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

(Certification Policy and Practice Statement - CPPS)

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	7. јул 2021.	Иницијална верзија

Садржај

1. УВОД

Канцеларија за информационе технологије и електронску управу (у даљем тексту: ITE CA) изградила је инфраструктуру јавних криптографских кључева (*Public Key Infrastructure - PKI*) и у улози сертификационог тела уписана је у Регистар пружалаца квалификованих услуга од поверења за услугу управљања квалификованим средством за креирање електронског потписа на даљину (у даљем тексту: потпис у клауду), као и у Регистар пружалаца услуге електронске идентификације и шема електронске идентификације.

ITE CA издаје две врсте електронских сертификата:

1) квалификоване електронске сертификате за квалификовани електронски потпис на даљину
2) електронски сертификат за аутентикацију, смештен у мобилној апликацији, који обезбеђује представљање корисника у складу са захтевима шеме високог нивоа поузданости електронске идентификације и који се користи за одобрење квалификованог електронског потписивања на даљину.

Потпис у клауду подразумева да корисник не мора да поседује материјално средство у ком се налази приватни кључ повезан са сертификатом корисника, већ свој приватни кључ активира на даљину користећи свој мобилни уређај (паметан телефон или таблет). Наведено унапређује мобилност, будући да се корисник аутентикује са два фактора и ауторизује употребу квалификованог средства за креирање електронског потписа на даљину, тако да није везан за рачунар и потписивање може да обави у време и на месту које му одговара. Такође, омогућена је једноставнија и повољнија употреба електронског потписа, будући да се не захтева да корисник поседује хардверски крипто уређај нити инсталацију одговарајућих софтвера, и може се користити независно од оперативног система и интернет претраживача.

Осим што омогућавају креирање квалификованих електронских потписа, техничке карактеристике и систем издавања квалификованих електронских сертификата ITE CA (у даљем тексту: ITE CA QES), обезбеђују испуњеност свих услова за шему електронске идентификације високог нивоа поузданости, у складу са прописима.

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 чине правни оквир за обављање делатности пружања услуга електронске идентификације и услуге од поверења ITE CA.

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

ITE CA пружање услуга обавља 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.

1.1. Основне претпоставке

ITE CA користи у својој инфраструктури за издавање квалификованих сертификата хијерархију више *CA* (*Certification Authority*) сервера. Инфраструктуру ITE CA чине три сертификациона тела:
- „*EID RS CA Root* ", као *Root* сертификационо тело,
- „*EID RS Person Qualified*", као подређено (*subordinate*) сертификационо тело.
- „EID RS Person Non-Qualified", 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 Person Qualified*" као подређено (*subordinate*) сертификационо тело издаје квалификоване сертификате за удаљени серверски електронски потпис физичким лицима.. За потребе администрирања „*EID RS CA Root*" и „*EID RS Person Qualified*" сервера, „*EID RS Person Qualified*" издаје сертификате у складу са поверљивом улогом коју запослени обавља.

„EID RS Person Non-Qualified", као подређено (*subordinate*) сертификационо тело издаје сертификате за електронски потпис физичким лицима који се користе као ауторизациони електронски сертификати у мобилним уређајима којима се електронски потписује потврда односно одобрење за обављање удаљеног серверског квалификованог електронског потписивања.

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 потписа.

Корисници квалификованих сертификата ITE CA поседују два пара криптографских кључева (јавни и приватни кључ). Први пар криптографских кључева се користи за удаљено серверско електронско потписивање и валидацију електронског потписа и то тако да се приватни криптографски кључ користи за квалификовано електронско потписивање, а јавни криптографски кључ се користи за валидацију квалификованог електронског потписа. Други пар криптографских кључева се користи за електронско потписивање сагласности, односно ауторизацију удаљеног серверског електронског потписивања при чему се приватни криптографски кључ користи за електронско потписивање, а јавни криптографски кључ се користи за валидацију електронског потписа.

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 три сертификациона тела (*Certification Authority - CA*):
- *EID RS CA Root*, као *Root* сертификационо тело,
- *EID RS Person Qualified*, као подређено сертификационо тело.
- EID RS Person Non-Qualified, као подређено сертификационо тело.

1.3.2. Регистрациона тела

Регистрациона тела за сертификационо тело обављају проверу идентитета корисника и издавање параметара за активацију електронског сертификата за аутентикацију.

1.3.3. Корисници

Корисници услуга од поверења и услуге електронске идентификације у смислу овог документа (у даљем тексту: корисници), могу бити физичка лица која имају налог на Порталу за електронску идентификацију који је доступан на адреси https://eid.gov.rs/. Корисници су физичка лица која, осим што имају налог на Порталу за електронску идентификацију, уговарају коришћење услуга од поверења са ITE CA.

Корисници ITE CA су физичка лица која услугу могу користити као физичка лица односно као физичка лица у улози овлашћених лица.

1.3.4. Поуздајуће стране

Поуздајуће стране, односно трећа лица су физичка лица (појединци) и/или правна лица која прихватају сертификате и верификују електронски потпис 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 или сервиса за проверу опозваности

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* или *OCSP*) 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 потписивање и
- аутентикацију корисника.

