креирање и обнова профила *HSM* администратора и *HSM* оператера,
- промена заборављене лозинке *HSM* администратора и *HSM* оператера,
- генерисање приватног криптографског кључа апликације сертификационог тела,
- приступ медијима и подацима у вези са услугом која је предмет овог документа.

Остали послови који нису наведени у овој тачки, извршавају се уз ауторизацију једног овлашћеног лица ITE CA.

6.2.3. Идентификација и аутентикација овлашћених лица

ITE CA врши проверу својих запослених, пре него што им додели одређене привилегије које могу да буду:
- упис у одговарајућу приступну листу за улазак у заштићену просторију ITE CA,
- идентификациона бесконтактна картица за улазак у заштићену просторију,
- налог на оперативном систему сервера и радних станица ITE CA,
- налог на апликацији сертификационог тела и *HSM* приступни токен.

Налози и приступни токени из става 1. ове тачке, креирају се посебно за свако овлашћено лице ITE CA.

Заједничко коришћење налога или приступних токена између овлашћених лица ITE CA није дозвољено.

6.2.4. Разграничење овлашћења овлашћених лица

Активности запослених у ITE CA ограничене су путем овлашћења дефинисаних на нивоу:
- оперативног система сервера и радних станица,
- апликације сертификационог тела.

6.3. Контрола овлашћених лица

Послове ITE CA, у смислу ових практичних правила, за ITE CA обављају запослена и радно ангажована лица и организације (у даљем тексту: запослени).

Запослени у ITE CA морају бити квалификовани за обављање послова из овог документа и подлежу провери радне способности.

Запослени у ITE CA дужни су да не објављују, односно не саопштавају неовлашћеним лицима, поверљиве информације везане за безбедност ITE CA или информације о корисницима квалификованих сертификата.

Запослени ITE CA не преузимају на себе, нити им се додељују послови изван делокруга послова за које су ангажовани, а који би могли да доведу до сукоба интереса са овим пословима.

Запослени у ITE CA добијају од руководиоца послова ITE CA документацију са детаљним описом процедура којих су дужни да се придржавају.

6.3.1. Захтеви у вези са претходним радним ангажовањем, квалификацијама, искуством и безбедносна провера овлашћених лица

Запослени у ITE CA морају да задовоље одређене захтеве у погледу стручне квалификације за свако радно место на које се ангажују, као и у погледу радног искуства и искуства на сличним радним дужностима.

Приликом запошљавања узима се у обзир да лице које се ангажује није било осуђивано.

6.3.2. Поступци за проверу претходног радног ангажовања

Провера претходног радног ангажовања лица за рад у ITE CA врши се у складу са кадровском политиком ITE CA.

6.3.3. Обука

Обука запослених у ITE CA обухвата:
- упознавање са инфраструктуром ITE CA,
- упознавање са поступцима заштите инфраструктуре и података,
- оспособљавање за коришћење апликације сертификационог тела, регистрационог тела и локалног регистрационог тела, у складу са додељеном улогом,
- оспособљавање за креирање резервних копија података,
- предузимање поступака за опоравак система после катастрофе,
- упознавање са другим дужностима везаним за рад ITE CA.

Лица која похађају обуку, добијају одговарајућу литературу, у складу са темом обуке.

6.3.4. Учесталост поновних обука

Запослени у ITE CA похађају обуке за обнављање и усавршавање знања најмање једанпут годишње, а ванредно када се изврше промене техничких средстава (хардвера и софтвера) ITE CA и начина обављања делатности.

6.3.5. Учесталост и редослед ротације послова овлашћених лица

ITE CA није установило правила ротације послова, како не би дошло до нарушавања правила вршења различитих овлашћења и дужности, у вези са различитим поверљивим улогама запослених у ITE CA.

6.3.6. Санкције за неауторизоване активности

У случају извршене или сумње на извршене неауторизоване активности од стране овлашћеног лица ITE CA, истом ће бити онемогућен даљи приступ техничким средствима (хардверу и софтверу) ITE CA, а ITE CA ће суспендовати или опозвати

квалификоване сертификате које је издало то лице.

Извршене неауторизоване активности, пријављују се надлежним организационим деловима ITE CA, државним органима и институцијама, у складу са важећим законским и интерним прописима.

6.3.7. Захтеви за спољне сараднике

У случају да се додели поверљива улога спољном сараднику, за то лице важе исти услови као за запослене у ITE CA.

6.3.8. Документација за потребе овлашћених лица

Запосленима се даје одговарајућа документација са детаљним описом процедура којих морају да се придржавају.

6.4. Процедуре надгледања рада система

Догађаји који се односе на обављање делатности ITE CA записују се у електронске дневнике (*audit log*) и у евиденције које се ручно воде, са датумом и временом догађања.

6.4.1. Врсте догађаја који се евидентирају

Догађаји који се евидентирају су у вези са:
- корисничким криптографским кључевима и квалификованим сертификатима - издавање и промене статуса,
- криптографским кључевима апликације сертификационог тела,
- техничким средствима (хардвер и софтвер) ITE CA,
- администрацијом, креирањем резервних копија, сигурносним правилима и коришћењем апликација сертификационог тела,
- физичким приступом систему ITE CA,
- кадровским променама у оквиру ITE CA.

6.4.2. Учесталост прегледа електронских дневника и ручних евиденција

Овлашћена лица ITE CA прегледају електронске дневнике и ручне евиденције једанпут недељно.
Под прегледом, подразумева се:
- прикупљање свих електронских дневника и ручних евиденција од последњег прегледа,
- преглед и анализа записа у електронским дневницима и ручним евиденцијама,
- разрешавање евентуалних проблема или пријава руководиоцу послова ITE CA, који преузима даље кораке у циљу решавања проблема.

6.4.3. Време чувања евиденција

Копије електронских дневника и ручних евиденција чувају се најмање 10 година.

6.4.4. Заштита електронских дневника

Подаци за електронске дневнике, прикупљају се у заштићеној просторији ITE CA. Приступ заштићеној просторији дозвољен је само овлашћеним лицима, како је то дефинисано интерним правилима за приступ.

За електронске дневнике оперативног система се употребљавају заштите које омогућава сам оперативни систем, и могу да их прегледају само овлашћена лица ITE CA.

Електронским дневницима апликације сертификационог тела могу да приступе и прегледају само овлашћена лица ITE CA.

6.4.5. Креирање резервних копија електронских дневника

Електронски дневници се ажурирају свакодневно. За креирање резервних копија задужена су овлашћена лица ITE CA. Резервне копије електронских дневника, чувају се на централној локацији ITE CA.

6.4.6. Систем прикупљања података за електронске дневнике и ручне евиденције

Подаци за електронске дневнике и ручне евиденције се прикупљају аутоматски и ручно, како је дато у Табели 5.

