Практична правила цертификације за издавање и управљање електронским цертификатима Пореске управе Републике Српске

КРЕИРАЊЕ ДОКУМЕНТА

Име и презиме	Радно мјесто
Владимир Перишић, дипл. инг. ел.	Начелник одјељења за информациону безбједност и безбједност ИКТ система

ИСТОРИЈА ДОКУМЕНТА

Верзија	Датум	Опис промјена	Број документа
1.1.	15.04.2016. године	Иницијални документ	06/1.01/0103-014-1.2/2016

Садржај

1 Увод

Цертификационо тијело Пореске управе Републике Српске (у даљем тексту: *PURS CA*) доноси Практична Правила која се односе на издавање и управљање неквалификованим електронским цертификатима од стране *PURS CA* у складу са Законом о електронском потпису Републике Српске (у даљем тексту Закон), као и одговарајућим подзаконским актима Републике Српске.

PURS CA издаје електронске цертификате у складу са Законом, али и у складу са документима:

- *RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"* и
- *ETSI TS 102 280 V1.1.1 (2004-03) „X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons" .*

1.1 Преглед

PURS CA је одговорно за пружање комплетних услуга цертификације, које укључују сљедеће сервисе:

- Регистрацију корисника,
- Формирање асиметричног пара кључева за кориснике,
- Формирање електронског цертификата,
- Дистрибуцију приватног кључа и електронског цертификата корисницима на начин у складу са Законом,
- Управљање процедуром опозива и суспензије електронских цертификата и
- Обезбјеђивање статуса опозваности електронских цертификата.

PURS CA обезбјеђује средство за формирање електронског цертификата и придружени активациони код за инсталацију електронског цертификата, као и њихову безбједну дистрибуцију до корисника. *PURS CA* додатно обезбјеђује једнократни активациони код за приступ порталу путем којег се електронски цертификат преузима.

PURS CA утврђује Општа правила пружања услуге цертификације у складу са Законом која корисницима обезбјеђују довољно информација на основу којих се могу одлучити о прихватању услуга, као и о обиму самих услуга. Општа правила *PURS CA* су уграђена у документима:

1. Политика цертификације за издавање и управљање електронским цертификатима Пореске управе Републике Српске – (у даљем тексту: Политика цертификације или *CP*) и
2. Практична правила цертификације за издавање и управљање електронским цертификатима Пореске управе Републике Српске-овај документ (у даљем тексту: Практична правила или *CPS*).

Политика цертификације и Практична правила су јавни документи. Политика цертификације дефинише предмет рада цертификационог тијела, док Практична правила дефинишу процесе и

начин њиховог коришћења при формирању и управљању електронским цертификатима. Општа правила функционисања *PURS CA* су у складу са документом:

- *RFC 3647 „Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework".*

PURS CA утврђује и Интерна правила рада цертификационог тијела и заштите система цертификације (у даљем тексту: Интерна правила) у којима су садржани и детаљно описани поступци и мјере који се примењују у *PURS CA* приликом издавања и руковања електронским цертификатима. Интерна правила су власништво ПУРС и представљају пословну тајну. Интерна правила садрже детаље о:

1. систему физичке контроле приступа,
2. систему логичке контроле приступа
3. систему за управљање кључевима
4. систему дистрибуиране одговорности
5. поступцима и радњама у ванредним ситуацијама.

PURS CA је уписано у регистар цертификационих тијела Министарства науке и технологије Републике Српске.

1.2 Име документа и идентификација

Идентификациони подаци *PURS CA* су:

PURS CA

Пореска управа Републике Српске

Трг Републике Српске 8

78 000 Бања Лука

Република Српска

Босна и Херцеговина

Цертификационо тијело	Јединствено име (*DN*)
Root	*C = BA* *ST = Republika Srpska* *O = Poreska uprava* *CN = PURS ROOT CA*
Issuing	*C = BA* *ST = Republika Srpska* *O = Poreska uprava* *CN = PURS CA 1*

1.3 Учесници у *PKI* систему *PURS CA*

У овом поглављу су дате основне информације о учесницима у оквиру *PKI* система *PURS CA*.

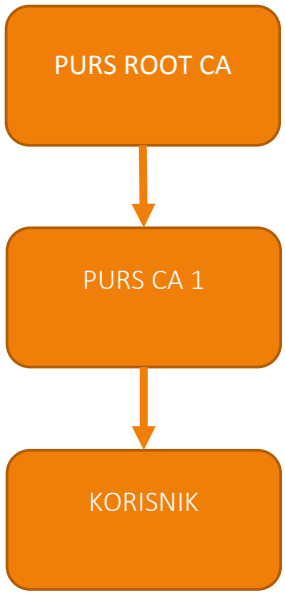
1.3.1 *PURS CA*

PURS CA је цертификационо тијело (*CA*) које издаје електронске цертификате. Политика цертификације и Практична правила, представљају одговарајућу политику и правила која се примјењују при издавању и управљању електронским цертификатима.

У циљу објављивања трећим странама информација које се односе на опозване и суспендоване цертификате (статус цертификата), врши се одговарајућа публикација листе опозваних цертификата (*CRL* – Certificate Revocation List). Провјера статуса цертификата је могућа директним увидом у *CRL*. *PURS CA* периодично објављује *CRL* листу у складу са условима дефинисаним у овом документу.

PURS CA представља хијерархијску структуру Инфраструктуре Јавних Кључева (У даљем тексту: *PKI*) за издавање електронских цертификата. У поменутој архитектури (слика 1), постоји:

- *PURS ROOT CA* – централно самопотписано цертификационо тијело (*Root CA*) које издаје цертификате потчињеним цертификационим тијелима (*Issuing CA*) и потписује своју *CRL* листу.
- *PURS CA 1* – потчињено цертификационо тијело (*Issuing CA*) од стране *PURS ROOT CA*, које издаје електронске цертификате корисницима и које потписује своју *CRL* листу.



Слика 1. Хијерархијска структура *PURS CA* система

Сва наведена цертификациона тијела налазе се и управљају на централној локацији Пореске управе Републике Српске, а у оквиру Сектора за информационе технологије.

Обавезе *PURS CA*

PURS CA гарантује да ће спроводити све процедуре дефинисане овом *CPS*. *PURS CA* се обавезује на:

1. Потпуну усаглашеност са званично објављеним *CP* и *CPS*
2. Регуларно ажурирање докумената *CP* и *CPS* и њихово јавно публиковање

3. Објављивање контакт детаља цертификационог ауторитета
4. Обезбјеђивање услуга цертификације у складу са Законом и осталим подзаконским актима
5. Обезбјеђивање инфраструктуре и цертификационих услуга, укључујући успоставу и одржавање *PURS CA* репозиторијума и одговарајућег *web* сајта у циљу пружања цертификационих услуга
6. Обезбјеђивање сигурних механизама који укључују механизам генерисања кључева, заштите кључева, као и процедуре дијељења тајни у складу са својом сопственом *PKI* инфраструктуром
7. Обезбјеђивање обавјештавања у случају компромитације сопственог приватног кључа
8. Безбједно генерисање кључева за кориснике
9. Издавање електронских цертификата у складу са *CP* и *CPS*, као и испуњавање сопствених преузетих обавеза
10. Обавјештавање корисника да су цертификати генерисани за њих, као и о начину како корисници могу да преузму цертификате
11. Обавјештавање апликанта уколико *PURS CA* није способно да изврши валидацију корисничке апликације за добијање цертификата у складу са *CP* и *CPS*
12. Након пријема валидног захтјева од стране *RA* које ради у оквиру *PURS CA* мреже издаје цертификат у складу са *CP* и *CPS*
13. Опозив цертификата који су издати у складу са *CP* и *CPS* након пријема валидног захтјева за опозив цертификата од стране ауторизованог лица које може да захтијева опозив
14. Обезбјеђивање подршке корисницима и трећим странама као што је описано у *CP* и *CPS*
15. Регуларно и периодично објављивање листе опозваних цертификата, *CRL* листе, у складу са *CP* и овим *CPS* која је увијек доступна свим заинтересованим странама
16. Обавјештавање трећих страна о статусу цертификата путем публиковања *CRL* листа на *PURS CA on-line* репозиторијуму
17. Достављања копије *CP* и *CPS*, као и осталих примјењивих докумената на захтјев неке од страна.

PURS CA потврђује да, осим горе наведених, нема других обавеза по овом *CPS* документу.

Одговорности *PURS CA*

PURS CA је одговорно за извршавање горе наведених обавеза у обиму који одређује законска регулатива Републике Српске.

1. *PURS CA* није одговорно за заштиту приватних кључева корисника намијењених за креирање електронског потписа по њиховом преузимању од стране корисника.
2. *PURS CA* није одговорно за неодговарајућу провјеру валидности цертификата од стране која се поуздаје у цертификат издат од стране *PURS CA*
3. *PURS CA* није одговорно за могућу злоупотребу цертификата која је настала усљед неиспуњавања обавеза корисника или треће стране која се поуздаје у цертификат издат од стране *PURS CA*
4. *PURS CA* није одговорно за неизвршавање својих обавеза које су посљедица ванредне ситуације или више силе.

1.3.2 Регистрационо тијело *PURS CA*

Захтјеви за издавањем цертификата за кориснике *PURS CA* подносе се на шалтерима Пореске управе Републике Српске, који обављају улогу Регистрационих ауторитета (*RA*).

RA комуницира са корисницима и *PURS CA* у циљу испоруке цертификационих услуга.

У том смислу, *RA PURS CA*:

1. Прихвата, анализира, потврђује или одбија регистрацију одговарајућих захтјева за цертификатима (апликације за цертификате).
2. Региструју кориснике за коришћење *PURS CA* цертификационих услуга.
3. Спроводе све кораке у процедури идентификације корисника у складу са Законом
4. Користе службене и овјерене документе у циљу провјере корисничке апликације.
5. Након потврде апликације корисника, обавјештавају *PURS CA* у циљу издавања цертификата.
6. Иницирају процес опозива или суспензије цертификата од стране *PURS CA*.

RA PURS CA делује у складу са праксом, процедурама и основним документима рада *PURS CA*. Не постоји ограничење на број регистрационих тијела која могу бити придружена *PURS CA PKI* инфраструктури.