Приватни криптографски кључеви који су придружени квалификованим сертификатима користе се у процесу квалификованог електронског потписивања 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 поступку пред државним органом, ако је законом којим се утврђује тај поступак, прописана употреба квалификованог електронског потписа.

Квалификовани сертификати потврђују везу између јавног криптографског кључа корисника и идентитета корисника који је извршио квалификовано електронско потписивање 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 потпис 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 Владе Републике Србије
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 примене Политика и практична 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 ових практичних правила са евентуалним променама насталим у пракси издавања квалификованих сертификата.

Такође, управна структура ITE CA редовно процењује усклађеност ових практичних правила 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 пословна функција надлежна за информационе технологије, електронске комуникације и развој, а правно - техничку редакцију врши пословна функција надлежна за правне послове. Директор Канцеларије доноси измене и/или допуне тог акта, уз претходну верификацију директора две поменуте пословне функције, 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** - документ у електронском облику који се користи у пословним и другим радњама;
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** - физичко лице које користи квалификовани сертификат издат од стране ITE CA и чији се подаци налазе у сертификату;
6) **квалификовани електронски потпис** - електронски потпис којим се поуздано гарантује идентитет потписника, 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 потписа** - подаци за креирање електронског потписа су јединствени подаци које користи потписник за креирање електронског потписа и који су логички повезани са одговарајућим подацима за валидацију електронског потписа;
9) **подаци за валидацију квалификованог електронског потписа** - подаци за валидацију електронског потписа су подаци на основу којих се проверава да ли електронски потпис одговара подацима који су потписани;
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 потписа** - средство за креирање електронског потписа је техничко средство (софтвер односно хардвер) које се користи за креирање електронског потписа уз коришћење података за креирање електронског потписа;
14) **средства за валидацију квалификованог потписа** - одговарајућа техничка средства (софтвер и хардвер) која служе за валидацију квалификованог потписа, уз коришћење података за валидацију електронског потписа;
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 Creation Device)	Квалификовано средство за креирање електронских потписа (HSM, смарт картица, *USB* смарт токен,...)
X.509	Стандард за електронске сертификате, описан у документу *RFC* 5280
LDAP (Lightweight Directory Access Protocol)	Протокол за приступ јавном директоријуму
UTC (Coordinated Universal Time)	Координисано универзално време
ETSI (European Telecommunications Standards Institute)	Европски институт за стандарде из области телекомуникација
IPS (Intrusion Prevention System)	Систем за превенцију упада
NTP (Network Time Protocol)	Протокол мрежног времена
SAM (Signature Activation Module)	Специјализовани уређај за обављање удаљеног електронског потписивања који омогућава механизам за поуздану ауторизацију активације потписа и обезбеђује да само власник криптографског кључа може да одобри употребу свог кључа.
SAD (Signature Activation Data)	Порука која садржи информације о потписнику, кључу за потписивање и подацима за потписивање
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:
- Политика и практична правила ITE CA, као документ који садржи и опште услове пружања услуга,
- корисничка упутства,
- сертификате *CA* сервера са придруженим *hash* вредностима,
- регистар опозваних сертификата,
- законску регулативу из подручја пружања услуга од поверења и електронске идентификације,
- друга акта и обавештења.

У делу који је доступан преко https протокола објављују се регистри опозваних сертификата.

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, као и приликом сваке промене у статусу сертификата која утиче на промену регистра
- све остале податке и документе објављује после евентуалних измена које су усвојене и одобрене од стране надлежних органа ITE CA или надлежног државног 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* (Табела 2. и Табела 3.) и име корисника сертификата, поље *Subject* (Табела 4, Табела 5. и Табела 6.), 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 Person Qualified*“ у квалификованим сертификатима

Име *CA* сервера (CN) =	*EID RS Sign*
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 подређеног сертификационог тела „*EID RS Person Non-Qualified*“ у електронским сертификатима

Име *CA* сервера (CN) =	*EID RS Usr*
Организација (O) =	Kancelarija za informacione tehnologije i elektronsku upravu
Идентификатор организације	VATRS-110177886

(OI) =	
Место (L) =	*Beograd*
Ознака државе (C) =	*RS*

Табела 5. Структура имена корисника квалификованог сертификата за електронски потпис

Јединствено име (CN) =	*Ime prezime JIK* (Име и презиме корисника ћириличним или латиничним писмом са додатком јединственог идентификатора корисника (ЈИК)).
Име (G) =	*Ime* (може да буде ћириличним или латиничним писмом)
Презиме (SN) =	*Prezime* (може да буде ћириличним или латиничним писмом)
Серијски број (SERIALNUMBER) =	*PNORS-JMBG* (Јединствени матични број (ЈМБГ) физичког лица).
Серијски број (SERIALNUMBER) =	*CA:RS-JIK* (Јединствени идентификатор корисника).
Ознака државе (C) =	*RS*

Табела 6. Структура имена корисника електронског сертификата за ауторизацију

Јединствено име (CN) =	*Ime prezime JIK* (Име и презиме корисника ћириличним или латиничним писмом са додатком јединственог идентификатора корисника (ЈИК)).
Име (G) =	*Ime* (може да буде ћириличним или латиничним писмом)
Презиме (SN) =	*Prezime* (може да буде ћириличним или латиничним писмом)
Серијски број (SERIALNUMBER) =	*PNORS-JMBG* (Јединствени матични број (ЈМБГ) физичког лица).
Серијски број (SERIALNUMBER) =	*CA:RS-JIK* (Јединствени идентификатор корисника).
Ознака државе (C) =	*RS*

3.1.2. Смисленост имена

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

У поље *Subject* квалификованог сертификата уписују се подаци о физичком лицу онако како су наведени у електронском идентификационом систему eid.gov.rs..