Табела 5. Догађаји који се записују у електронске дневнике и ручне евиденције, и начин прикупљања

Догађаји који се записују у електронске дневнике и ручне евиденције	**Начин прикупљања података**	**Одговорно лице или систем**
Догађаји повезани са корисничким квалификованим сертификатима	аутоматско	апликација сертификационог тела
Догађаји на апликацији еПечат	аутоматско	апликација еПечат
Догађаји на оперативном систему	аутоматско	оперативни систем
Догађаји на рачунарској мрежи	аутоматско	*firewall*-ови, оперативни систем
Креирање резервних копија и обнова базе корисника квалификованог сертификата	аутоматско	оперативни систем, апликација сертификационог тела
Креирање резервних копија и обнова логова конфигурације сертификационог тела	аутоматско	оперативни систем, апликација сертификационог тела
Физички приступ до заштићене просторије сертификационог тела	ручно, аутоматско	запослени Сертификационог тела, систем за контролу приступа
Промене хардвера и софтвера на систему	ручно	запослени Сертификационог тела
Техничко одржавање на систему и у заштићеној просторији	ручно	запослени Сертификационог тела
Кадровске промене	ручно	запослени

		Сертификационог тела

6.4.7. Обавештавање лица које је изазвало догађај

О догађају се обавештава руководилац организационе целине надлежне за пружање услуга од поверења у ITE CA. Лице које је изазвало догађај се не обавештава.

6.4.8. Процена рањивости система

Процена рањивости система врши се у склопу свакодневних активности које се спроводе на систему, анализама ризика, разменом искустава са сертификационим телима из окружења и прегледом електронских дневника и ручних евиденција.

Тест пенетрације се спроводи једном годишње или после великих промена на систему.

6.5. Архивирање података

6.5.1. Подаци који се архивирају

ITE CA архивира следеће податке и документа:
- електронске дневнике,
- уговоре и документацију корисника,
- захтеве за издавање квалификованог електронског сертификата,
- захтеве за промену статуса електронског сертификата (опозив),
- квалификоване електронске сертификате,
- регистре опозваних сертификата,
- општа акта ITE CA везана за обављање делатности ITE CA.

6.5.2. Период чувања података у архиви

ITE CA је дужно да чува комплетну документацију о издатим и опозваним квалификованим сертификатима 10 година по престанку важења сертификата.

6.5.3. Заштита архиве

Архива докумената се чува на централној локацији ITE CA.

Архива је заштићена одговарајућим сигурносним механизмима ITE CA (физичко-техничком заштитом и надзором, ограниченим приступом, шифрама и кључевима). Приступ архивама дозвољен је само овлашћеним лицима.

ITE CA обезбеђује тајност текућих и архивираних записа о квалификованим сертификатима.

6.5.4. Процедуре архивирања

Папирни документи архивирају се на централној локацији ITE CA.

ITE CA свакодневно ради архивирања израђује копије електронских дневника и података.

6.5.5. Временска ознака архивираних података

Архивирани подаци носе временску ознаку са сервера који је синхронизован са извором тачног времена. Временска ознака није криптографски/електронски временски жиг.

6.5.6. Систем архивирања (интерни или екстерни)

ITE CA користи интерни систем архивирања. Архивирање електронских података извршава се аутоматски техничким средствима за архивирање у заштићеној просторији ITE CA.

Документација у папирном облику се прикупља и архивира ручно на централној локацији ITE CA, а може да се архивира и у електронском облику.

6.5.7. Процедуре контроле приступа архивираним подацима

Архивирани електронски подаци чувају се у заштићеним просторијама на централној и удаљеној локацији. Просторије су са рестриктивним и ауторизованим приступом и под сталним надзором овлашћених лица.

6.6. Замена кључева сертификационог тела

Замена криптографских кључева ITE CA, врши се пет година пре истека рока важности постојећих кључева.
Замену кључева могуће је спровести и раније, због:
1) промене криптографског алгоритма којим сертификационо тело потписује сертификате и регистре опозваних сертификата;
2) промене дужине кључева сертификационог тела;
3) промене рока важности кључева сертификационог тела;
4) промене *hash* алгоритма сертификационог тела, применом кога се израчунава *hash* вредност сертификата и регистра опозваних сертификата;
5) промене садржаја постојећих поља (екстензија) сертификата сертификационог тела или додавања нових поља (екстензије) сертификата сертификационог тела;
6) оштећења или компромитовања приватног криптографског кључа сертификационог тела.

6.7. Опоравак система после катастрофе

6.7.1. Процедуре рада у инцидентним ситуацијама приликом компромитације система

ITE CA врши континуирани надзор рада система и у случају појаве грешке или инцидентне ситуације на систему спроводи правовремене и координисане активности у складу са интерним правилима рада. Обавештавање у случају појаве грешке или инцидентне ситуације врши се у складу са овом Политиком и практичним правилима ITE CA и интерним правилима.

У случају компромитовања или сумње у компромитовање приватног криптографског кључа апликације сертификационог тела, спроводе се следеће операције:
- опозив издатих квалификованих сертификата корисника,
- опозив сертификата апликације сертификационог тела,
- објављивање опозваних сертификата у регистру опозваних сертификата.

Затим се, уколико је то могуће, врши отклањање узрока компромитације.

6.7.2. Уништење техничких средстава или података

У случају штете настале на техничким средствима (хардверу и софтверу) или подацима, при чему приватни криптографски кључ апликације сертификационог тела није уништен или оштећен, сервиси апликације сертификационог тела биће поново успостављени у најкраћем могућем року.

У случају уништења или оштећења приватног криптографског кључа апликације сертификационог тела, после отклањања узрока уништења или оштећења, спроводи се поступак реконструисања кључа.

6.7.3. Компромитовање приватног криптографског кључа апликације сертификационог тела

ITE CA ће, у случају компромитовања приватног криптографског кључа апликације сертификационог тела, одмах да:
- опозове издате квалификоване сертификате,
- опозове сертификат апликације сертификационог тела,
- објави регистар опозваних сертификата,
- обавести кориснике издатих квалификованих сертификата.

ITE CA ће, у случају компромитовања приватног криптографског кључа апликације сертификационог тела, после отклањања узрока компромитовања, да:
- генерише нове криптографске кључеве апликације сертификационог тела,
- изда корисницима нове квалификоване сертификате.

6.7.4. Наставак рада после катастрофе

После престанка катастрофе и отклањања њеног узрока, ITE CA ће у најкраћем могућем року да доведе систем у продукционо стање и настави са радом.

6.8. Престанак рада сертификационог тела

ITE CA, у случају престанка рада, има обавезу да:
- обавести све заинтересоване стране о престанку обављања услуга;
- пренесе своје обавезе другом сертификационом телу, уколико постоје могућности за то;
- опозове све издате квалификоване сертификате, којима није истекао рок важности, уколико не успе да пренесе своје обавезе на друго сертификационо тело;
- уништи или потпуно онемогући коришћење својих приватних кључева, који су коришћени за креирање сертификата и регистра опозваних сертификата, тако да се исти не могу реконструисати.