PURS CA обезбјеђује регистрационим тијелима у својој инфраструктури неопходну технологију и *know-how*, као и одговарајући обуку, у циљу постизања високог нивоа обучености у складу са *PURS CA* фунцкионалним захтјевима.

***RA* обавезе**

1. Пријем апликација за издавање електронског цертификата у складу са *CP* и *CPS*.
2. Извршавање свих активности на верификацији и провјери аутентичности апликаната у складу са описом *PURS CA* процедура, *CP* и овим *CPS*
3. Достављање захтјева апликаната до *PURS CA* у електронском формату (захтјев за издавањем цертификата), у складу са *CP* и *CPS*
4. Записивање свих активности у журналу догађаја
5. Пријем, верификацију и прослеђивање ка *PURS CA* свих захтјева за опозивом и суспензијом *PURS CA* издатих цертификата у складу са *PURS CA* процедурама, *CP* и *CPS.*

PURS CA одговорна је за поштовање политике цертификације. *PURS CA* обезбјеђује механизам да оствари пуну линију одговорности у процесу издавања и управљања издатим цертификатима.

1.3.3 Корисници

Корисници су физичка, правна лица и предузетници који користе услуге *PURS CA* и који потписују уговор са Пореском управом. Корисници и лица овлашћена од стране корисника (физичка лица по овлашћењу правног лица/предузетника), подносе захтјев за издавање електронског цертификата, који су идентификовани као власници цертификата у самом цертификату, те поседују приватни кључ који математички одговара јавном кључу наведеном у корисниковом цертификату. Подносиоци захтјева могу бити:

- физичка лица по овлашћењу даваоца сагласности.

- физичка лица.

Давалац сагласности може бити правно лице или предузетник.

Корисник потписује уговор са *PURS CA* за услуге издавања и управљања електронским цертификатом које пружа *PURS CA*.

Корисник као физичко лице, након извршене идентификације и потписивања уговора, подноси Захтјев за издавање електронског цертификата.

Корисник као правно лице или предузетник, након извршене идентификације и потписивања уговора, доставља Сагласност за издавање електронског цертификата физичком лицу, који у електронском пословању могу користити електронски цертификат за потребе даваоца сагласности, те који на основу тога могу поднијети Захтјев за издавање електронског цертификата.

Идентификациони подаци даваоца сагласности (назив правног лица и ЈИБ) у издатом електронском цертификату за правно лице наводе се у атрибуту *Organization*. Идентификациони подаци о физичком лицу увијек се наводе у атрибуту *Common Name*. Електронски цертификат за физичко лице не посједује атрибут *Organization.*

Сагласност која се даје физичком лицу омогућава даваоцу сагласности да поднесе захтјев за опозивом или суспензијом електронских цертификата свих корисника код којих се у атрибуту *Organization* налази идентификациони податак даваоца сагласности.

Захтјев за издавање електронског цертификата увијек подноси физичко лице и то физичко лице као корисник и физичко лице по овлашћењу правног лица, укључујући и физичко лице које заступа правно лице. У овом процесу лице увијек мора бити физички присутно и мора да посједује важећи идентификациони документ (личну карту или путну исправу). Корисници не плаћају накнаду за издавање електронског цертификата.

Корисници са ПУРС потписују уговор за услуге издавања и управљања електронским цертификатом које пружа *PURS CA* – кориснички уговор. Кориснички уговор омогућава кориснику да поднесе захтјев за опозив, суспензију и реиздавање електронског цертификата.

Обавезе корисника

Корисници цертификационих услуга *PURS CA* су одговорни за:

1) Поштовање Политике цертификације (*CP*) и Практичних правила рада (*CPS*) публикованих од стране *PURS CA*,
2) Обезбјеђивање тачних информација у њиховој комуникацији са *RA PURS CA*,
3) Упознавање, разумијевање и сагласност са свим ставовима и условима у *CP* и овој *CPS*, као и другим документима који су објављени на *PURS CA* репозиторијуму,
4) Обавјештавање *RA* тијела о било којим промјенама информација које су раније достављене,
5) Посједовање одговарајућих знања и ако је неопходно, похађање одговарајуће обуке за коришћење електронских цертификата и цертификационих услуга,
6) Уздржавање од нарушавања интегритета и произвођења неисправним, цертификата издатог од стране *PURS CA*,

7) Коришћење *PURS CA* цертификата само за легалне и ауторизоване сврхе у складу са *CP* и *CPS*, као и важећим законским и подзаконским актима,
8) Прекид коришћења електронског цертификата уколико је било која информација у цертификату постала невалидна,
9) Прекид коришћења електронског цертификата уколико сам цертификат постане невалидан,
10) Уздржање од коришћења свог приватног кључа који одговара јавном кључу који је цертификован од стране *PURS CA*, у издатом цертификату, под истим именом за потребе издавања других цертификата,
11) Спрјечавање компромитације, губљења, објављивања, модификације или било ког другог неауторизованог коришћења свог приватног кључа,
12) Захтијевање опозива цертификата у случају догађаја који материјално утиче на интегритет издатог цертификата од стране *PURS CA*,
13) Пријављивање сваке могуће злоупотребе свог приватног кључа и захтијевање да се цертификат опозове у том случају.

1.3.4 Треће стране

Треће стране су физичка лица и/или правна лица који прихватају и верификују електронски потпис. Треће стране могу да корисника идентификују као припадника правног лица/предузетника на основу вриједности атрибута *Organization* у тијелу електронског цертификата.

Верификација електронског потписа обухвата:

- Провјеру валидности путање цертификације корисниковог електронског цертификата. У циљу провјере валидности електронског цертификата, треће стране морају увијек да провјере статус опозваности датог цертификата у оквиру *PURS CA*. На располагању су *CRL* листе (*PURS ROOT CA* і *PURS CA 1*).
- Провјеру потписа електронског документа на бази јавног кључа који се налази у корисниковом електронском цертификату.

Обавезе трећих страна

Страна која се ослања на *PURS CA* издати цертификат обавезна је да:

1) Посједује одговарајућа знања о коришћењу електронских цертификата и других технологија везаних за услуге цертификације
2) Упозна се са Политиком цертификације (*CP*) и Практичним правилима рада (*CPS*) у вези наведених услова који важе за треће стране
3) Поштује и спроводи одредбе из *CP* и *CPS*
4) Верификује *PURS CA* издати цертификат:
    a. Провјером да је комплетан ланац цертификата од *Root CA* цертификата
    b. Провјером опозваности цертификата у ланцу
    c. Провјером да су сви цертификати у ланцу валидни у временском тренутку провјере цертификата
5) Провјери комплетност података у цертификату издатом од стране *PURS CA*, као и да провјери да ли дати цертификат служи одговарајућој области примјене која је наведена у цертификату

6) Верификује електронски потпис
7) Разумно ослони и поузда на *PURS CA* издати цертификат у складу са одговарајућим околностима.

1.4 Коришћење цертификата

1.4.1 Прихватљиво коришћење цертификата

У складу са Законом, електронски цертификат се користи за верификацију електронског потписа. *PURS CA* електронски цертификати се могу користити за одређене трансакције електронског пословања са Пореском управом Републике Српске, а које се базирају на употреби електронског потписа. Примјери оваквих трансакција су:

- Електронско потписивање докумената и
- Приступ безбједним *web* сајтовима и порталима (*SSL/TLS* аутентификација) и другим *on-line* садржајима Пореске управе Републике Српске.

1.4.2 Забрањено коришћење цертификата

Свака друга употреба електронског цертификата која није прописана овим документом или није у сагласности са одредбама Закона о електронском потпису и другим документима који регулишу ову област сматра се недозвољеном.

1.5 Администрација Практичних правила цертификације

1.5.1 Организација администрирања Практичних правила цертификације

PURS CA је одговорно за прописну администрацију Практичних правила цертификације и то у смислу периодичног прегледа и ажурирања, као и ванредних промјена одговарајућих одредби које проистичу из евентуалних промјена у законској регулативи или техничким карактеристикама криптографских алгоритама и дужина кључева које *PURS CA* користи.

1.5.2 Контакт подаци

PURS CA

Пореска управа Републике Српске

Трг Републике Српске 8

78 000 Бања Лука

Република Српска

Босна и Херцеговина

тел: +387 51 332-360 фах: +387 51 332-350

e-mail: ca@poreskaupravars.org

1.5.3 Особа која одређује погодност документа Практичних правила цертификације

Особа у Пореској управи Републике Српске, одговорна за Практична правила цертификације је:

Владимир Перишић

Пореска управа Републике Српске

Трг Републике Српске 8

78 000 Бања Лука

Република Српска

Босна и Херцеговина

тел: +387 51 337-788; фах: +387 51 332-350

e-mail: vladimir.perisic@poreskaupravars.org

1.5.4 Процедура одобравања *CPS* документа

Документ се редовно периодично прегледа и врше се његове измјене од стране одговорних лица за *PURS CA* систем у Пореској управи Републике Српске.

1.6 Дефиниције и скраћенице

У овом документу поједини изрази имају сљедеће значење:

Активациони подаци – Подаци, који нису криптографски кључеви, који су захтијевани у циљу рада криптографских модула и који морају бити заштићени (као на примјер једнократни активациони код или приступна шифра).

Захтјев за цертификат – Захтјев поднесен од стране лица које захтијева електронски цертификат Цертификационом тијелу у циљу издавања електронског цертификата.

Подносилац захтјева/апликант – физичко лице које је подносилац захтјева за издавањем електронског цертификата у временском периоду до уручења када постаје корисник.

Асиметрични криптографски алгоритми – криптографски алгоритми који користе различите кључеве за шифровање и дешифровање.

Асиметрични пар кључева – Приватни кључ и јавни кључ, као математички пар који се користе за потребе рада асиметричног криптографског алгоритма, као што је на примјер *RSA* алгоритам.

Аутентикација – процедура провјере идентитета појединца или организације.

CA цертификат – Цертификат за дато *CA* издат (дигитално потписан) од стране другог *CA* (*Issuing CA*) или самопотписан (уколико се ради о *Root CA*).

Дијељена тајна – Дио криптографске тајне која је подијељена на унапријед дефинисан број дијелова.