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.

ITE CA одбија било који захтев за анонимношћу.

3.1.4. Правила за тумачење различитих врста имена

У квалификованим сертификатима су имена корисника верно представљена латиничним и ћириличким словима српског језика.

Коришћење специјалних знакова у именима корисника није дозвољено. Исте је потребно изоставити или заменити другим знацима.

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 идентитета се обавља на Порталу еИД (https://eid.gov.rs), на основу аутентикације средством електронске идентификације које је издато у оквиру шеме електронске идентификације високог нивоа поузданости, односно квалификованим сертификатом за електронски потпис чији је издавалац уписан у Регистар пружалаца квалификованих услуга од поверења за услугу издавања квалификованих сертификата за електронски потпис .

3.2.1. Метод доказивања поседа приватног кључа

Приватни криптографски кључ корисника генерише се у ITE CA на квалификованом средству за креирање електронских потписа.

3.2.2. Аутентикација идентитета правног лица

Није применљиво.

3.2.3. Аутентикација идентитета физичког лица

Квалификовани сертификат за електронски потпис може се издати само физичком лицу. Физичко лице има право да у име правног лица користи квалификовани сертификат за електронски потпис, уколико га правно лице за то овласти.

Аутентикација корисника се обавља на Порталу еИД (https://eid.gov.rs) средством електронске идентификације које је издато у оквиру шеме електронске идентификације

високог нивоа поузданости, односно квалификованим сертификатом за електронски потпис чији је издавалац уписан у Регистар пружалаца квалификованих услуга од поверења за услугу издавања квалификованих сертификата за електронски потпис.

3.2.4. Непроверени подаци о кориснику

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

3.2.5. Провера тачности података правног лица

Није применљиво.

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.

3.3.2. Идентификација и аутентикација захтева за заменом кључа после опозива

ITE CA не дозвољава замену кључа после опозива.

3.4. Идентификација и аутентикација захтева за опозивом

Корисник захтева опозив квалификованог сертификата по једној од следећих процедура:

- корисник се лично идентификује и предаје својеручно потписан захтев на једној од локација које је за ту намену одредило ITE CA. Списак локација доступан је на веб презентацији ITE CA,
- корисник шаље попуњен образац захтева за промену статуса потписан важећим квалификованим сертификатом издатим од стране сертификационог тела уписаног у Регистар пружалаца квалификованих услуга од поверења путем електронске поште ITE CA, на унапред одређену адресу електронске поште, или,
- корисник аутентикован средством средњег или високог нивоа поузданости на Порталу за електронску идентификацију (Портал еИД), самостално може опозвати ITE CA QES.

4. ОПЕРАТИВНИ ЗАХТЕВИ У ПРОЦЕСУ ИЗДАВАЊА СЕРТИФИКАТА

4.1. Подношење захтева за издавање сертификата

Подношење захтева за издавање сертификата се обавља у два корака. Први корак је издавање аутентикационог сертификата који ће се користити у мобилној апликацији за одобравање квалификованог електронског потписа на даљину. Други корак је издавање квалификованог електронског сертификата за потпис на даљину.

Издавање електронског сертификата за аутентикацију преко мобилне апликације је описано у документу „Практична правила пружања услуге електронске идентификације и шеме електронске идентификације „Шема електронске идентификације високог нивоа поузданости – еУправа“ („Шема еУправа“)“ који је објављен на страници https://cloud.eid.gov.rs/ca/. Исти електронски сертификат који се смешта у мобилни уређај корисника се користи за аутентикацију високим нивоом поузданости и за одобрење квалификованог електронског потписа на даљину.

Издавање квалификованог електронског сертификата за потпис на даљину се обавља искључиво електронским путем, преко интернет странице од стране самог корисника. Корисник мора да буде пријављен преко Портала за електронску идентификацију средством издатим у оквиру регистроване шеме електронске идентификације високог нивоа поузданости или квалификованим сертификатом за електронски потпис чији је издавалац уписан у Регистар пружалаца квалификованих услуга од поверења. Неопходан услов да корисник може себи да изда квалификовани сертификат за електронски потпис на даљину је да има активиран електронски сертификат за аутентикацију у свом мобилном уређају.