ITE CA ће о планираном престанку обављања послова обавестити своје кориснике и надлежни државни орган писаним путем најмање три месеца пре престанка рада, у складу са важећим прописима. Корисници издатих квалификованих сертификата биће обавештени о престанку рада, преко веб презентације ITE CA или на други начин, посредством средстава јавног информисања или електронском поштом.

ITE CA ће предузети све што могућности у датом тренутку буду дозвољавале, како би обезбедило наставак обављања услуге сертификације код другог сертификационог тела за своје кориснике. ITE CA има обавезу да сертификационом телу код кога је обезбедило наставак пружања услуге сертификације према својим корисницима, достави сву постојећу документацију и архиву, која се односи на обављање услуге сертификације.

Ако се не постигне пренос обавеза на друго сертификационо тело, ITE CA има обавезу да сву постојећу документацију и архиву, која се односи на обављање услуга сертификације достави надлежном државном органу.

Уколико нема могућности за пренос обавеза пружања услуге сертификације на друго сертификационо тело, ITE CA ће раскинути уговоре о издавању и коришћењу квалификованих електронских сертификата са својим корисницима и опозвати све важеће квалификоване сертификате, о чему ће обавестити кориснике и надлежни државни орган.

7. КОНТРОЛЕ ТЕХНИЧКЕ ЗАШТИТЕ

7.1. Генерисање пара криптографских кључева и инсталација

Пар криптографских кључева апликације сертификационог тела је генерисан током церемоније генерисања (*Key Generation Ceremony*) по прецизно дефинисаној процедури. У току генерисања пара криптографских кључева користи се заштита која важи за просторије ITE CA, заштита коју пружа хардверски криптографски модул (*Hardware Security Module - HSM*), оперативни систем, апликација сертификационог тела и вишеструка аутентикација овлашћених лица.

7.1.1. Генерисање пара криптографских кључева

Пар криптографских кључева апликације сертификационог тела генерише се у хардверском криптографском модулу.

Пар криптографских кључева корисника генерише се у квалификованом средству за креирање електронских печата (*Qualified Signature Creation Device - QSCD*).

7.1.2. Уручење приватног криптографског кључа кориснику

Након потписивања уговора и генерисања пара кључева, јавног и приватног, у квалификованом средству за креирање електронског печата, ITE CA издаје квалификовани сертификат за електронски печат кориснику и обавештава корисника.

Корисник не преузима сертификат већ га користи кроз свој информациони систем (систем корисника), путем веб сервиса.

7.1.3. Слање сертификационом телу јавног криптографског кључа корисника

Јавни и приватни криптографски кључ корисника генеришу се у ITE CA на квалификованом средству за креирање електронског печата.

7.1.4. Уручење јавног криптографског кључа трећим лицима

Јавни криптографски кључ апликације сертификационог тела у форми сертификата је јавно доступан на веб презентацији ITE CA.

Корисничке јавне криптографске кључеве и сертификате, ITE CA јавно не објављује, нити уручује трећим лицима.

7.1.5. Дужине криптографских кључева

Дужине криптографских кључева за које ITE CA издаје квалификоване сертификате су:
- Криптографски кључеви апликације сертификационог тела: *RSA* кључеви дужине 4096 бита.
- Кориснички кључеви: *RSA* кључеви дужине 2048 бита.

7.1.6. Генерисање параметара јавног криптографског кључа и провера квалитета

Генерисање параметара јавног криптографског кључа апликације сертификационог тела врши се у хардверским криптографским модулима ITE CA, а параметри јавних криптографских кључева корисника генеришу се у квалификованим средствима за креирање електронског печата. Параметри су врста алгоритма и дужина кључа.

Провера квалитета параметара криптографских кључева и сертификата апликације сертификационог тела се врши током и непосредно после генерисања криптографских кључева.

Управна структура ITE CA задаје параметре јавних кључева апликације сертификационог тела и корисника.

7.1.7. Намена кључа (дефинисано у *X*.509 вер. 3 пољу *Key Usage* сертификата)

За потписивање квалификованих сертификата и регистра опозваних сертификата употребљава се искључиво приватни криптографски кључ апликације сертификационог тела. Јавни криптографски кључ апликације сертификационог тела се употребљава за валидацију електронског потписа квалификованих сертификата и регистра опозваних сертификата (*Key Usage = Certificate Signing, Off-line CRL Signing, CRL Signing*).

Намена јавног криптографског кључа квалификованог сертификата корисника је валидација квалификованог електронског печата и обезбеђивање непорецивости. Додатна намена јавног криптографског кључа квалификованог сертификата корисника

за електронски печат који се користи за валидацију временских жигова је валидација временских жигова. Наведено у Табели 6.

Табела 6. Садржај поља *Key Usage* у квалификованим сертификатима које издаје ITE CA

Врста сертификата	**Садржај поља *Key Usage***
Квалификовани сертификат	*Digital Signature, Non-Repudiation* (електронски потпис и непорецивост)
Квалификовани сертификат	*Extended Key Usage = Time Stamping* (валидација временских жигова)

7.2. Заштита приватног криптографског кључа

7.2.1. Стандарди за хардверски криптографски модул

Хардверски криптографски модул на серверу апликације сертификационог тела задовољава стандард *FIPS* 140-2 ниво 3 или виши или *EAL* 4+.

Квалификовано средство за креирање електронског печата корисника задовољава стандард *FIPS* 140-2 ниво 2 или виши или *EAL* 4+.

7.2.2. Контрола приступа приватном криптографском кључу од стране *n* од *m* овлашћених лица

ITE CA има имплементирану вишеструку ауторизацију за приступ приватном криптографском кључу апликације сертификационог тела. *Root* сертификационо тело је у *off-line* режиму.

Приступ корисничком приватном криптографском кључу ограничен је само на корисника.

7.2.3. Откривање приватног криптографског кључа

ITE CA не нуди могућност откривања приватног криптографског кључа.

7.2.4. Креирање копије приватног криптографског кључа

После генерисања криптографских кључева апликације сертификационог тела (*Key Generation Ceremony*), уз присуство овлашћених лица ITE CA, креира се копија приватног криптографског кључа апликације сертификационог тела. Приватни криптографски кључ апликације сертификационог тела је шифрован *AES* (*Rijndael*) алгоритмом и никад се не налази изван хардверског криптографског модула у дешифрованом облику. Дешифровање приватног криптографског кључа је могуће само у хардверском криптографском модулу, на основу копије приватног криптографског кључа, уз помоћ два администраторска и оператерска *HSM* токена за приступ хардверском криптографском модулу и њихових лозинки.

Креирање копија приватних криптографских кључева корисника се не ради.

После генерисања криптографских кључева апликације сертификационог тела (*Key Generation Ceremony*), уз присуство овлашћених лица ITE CA, креира се резервна копија приватног криптографског кључа апликације сертификационог тела. Приватни криптографски кључ апликације сертификационог тела се складишти на HSM који је намењен за чување резервних копија кључева који је по уграђеним безбедносним механизмима еквивалентан HSM уређају чији се садржај копира и никада се не налази изван HSM уређаја. Такође није могућ експорт приватног кључа ни у облику шифрата.