Дигитални потпис – Технички поступак реализације електронског потписа гдје се *hash* вриједност бинарне репрезентације електронског документа шифрује асиметричним криптографским алгоритмом.

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

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

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

Hash алгоритми – једносмјерне иреверзибилне функције помоћу којих се врши трансформација информације произвољне величине у *hash* вриједност фиксне величине (128, 160, 224, 256, 374, 512 битова (или више).

Идентификација – процес декларисања идентитета физичког или правног лица/предузетника.

Управљање цертификатима – Активности придружене управљању цертификатима укључују генерисање, чување, испоруку, објављивање и опозив цертификата.

Скраћенице које се користе у овом документу:

CA (*Certification Authority*) - Цертификационо тијело

CP (*Certificate Policy*) - Политика цертификације

CPS (*Certificate Practise Statement*) - Практична правила

CRL (*Certificate Revocation List*) - Листа опозваних цертификата

ПУРС – Пореска управа Републике Српске

ETSI – European Telecommunication Standardization Institute

OID (*Object Identifier*) - јединствени идентификатор

PKI (*Public Key Infrastructure*) - Инфраструктура јавних кључева

PURS CA –Цертификационо тијело Пореске управе Републике Српске

RA (*Регистратион Аутхорити*) - Регистрационо тијело

RFC – Request For Comments

2 ОДГОВОРНОСТИ ЗА ПУБЛИКОВАЊЕ И РЕПОЗИТОРИЈУМЕ

Ово поглавље се односи на све аспекте публиковања информација, као и на локације гдје се те информације публикују, у оквиру *PURS CA*.

2.1 РЕПОЗИТОРИЈУМ

PURS CA публикује информације неопходне за провјеру статуса електронских цертификата (цертификате *CA* тијела и *CRL* листе *CA* тијела) које издаје на *on-line* репозиторијуму *http://ca.poreskaupravars.org. PURS CA* задржава право да публикује статусне информације о цертификатима и на репозиторијуму неке треће стране уколико је то потребно.

PURS CA на поменутом *on-line* репозиторијуму објављује информације о практичним правилима и процедурама рада, укључујући *CP*, као и ова *CPS*. *PURS CA* задржава право да учини расположивим и публикује информације у вези сопствених политика и процедура рада путем било ког погодног начина.

2.2 ПУБЛИКОВАЊЕ ИНФОРМАЦИЈА О ЦЕРТИФИКАТИМА

PURS CA публикује информације о цертификатима *PURS CA* (*Root i Issuing CA*) на претходно поменутим репозиторијумима.

Учесници у цертификационим услугама се обавјештавају да ће *PURS CA* публиковати поједине информације које су они доставили на јавно приступачним директоријумима уз придружене статусне информације о електронским цертификатима у формату и садржају који прописује Закон.

Из разлога њихове осјетљивости и пословне тајне, *PURS CA* неће публиковати интерна правила рада која се односе на неке подкомпоненте и елементе који укључују одређене безбједносне контроле, процедуре које се односе на управљање кључевима, дистрибуирану одговорност, безбједност регистрациона тијела, поступке у ванредним ситуацијама и све остале безбједносно осетљиве процедуре.

2.3 ВРИЈЕМЕ И ФРЕКВЕНЦИЈА ПУБЛИКОВАЊА

PURS CA публикује информације о статусу опозваности издатих електронских цертификата (*CRL* листе), као што је назначено и прецизирано у овом документу.

Максимално дозвољено кашњење од издавања *CRL* листе до публиковања је један сат.

2.4 КОНТРОЛЕ ПРИСТУПА РЕПОЗИТОРИЈУМИМА

PURS CA одржава расположивим приступ до свог јавног репозиторијума трећим странама са сврхом:

- Добављања *CA* цертификата *PURS ROOT CA* и *PURS CA*1
- *CRL* листе *PURS ROOT CA* и *PURS CA*1

PURS CA ће ограничити или забранити приступ одређеним услугама, као што су публиковање статусних информација о базама података треће стране, одређеним приватним директоријумима, итд.

3 ИДЕНТИФИКАЦИЈА И АУТЕНТИКАЦИЈА КОРИСНИКА

У овом поглављу су наведени услови које је неопходно испунити приликом подношења захтјева за издавањем/обновом/промјеном статуса електронског цертификата.

Услови се односе на:

- Идентификацију физичког лица
- Идентификацију правног лица/предузетника,
- Идентификацију подносиоца захтјева, овлашћеног од стране правног лица/предузетника.

3.1 НАЗИВИ

Идентификациони подаци корисника и подносиоца захтјева, овлашћених од стране корисника који се уграђују у електронски цертификат, структуирани су по *X.500 distinguished name* форми.

PURS CA издаје електронске цертификате подносиоцима захтјева. Правно лице или предузетник доставља документовану сагласност која садржи називе који се могу верификовати (назив и ПИБ), док физичко лице доставља документован захтјев који садржи називе који се могу верификовати (име, презиме и ЈМБ подносиоца захтјева). ЈМБ се неће наћи у издатом електронском цертификату.

PURS CA не издаје анонимне цертификате корисницима.

Имена придружена корисницима цертификата су јединствена у домену *PURS CA*, пошто се увијек користе заједно са јединственим идентификационим бројем корисника (у *CN* пољу *Subject*-а).

PURS CA не прихвата "*trademark*" ознаке, лога или друге графичке или текстуалне материјале који су заштићени од копирања, а разматрани су за укључење у цертификате.

3.2 ИНИЦИЈАЛНА ПРОВЈЕРА ИДЕНТИТЕТА

- Идентификација физичког, правног лица или предузетника, као корисника. Достављени подаци се провјеравају. Консултују се базе података које једнозначно идентификују кориснике.
- Идентификовано правно лице или предузетник, доставља сагласност за издавање електронског цертификата физичким лицима, ради подношења захтјева за издавање електронског цертификата.
- Подносиоци захтјева се уз лично присуство у регистрационом тијелу и валидним идентификационим документом идентификују. Провјеравају се идентификовани подаци са подацима у достављеном овлашћењу.

Идентификовани подаци корисника и подносиоца захтјева, се структуирају *у X.500 distinguished name* форму и електронски од стране *RA* оператера достављају у *CA*.

3.3 ИДЕНТИФИКАЦИЈА И АУТЕНТИКАЦИЈА ЗАХТЈЕВА ЗА ОПОЗИВ ЦЕРТИФИКАТА

Правно лице или предузетник може да захтијева промјену статуса електронских цертификата у којима су његови идентификациони подаци, тако што ће пријавити промјене у податку електронског цертификата. Захтјев, потписан од стране законског заступника правног лица/предузетника, подноси се лично у *RA* тијело, уз обавезну идентификацију законског заступника идентификационим документом.

Физичко лице може да захтијева опозив/суспензију свог цертификата. Захтјев се подноси лично у *RA* тијело, уз обавезну идентификацију идентификационим документом.

Опозив цертификата може бити захтијеван и од стране *PURS CA* због уочених нерегуларности у раду.

Подносиоци захтјева за промјену статуса електронског цертификата се обавјештавају након обраде захтјева. Обрађен захтјев за промјену статуса је видљив на *CRL* листи у року од 24 сата по пријему захтјева.

4 ОПЕРАТИВНИ ЗАХТЈЕВИ У ВЕЗИ ЖИВОТНОГ ЦИКЛУСА ЦЕРТИФИКАТА

За све кориснике *PURS CA* или друге учеснике постоји стална обавеза да информишу *PURS CA* о свим промјенама у информацијама које су објављене у цертификату за читав период важења таквог цертификата. Одређене друге обавезе се такође могу додатно успоставити.

4.1 ПОДНОШЕЊЕ ЗАХТЈЕВА ЗА ДОБИЈАЊЕ ЦЕРТИФИКАТА

Физичка, правна лица или предузетници, потписују са Пореском управом Републике Српске Уговор о пружању услуга цертификације. Правна лица и предузетници достављају сагласност за издавање електронских цертификата, користећи образац *„Сагласност за издавање електронских цертификата/измјену података на постојећим електронским цертификатима“.*

RA спроводи процес идентификације, аутентикације и регистрације корисника ради закључења уговора, а у циљу спровођења поступка подношења захтјева за издавање електронских цертификата који захтјева:

- Давање сагласности уколико је корисник правно лице или предузетник,
- Достављање друге документације уколико је то потребно и
- Прихватање уговора.

Потребни подаци форме сагласности за електронске цертификате су:

1) Назив организације (податак даваоца сагласности)
2) ЈИБ (податак даваоца сагласности)
3) Поштанска адреса (податак даваоца сагласности)
4) Име (податак подносиоца захтјева)
5) Презиме (податак подносиоца захтјева)
6) ЈМБ (податак подносиоца захтјева)
7) Контакт телефон (податак подносиоца захтјева)
8) *E-mail* адреса корисника (податак подносиоца захтјева)

Процес одржавања података о корисницима реализује се унутар *RA* тијела и обухвата континуалну провјеру и ажурирање података.

Пријем сагласности за издавање електронског цертификата у *RA* мора да стигне у папирном облику, али искључиво у форми попуњеног прописаног обрасца овјереног потписом законског заступника.

Након провјере валидности података, *RA* оператер шаље поруке подносиоцима захтјева из листе са сагласности, или кориснику уколико је подносилац захтјева (користећи податке уписане у пољу *e-mail*) да дођу на локацију *RA* тијела у циљу личне идентификације.

У позиву за долазак који се шаље *e-mail*-ом приложени су:

- Елементи сагласности за издавање електронског цертификата који су дефинисани од стране даваоца сагласности (датум слања, број под којим је заведен у пословном систему правног лица, заступник који је послао захтјев и сл.),

- Локације на којима се могу прочитати документи Политике цертификације и Практичних правила,
- Молба да са собом понесе овај позив, с обзиром да је на тај начин верификована исправност унесене *e-mail* адресе.

Уколико је корисник физичко лице, након потписивања уговора и провјере валидности података, физичко лице подноси захтјев RA оператеру за издавање електронског цертификата.

4.2 Обрада захтјева за добијање цертификата

Подносилац захтјева се јавља *RA* оператеру. RA оператер се налази у подручној јединици Пореске управе. Мјесно надлежна подручна јединица Пореске управе одређује се према сједишту правног лица/предузетника или органа управе које се налази у Републици Српској, а за физичка лица према мјесту пребивалишта, односно боравишта у Републици Српској.