Издавање квалификованог електронског сертификата за потпис на даљину се врши тако што корисник пријављен преко Портала за електронску идентификацију средством издатим у оквиру регистроване шеме електронске идентификације високог нивоа поузданости или квалификованим сертификатом за електронски потпис чији је издавалац уписан у Регистар пружалаца квалификованих услуга од поверења кликне на дугме за издавање квалификованог сертификата за електронски потпис на даљину. Том приликом се генерише уговор и приказује се на страници у прозору који не може да се уклони осим ако корисник не прихвати или не одустане од прихватања уговора. Приказани прозор садржи следеће елементе:

- комплетан текст уговорних обавеза,
- линк преко којег корисник може на свој уређај да преузме текст уговора и да се пре издавања сертификата за електронски потпис на даљину детаљно упозна са условима за коришћење услуге,
- дугме „Прихватам“,
- дугме „Одустајем“.

Ако корисник кликне на дугме „Прихватам“ и тиме прихвати уговор за вршење услуга електронског потписивања на даљину, сматра се да је исказао своју вољу и дао пристанак на услове под којима се пружа услуга, односно да је извршио потписивање уговора за коришћење услуга од поверења. Тада се врши процес издавања квалификованог електронског сертификата за потпис на даљину и обавештава се корисник о исходу. Ако је сертификат успешно издат, кориснику се на адресу електронске поште која је регистрована преко Портала за електронску идентификацију шаље уговор и упутство за коришћење.

4.1.1. Ко може да поднесе захтев за издавање сертификата

Захтев може да поднесе физичко лице које испуњава услове наведене у овом документу.

4.1.2. Услови за издавање сертификата

За издавање квалификованог сертификата за електронски потпис на даљину корисник је дужан да:
- испуни захтеве за идентификацију,
- сагласи се са условима пружања услуге од поверења односно потпише уговор.

Уговор о пружању услуга ITE CA садржи услове издавања и коришћења сертификата.

Коришћење сертификата за електронски потпис на даљину 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 потписа.

Коришћење сертификата за ауторизацију квалификованог електронског потписивања је ограничено на три године и везује се за датум издавања сертификата. Под датумом издавања сертификата сматра се датум када је он креиран у ITE CA и уписан у клијентски уређај за ауторизацију.

4.2. Обрада захтева за издавање сертификата

4.2.1. Обављање функција идентификације и потврђивања аутентичности

ITE CA идентификује корисника на основу аутентикације на Порталу еИД средством електронске идентификације које је издато у оквиру регистроване шеме високог нивоа поузданости или квалификованим сертификатом за електронски потпис чији је издавалац уписан у Регистар пружалаца квалификованих услуга од поверења.

4.2.2. Одобрење или одбијање захтева за издавање сертификата

Није применљиво.

4.2.3. Време обраде захтева за издавање сертификата

Није применљиво.

4.3. Издавање сертификата

4.3.1. Активности током издавања сертификата

Активности током издавања електронског сертификата за аутентикацију преко мобилне апликације су описане у документу „Практична правила пружања услуге електронске идентификације и шеме електронске идентификације „Шема електронске идентификације високог нивоа поузданости – еУправа“ („Шема еУправа“)“ који је објављен на страници https://cloud.eid.gov.rs/ca/. Исти електронски сертификат који се

смешта у мобилни уређај корисника се користи за аутентикацију високим нивоом поузданости и за одобрење квалификованог електронског потписа на даљину.

Током издавања електронског сертификата за аутентикацију се у мобилном уређају корисника генерише асиметрични криптографски пар кључева (приватни и јавни кључ). Од јавног кључа и атрибута корисника са Портала за електронску идентификацију креира се захтев за издавање сертификата који се прослеђује EID RS Person Non-Qualified CA телу ради издавања електронског сертификата за аутентикацију. На основу захтева се генерише електронски сертификат који се у заштићеном криптографском модулу (HSM уређају) електронски потписује приватним кључем EID RS Person Non-Qualified CA тела. Тако генерисан и електронски потписан сертификат се смешта на мобилни уређај корисника.

Да би корисник могао себи да изда квалификовани електронски сертификат за потпис на даљину, мора да се прво пријави преко Портала за електронску идентификацију средством издатим у оквиру регистроване шеме електронске идентификације високог нивоа поузданости или квалификованим сертификатом за електронски потпис чији је издавалац уписан у Регистар пружалаца квалификованих услуга од поверења. Корисник затим бира опцију за издавање квалификованог сертификата за електронски потпис на даљину. Том приликом се генерише уговор и приказује се на страници у прозору који не може да се уклони осим ако корисник не прихвати или не одустане од прихватања уговора.

Ако корисник прихвати услове за издавање, тада отпочиње процес издавања квалификованог електронског сертификата за потпис на даљину. Процес подразумева генерисање асиметричног пара криптографских кључева (приватног и јавног) у заштићеном криптографском модулу (SAM уређај), генерисање захтева за издавање сертификата на основу јавног кључа и корисникових атрибута са Портала за електронску идентификацију, слање захтева за издавање квалификовано електронског сертификата EID RS Person Qualified CA телу. CA тело генерише електронски сертификат на основу захтева и у заштићеном криптографском модулу (HSM уређају) електронски га потписује својим приватним кључем. Тако генерисан и електронски потписан сертификат се смешта у SAM уређај и даље може да се користи за квалификовано електронско потписивање на даљину.