Израда резервне копије приватног кључа могућа је само уз интеракцију корисника са улогама:

1. минимум две од три особе са улогом SO - Security Officer које су власници одговарајућег BLUE PED кључа за аутентикацију.
2. минимум две од укупно три особе које су власници Domain ID, RED PED кључа за аутентикацију.

Власници поменутих PED кључева морају се додатно идентификовати укуцавањем свог ПИН-а.

7.2.5. Архивирање приватног криптографског кључа

ITE CA архивира копију приватног криптографског кључа апликације сертификационог тела после његовог креирања на HSM уређају који је намењен за чување резервних копија кључева, на локацији ITE CA и на другој удаљеној локацији, у заштићеним просторијама за дуготрајно чување.

HSM уређај који је намењен за чување резервних копија кључева се под двоструком контролом овлашћених особа смешта у заштићену просторију Државног дата центра која је под сталним надзором овлашћених лица.

Архивирање приватних криптографских кључева корисника се не ради.

7.2.6. Пребацивање приватног криптографског кључа у криптографски модул или из њега

Приватни криптографски кључ апликације сертификационог тела је генерисан у хардверском криптографском модулу. Само уколико наступи хардверски квар хардверског криптографског модула апликације сертификационог тела, он ће бити замењен новим модулом, а приватни кључ пребачен (импортован) у тај модул, уз писану одлуку управне структуре највишег нивоа ITE CA и уз вишеструку ауторизацију запослених ITE CA.

Приватни криптографски кључ корисника генерисан је у квалификованом средству за креирање електронског печата и не експортује се.

7.2.7. Чување приватног криптографског кључа у криптографском модулу

Криптографски кључеви се чувају у хардверским криптографским модулима и могу да се користе само уколико су на правилан начин активирани.

7.2.8. Поступак за активирање приватног криптографског кључа

За реконструкцију и активирање приватног криптографског кључа апликације

сертификационог тела потребна је ауторизација два *HSM* администратора и два *HSM* оператера са својим токенима и лозинкама. Приватни криптографски кључ апликације сертификационог тела се активира после стартовања апликације сертификационог тела.

Кориснички приватни криптографски кључеви се активирају после успешне аутентификације корисника са лозинком у корисничкој апликацији приликом електронског печатирања.

7.2.9. Поступак за деактивирање приватног криптографског кључа

Приватни криптографски кључ апликације сертификационог тела се деактивира заустављањем апликације сертификационог тела, искључењем сервера на ком се налази апликација сертификационог тела или искључењем хардверског криптографског модула.

Приватни криптографски кључ апликације сертификационог тела се деактивира уклањањем приступа апликације сертификационог тела партицији HSM на којој се налази приватни кључ. Тиме је онемогућен приступ апликације и сервера на коме се налази апликација приватном кључу.

Корисничке апликације деактивирају приватни криптографски кључ корисника после електронског печатирања.

7.2.10. Поступак за уништавање приватног криптографског кључа

Приватни криптографски кључ апликације сертификационог тела се уништава само у случају планираног престанка рада сертификационог тела, а спроводе га овлашћени запослени са поверљивим улогама у ITE CA.

7.2.11. Класификовање криптографских модула

Стандарди за криптографске модуле према којима може да се врши њихово класификовање су *FIPS* и *EAL*.

7.3. Остали видови управљања паром кључева

7.3.1. Архивирање јавног криптографског кључа

ITE CA архивира јавни криптографски кључ апликације сертификационог тела и јавне криптографске кључеве корисника.

7.3.2. Рок важности сертификата и криптографских кључева

Рок важности сертификата ITE CA је:
- Root сертификати апликације сертификационог тела: 20 година.
- Сертификати подређених сертификационих тела: 10 година.
- Квалификовани сертификати корисника: 5 година

Временски период важности приватног кључа апликације сертификационог тела једнак је временском периоду важности припадајућег сертификата.

Рок важности приватног кључа квалификованог сертификата једнак је временском периоду важности припадајућег сертификата, изузев квалификованог сертификата за електронски печат који се користи за валидацију временских жигова код кога је рок важности приватног кључа једна година.

7.4. Подаци за активирање

7.4.1. Генерисање и употреба података за активирање

Подаци за активирање приватног кључа апликације сертификационог тела генеришу се приликом генерисања криптографских кључева (*Key Generation Ceremony*) и могу да их користе искључиво овлашћена лица ITE CA.

Кориснички приватни криптографски кључеви се активирају после успешне аутентификације корисника са лозинком у корисничкој апликацији приликом електронског печатирања.

ПИН за приступ приватном кључу корисника (ПИН за приступ кључу) се састоји од четири или више нумеричких карактера и креира га и поставља корисник на церемонији генерисања криптографских кључева (Key Generation Ceremony). Корисник га уписује у апликацију за шифровање, након чега се у криптованом облику уписује у апликацију еПечат. Корисник има могућност промене ПИН-а за приступ кључу и његове дужине. ПИН за приступ кључу је познат само кориснику.

Приликом сваког захтева за печатирање, систем корисника мора као параметар да проследи ПИН за приступ кључу у криптованом облику како би ауторизовао печатирање. Прво прослеђивање ПИН-а за приступ кључу сматра се тренутком активације квалификованог сертификата за електронски печат корисника.

7.4.2. Заштита података за активирање

Овлашћена лица ITE CA су дужна да чувају податке који се користе за активирање кључева сертификационог тела.

Корисници су дужни да чувају ПИН за приступ приватним криптографским кључевима који се налазе на квалификованом средству за креирање електронског печата, као и лозинку која се користи за повезивање система корисника и апликације еПечат.

7.4.3. Остали видови података за активирање

Не постоје.

7.5. Безбедносне контроле рачунарског система

7.5.1. Специфични безбедносно-технички захтеви за рачунаре

У рачунарском систему ITE CA, имплементиране су техничко-безбедносне контроле и механизми, и то:
- контрола приступа до системских сервиса сертификационог тела,
- контрола приступа функцијама апликације сертификационог тела,
- строга подела улога између овлашћених лица сертификационог тела,
- употреба приступних токена за смештање криптографских кључева овлашћених лица сертификационог тела,
- шифровање тајних података у бази података апликације сертификационог тела,
- безбедно архивирање података апликације сертификационог тела и електронских дневника,
- заштита електронских дневника, односно података у истима о свим догађајима који се односе на безбедност,
- успостављање механизама обнове система, криптографских кључева и базе података апликације сертификационог тела.

ITE CA спроводи континуирано праћење и поседује алармни систем који се користи у сврху откривања, бележења и правовременог реаговања на покушаје недозвољеног приступа ресурсима система.