За правна лица/предузетнике или органе управе чије је сједиште изван Републике Српске и физичка лица чије је пребивалиште, односно боравиште изван Републике Српске мјесно је надлежна подручна јединица Пореске управе којој је поднесен Захтјев.

RA оператер врши идентификацију лица. Да би се идентификација сматрала успјешном потребно је да:

- Подносилац захтјева поседује идентификациони документ који по броју и врсти одговара документу наведеном у сагласности
- Да подаци из захтјева одговарају подацима из презентованог идентификационог документа
- Да се подносилац захтјева појавио у року важења захтјева
- Да подносилац захтјева има код себе e-mail поруке (на увид)
- Подносилац захтјева обавјештава се о једнократном коду за приступ *on-line* репозиторијуму http://ca.poreskaupravars.org.

Уколико одбија захтјев *RA* оператер мора да наведе разлог одбијања и о истом обавијестити подносиоца захтјева путем *e-mail-a*.

RA оператер структуира податке из апликације у електронски документ. *RA* оператер овај документ заштићеним каналом доставља у *PURS CA*.

RA оператер врши обезбјеђење документације, захтјева који је достављен, од отуђења и уништења.

Генерисање асиметричног приватног и јавног кључа врши се само у заштићеним просторијама *PURS CA*.

Технички и безбједносни детаљи су описани у интерним правилима рада.

4.3 Издавање цертификата

Након доставе валидног електронског документа за издавањем цертификата, *CA* оператер *PURS CA* спроводи процес издавања одговарајућег цертификата који се састоји од:

- Контроле свих елемената из захтјева,

- Одобрење или одбијање захтјева,
- *CA* оператер покреће процедуру генерисања пара кључева асиметричног алгоритма,
- *CA* оператер у електронски документ захтјева укључује и генерисани асиметрични јавни кључ,
- *CA* оператер врши издавање електронског цертификата за одобрени захтјев,
- *PURS CA* систем путем *e-mail-a* обавјештава подносиоца захтјева о томе да му је цертификат издат и како може да га преузме.
- PURS CA систем такође обавјештава подносиоца захтјева да у року од петнаест (15) дана мора да преузме електронски цертификат, уз упозорење да уколико у датом року не преузме цертификат, исти се аутоматски повлачи. У случају аутоматског повлачења цертификата процедура за добијање новог цертификата је иста као за иницијално подношење захтјева.
- PURS CA систем обавјештава *RA* тијело о статусу обраде просљеђеног захтјева.

Постоје два кода:

- једнократни код за приступ *on-line* репозиторијуму *http://ca.poreskaupravars.org*
- активациони код (за инсталацију електронског цертификата).

Технички и безбједносни детаљи су описани у интерним правилима рада.

4.4 Прихватање цертификата

Уручење електронског цертификата врши се путем *on-line* репозиторијума *http://ca.poreskaupravars.org.* Издати цертификат од стране *PURS CA* сматра се прихваћеним од стране корисника уколико је корисник преко *on-line* репозиторијума *http://ca.poreskaupravars.org* коришћењем једнократног кода преузео електронски цертификат.

Било која примједба на прихватање издатог цертификата мора бити достављена до *PURS CA*, као цертификационом тијелу – издаваоцу. Примједбе могу бити достављене у *RA* тијело које их просљеђује до *PURS CA*.

4.5 Коришћење цертификата и асиметричног пара кључа

У овом поглављу се дефинишу одговорности које се односе на коришћење асиметричног пара кључева и цертификата, и то:

- Одговорности корисника – сви корисници се обавезују да ће користити приватни кључ и цертификат издат од стране *PURS CA* у складу са дефинисаним начином коришћења кључа у самом цертификату (*Key Usage* и *Enhanced Key Usage* екстензије). Корисник може користити свој приватни кључ само након прихватања одговарајућег цертификата. Такође, корисник мора престати да користи свој приватни кључ након истицања периода валидности или опозива издатог цертификата.
- Одговорност треће стране – трећа страна је обавезна да прихвата издате цертификате *PURS CA* са предвиђеним начином коришћења цертификата дефинисаним у самом цертификату. Трећа страна је обавезна да прописно и успјешно примјењује операцију јавног кључа који

екстрахује из издатог цертификата и одговорна је да спроводи провјеру статуса опозваности датог цертификата коришћењем метода који је дефинисан у *CP* и *CPS* документима *PURS CA*.

4.6 Обнављање цертификата

Обнављање цертификата се може урадити само ако је постојећи цертификат валидан и у периоду од 30 дана прије истека активног цертификата.

Законом је предвиђено да се корисник цертификата лично идентификује као мјера провјере да су подаци који се налазе у цертификату и даље валидни. Због тога се примјењује иста процедура као и за иницијално издавање цертификата. На захтјеву за идавање цертификата се наводи да је већ регистрован да би се користио исти јединствени идентификатор корисника (ЈИК) у новом цертификату.

Обновљени цертификат се издаје са новим асиметричним паром кључева и новим једнократним кодовима за преузимање и инсталацију електронског цертификата. Операција опозива старог и активирања обновљеног цертификата је аутоматска.

4.7 Генерисање новог пара кључева и цертификата корисника

Корисници којима је цертификат истекао или је опозван, уколико желе да добију нови цертификат, морају да поднесу захтјев за издавање новог цертификата. Процедура је иста као и за иницијално издавање цертификата. Нови цертификат се издаје са новим асиметричним паром кључева и новим једнокраним кодовима за преузимање и инсталацију електронског цертификата.

Корисник је већ регистрован у оквиру *PURS CA* и посједује јединствени идентификатор корисника (ЈИК). На захтјеву за издавање цертификата се наводи да је већ регистрован да би се користио исти ЈИК у новом цертификату.

Правила прихватања цертификата у овом случају су иста као што је описано у поглављу 4.4.

4.8 Модификације цертификата корисника

Модификације постојећег цертификата нису дозвољене. Уколико су потребне модификације ради се поступак издавања новог цертификата уз опозив претходног.

4.9 Суспензија и опозив цертификата

PURS CA врши опозив издатог електронског цертификата у случају:

- Губитка, крађе, модификације, објављивања или неке друге компромитације приватног кључа корисника цертификата,
- Да извршење одговарајућих обавеза лица која су наведена у овој *CPS* касни или је спријечено усљед природне катастрофе, рачунарског или комуникационог отказа, или усљед другог узрока који излази ван контроле датог лица и као резултат информације о другом лицу су материјално угрожене или компромитоване,

- Да се десила промјена информација које су садржане у цертификату датог лица,
- На захтјев даваоца сагласности које опозива сагласност дату физичком лицу да у електронском пословању може користити електронски цертификат у његово име,
- На захтјев корисника.

PURS CA врши суспензију издатог електронског цертификата у случају:

- На захтјев корисника, даваоца сагласности или надзора *PURS CA* уколико имају сумњу у компромитацију приватног кључа,
- На захтјев даваоца сагласности када привремено укида право физичком лицу (нпр. запосленом у датом правном лицу или код предузетника) да (у електронском пословању) може користити електронски цертификат у његово име.

Процес опозива електронских цертификата може се иницирати из сљедећих извора:

- Овјереним захтјевом даваоца сагласности које је дало сагласност за издавање цертификата за физичко лице,
- Овјереним захтјевом корисника,
- *PURS CA* уколико је установљен ризик од компромитације приватног кључа за један или више издатих електронских цертификата.

У другом случају, по Закону о електронском потпису РС, у члану 28. предвиђено је да је корисник обавезан да одмах затражи опозив свог цертификата у свим случајевима губитка, оштећења средстава или промјена података за израду електронског потписа. Корисник овјерени захтјев у папирној форми подноси у *RA* тијело. *RA* верификује идентитет стране која је захтијевала опозив на основу информационих елемената који су садржани у идентификационим подацима које је корисник доставио до *RA* тијело. *RA* оператер је дужан да обради и прослиједи у *CA* тијело у току истог радног дана у којем је захтјев стигао. Уколико подаци из захтјева нису вјеродостојни, захтјев се одбија и о томе обавјештава корисник и надзор *PURS CA*. *CA* оператер је дужан да у току истог радног дана обради захтјев за опозивом и обавијести корисника о опозиву.

У трећем случају, *PURS CA* спроводи провјеру свих уочених и пријављених неправилности у раду цијелог *CA* система. На све потврђене невалидности подноси захтјев *CA* оператерима за опозив једног или више електронских цертификата. *CA* оператер је дужан да у току истог радног дана обради захтјев за опозивом и обавијести корисника и подносиоца захтјева о опозиву.

PURS CA спроводи надзор рада цијелог система и излаз из уочене неправилности. Уочене неправилности у случају компромитације једног или више електронских цертификата повлаче захтјев за опозивом истих.

PURS CA провјерава сваку пријављену неправилност. Пријаву неправилности могу урадити службеници *PURS CA*, службеници *RA*, корисници или треће стране. Пријављена неправилност у случају компромитације једног или више електронских цертификата повлаче захтјев за опозивом истих.

У случају да је потребно више од 24 сата да се потврди сумња у компромитацију приватног кључа, подноси се захтјев за суспензијом цертификата у *RA* тијело исти радни дан када је установљена сумња. Оператер *RA* тијела је дужан да изврши идентификацију подносиоца захтјева и обради

захтјев исти радни дан по пријему захтјева. Потврдно обрађен захтјев исти радни дан подноси у *CA* тијело. *CA* оператер валидира и обрађује захтјев истог радног дана.

За вријеме трајања суспензије подносилац захтјева дужан је да испита сумњу и ,ако је потврдна сумња, поднесе захтјев за опозивом. Уколико се у току трајања суспензије не поднесе захтјев за опозивом, то значи да су сумње неоправдане и електронски цертификат се враћа у стање валидног.

Суспензија цертификата траје онолико дуго колико трају и услови због којих је суспензија и захтијевана, а најдуже тридесет (30) дана. У случају да услови захтијевају да суспензија треба да је дужа од 30 дана, мора се користи процедура опозива.