Након успешног издавања квалификованог електронског сертификата за потписивање на даљину корисник добија обавештење на веб страници и путем електронске поште када се шаље информација о издатом квалификованом електронском сертификату за потпис на даљину, уговор за пружање услуге и упутство за коришћење.

4.3.2. Обавештавање корисника о издавању сертификата

ITE CA корисника обавештава о издавању сертификата преко веб странице на којој је упутио захтев за издавање сертификата, као и електронском поштом.

4.4. Преузимање сертификата

4.4.1. Поступак преузимања сертификата

Оба електронска сертификата којима корисник располаже се преузимају у електронској процедури, односно смештају се на одговарајуће уређаје и тиме се сматрају преузетим од стране корисника. Електронски сертификати се не преузимају физички.

Електронски сертификат за аутентикацију и ауторизацију квалификованог електронског потписа на даљину се смешта у мобилни уређај корисника, а квалификовани сертификат за електронски потпис на даљину се смешта у заштићени криптографски модул (SAM уређај) и њим корисник располаже на даљину.

4.4.1.1. Активација сертификата за аутентикацију

Активација сертификата за аутентикацију се обавља у процедури активације апликације ConsentID и ближе је описана у документу „Практична правила пружања услуге електронске идентификације и шеме електронске идентификације „Шема електронске идентификације високог нивоа поузданости – еУправа“ („Шема еУправа“)“ који је објављен на страници https://cloud.eid.gov.rs/ca/.
ConsentID апликација се може преузети из продавница Apple Store односно Play Store, и у њу се уносе параметри („ИД корисника“ и „Регистрациони код“). Ове параметре издају регистрациона тела или се преузимају на Порталу еИД на основу пријаве средством електронске идентификације издатим у оквиру шеме високог нивоа поузданости или квалификованим сертификатом за електронски потпис. Параметри су јединствени за сваког корисника, не садрже личне податке корисника, а регистрациони код је различит код сваког издавања параметара у таквом облику да се не може наслутити.
Након уноса параметара, од корисника се тражи унос личног идентификационог броја (PIN) по избору и потврда избора PIN-а узастопним уносом. Унос одабраног PIN-а ће бити неопходан при сваком наредном приступу апликацији ConsentID.
Када корисник одабере свој PIN, отпочиње поступак генерисања електронског сертификата за аутентикацију и након завршене процедуре сертификат се сматра активним и може се користити за сврху за коју је намењен.

4.4.1.2. Активација сертификата за електронски потпис на даљину

Квалификовани сертификат за електронски потпис на даљину се активира аутоматски одмах након издавања, а првом употребом од стране корисника, сертификат се сматра прихваћеним.
Уколико се накнадно утврди да у квалификованом сертификату постоје погрешни подаци, корисник је дужан да се обрати ITE CA, ради издавања новог квалификованог сертификата.

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 удаљеног серверског квалификованог електронског потписа, а квалификовани сертификат за валидацију квалификованог потписа.

Приватни криптографски кључ који се налази у мобилном уређају се користи за аутентикацију, односно за електронско потписивање трансакције одобрења удаљеног серверског квалификованог потписивања. Ауторизациони сертификат се користи за валидацију електронског потписа одобрења за квалификовано потписивање.

4.5.2. Коришћење јавног кључа и сертификата од стране трећег лица

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

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 потпис 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 захтева опозив квалификованог сертификата по једној од следећих процедура:

- корисник се лично идентификује и предаје својеручно потписан захтев на једној од локација које је за ту намену одредило ITE CA. Списак локација доступан је на веб презентацији ITE CA, или,
- корисник шаље попуњен образац захтева за промену статуса потписан важећим квалификованим сертификатом издатим од стране сертификационог тела уписаног у Регистар пружалаца квалификованих услуга од поверења путем електронске поште ITE CA, на унапред одређену адресу електронске поште,
- корисник аутентикован средством средњег или високог нивоа поузданости на Порталу за електронску идентификацију (Портал еИД), самостално може опозвати ITE CA QES.

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.

4.9.7. Учесталост објављивања регистра опозваних сертификата

Регистар опозваних сертификата подређеног (*subordinate*) сертификационог тела редовно се објављује на свака 24 сата, као и ванредно приликом сваке промене у регистру.

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

Регистар опозваних сертификата је расположив на веб страни ITE CA.

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 применљиво.

4.9.14. Ко може да захтева суспензију и прекид суспензије сертификата

Није применљиво.

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 стално доступан.

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

ITE CA не чува приватне кључеве корисника и не може да их открије нити обнови.

4.12.2. Политика енкапсулације кључа сесије и обнове

Не врши се.