7.5.2. Ниво заштите рачунара

Оперативни систем на серверима ITE CA, је оперативни систем компаније *Microsoft*, који је у складу са *EAL* стандардом заштите, како би се омогућио сигуран рад апликације сертификационог тела.

7.6.Технички надзор у току обављања делатности

7.6.1. Развој система

Приликом развоја система спроводи се анализа безбедносних захтева како би се осигурало да је безбедност имплементирана у *PKI* систему за издавање квалификованих сертификата. Софтвер који се користи приликом пружања услуге издавања квалификованих сертификата је од поузданог произвођача. Нове верзије софтвера тестирају се у тестном окружењу. Имплементација софтвера у продукционом окружењу спроводи се у складу са документованим поступцима.

7.6.2. Управљање безбедношћу

ITE CA има механизме и процедуре које примењује у контроли и надзору свих техничких система сертификационог тела.

У случају нарушавања безбедности система ITE CA или губитка његовог интегритета који може да има значајан утицај на пружање услуге издавања квалификованих сертификата или на заштиту личних података, ITE CA ће у року од 24 сата о томе обавестити надлежни државни орган. У случају да губитак интегритета може да има негативан утицај на кориснике услуга од поверења, ITE CA ће о томе без одлагања обавестити сва физичка и правна лица на које нарушавање безбедности може да има утицај.

7.6.3. Животни циклус безбедносне контроле

Безбедносна контрола се периодично извршава проверавањем рада компонената ITE CA. Интегритет компонената система и података штити се антивирусном заштитом и употребом ауторизованог софтвера.

7.7. Управљање безбедношћу рачунарске мреже

Рачунарску мрежу ITE CA чине повезани мрежни сегменти, на којима се налазе сервери и радне станице. Сегменти су подељени у логичке целине, односно зоне са различитим нивоима безбедности. Сегменти су међусобно повезани *firewall*-овима. Безбедносна правила на *firewall*-овима дозвољавају саобраћај само између сервера и радних станица по протоколима који су потребни за обављање делатности ITE CA и за приступ сервисима ITE CA.

Мрежни сегмент у ком се налазе радне станице за администрацију сертификационог тела је одвојен *firewall* уређајем од осталих мрежних сегмената и рачунара који се налазе у тим сегментима.

Опрема за заштиту рачунарске мреже бележи саобраћај и покушаје приступа сервисима ITE CA применом *IPS* система.

Непотребне комуникације, кориснички налози, портови, протоколи и сервиси су експлицитно забрањени или деактивирани.

Интерна рачунарска мрежа ITE CA заштићена је од неовлашћеног приступа, укључујући приступ корисника и трећих лица.

Сви критични системи за пружање услуге издавања квалификованих сертификата смештени су у заштићену просторију и распоређени су у више различитих безбедносних мрежних зона.

Системи ITE CA посебно су безбедносно подешени и ојачани.

Мрежне компоненте система ITE CA чувају се у физички и логички сигурном окружењу. Усклађеност њихове конфигурације се периодично проверава.

7.8. Временска ознака

Квалификовани сертификати и регистри опозваних сертификата имају временску ознаку датума и времена издавања, датума и времена престанка важења сертификата и датума и времена издавања следећег регистра опозваних сертификата. Временска ознака није криптографски/електронски временски жиг.

Криптографски/електронски временски жиг се не употребљава у опсегу услуга од поверења из овог документа.

Систем се усклађује са интерним сервисом тачног времена који је усклађен са спољним *UTC* (*Coordinated Universal Time*) извором тачног времена применом *NTP* (*Network Time Protocol*) протокола, најмање једном у 24 сата.

8. ПРОФИЛ СЕРТИФИКАТА, РЕГИСТРА ОПОЗВАНИХ СЕРТИФИКАТА

8.1. Профил сертификата

8.1.1. Верзија сертификата

ITE CA издаје *X*.509 сертификате верзије 3. Профил квалификованог сертификата је у складу са документима: *RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“, RFC 3739 „Internet X.*509 *Public Key Infrastructure: Qualified Certificates Profile“, ETSI EN 319 412-1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures”, ETSI EN 319 412-2 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons”, ETSI EN 319 412-3 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons”* и *ETSI EN 319 412-5 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements”.*

Сертификати *X*.509 ITE CA садрже основна поља *X*.509 сертификата (Табела 7) и екстензије *X*.509 сертификата (Табела 8).

Табела 7. Основна поља *X*.509 сертификата

Назив поља	**Опис поља**
Version	Верзија *X*.509 сертификата.
Serial Number	Јединствени серијски број квалификованог сертификата
Signature Algorithm	*Hash* алгоритам и асиметрични криптографски алгоритам коришћен за потписивање сертификата од стране апликације сертификационог тела
Issuer	Јединствено име сертификационог тела
Valid From	Датум и време почетка важења квалификованог електронског сертификата
Valid To	Датум и време престанка важења квалификованог електронског сертификата
Subject	Јединствено име корисника сертификата
Subject Public Key Info	Јавни криптографски кључ корисника сертификата, дужина јавног кључа и назив алгоритма јавног кључа
Signature	Електронски потпис квалификованог сертификата приватним криптографским кључем апликације сертификационог тела

8.1.2. Екстензије сертификата

Екстензије *X*.509 сертификата које апликација сертификационог тела уписује у квалификоване сертификате, и њихов опис, дати су у Табели 8.

Табела 8. Екстензије *X*.509 сертификата

Назив поља - екстензије	**Опис поља - екстензије**
Authority Key Identifier	Идентификатор јавног криптографског кључа сертификационог тела који се рачуна као *SHA*-1 *hash* поља *Issuer* сертификата сертификационог тела
Subject Key Identifier	Идентификатор јавног криптографског кључа корисника сертификата који се рачуна као *SHA*-1 *hash* поља *Subject Public Key Info* квалификованог сертификата корисника
Key Usage	Намена јавног криптографског кључа корисника квалификованог сертификата
Certificate Policies	Идентификација политике сертификације и адреса веб стране на којој се налазе ова практична правила
Subject Alternative Name	Алтернативно име корисника квалификованог сертификата. У овом пољу се наводи адреса електронске поште корисника сертификата наведена у уговору
Basic Constraints	Ознака која указује да је сертификат кориснички и она садржи „*Subject Type=End Entity*“
CRL Distribution Points	Локација на којој се налазе регистри опозваних сертификата
Qualified Certificate Statements	Ознака да је сертификат издат као квалификовани сертификат (*OID*: 1.3.6.1.5.5.7.1.3), која садржи објекте *QcCompliance, QcType* и *QcSSCD*
Extended Key Usage	Додатна намена јавног криптографског кључа корисника квалификованог сертификата за електронски печат и квалификованог сертификата који се користи за валидацију временских жигова (Time Stamping)
Private Key Usage Period	Рок важности приватног криптографског кључа корисника, који је пар јавном криптографском кључу из квалификованог електронског сертификата за електронски печат и квалификованог сертификата који се користи за валидацију временских жигова.