CA оператер опозивом и суспензијом електронског цертификата мијења његов статус у бази одговарајућег *CA* тијела која се користи приликом генерисања *CRL* листе.

4.10 Сервиси провјере статуса цертификата

Опозвани или суспендовани електронски цертификат је видљив на *CRL* листи у року од 24 сата од подношења захтјева за опозивом или суспензијом. Опозвани или суспендовани цертификати који су временски истекли нису видљиви на *CRL* листи. У случају опозива *Issuing CA* електронског цертификата *PURS CA* обавјештава кориснике директно, а треће стране преко *on-line* репозиторијума *http://ca.poreskaupravars.org* у року од 24 сата од поднесеног захтјева за опозивом или суспензијом *Issuing CA* електронског цертификата *PURS CA*.

Листа опозваних цертификата (*CRL*) *PURS CA*1 се ажурира на сваких 24 сата, а *CRL PURS ROOT CA* на сваких 6 мјесеци. Треће стране морају користити *on-line* репозиторијум *http://ca.poreskaupravars.org PURS CA* да преузму *CRL* листу.

Технички и безбједносни детаљи су описани у интерним правилима рада.

4.11 Престанак коришћења цертификата

Након престанка коришћења цертификата издатог од стране *PURS CA*, дати цертификат мора бити опозван уколико је у том тренутку и даље активан.

Престанак коришћења цертификата може бити из сљедећих разлога:

- Корисник жели да прекине коришћење цертификационих сервиса *PURS CA*.
- *PURS CA* је престало са пружањем услуга цертификације.

Временски истекли електронски цертификати се не опозивају и тренутком истека наступа престанак коришћења цертификата.

Временски истекли опозвани електронски цертификати се уклањају са листе опозваних електронских цертификата.

4.12 Чување и реконструкција приватног кључа корисника

Асиметрични приватни кључ корисника који одговара јавном кључу садржаном у издатом електронском цертификату се не чува и налази се само у инсталационом фајлу којег преузима корисник путем *on-line* репозиторијума *http://ca.poreskaupravars.org.*

5 УПРАВНЕ, ОПЕРАТИВНЕ И ФИЗИЧКЕ БЕЗБЈЕДНОСНЕ КОНТРОЛЕ

Ово поглавље описује све безбједносне контроле које користи *PURS CA* за обављање функција креирања пара кључева асиметричног алгоритма, провјере захтјева, издавања електронског цертификата, опозив електронског цертификата, провјере/аудитинга и архивирања.

PURS CA планира и изводи све безбједносне мјере у складу са стандардом *ISO/IEC 27001.*

5.1 ФИЗИЧКЕ БЕЗБЈЕДНОСНЕ КОНТРОЛЕ

PURS CA захтијева и имплементира физичке безбједносне контроле на свим локацијама на којима се обавља било који дио рада.

Детаљан опис примијењених контрола описан је у интерним правилима везаним за физичке безбједносне контроле.

5.1.1 Локација и зграда

Опрема *PURS CA* налази се у посебним просторијама које одговарају потребама извршења операција високе безбједности.

5.1.2 Физички приступ

Физички приступ је ограничен имплементацијом одговарајућих механизама контроле приступа у и из зона безбједности свих нивоа.

5.1.3 Електрично напајање и климатизација

Напајање и вентилација се извршавају са редундансом.

5.1.4 Изложеност поплавама

Просторије *PURS CA* су заштићене од поплава.

5.1.5 Превенција и заштита од пожара

Превенција и заштита од пожара су имплементиране.

5.1.6 Медијуми за чување података

Backup медијуми чувају се на одвојеној локацији која је физички обезбјеђена и заштићена од пожара и поплава.

5.1.7 Одлагање смећа

Изношење смећа се контролише. Папирни отпад се уништава на машини. Електрични уређаји се прије одлагања физички уништавају.

5.1.8 Одлагање резервних копија

Backup система на другу локацију која је физички обезбјеђена и заштићена од пожара и поплава се врши преко одговарајућих *backup* медија.

5.2 ПРОЦЕДУРАЛНЕ КОНТРОЛЕ

PURS CA спроводи кадровску и управну праксу која обезбјеђује разумну сигурност у повјерљивост и компетенцију запослених у домену технологија које се односе на електронски потпис и *PKI* системе.

5.2.1 Повјерљиве позиције запослених

Дужности запослених у *PURS CA* који извршавају операције повезане са управљањем кључевима *Root* и *Issuing CA* тијела, као и било које друге операције које материјално утичу на такве операције, сматрају се дужностима на повјерљивим позицијама. Повјерљиве дужности у *PURS CA* су:

- Администратор безбједности,
- Систем администратори и
- Систем оператери.

PURS CA спроводи провјеру свих запослених који су кандидати за повјерљиве позиције због стицања увида у њихову поузданост и компетенције.

Дужности запослених у *PURS CA* који извршавају операције повезане са управљањем кључевима, као и било које друге операције које материјално утичу на такве операције, сматрају се дужностима на овлашћеним позицијама. Овлашћене дужности у *PURS CA* су:

- *RA* оператер и
- *CA* оператер.

5.2.2 Број особа које се захтијевају по сваком задатку

Тамо гдје се захтијева дуална контрола, потребно је да најмање два запослена *PURS CA* на повјерљивим дужностима искажу њихова подијељена знања у циљу омогућавања извршења текућих операција. У оперативном раду са корисницима *PURS CA* потребно је да се користе обје овлашћене дужности исказивањем њихових знања у циљу омогућавања извршења текућих операција. Свака повјерљива или овлашћена дужност дефинише одговарајуће захтјеве у погледу идентификације и аутентикације.

Операције на којима се захтијева дуална контрола су:

- Креирање, активирање коришћења, *backup*-овање или уништење асиметричног приватног кључа *Root* и *Issuing CA* тијела и
- Конфигурација/реконфигурација *PURS CA* окружења.

5.2.3 Идентификација и за сваку улогу

Свака повјерљива или овлашћена дужност дефинише одговарајуће захтијеве у погледу идентификације и . Детаљније описано у интерним правилима.

5.2.4 Улоге које захтијевају раздвајање дужности

Запослени у *PURS CA* може да има само једну повјерљиву дужност и/или једну овлашћену дужност. Док обавља повјерљиву дужност може да обавља само *RA* овлашћену дужност, осим за сврху церемоније.

5.3 КАДРОВСКЕ БЕЗБЈЕДНОСНЕ КОНТРОЛЕ

5.3.1 Квалификација и искуство

PURS CA извршава неопходне активности у циљу провјере захтијеване биографије, квалификација, као и неопходног искуства у циљу реализације у оквиру контекста компетенције специфичног посла. Такве провјере биографије кандидата укључују:

- Да није осуђиван за кривично дјело,
- Да не постоје погрешне презентације информација од стране кандидата,
- Да постоје одговарајуће референце.

5.3.2 Процедура провере биографије

PURS CA реализује релевантне провјере евентуалних запослених на бази статусних извештаја који су издати од стране компетентних ауторитета, изјава трећих страна или изјава самих потенцијалних запослених.

5.3.3 Захтијеви за обученошћу

PURS CA обезбјеђује обуку за своје запослене на повјерљивим и овлашћеним дужностима у циљу реализације функција пословања *CA* и *RA*.

5.3.4 Поновна обука

Периодично ажурирање обуке и дообука запослених ради се у циљу успоставе континуитета и ажурности знања запослених, као и одговарајућих процедура.

5.3.5 Ротација послова

PURS CA примјењује ротацију запослених на повјерљивим дужностима сваке 3 године. Ротација запослених повлачи измјену подијељених знања запослених и реконфигурације *PURS CA* система тако да не утичу на континуитет пословања.

5.3.6 Документација за иницијалну обуку и поновну обуку

PURS CA чини доступном документацију запосленима на повјерљивим и овлашћеним дужностима која се односи на иницијалну обуку, дообуку или за друге сврхе.

5.3.7 Казнене мјере у односу на запослене

PURS CA примјењује одговарајуће мјере за санкционисање запослених за неовлашћене активности.

5.4 ПРОЦЕДУРЕ БЕЗБЈЕДНОСНИХ ПРОВЈЕРА/АУДИТИНГ

PURS CA води ажурну, тачну и безбједну евиденцију издатих цертификата која није јавно доступна.

Евиденција о свим догађајима у раду *PURS CA* води се електронски (*Audit log*), а гдје то није могуће ручно са датумом, временом и описом догађаја.

5.4.1 Типови забиљежених догађаја

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

5.4.2 Учесталост прегледа евидентираних догађаја

Сви евидентирани догађаји се чувају и прегледају једанпут мјесечно. Рад *RA* оператера се периодично провјерава од стране запослених на повјерљивим дужностима са паузом провјере не дужом од 6 мјесеци. Рад *CA* оператера се периодично провјерава од стране запослених на повјерљивим дужностима са паузом провјере не дужом од 3 мјесеца.

5.4.3 Вријеме чувања евиденције

Аудит логови се архивирају минимално једанпут у 3 месеца а чувају се најмање 10 година.

5.4.4 Заштита *Audit log*

Документација достављена у *RA* тијело се чува у обезбјеђеном простору. Достављена документација чува се у *RA* тијелу. Цјелокупна размјена информација између *RA* тијела и *PURS CA* су електронски документи. Аудит логови рада *RA* оператера са системом и електронски документи налазе се на обезбјеђеном рачунару за ту намјену, а медиј са *backup*-ом се чува у обезбјеђеном простору.

5.4.5 Процедура *backup*-а аудит логова

PURS CA имплементира процедуре *backup*-а аудит логова.

5.4.6 Систем сакупљања аудит логова

Логови се скупљају у реалном времену.

5.4.7 Обавјештење субјекта који је проузроковао догађај

Субјекат који је проузроковао одређени инцидентни догађај се не обавјештава о самој аудит активности. У случају инцидентног догађаја, обавјештава се администратор безбједности *PURS CA*.

5.4.8 Процјена рањивости система

PURS CA реализује периодичну процјену рањивости система.

5.5 Архивирање записа

Захтјеви за чувањем записа се примјењују на *PURS CA* систем у цјелини, како на *CA* тако и на *RA*.

Детаљни опис процедуре се налази у интерним правилима рада.