5. УСЛУГА УПРАВЉАЊА СРЕДСТВОМ ЗА КРЕИРАЊЕ ЕЛЕКТРОНСКОГ ПОТПИСА НА ДАЉИНУ

Систем за издавање електронских сертификата ITE CA и извршавање удаљеног серверског електронског потписивања се састоји од следећих компоненти:

- QSCD – Qualified Signature Creation Device је криптографски модул који има функционалности за ауторизацију употребе тајних кључева према eIDAS стандарду и користи се као хардверско-софтверски уређај за удаљено квалификовано електронско потписивање. Испуњава процедуралне и безбедносне захтеве дефинисане у различитим ETSI техничким стандардима (ETSI EN 319 401, EN 319 411, EN 319 421). Хардверски процесор је сертификован према Common Criteria стандарду у складу са eIDAS Protection Profile (PP) EN 419 221-5. QSCD се састоји од два модула:
    - SAM – Signature Activation Module који пружа механизам за поуздану ауторизацију по CEN протоколу активације потписа (Signature Activation Protocol – SAP) и обезбеђује да само власник криптографског кључа може да одобри употребу свог кључа у уређају за извођење квалификованог

удаљеног потписа (Qualified Remote Signature). Уређај поседује потврду/сертификат Common Criteria EAL4+ о испуњавању захтева за заштитни профил (Protection Profile – PP) eIDAS ETSI EN 419 241-2 Level 2 Sole Control (QSCD for Remote Signing) и испуњава захтеве по стандарду ETSI EN 419 241-1, FIPS 140-2 Level 3. Уређај има подршку за креирање електронског потписа и проверу потписа за потписе PDF, XML DSig, PKCS#7/CMS, ETSI XAdES и CAdES.

  - HSM – Hardware Security Module је хардверски модул који омогућава криптографске операције генерисања пара криптографских кључева и квалификованог електронског потписивања. Поседује сертификат Common Criteria за уграђени о испуњавању захтева за заштитни профил PP eIDAS EN 419 221-5.

- Софтвер ЦА 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 http или https протокола.
- HSM – Hardware Security Module је посебан хардверски уређај који се користи за издавање електронских сертификата тако што чува, штити и користи криптографске кључеве ЦА тела за потписивање свих захтева за издавање сертификата. Поседује FIPS 140-2 Level 3 и Common Criteria (PP 419 221-5) сертификацију, као и eIDAS усклађеност за QSCD уређаје.
- Систем за управљање издавањем сертификата омогућава управљање свим фазама процеса издавања и управљања електронским сертификатима након издавања. Систем је сертификован као систем од поверења према CWA 14167-1:2003, CEN/TS 419261:2015 и ANSSI CSPN.
- Систем за ауторизацију електронског потписивања омогућава поуздано утврђивање идентитета корисника који обавља процес електронског потписивања. Систем је заснован на употреби корисничких ауторизационих електронских сертификата који се налазе у мобилном уређају корисника и могу да се користе посредством мобилне апликације за ауторизацију која електронски потписује захтеве за ауторизацију. Систем се састоји од:
  - серверске компоненте која управља слањем и обрадом захтева за ауторизацију и
  - клијентске мобилне апликације заштићене корисничким ПИН бројем којом корисник мануелно одобрава или одбија захтев за удаљеним серверским електронским потписивањем.

Издавање електронских сертификата за употребу је описано у 4.3. овог документа.
Услуга удаљеног серверског квалификованог електронског потписивања се обавља на следећи начин:

1) корисник се преко еИД система пријављује на корисничку апликацију из које је омогућено удаљено серверско потписивање;
2) корисничка апликација шаље идентификациони број пријављеног корисника заједно са електронским документом који треба да се потпише сервису за удаљено серверско потписивање;
3) сервис за удаљено серверско потписивање прима, обрађује и смешта документ и враћа корисничкој апликацији јединствени идентификатор документа као резултат пријема документа за потписивање;

4) као засебан корак у процесу удаљеног електронског потписивања, корисничка апликација шаље захтева за електронско потписивање документа са идентификатором из тачке 3);
5) сервис за удаљено серверско потписивање шаље захтев SAM уређају да генерише SAD (Signature Activation Data) поруку за захтев за потписивање;
6) SAM враћа сервису за удаљено серверско потписивање непотписану SAD поруку;
7) сервис за удаљено серверско потписивање прослеђује SAD поруку мобилном уређају корисника;
8) корисник путем мобилне апликације електронски потписује SAD коришћењем ауторизационог кључа који се налази заштићен на његовом мобилном уређају.
9) електронски потписана SAD порука се враћа сервису за удаљено серверско потписивање;
10) сервис за удаљено серверско потписивање прослеђује потписану SAD поруку SAM уређају који врши валидацију поруке и потписа.
11) SAM уређај прослеђује захтев HSM уређају који се налази у оквиру QSCD да потпише документ;
12) HSM уређај враћа потписан документ SAM уређају који га враћа сервису за удаљено серверско потписивање;
13) сервис за удаљено серверско потписивање саставља коначни документ са електронским потписом и временом потписивања;
14) корисничка апликација може да новим позивом ка сервису за удаљено серверско потписивање преузме електронски потписан документ.

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, 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 електронски се бележи и уноси у електронски 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,
- смешта картице *HSM* администратора и оператера и друге медије који садрже криптографске кључеве у безбедну касу-контејнер, за чије отварање је потребан пар кључева и шифра,
- смешта резервне копије приватног кључа у безбедну касу-контејнер,
- 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 у оквиру локалног регистрационог тела, 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, смештају се у ватроотпорне безбедне касе-контејнере, од којих се једна налази на централној локацији ITE CA, а друга на удаљеној, безбедној локацији.