8.1.3. Идентификациона ознака алгоритма

ITE CA потписује квалификоване сертификате применом алгоритма *sha512RSA* (*OID*: 1.2.840.113549.1.1.13, *SHA-512 with RSA Encryption*) у складу са документима *RFC* 5280 *„Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“*, *RFC* 4055 *„Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.*509 *Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“* и *ETSI TS 119 312 „Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”* .

8.1.4. Форме имена

У квалификованим сертификатима које издаје ITE CA, име ITE CA које је наведено у пољу *Issuer,* и име корисника сертификата, које је наведено у пољу *Subject*, су јединствена имена (*Distinguished Name – DN*), као што је дефинисано у тачки 3.1.1. Јединствена имена су уписана у квалификованом сертификату применом *UTF8 String* кодирања.

8.1.5. Ограничења у именима

Коришћење специјалних знакова у именима корисника није дозвољено, изузев цртице (-) или астериска односно звездице (*).

8.1.6. Идентификациона ознака политике сертификације

ITE CA користи поље *Certificate Policies* сертификата, у коме објављује *Policy Identifier OID* (*Object Identifier*) идентификациону ознаку политике сертификације, које су дате у Табели 9.

Табела 9. Ознаке политике сертификације

Врста сертификата	**Ознака политике (*OID*)**
Квалификовани сертификат за електронски печат	0.4.0.194112.1.3, 1.3.6.1.4.1.55016.2.2.0
Квалификовани сертификат за електронски печат који се користи за валидацију временских жигова	0.4.0.194112.1.3, 1.3.6.1.4.1.55016.2.2.0

8.1.7. Употреба екстензије за раздвајање политика

Не користи се.

8.1.8. Квалификатори политике сертификације

ITE CA користи потпоље *Policy Qualifier=CPS* поља *Certificate Policies* сертификата у коме објављује тачну веб адресу где се налази ова Политика и практична правила ITE CA и потпоље *Policy Qualifier=User Notice* у коме је наведено да је електронски сертификат квалификован.

8.1.9. Процесирање критичних екстензија сертификата

Корисничке апликације морају да процесирају екстензије сертификата које су означене као критичне (*critical*).

8.2. Профил регистра опозваних сертификата

8.2.1. Верзија регистра опозваних сертификата

ITE CA издаје *X*.509 регистре опозваних сертификата (*Certificate Revocation List - CRL*) верзије 2. Профил регистра опозваних сертификата је у складу са документом *RFC* 5280 „*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"*. Регистри опозваних сертификата ITE CA садрже основна поља *X*.509 регистра (Табела 10.) и екстензије *X*.509 регистра (Табела 11.).

Табела 10. Основна поља *X*.509 регистра опозваних сертификата

***Н*азив поља**	**Опис поља**
Version	Верзија *X*.509 регистра опозваних сертификата.
Signature Algorithm	*Hash* алгоритам и асиметрични криптографски алгоритам коришћен за потписивање регистра опозваних сертификата од стране апликације сертификационог тела
Issuer	Јединствено име сертификационог тела
Effective Date (This Update)	Датум и време издавања регистра опозваних сертификата
Next Update	Датум и време следећег издавања регистра опозваних сертификата
Revoked Certificates	Списак серијских бројева опозваних сертификата и датума и времена њиховог опозивања
Signature	Електронски потпис регистра опозваних сертификата приватним криптографским кључем апликације сертификационог тела

8.2.2. Екстензије регистра опозваних сертификата

Екстензије *X*.509 регистра опозваних сертификата које апликација сертификационог тела уписује у регистре, и њихов опис, дати су у Табели 11.

Табела 11. Екстензије *X*.509 регистра опозваних сертификата

***Н*азив поља - екстензије**	**Опис поља – екстензије**
Authority Key Identifier	Идентификатор јавног криптографског кључа сертификационог тела који се рачуна као *SHA*-1 *hash* поља *Issuer* сертификата сертификационог тела
CRL Number	Редни број регистра опозваних сертификата
Reason Code	Разлог опозива сертификата
Invalidity Date	Датум компромитовања или сумње у компромитовање приватног криптографског кључа или датум када је квалификовани сертификат на неки други начин престао да буде важећи (*OID*: 2.5.29.24)

9. РЕВИЗИЈА УСКЛАЂЕНОСТИ РАДА СЕРТИФИКАЦИОНОГ ТЕЛА И ДРУГЕ ПРОЦЕНЕ

ITE CA извршава редовне унутрашње ревизије рада (*internal audit*).

Надлежни орган има право да захтева спољну ревизију, у складу са законом и подзаконским актима.

9.1. Учесталост ревизије

ITE CA извршава редовне унутрашње ревизије рада једном годишње.

Могуће је извршити и више од једне ревизије годишње уколико је то захтевано од надлежног органа или је то последица незадовољавајућих резултата претходне ревизије.

Учесталост и околности спољашње ревизије регулисани су законским прописима, општим актима и другим документима који регулишу ову област.

9.2. Квалификација лица које врши ревизију

Законски заступник ITE CA одговоран је за спровођење унутрашњих ревизија и одређивање лица која их спроводе. Законски заступник може да одлучи да се ревизија спроведе ангажовањем стручног лица из или ван ITE CA, које мора да има искуства на подручју:
- технологије инфраструктуре јавних криптографских кључева,
- вршења делатности сертификационог тела,
- спровођења ревизије сертификационог тела или другог информационо-комуникационог система.

Спољашња ревизија спроводи се у складу са законом којим се уређују електронски документ, електронска идентификација и услуге од поверења у електронском пословању.

9.3. Однос лица које врши ревизију према предмету ревизије

Лице које врши ревизију може бити запослени ITE CA или спољно стручно лице, према избору законског заступника ITE CA.

Лица која врше ревизију независна су од ITE CA и не сме да постоји сукоб интереса.

9.4. Предмет ревизије

У оквиру ревизије проверава се:
- целовитост и тачност документације,
- усклађеност са законским прописима,
- организациони процеси и процедуре,
- технички процеси и процедуре,
- физичка сигурност предметних локација,
- примењене мере информационе безбедности.

9.5. Предузете активности као резултат пронађених недостатака

У случају пронађених недостатака, спроводе се активности на отклањању истих у што краћем року.

9.6. Објављивање извештаја ревизије

Извештај ревизије представља интерни документ ITE CA и не објављује се јавно. Намењен је искључиво овлашћеним лицима ITE CA за потребе отклањања евентуално пронађених недостатака.

10.ОСТАЛИ ПОСЛОВИ И ПРАВНА ПИТАЊА

10.1. Накнада за пружање услуга

ITE CA не наплаћује пружање квалификованих услуга које су премет овог документа, односно обавља их без накнаде.

10.2. Одговорност

ITE CA сноси финансијску одговорност за обављање своје делатности у складу са законским прописима.

10.2.1. Осигурање

ITE CA обезбеђује средства за могућу штету насталу вршењем услуга издавања квалификованих сертификата у складу са важећим прописима.