5.5.1 Типови архивираних записа

PURS CA чува на безбједан начин записе о издатим електронским цертификатима, аудит подацима, информацијама о апликацијама за добијањем цертификата, као и документацију о самим апликацијама за издавање цертификата.

5.5.2 Период чувања архиве

PURS CA чува на безбједан начин поменуте записе о *PURS CA* електронским цертификатима за период који је назначен у *PURS CA CPS* документу, а што је усклађено са Законом,

5.5.3 Заштита архиве

PURS CA спроводи одговарајућу процедуру заштите медија *backup*-а архиве у обезбјеђеном простору.

5.5.4 Процедура *backup*-а архиве

PURS CA спроводи одговарајућу процедуру *backup*-а архиве.

5.5.5 Систем сакупљања записа

Спроводи се одговарајући систем скупљања записа који се архивирају.

5.5.6 Процедуре за добијање и верификацију информација из архиве

PURS CA чува записе у електронској или папирној форми. *PURS CA* може захтијевати од *RA*, корисника или њихових овлашћених лица да доставе одговарајућа документа у циљу провјере испуњености овог захтјева. Ови записи могу бити чувани у електронској, папирној и у било којој другој форми за коју *PURS CA* сматра да је одговарајућа.

5.6 Измјена кључева

PURS CA посједује процедуру, детаљно описану у интерним правилима, која се спроводи у случају истека цертификата цертификационог тијела или опозива цертификата цертификационог тијела у складу са условима дефинисаним у овој *CPS*. У оба случаја, врши се генерисање новог пара кључева церитификационог тијела и дистрибуција цертификата *CA* свим корисницима и заинтересованим странама, као и у случају првог генерисаног цертификата *CA*.

5.7 Компромитација и опоравак у случају катастрофе

5.7.1 Процедуре за поступање у инцидентним и компромитујућим ситуацијама

У интерним правилима рада, *PURS CA* документује процедуре које треба извршити при рјешавању инцидената, као и извјештавања у вези са евентуалном компромитацијом кључева *CA*.

5.7.2 Рачунарски ресурси, софтвер или подаци који су оштећени

PURS CA, такође, документује процедуре опоравка које се користе уколико су рачунарски ресурси, софтвер, и/или подаци неисправни или се сумња да су неисправни.

5.7.3 Процедуре које се спроводе код компромитације приватног кључа корисника

Врши се опозив компромитованог електронског цертификата и издавање новог са новим паром кључева.

5.7.4 Могућности континуитета пословања након катастрофе

План континуитета пословања се имплементира да осигура наставак пословања након природне или друге катастрофе и описан је у интерним правилима *PURS CA*.

5.8 Завршетак рада *CA* или *RA*

Прије него што прекине своје активности пружања цертификационих услуга, *PURS CA*:

- Обезбјеђује својим корисницима који имају валидне цертификате обавјештење о намјери да престаје са пружањем цертификационе услуге, тј. да престане да извршава активности у својству *CA*,
- Опозива све цертификате који су још увек валидни (тј. оне који нису опозвани или им је истекао рок важности) након обавјештења, а без захтјева за сагласношћу корисника,
- Правовремено обавјештава о опозиву цертификата све кориснике на које се то односи,
- Предузима мјере у циљу заштите записа које чува у складу са *CPS*,
- Уколико је то могуће, обезбјеђује одговарајуће мјере обезбјеђења сукцесије у смислу поновног издавања цертификата од стране другог *CA* које је сукцесор.

У случају прекида рада одређеног шалтера *RA* тијела, *PURS CA*:

- Преноси комплетну документацију, папирну и електронску, насталу радом датог шалтера *RA* у централно *RA* тијело у оквиру *PURS CA*,
- *PURS CA* врши надзор свих записа рада *RA* оператера, и цертификате за које постоји нерегуларност у раду *RA* тијела опозива,
- Укида овлашћења свим *RA* оператерима за овлашћену дужност у *PURS CA* систему,
- Ажурира јавно доступан списак шалтера *RA* тијела *PURS CA* система на репозиторијуму *http://ca.poreskaupravars.org* .

6 ТЕХНИЧКЕ БЕЗБЈЕДНОСНЕ КОНТРОЛЕ

Ово поглавље дефинише техничке безбједносне мјере које примјењује *PURS CA* у циљу заштите криптографских кључева и активационих података (једнократни активациони код, …). Безбједносно управљање кључевима је критично у циљу осигурања да су сви кључеви и активациони подаци заштићени и да се користе искључиво од стране ауторизованих запослених.

Такође, дефинисане су и друге техничке безбједносне контроле које се користе од стране *PURS CA* да се безбједно извршавају функције генерисања кључева, корисника, регистрације корисника, издавања цертификата, опозива цертификата, аудитинга и архивирања. Техничке контроле укључују животни циклус безбједносних контрола као и оперативне безбједносне контроле.

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

6.1 ГЕНЕРИСАЊЕ И ИНСТАЛАЦИЈА АСИМЕТРИЧНОГ ПАРА КЉУЧЕВА

6.1.1 Генерисање асиметричног пара кључева

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

6.1.2 Испорука приватног кључа кориснику

Уручење електронског цертификата врши се путем *on-line* репозиторијума *http://ca.poreskaupravars.org.* Издати цертификат од стране *PURS CA* сматра се прихваћеним од стране корисника уколико је корисник преко *on-line* репозиторијума *http://ca.poreskaupravars.org* коришћењем једнократног кода преузео електронски цертификат. Овим путем преузима се и приватни кључ.

6.1.3 Достава јавног кључа издаваоца цертификата трећим странама

PURS CA доставља своје јавне кључеве *Root* и *Issuing CA* тијела у облику *X.509v3* електронских цертификата на свом јавно доступном репозиторијуму *http://ca.poreskaupravars.org.*

6.1.4 Дужине кључева

За потребе свог *Root CA* приватног кључа и одговарајуће потписивање, *PURS CA* користи *SHA-256/RSA* комбинацију *hash* и асиметричног алгоритма. Дужина *RSA* кључа је 4096 бита. Период валидности *Root* цертификата је 30 година. Период валидности издатих цертификата *Issuing CA* је до 20 година.

За свој *Issuing CA* приватни кључ и одговарајући алгоритам за електронско потписивање, *PURS CA*1 користи *SHA-256/RSA* комбинацију hash и асиметричног алгоритма. Дужина *RSA* кључа је 4096 бита. Период валидности цертификата *Issuing CA* тијела је 20 година. Период валидности издатих електронских цертификата је до 5 година.

6.1.5 Намјена кључа (*Key Usage*)

Root CA тијело има намјену кључа за *Certificate Signing, CRL Signing.*

Издавајуће *CA* тијело има намјену кључа за *Certificate Signing, CRL Signing.*

Електронски цертификат има намјену кључа за *Digital Signature, Non-Repudiation*.

6.2 Заштита приватног кључа

PURS CA користи одговарајуће криптографске уређаје, криптографске софтверске компоненте и криптографске механизме у циљу реализације задатака управљања кључевима *CA*.

Генерисање приватног кључа *PURS ROOT CA* и *PURS CA*1 захтијева спровођење одговарајућих контрола од стране више запослених са поверљивим дужностима. Ауторизација процедуре генерисања кључева се мора извршити од стране више од једног члана управне структуре *PURS CA*.

Хардверски и софтверски механизми који штите приватне кључеве *CA* су документовани у интерним правилима рада.

Опрема и уређаји на којима је изграђен систем *PURS CA* не смију да напуштају *PURS CA* просторије изузев ријетких прилика, као што је унапријед дефинисано премјештања или пресељење. *PURS CA* чува записе у вези свих тих премјештања или пресељења.

Приватни кључ *PURS ROOT CA* и *PURS CA1* се не обнавља.

PURS ROOT CA и *PURS CA1* приватни кључ се *backup-yje* у складу са процедуром дефинисаном у *CPS* документу.

Приватни кључ *PURS ROOT CA* и *PURS CA1* ће бити уништен на крају свог животног циклуса. Уништавају се и *backup* копије.

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

6.3 Други аспекти управљања паром кључева

6.3.1 Архивирање јавног кључа

PURS ROOT CA и *PURS CA1* архивирају свој сопствени јавни кључ.

6.3.2 Периоди валидности цертификата и приватног кључа

Вријеме валидности *PURS CA Root CA* електронског цертификата је 30 (тридесет) година.

Вријеме валидности *PURS CA Issuing CA* електронског цертификата је 20 (двадесет) година

Вријеме валидности електронског цертификата је 5 (пет) година.

6.4 Активациони подаци

PURS CA безбједно процесира активационе податке придружене приватним кључевима *CA*, као и свим другим приватним кључевима у датом *PKI* систему (*Root CA*, *Issuing CA*, *RA* и *CA* Операторима, корисници).

6.5 Безбједносне контроле рачунара

PURS CA имплементира безбједносне контроле над рачунарима који се користе у оквиру *PURS CA PKI* система.

6.5.1 Специфични захтјеви за безбједност рачунара

Рачунари који се користе за *PURS CA* чувају се у посебно заштићеним просторијама.

6.5.2 Рангирање безбједности рачунара

Није примјењиво.

6.6 Животни циклус техничких безбједносних контрола

PURS CA реализује контроле периодичног развоја система и управљања безбједношћу система у складу са *ISO 27001* стандардом.

6.7 Мрежне безбједносне контроле

PURS CA одржава и примјењује висок ниво система мрежне безбједности, укључујући примјену *firewall* уређаја.

6.8 Временски жиг

Временски жиг се користи само за интерни оперативни рад *PURS CA*.

7 ПРОФИЛИ ЦЕРТИФИКАТА И *CRL* ЛИСТА

Ово поглавље специфицира формате цертификата и *CRL* листа које издаје *PURS CA*.

7.1 ПРОФИЛИ ЦЕРТИФИКАТА

PURS CA издаје сљедеће врсте цертификата:

- *Root CA* тијело,
- *Issuing CA* тијело,
- Електронски цертификат за кориснике.