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, пре него што се медији пошаљу на одељење где се уништавају.

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 касу-контејнер. Просторију у којој је смештена ватроотпорна безбедна каса-контејнер на поменутој удаљеној локацији надзиру овлашћена лица организационог дела ITE CA надлежног за безбедност и заштиту.

6.2. Контрола процедура

6.2.1. Поверљиве улоге овлашћених лица

Апликација сертификационог тела и апликација централног 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 централног 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 потписа 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 безбедним касама-контејнерима.

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* смарт картица.

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

Заједничко коришћење налога или сертификата 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, обављају запослени који су у радном односу.

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.

Запосленима у ITE CA не додељују се 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, централног 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, преузимање, опозив, суспензија, прекид суспензије и други,
- 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.

Електронски дневници апликације сертификационог тела су шифровани тако да могу да их 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 7.

Табела 7. 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 и централног

		регистрационог тела
Догађаји повезани са апликацијом сертификационог и централног регистрационог тела	аутоматско	апликација сертификационог и централног регистрационог тела
Догађаји на апликацији локалног регистрационог тела	аутоматско	апликација локалног регистрационог тела
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 касама-контејнерима за чије отварање су потребна два кључа и шифра. Касе-контејнери се налазе у заштићеним просторијама на централној и удаљеној локацији. Просторије су са рестриктивним и ауторизованим приступом.

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* алгоритам 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 потписа (*Qualified Signature Creation Device - QSCD*).

7.1.2. Уручење приватног криптографског кључа кориснику

Након потписивања уговора, у квалификованом средству за креирање електронског потписа се генерише пар тајног и јавног кључа и ITE CA издаје квалификовани сертификат за електронски потпис на даљину.

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 потписа.

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 потписа. 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 потписа и обезбеђивање непорецивости, како је дато у Табели 8.

Табела 8. 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)

Табела 9. Садржај поља *Key Usage* у ауторизационим сертификатима које издаје ITE CA

Врста сертификата	**Садржај поља *Key Usage***
Ауторизациони сертификат	*Digital Signature, Non-Repudiation, Key encipherment* (електронски потпис, непорецивост, шифровање кључа)

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 потписа 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 две администраторске и оператерске *HSM* смарт картице 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 у касама-контејнерима за дуготрајно чување.

HSM уређај који је намењен за чување резервних копија кључева се под двоструком контролом овлашћених особа смешта у сеф, а приступ сефу је могућ само уз двоструку

контролу кроз укуцавање лозинки/ ПИН-ова сваке од овлашћених особа или њихових именованих заменика.

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 потписа 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 картицама 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 потписивања.

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.

Коришћење корисничког приватног кључа је могуће једино уз активацију ауторизационог кључа кроз мобилну апликацију, стога деактивација корисничког квалификованог корисничког приватног кључа може да се изврши уклањањем или деактивацијом мобилне апликације за ауторизацију употребе приватног кључа. Деактивирање свих корисничких кључева се обавља искључењем сервера на ком се

налази апликација за управљање употребом корисничких криптографских кључева или искључењем SAM уређаја.

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.

Приватни криптографски кључ корисника се уништава уколико га корисник посредством корисничке апликације обрише са квалификованог средства за креирање електронског потписа (SAM уређаја).

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.
- Ауторизациони сертификати корисника: 3 године.

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.

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.

Лозинку за активирање приватног кључа корисника генерише генератор лозинке, после чега се она доставља кориснику одвојено од квалификованог средства за креирање електронског потписа.

Лозинка има четири или више нумеричких карактера.

Корисник има могућност промене лозинке и њене дужине.

7.4.2. Заштита података за активирање

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

Корисници су дужни да чувају лозинке за приступ приватним криптографским кључевима који се налазе на квалификованом средству за креирање електронског потписа.

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 смарт картица 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. ITE CA омогућава издавање сертификата за потребе тестирања. Сертификати за потребе тестирања су јасно означени.

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 сегемнтима.

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 9.) и екстензије *X*.509 сертификата (Табеле 10. и 11.).

Табела 9. 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 10.

Табела 10. 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 *Subject Public Key Info* 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 може да се наведе адреса електронске поште корисника сертификата, ако је адреса електронске поште 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*

Private Key Usage Period	Рок важности приватног криптографског кључа корисника, који је пар јавном криптографском кључу из квалификованог електронског сертификата.
Extended Key Usage	Додатна намена јавног криптографског кључа корисника квалификованог сертификата.

8.1.3. Идентификациона ознака алгоритма

ITE CA потписује квалификоване сертификате и регистре опозваних сертификата, 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. Исте је потребно изоставити или заменити другим знацима.

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 12.

Табела 12. Ознаке политике сертификације

Врста сертификата	**Ознака политике (*OID*)**
Квалификовани сертификат за удаљени серверски електронски потпис	0.4.0.194112.1.2, 1.3.6.1.4.1.55016.2.1.0
Аутентикациони сертификат за одобрење електронског потписа	0.4.0.2042.1.1, 1.3.6.1.4.1.55016.2.1.0

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 13.) и екстензије *X*.509 регистра (Табела 14.).