ITE CA може осигурање од ризика одговорности за могућу штету насталу вршењем услуга издавања квалификованих сертификата у складу са важећим прописима уговорити са осигуравајућим друштвом, и то тако да:
- осигурана сума на коју мора бити уговорено осигурање по једном штетном догађају не може износити мање од 20.000 евра у динарској противвредности, подразумевајући при том као штетни догађај појединачну штету насталу употребом једног квалификованог сертификата у једном акту у правном промету;
- укупна осигурана сума на коју мора бити уговорено осигурање од одговорности сертификационог тела кумулативно на годишњем нивоу, по свим штетним догађајима, не може бити нижа од 1.000.000 евра у динарској противвредности.

10.2.2. Други фондови

Није примењено.

10.2.3. Осигурање или гаранција за крајње кориснике

Осигурање или гаранције за крајње кориснике описане су у оквиру тачке 10.2.1.

10.3. Тајност пословних података

10.3.1. Опсег тајних података

Тајни подаци су сви подаци које ITE CA прибави и креира у обављању своје делатности.

Приступ подацима, који се сматрају тајним, може бити одобрен овлашћеним лицима ITE CA и надлежним државним органима, ако су испуњени законом прописани услови.

10.3.2. Подаци који се не сматрају тајним

Подаци који се не сматрају тајним су:
- регистри опозваних сертификата, као и подаци које они садрже,
- Политика и практична правила ITE CA,
- подаци и документа који су објављени на званичној веб презентацији ITE CA,
- документа за која постоји писана сагласност за јавно објављивање.

10.3.3. Одговорност за заштиту тајних података

Овлашћена лица ITE CA и корисници обавезују се:
- да чувају тајност података применом мера које користе за заштиту својих тајних података и да ће их користити само за потребе због којих су били прикупљени или формирани у односу на одредбе документа Политика и практична правила ITE CA,
- да неће неовлашћено откривати тајне податке, без претходног одобрења, које даје корисник или надлежни орган, у писаној форми.

10.4. Заштита података о личности

Пружалац услуге је дужан да се у свом пословању придржава одредби које се односе на заштиту података о личности, у складу са важећим прописима.

У оквиру пружања услуге врши се обрада података о личности у складу са прописима којима се уређује право на заштиту физичких лица у вези са обрадом података о личности, на начин да интегритет и поверљивост тих података не буду угрожени.

Пружалац услуге врши обраду личних података овлашћених лица корисника која подносе захтев за издавање и промену статуса квалификованог сертификата за електронски печат (у даљем тексту: подносиоци захтева), и то: имена, презимена, јединственог матичног броја грађана (ЈМБГ), регистрационог броја идентификационог документа, назива радног места и адресе електронске поште. Подносиоци захтева се у процедури подношења захтева обавештавају и потврђују своју сагласност са обрадом података о личности.

Лични подаци подносилаца захтева се користе искључиво у вези са пружањем услуге, у процедурама идентификације и аутентикације захтева за издавање и промену статуса сертификата.

Пружалац услуге поштује приватност подносилаца захтева. Трећој страни су доступни подаци о подносиоцима захтева само у случајевима када је таква обавеза регулисана законом односно политиком и практичним правилима пружања услуге.

Подносиоцу захтева је омогућено да изврши увид у податке о себи који се чувају у ITE CA, као и да оствари друга права загарантована прописима.

Пружалац услуге не обрађује податке о личности овлашћених службених лица корисника која из информационог система корисника користе квалификовани сертификат за електронски печат корисника.

Руковалац обраде података о личности је пружалац услуге - Канцеларија за информационе технологије и електронску управу, Немањина 11, 11000 Београд, контакт телефон +381 11 7358 400, адреса електронске поште kancelarija@ite.gov.rs.

Адреса електронске поште лица одређеног за заштиту података о личности је lzzpol@ite.gov.rs.

10.5. Права и обавезе

10.5.1. Права и обавезе сертификационог тела

ITE CA гарантује пружање услуге у складу са законом, другим прописима, овим документом и другим актима ITE CA, који су усклађени са важећим прописима Републике Србије.

ITE CA има обавезу да:
- пре успостављања уговорног односа са корисником сертификата, јавно информише корисника сертификата о релевантним условима коришћења сертификата,
- изврши проверу идентитета и овлашћење подносиоца захтева односно овлашћеног лица који учествује у поступку издавања или промене статуса сертификата као и проверу тачности података у захтеву за издавање или промену статуса сертификата,
- подаци садржани у сертификату буду поуздани и тачни,
- са корисником сертификата закључи Уговор и исти чува десет година по престанку важења сертификата,
- изда сертификат у складу са условима дефинисаним законом,
- обезбеди да сертификат садржи све потребне податке, у складу са важећим прописима и захтевима стандарда који су тим прописима прописани да се примењују,
- унесе у сертификат основне податке о свом идентитету и идентитету корисника сертификата, као и јавни криптографски кључ корисника сертификата који је пар његовом приватном криптографском кључу,
- обезбеди видљив податак у сертификату о тачном датуму и времену (сат и минут) издавања сертификата,
- изврши или одбије да изврши захтев за промену статуса сертификата, у складу са условима дефинисаним законом,
- води ажуран, тачан и безбедним мерама заштићен регистар опозваних сертификата који је јавно доступан,
- обезбеди видљив податак у регистру опозваних сертификата о тачном датуму и времену (сат и минут) опозива сертификата,
- обавља делатност у складу са важећим прописима и општим актима ITE CA, којима се уређује пружање услуга издавања сертификата, као и прописима и општим актима којима се уређује заштита података о личности.

10.5.2. Права и обавезе корисника

ITE CA обезбеђује поштовање свих права корисника, односно омогућава остваривање обавеза корисника, које су утврђене прописима која се односе на квалификовани сертификат и овом Политиком и практичним правилима ITE CA.

Корисник је обавезан да:
- омогући пружаоцу услуге да изврши проверу идентитета на начин дефинисан Политиком и практичним правилима ITE CA;
- обавештава ITE CA о промени података садржаних у сертификату, најкасније у року од 24 сата од настанка промене,
- прегледа податке садржане у сертификату и обавештава ITE CA о евентуалним грешкама, после преузимања, а пре коришћења сертификата,
- користи средство за креирање електронских печата које обезбеђује ITE CA,

- употребљава сертификат само за намене одређене у овим практичним правилима,
- у тајности чува ПИН за приступ приватном криптографском кључу и лозинку за повезивање система корисника и апликације еПечат,
- у случају оштећења или злоупотребе техничких средстава (хардвера или софтвера) или приватног криптографског кључа, односно компромитовања или сумње у компромитовање приватног криптографског кључа, без одлагања, поднесе захтев за опозив сертификата,
- испуњава друге обавезе у складу са законом и преузетим уговорним обавезама.