7.1.1 *Root CA* тијело

Polja Verzije1	Vrijednost
Version	*V3*
Serial Number	*20 hex karaktera bez vodećih nula*
Signature Algorithm	*Sha256RSA*
Signature hash algorithm	*Sha256*
Issuer	*CN = PURS ROOT CA, O = Poreska uprava, ST = Republika Srpska, C = BA*
Valid From	*UTC datum i vrijeme*
Valid To	*UTC datum i vrijeme + 30 godina*
Subject	*CN = PURS ROOT CA, O = Poreska uprava, ST = Republika Srpska, C = BA*
Public Key	*4096bit*
Polja Ekstenzije	Vrijednost
Key Usage (Critical)	*Certificate Signing, CRL Signing (06)*
Basic Constraints (Critical)	*Subject Type=CA* *Path Length Constraint=1*
Enhanced Key Usage	*Nema*
Application Policies	*Nema*
Certificate Policies	*Nema*
Qualified Certificate Statements	*Nema*
Subject Key Identifier	*40 hex karaktera* *Hash vrijednost PublicKey – koristi se za konstrukciju putanje sertifikata*
Authority Key Identifier	*Nema*
CRL Distribution Points	*Nema*
Authority Information Access	*Nema*
Subject Alternate Name	*Nema*
Polja Atributa	Vrijednost
Thumbprint algorithm	*Sha1*
Thumbprint	*40 hex karaktera*
Frendly Name	*PURS ROOT CA*

7.1.2 *PURS CA* 1

Polja Verzije1	Vrijednost

Version	*V3*
Serial Number	*20 hex karaktera bez vodećih nula*
Signature Algorithm	*Sha256RSA*
Signature hash algorithm	*Sha256*
Issuer	*CN = PURS ROOT CA, O = Poreska uprava, ST = Republika Srpska, C = BA*
Valid From	*UTC datum i vrijeme*
Valid To	*UTC datum i vrijeme + 20 godina*
Subject	*CN = PURS CA 1, O = Poreska uprava, ST = Republika Srpska, C = BA*
Public Key	*4096bit*
Polja Ekstenzije	Vrijednost
Key Usage (Critical)	*Certificate Signing, CRL Signing (06)*
Basic Constraints (Critical)	*Subject Type=CA* *Path Length Constraint=0*
Enhanced Key Usage	*Nema*
Application Policies	*Nema*
Certificate Policies	*Policy Identifier=All issuance policies*
Qualified Certificate Statements	*Nema*
Subject Key Identifier	*40 hex karaktera* *Hash vrijednost PublicKey – koristi se za konstrukciju putanje sertifikata*
Authority Key Identifier	*KeyID=40 hex karaktera* *Način identifikovanja javnog ključa čijim privatnim ključem je potpisan sertifikat = Subject Key Identifier Issuer-a*
CRL Distribution Points	*http putanja do CRL liste Root CA na http://ca.poreskaupravars.org repozitorijumu*
Authority Information Access	*http putanja do fajla Root CA sertifikata na http://ca.poreskaupravars.org repozitorijumu*
Subject Alternate Name	*Nema*
Polja Atributa	Vrijednost
Thumbprint algorithm	*Sha1*
Thumbprint	*40 hex karaktera*
Frendly Name	*PURS CA 1*

7.1.3 Електронски цертификат за правна лица/предузетнике

Polja Verzije1	Vrijednost
Version	*V3*
Serial Number	*20 hex karaktera bez vodećih nula*
Signature Algorithm	*Sha256RSA*
Signature hash algorithm	*Sha256*
Issuer	*CN = PURS CA 1, O = Poreska uprava, ST = Republika Srpska, C = BA*
Valid From	*UTC datum i vrijeme*
Valid To	*UTC datum i vrijeme + 5 godina*
Subject	*CN=prezime ime JIK, OU="Pravno lice", O=JIB company name, ST=Republika Srpska, C=BA*
Public Key	*2048bit*
Polja Ekstenzije	Vrijednost

Key Usage (Critical)	*Digital Signature, Non-Repudiation (c0)*
Enhanced Key Usage	*Nema*
Application Policies	*Nema*
Certificate Policies	*Nema*
Qualified Certificate Statements	*Nema*
Subject Key Identifier	*40 hex karaktera* *Hash vrijednost PublicKey – koristi se za konstrukciju putanje sertifikata*
Authority Key Identifier	*KeyID=40 hex karaktera* *Način identifikovanja javnog ključa čijim privatnim ključem je potpisan sertifikat = Subject Key Identifier Issuer-a*
CRL Distribution Points	*http putanja do CRL liste Issuing CA na http://ca.poreskaupravars.org repozitorijumu*
Authority Information Access	*http putanja do fajla Issuing CA sertifikata na http://ca.poreskaupravars.org repozitorijumu*
Subject Alternate Name	*Nema*
Polja Atributa	*Vrijednost*
Thumbprint algorithm	*Sha1*
Thumbprint	*40 hex karaktera*
Frendly Name	*PURS CA 1*

7.1.4 Електронски цертификат за физичка лица

Polja Verzije1	Vrijednost
Version	*V3*
Serial Number	*20 hex karaktera bez vodećih nula*
Signature Algorithm	*Sha256RSA*
Signature hash algorithm	*Sha256*
Issuer	*CN = PURS CA 1, O = Poreska uprava, ST = Republika Srpska, C = BA*
Valid From	*UTC datum i vrijeme*
Valid To	*UTC datum i vrijeme + 5 godina*
Subject	*CN=prezime ime JIK, OU="Fizicko lice", ST=Republika Srpska, C=BA*
Public Key	*2048bit*
Polja Ekstenzije	Vrijednost
Key Usage (Critical)	*Digital Signature, Non-Repudiation (c0)*
Enhanced Key Usage	*Nema*
Application Policies	*Nema*
Certificate Policies	*Nema*
Qualified Certificate Statements	*Nema*
Subject Key Identifier	*40 hex karaktera* *Hash vrijednost PublicKey – koristi se za konstrukciju putanje sertifikata*
Authority Key Identifier	*KeyID=40 hex karaktera* *Način identifikovanja javnog ključa čijim privatnim ključem je potpisan sertifikat = Subject Key Identifier Issuer-a*
CRL Distribution Points	*http putanja do CRL liste Issuing CA na http://ca.poreskaupravars.org repozitorijumu*

Authority Information Access	*http putanja do fajla Issuing CA sertifikata na http://ca.poreskaupravars.org repozitorijumu*
Subject Alternate Name	*Nema*
Polja Atributa	Vrijednost
Thumbprint algorithm	*Sha1*
Thumbprint	*40 hex karaktera*
Frendly Name	*PURS CA 1*

7.2 Профил *CRL* листе

PURS CA подржава издавање *CRL* листа које су у сагласности са сљедећим условима:

- Бројеви верзија су подржани за *CRL* листе,
- *CRL* и *CRL* екстензије су попуњене и њихова критичност је посебно назначена.

PURS CA издаје *CRL* верзије 2 са основним пољима и екстензијама.

Опозвани цертификати којима је истекла временска валидност не налазе се у *CRL* листи.

7.2.1 Profil *CRL* листе *PURS ROOT CA*

Polja	Vrijednost
Version	*V2*
Issuer	*CN = PURS ROOT CA, O = Poreska uprava, ST = Republika Srpska, C = BA*
Signature Algorithm	*Sha256RSA*
Signature hash algorithm	*Sha256*
Effective Update	*UTC datum i vrijeme*
Next Update	*UTC datum i vrijeme + 26 sedmica*
CRL Number	*Redni broj*
Authority Key Identifier	*KeyID=hash javnog ključa CA tijela koje potpisuuje CRL listu*
Revocated Certificate	*Serial Number* *UTC datum i vrijeme opoziva* *razlog opoziva*

7.2.2 Profil *CRL* листе *PURS CA* 1

Polja	Vrijednost
Version	*V2*
Issuer	*CN = PURS CA 1, O = Poreska uprava, ST = Republika Srpska, C = BA*
Signature Algorithm	*Sha256RSA*
Signature hash algorithm	*Sha256*
Effective Update	*UTC datum i vrijeme*
Next Update	*UTC datum i vrijeme + 1 dan*
CRL Number	*Redni broj*
Authority Key Identifier	*KeyID=hash javnog ključa CA tijela koje potpisuuje CRL listu*
Revocated Certificate	*Serial Number* *UTC datum i vrijeme opoziva*

	razlog opoziva

7.3 *OCSP* ПРОФИЛ

OCSP сервис се не користи.

8 ПРОВЈЕРА САГЛАСНОСТИ СА ПОЛИТИКОМ ЦЕРТИФИКАЦИЈЕ

PURS CA прихвата периодичну провјеру сагласности својих политика, укључујући *CPS* што укључује и периодичну супервизију од стране надлежног органа Републике Српске.

У домену издавања електронских церификата, *PURS CA* ради у оквиру ограничења дефинисаних у оквиру Закона о електронском потпису Републике Српске, као и одговарајућим подзаконским актима.

PURS CA прихвата под одређеним условима и контролу интерних процедура и правила рада која нису јавно доступна у циљу унапрјеђења својих услуга. *PURS CA* евалуира резултате оваквих провјера пре него што их имплементира.

PURS CA спроводи редовне годишње интерне audit-е усклађености пословања са *CPS*, као и са *CP* документом. Интерни аудит спроводе одговарајући запослени Пореске управе Републике Српске са датим задужењима. У случају неусаглашености рада са Политиком цертификације, *PURS CA* обуставља даље издавање електронских цертификата, осим пробних, док се не отклони неусаглашеност.

9 ДРУГИ ПОСЛОВНИ И ПРАВНИ АСПЕКТИ

9.1 ЦИЈЕНЕ

9.1.1 Цијена издавања или обнове цертификата

PURS CA не наплаћује издавање и обнову електронских цертификата.

9.1.2 Цијена приступа цертификатима

Ово поглавље није примјенљиво у оквиру *CPS*.

9.1.3 Цијена приступа информацијама о статусу цертификата

Приступ регистру опозваних цертификата (*CRL*) је бесплатан.

9.1.4 Цијене за друге сервисе

Ово поглавље није примјенљиво у оквиру *CPS*.

9.1.5 Политика повраћаја новца

Ово поглавље није примјенљиво у оквиру *CPS*.

9.2 ФИНАНСИЈСКА ОДГОВОРНОСТ

9.2.1 Покривање осигурања

Ово поглавље није примјенљиво у оквиру *CPS*.