Табела 13. Основна поља *X*.509 регистра опозваних сертификата

Назив 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 14.

Табела 14. Екстензије *X*.509 регистра опозваних сертификата

Назив поља - екстензије	**Опис поља – екстензије**

Authority Key Identifier	Идентификатор јавног криптографског кључа сертификационог тела који се рачуна као *SHA*-1 *hash* поља *Subject Public Key Info* 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.

Тело за оцењивање усаглашености и његови ревизори независни 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.

Извештај о оцењивању усаглашености ITE CA доставља надлежном органу у складу са законом којим се уређују електронски документ, електронска идентификација и услуге од поверења у електронском пословању.

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 је дужно да обезбеди најнижи износ осигурања од ризика одговорности за могућу штету насталу вршењем услуга издавања квалификованих сертификата у складу са важећим прописима, 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

ITE CA дужно је да се у свом пословању придржава одредби које се односе на заштиту података о личности, у складу са важећим прописима.

Корисници пре издавања квалификованих сертификата потврђују да су сагласни да се врши обрада њихових података о личности.

10.4.1. Подаци о личности који се сматрају тајним

Сви подаци о корисницима који су заштићени законом сматрају се тајним подацима о личности.

10.4.2. Подаци о личности који се не сматрају тајним

Сви подаци који су јавно доступни се не сматрају тајним подацима о личности.

10.4.3. Одговорност за заштиту тајних података о личности

ITE CA одговорно је за тајне податке о личности и за заштиту тих података, у складу са тачком 10.3.3.

10.4.4. Упозорење и сагласност за коришћење тајних података о личности

ITE CA ће, за потребе пружања услуге сертификације, користити тајне податке о личности само ако корисник да сагласност током процеса регистрације. Сматра се да је корисник дао сагласност уколико је прихватио услове пружања услуге током процеса регистрације и потписао уговор о издавању и коришћењу квалификованих електронских сертификата.

10.4.5. Откривање тајних података о личности у складу са судским или административним поступком

ITE CA ће открити или обелоданити тајне податке о личности на захтев надлежног органа и у другим случајевима, у складу са законом.

10.4.6. Друге околности за откривање тајних података о личности

ITE CA ће открити податке о личности заштићене законом уз предходну сагласност корисника или на захтев надлежног органа и у другим случајевима предвиђеним законом.

10.5. Заштита права интелектуалне својине

Овај документ, као и друга документација ITE CA објављена на веб презентацији ITE CA, представља право интелектуалне својине и власништво је ITE CA, осим уколико то није другачије означено.

Сва права интелектуалне својине ITE CA, укључујући заштитне знаке и ауторска права, остају искључиво власништво ITE CA.

ITE CA не полаже право интелектуалне својине на софтвер који се користи у *PKI* систему за издавање квалификованих сертификата, а који је у власништву трећих лица.

Софтвер треће стране ITE CA користи у складу с одредбама важеће лиценце.

10.6. Права и обавезе

10.6.1. 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 корисника сертификата који учествује у поступку издавања или промене статуса сертификата као и проверу тачности података у захтеву за издавање - 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.

10.6.2. Права и обавезе корисника

ITE CA обезбеђује поштовање свих права корисника, односно омогућава остваривање обавеза корисника, која су утврђена 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 о идентитету и осталих 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 потписа које обезбеђује ITE CA,
- употребљава сертификат само за намене одређене у овим практичним правилима,
- чува приватни криптографски кључ и у тајности чува лозинку за приступ приватном криптографском кључу,
- у случају губитка, 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.

10.6.3. 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 овим документу и другим актима објављеним на веб презентацији ITE CA.

10.6.4. 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.

10.7. Непризнавање права

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

10.8. Одговорност и ограничења од одговорности

10.8.1. 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) или приватног криптографског кључа код корисника, односно компромитовања приватног криптографског кључа, код корисника,
- 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.

10.8.2. 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 10.6.2. ових практичних правила.

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

Корисник сертификата одговора за штету уколико са намером, крајњом непажњом или из нехата обрише сертификат или криптографске кључеве са средства за креирање квалификованог електронског потписа, као и када на било који начин оштети средство или перманентно блокира средство (*PUK Status = LOCKED*), тако да онемогући његово коришћење.

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

10.9. Накнаде

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

10.10. Ступање на снагу и престанак важења правних аката

10.10.1. 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.

10.10.2. Престанак важења правних аката

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

10.10.3. 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.

10.11. 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.

10.12. Допуне Политике и практичних правила ITE CA

10.12.1. 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.

10.12.2. 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.

10.12.3. 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.

10.13. 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.

10.14. Меродавно право

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

10.15. Усклађеност са важећим законодавством

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

10.16. Остале одредбе

10.16.1. Уговор са корисницима

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

10.16.2. 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.

10.16.3. 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.

10.16.4. Применљивост за адвокатске накнаде и одрицање од права

Није применљиво.

10.16.5. 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.

10.17. Друге одредбе

10.17.1. 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.

10.17.2. Језик

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

10.17.3. 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/.

ДИРЕКТОР

др Михаило Јовановић