10.5.3. Права и обавезе поуздајућих страна

Поуздајућим странама гарантује се да ITE CA услуге сертификације пружа трећим лицима у складу са законом и другим сродним прописима, овим документом и другим општим актима и интерним правилима рада ITE CA, у складу са важећим прописима.

Обавезе поуздајућих страна, пре него што се поуздају у квалификовани сертификат издат од стране ITE CA су:
- да провере статус квалификованог сертификата,
- да се не поуздају у неважећи сертификат (опозван, суспендован или истекао),
- да се упознају са одговорностима и ограничењима одговорности ITE CA дефинисаним у овом документу и другим актима објављеним на веб презентацији ITE CA.

10.5.4. Права и обавезе других учесника

Сваком учеснику гарантује се да ITE CA услуге сертификације пружа у складу са законом и другим сродним прописима, овим документом и другим општим актима и интерним правилима рада ITE CA.

10.6. Непризнавање права

ITE CA признаје права корисника која су у складу са важећим прописима у Републици Србији.

10.7. Одговорност и ограничења од одговорности

10.7.1. Одговорност и ограничења од одговорности сертификационог тела

ITE CA дужно је да на прописан начин издаје квалификоване сертификате и одговорно је за штету причињену лицу које се поуздало у тај сертификат, у складу са законом, актима сертификационог тела и уговором закљученим између ITE CA и корисника.

ITE CA је дужно да чува доказе о томе да је поступало у складу са важећим прописима.

ITE CA не одговара за штету (директну или индиректну), губитке, трошкове и потраживања која произилазе из или су настала због употребе сертификата, ако је:
- сертификат био употребљен супротно овом документу, као и супротно другим прописима који регулишу ову област,
- сертификат био на било који начин промењен од стране корисника,
- дошло до злоупотребе техничких средстава (хардвера или софтвера) код корисника чија би последица могла да буде злоупотреба приватног кључа,

- дошло до нефункционисања или грешке у функционисању техничких средстава (хардвера или софтвера) корисника или трећег лица, у ком случају, ITE CA није дужно да пружи техничку подршку у отклањању проблема насталог у функционисању техничких средстава ових субјеката.

ITE CA не одговара за штету која настане као последица околности, које су изван контроле ITE CA.

10.7.2. Одговорност и ограничења од одговорности корисника квалификованог сертификата

Корисник сертификата је одговоран за штету која настане у случају коришћења сертификата после истека рока важности сертификата, опозива или суспензије, као и у другим случајевима недозвољеног коришћења сертификата, укључујући и неиспуњења обавеза утврђених у тачки 10.5.2. ових практичних правила.

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

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

10.8. Накнаде

ITE CA не наплаћује накнаду за пружање квалификованих услуга које су премет овог документа, односно обавља их без накнаде.

10.9. Ступање на снагу и престанак важења правних аката

10.9.1. Ступање на снагу правних аката

Правна акта ITE CA објављују се на веб презентацији Канцеларије за информационе технологије и електронску управу пре ступања на снагу и ступају на снагу у року утврђеном у сваком од тих аката, у складу са законом.

Ова Политика и практична правила ITE CA доступна су свим заинтересованим лицима и објављују се на веб презентацији ITE CA.

10.9.2. Престанак важења правних аката

Престанак важења правних аката ITE CA објављује се на веб презентацији Канцеларије за информационе технологије и електронску управу.

10.9.3. Ефекат трајања

ITE CA ће и после престанка важења квалификованог сертификата поштовати тајност личних и других података корисника, као и после престанка важења својих аката.

10.10. Појединачна обавештења и комуникација са корисницима

ITE CA комуницира са корисницима путем електронске поште и веб презентације, осим ако није другачије одређено овим практичним правилима.

10.11. Допуне Политике и практичних правила ITE CA

10.11.1. Поступак за допуну

ITE CA ће имплементирати промене у своје важеће акте у случају промене регулативе и процедура рада.

Измене и допуне Политике и практичних правила ITE CA, које се односе на рад ITE CA и издавање квалификованих сертификата, по правилу се усвајају тридесет дана пре почетка важења. Измене и допуне Политике и практичних правила ITE CA, које по процени ITE CA не утичу битно на кориснике усвајају се седам дана пре почетка важења.

10.11.2. Механизам и период обавештавања

О изменама и допунама Политике и практичних правила ITE CA и осталих докумената везаних за тај документ, ITE CA обавештава надлежни орган и исте објављује на веб презентацији ITE CA.

10.11.3. Околности под којима *OID* мора да се промени

Промена *OID*-а ће се извршити уколико управна структура највишег нивоа ITE CA одлучи да направи промене у Политици и практичним правилима ITE CA, а наведене промене буду захтевале промену *OID*-а.

10.12. Спорови између сертификационог тела и корисника

Уколико дође до спора између ITE CA и корисника квалификованог сертификата, у вези међусобних права и обавеза и тумачења уговора и овог документа, ITE CA ће настојати да спор реши мирним путем, споразумно, а уколико до споразума не дође, спор ће решавати надлежни суд у Београду.

Сви спорови између ITE CA, корисника и трећег лица биће решавани договором, а у случајевима када то није могуће, спор ће решавати надлежни суд у Београду.

10.13. Меродавно право

За тумачење и примену ових практичних правила меродавно је право Републике Србије.

10.14. Усклађеност са важећим законодавством

Правна акта ITE CA донета су у складу са законом и другим прописима Републике Србије, који регулишу ову област.

10.15. Остале одредбе

10.15.1. Уговор са корисницима

Пружање услуга регулише се посебним уговором између ITE CA и корисника, у складу са законом и другим прописима.

10.15.2. Преношење права

Корисник квалификованог сертификата нема право да права из закљученог уговора са ITE CA, у целини или делимично, пренесе на трећа лица.

ITE CA има право да уговор закључен са корисником, односно права и обавезе из тог уговора, у потпуности или делимично, без сагласности корисника, пренесе на друго регистровано сертификационо тело у Републици Србији или надлежни орган.

10.15.3. Измена или неважење одредби овог документа

Измене или допуне појединих одредби овог документа или аката донетих на основу овог документа не утичу на важење осталих одредби из овог акта.

10.15.4. Применљивост за адвокатске накнаде и одрицање од права

Није применљиво.

10.15.5. Виша сила

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

10.16. Друге одредбе

10.16.1. Доступност услуге особама са инвалидитетом

Где је то могуће, ITE CA омогућава да услуге сертификације и производи за крајњег корисника који се користе при пружању тих услуга буду доступни особама с инвалидитетом.

10.16.2. Језик

Ова практична правила и друга акта ITE CA доносе се и објављују се на српском језику.

10.16.3. Ступање на снагу

Ова практична правила, након оцене испуњености услова за пружање квалификованих услуга од поверења, ступају на снагу осмог дана од дана објављивања на веб презентацији ITE CA на адреси https://cloud.eid.gov.rs/ca/.

в.д. ДИРЕКТОРА

Милан Латиновић