9.2.2 Осигурање или гаранцијско покривање за кориснике

Корисник је дужан да надокнади штету причињену *PURS CA* у односу на било које активности или пропусте у одговорности, било које губитке или штету, као и за било какве трошкове било које врсте, које би *PURS CA* могао да има као резултат:

- Било ког лажног или погрешно презентованог податка достављеног од стране корисника,
- Било ког пропуста корисника да достави материјалну чињеницу да је погрешна презентација или пропуст учињен из немарности или са намером да се превари *PURS CA*, или било које лице које прима и односи се према добијеном цертификату.
- Необезбјеђивања одговарајуће заштите корисниковог приватног кључа, некоришћења безбједног система како је захтијевано, или неизвршења одговарајућих превентивних мјера неопходних да се спријечи компромитација, губитак, објављивање, модификација или неауторизовано коришћење корисниковог приватног кључа, или напада на интегритет *PURS ROOT CA* и *PURS CA*1 приватних кључева,
- Кршења било којих закона који су примјенљиви, укључујући оне који се односе на заштиту интелектуалних права, вирусе, приступ рачунарским системима, итд.

9.3 ПОВЈЕРЉИВОСТ ПОСЛОВНИХ ИНФОРМАЦИЈА

9.3.1 Опсег повјерљивих информација

Цертификационо тијело *PURS CA* поступа повјерљиво са сљедећим подацима:

- Са свим захтјевима за добијање електронског цертификата или других услуга,
- Све могуће повјерљиве податке везане за финансијске обавезе,
- Све могуће повјерљиве податке који представљају предмет међусобних уговора са трећим лицима и
- Све остале податке који су наведени у интерним правилима рада цертификационог тијела *PURS CA*.

9.3.2 Информације које нису у опсегу поверљивих информација

Цертификационо тијело *PURS CA* јавно објављује само оне пословне податке који нису повјерљиве природе, а у складу са важећим законодавством.

9.3.3 Одговорност за заштиту поверљивих информација

Цертификационо тијело *PURS CA* не преузима никакве одговорности за садржај података које власник електронског цертификата електронски потписује. Такође, *PURS CA* не преузима никакве одговорности за питања да ли су власник или треће лице поштовали све важеће прописе, све одредбе политике цертификације и других правила цертификационог тијела *PURS CA*, односно водили рачуна о свим објављеним упутствима.

Цертификационо тијело *PURS CA* не преузима никакве одговорности за посљедице до којих долази уколико власник електронског цертификата није поступао у складу са сигурносним захтјевима из поглавља 5 овог *CPS* документа.

9.4 ПРИВАТНОСТ И ЗАШТИТА ЛИЧНИХ ИНФОРМАЦИЈА

9.4.1 План приватности

PURS CA се придржава правила заштите приватности личних података и правила повјерљивости како је прописано у *CPS* документу, као и у одговарајућим законским и подзаконским актима.

9.4.2 Информације које се третирају као приватне

Лични подаци који се чувају су сви лични подаци које цертификационо тијело *PURS CA* прикупи у оквиру захтјева за своје услуге или у одговарајућим регистрима за доказивање идентитета власника.

9.4.3 Информације које се не сматрају приватним

PURS CA цертификационо тијело не сматра приватним искључиво оне информације корисника за које је сам корисник дао сагласност да се могу публиковати.

PURS CA у процесу регистрације правног лица/предузетника и припадника правног лица/предузетника прикупља идентификационе податке. Идентификациони подаци правног лица/предузетника као што су назив и ЈИБ наћи ће се на електронском цертификату у пољу

Organization. Идентификациони подаци физичког лица и припадника правног лица/предузетника као што су Име и Презиме наћи ће се на електронском цертификату у пољу *Common Name*.

9.4.4 Одговорност за заштиту приватних информација

PURS CA је одговорно за заштиту приватности корисникових информација прикупљених у оквиру захтјева за своје услуге или у одговарајућим регистрима за доказивање идентитета власника.

9.4.5 Обавјештење и сагласност за коришћење приватних информација

PURS CA цертификационо тијело дефинише услове у вези објављивања приватних информација за које дати корисник треба да да сагласност и ти су услови наведени у Закону о пореском поступку Републике Српске и Закону о заштити личних података.

Власник овлашћује цертификационо тијело *PURS CA* за коришћење личних података који се налазе на захтјеву за добијање електронских цертификата, у складу са Законом о пореском поступку Републике Српске и Законом о заштити личних података.

9.4.6 Откривање информација сходно правним и административним процесима

PURS CA не објављује, нити се захтијева да објављује, било коју повјерљиву информацију без аутентикованог и потврђеног захтјева од стране:

- Саме стране за коју се таква информација и чува,
- Надлежног суда.

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

9.5 Права интелектуалног власништва

ПУРС поседује и задржава сва права интелектуалног власништва придружена његовим базама података, *web* сајтовима, електронским цертификатима које издаје, као и било којим другим публикацијама које на било који начин припадају или потичу од стране *PURS CA*, укључујући и ову *CPS*.

PURS CA омогућава корисницима и трећим странама да користе, копирају, дистрибуирају и у своје електронске документе уграђују издате електронске цертификате, *CRL* листе.

9.6 Изјава о гаранцији

Ово поглавље није примјенљиво у оквиру *CPS*.

9.7 Непризнавање гаранције

Ово поглавље није примјенљиво у оквиру *CPS*.

9.8 Ограничења одговорности

PURS CA не прихвата било какву другу одговорност осим оне која је експлицитно дефинисана у овом документу.

PURS CA није одговорна за:

- коришћење електронских цертификата за намјене и на начин који није изричито предвиђен у политици цертификације и *CPS* документу,
- неправилног или погрешног обезбјеђења лозинки или приватних кључева власника електронског цертификата, откривање повјерљивих података или кључева трећим лицима и неодговорног поступања власника електронског цертификата,
- злоупотребе односно упада у информациони систем власника електронског цертификата и на тај начин доласка до података о електронским цертификатима од стране неовлашћених лица,
- непоступања или лошег поступања са подацима у оквиру информационе инфраструктуре власника електронског цертификата или трећих лица,
- непровјеравања података и валидности (статуса повучености) електронских цертификата у регистру опозваних електронских цертификата,
- непровјеравања времена валидности електронских цертификата,
- поступања власника електронског цертификата или трећег лица супротно информацијама и обавјештењима које објављује цертификационо тијело *PURS CA*, Политиком цертификације, *CPS* документом и другим прописима,
- омогућеног коришћења односно злоупотребе власниковог електронског цертификата од стране неовлашћених лица,
- садржај самих података који се потписују коришћењем електронских цертификата, већ само да је код потписа над тим подацима коришћен електронски цертификат *PURS CA*,
- употребе и поузданости рада машинске и програмске опреме власника електронског цертификата.

9.9 Одштете

За штету насталу употребом електронског цертификата и њему придруженог приватног кључа усљед непоштовања одредби уговора, Политике цертификације, Практичних правила рада и важећих закона, одговорна је странка која је исту проузроковала.

9.10 Период важности и крај валидности Политике цертификације

Цертификационо тијело *PURS CA* задржава право да измјени Политику цертификације и овај *CPS* документ и да надогради инфраструктуру без претходног обавјештавања власника електронског цертификата.

Важећи цертификати тако остају важећи до истека њихове валидности и за њих још увек важи онај *CPS* документ који је важио у вријеме њиховог издавања. За све цертификате издате након почетка валидности новог *CPS* документа, важи тај нови.

Овај *CPS* документ ступа на снагу онога дана када је одобрен и објављен од стране цертификационог тијела ПУРС.

9.10.1 Важност

Нова верзија *CPS* документа цертификационог тијела ПУРС претходно се, осам (8) дана прије званичног датума валидности, објављује на *web* страници цертификационог тијела ПУРС са новим идентификационим бројем и означеним датумом почетка валидности.

9.10.2 Крај валидности

Крај валидности *CPS* документа није одређен нити је повезан са периодом валидности електронских цертификата издатих на основу овог *CPS*.

9.10.3 Ефекат завршетка и поновног рада

Приликом објављивања новог *CPS*, сви електронски цертификати издати након тог датума издају се према новом *CPS* документу.

9.11 Појединачна обавјештења и комуникација са учесницима

Контактни подаци цертификационог тијела објављени су на *web* страницама истог и наведени у поглављу 1.2 овог документа.

Контактни подаци корисника прикупљени приликом регистрације користе са само за обавјештавање када процедуре рада *PURS CA* то налажу.

9.12 Исправке

9.12.1 Процедуре за исправку

Промјене или допуне овог *CPS* документа цертификационо тијело може да објави у облику промјена или допуна овог *CPS*.

Измјене се усвајају и прихватају истим поступком као и сама практична правила рада.

9.12.2 Механизам и период обавјештавања

Ово поглавље није примјенљиво у оквиру *CPS*.

9.12.3 Услови промјене објектног идентификатора (*OID*)

Ово поглавље није примјенљиво у оквиру *CPS*.

9.13 Процедуре рјешавања спорова

У случају спорова који се односе на ову *CPS*, стране ће спор ријешити споразумно. Уколико се спор не ријеши на наведени начин, за све евентуалне спорове надлежни су судови у Републици Српској.

9.14 Примјена закона

Овај *CPS* је у потпуности у складу са позитивном законском регулативом Републике Српске и то прије свега са Законом о електронском потпису Републике Српске и одговарајућим подзаконским актима. Сви спорови које се односе на *PURS CA* и/или који се односе на цертификате издате од стране *PURS CA*, ће бити процесуирани од стране надлежног суда у Републици Српској.

9.15 Сагласност са позитивним прописима

Ово поглавље није примјенљиво у оквиру ове *CPS*.

9.16 Друге одредбе

Ово поглавље није примјенљиво у оквиру ове *CPS*.

10 РЕФЕРЕНЦЕ

- Закон о електронском потпису Републике Српске, Службени гласник Републике Српске, бр. 106/2015
- *RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework*
- *RFC 5280 – Request For Comments 5280, Internet X.509 Public Key Infrastructure / Certificate and CRL Profile*
- Практична правила цертификације цертификационог тијела Пореске управе Републике Српске.

ДИРЕКТОР

_____

ЗОРА ВИДОВИЋ