ПРАВИЛНИК

О ПОСЕБНИМ УСЛОВИМА КОЈЕ МОРАЈУ ДА ИСПУЊАВАЈУ ЦЕРТИФИКАЦИОНА ТИЈЕЛА

На основу члана 21. став 2. Закона о електронском потпису Републике Српске („Службени гласник Републике Српске“, број 106/15) и члана 82. став 2. Закона о републичкој управи („Службени гласник Републике Српске“, бр. 118/08, 11/09, 74/10, 86/10, 24/12 и 121/12), министар науке и технологије доноси:

ПРАВИЛНИК О ПОСЕБНИМ УСЛОВИМА КОЈЕ МОРАЈУ ДА ИСПУЊАВАЈУ ЦЕРТИОФИКАЦИОНА ТИЈЕЛА

Члан 1.

Овим правилником прописују се посебни услови које морају испуњавати цертификациона тијела која издају неквалификоване и квалификоване електронске цертификате као и најнижи износ обавезног осигурања којим је цертификационо тијело обавезно да осигура ризик од одговорности за штету која настане обављањем услуга електронске цертификације.

Члан 2.

(1) Цертификационо тијело које издаје неквалификоване електронске цертификате (у даљем тексту: Цертификационо тијело) мора прије почетка обављања услуга утврдити Општа правила давања услуга цертификације која корисницима услуга пружају довољно информација на основу којих могу одлучити о прихватању услуга и у ком обиму.

(2) Општа правила из става 1. овог члана Цертификационо тијело уграђује у документе

1) Политика цертификације (Certificate Policy-CP);

2) Практична правила пружања услуге цертификације (Certification Practices Statement - CPS) (у даљем тексту: Практична правила).

(3) Политика цертификације дефинише предмет рада цертификационог тијела и дефинише захтјеве пословања цертификационог тијела.

(4) Практична правила пружања услуга цертификације дефинишу процесе и начин њиховог коришћења при формирању и управљању електронским цертификатима односно дефинишу оперативне процедуре у циљу испуњења захтјева из Политике сертификације

(5) Практична правила дефинишу начин на који цертификационо тијело испуњава техничке, организационе и процедуралне захтјеве пословања који су идентификовани у Политици цертификације.

(6) Политика сертификације и Практична правила пружања услуге цертификације су јавни документи.

Члан 3.

(1) Политика цертификације и Практична правила пружања услуга цертификације требају бити структуирсани по RFC 3647, односно међународно прихваћеном обрасцу ETSI EN 319 411-2 – Policy Requirements for Certification Authorities Issuing Qualified Certificates.

(2) Обавезан садржај документације коју цертификационо тијело мора израдити прије почетка обављања услуга цертификације налази се у прилогу 1. овог Правилника.

Члан 4.

(1) Цертификационо тијело које издаје квалификоване електронске цертификате (у даљем тексту: Квалификовано цертификационо тијело) мора донијети и додатни скуп правила (интерна правила) којима се осигурава исправно провођење заштитних и безбједносних мјера у систему цертификације.

(2) Интерна правила уређују допунски:

1) поступке приступа и кретања кроз пословни простор квалификованог цертификационог тијела,

2) поступке и технике допунске заштите информационог система, употребе телекомуникационе опреме/система у радњама са подацима у систему цертификације,

3) поступке и радње у ванредним ситуацијама, посебно код пожара и других непогода, непредвидивих упада у физички простор (сједиште) квалификованог цертификационог тијела, односно упада у информациони систем,

4) правила вођења евиденције о присуству запослених у систему цертификације и приступа систему цертификације.

(3) Интерна правила представљају пословну тајну квалификованог цертификационог тијела.

Члан 5.

У случајевима приговора у вези одступања садржаја услуга у односу на утврђена правила садржана у документацији цертификационог тијела, одговорно лице цертификационог тијела дужно је отклонити одступања.

Члан 6.

(1) Квалификовано цертификационо тијело мора примјењивати смјернице Европске уније те Европске норме (ЕН) које се односе на поступке осигуравања и заштите опреме и простора.

(2) Квалификовано цертификационо тијело мора обављање услуга прилагодити новим нормама, одлукама и препорукама из става 1. овог члана, које се доносе након добијања дозволе.

(3) Испуњење одређеног услова из става 1. овог члана може услиједити и послије добијања дозволе, а прије почетка обављања дјелатности, нарочито ако се ради о већим улагањима у специјализовани простор или опрему, или се ради о запошљавању одређених стручних лица.

(4) У том случају, уз захтјев за добијање дозволе потребно је приложити и увјерљив доказ из којег је видљиво да је могуће испунити услов у предложеном року.

Члан 7.

(1) Квалификовано цертификационо тијело мора услугу цертификације за коју је добило дозволу обављати својим средствима за рад и са радницима који су у сталном радном односу.

(2) Поступке у вези са софистицираном опремом (хардвер, софтвер) који се могу провести једино од стране произвођача те опреме, Квалификовано цертификационо тијело може обавити уз одговарајуће учешће запослених код произвођача те опреме и уз помоћ њихове опреме.

Члан 8.

(1) Квалификовано цертификационо тијело мора за обављање услуга цертификације имати пословни простор у свом власништву или у најму на рок од најмање годину дана од дана подношења захтјева.

(2) Пословни простор мора бити задовољавајуће величине за смјештај опреме и рад особља које обавља услуге цертификације.

(3) Квалификовано цертификационо тијело мора послове генерисања криптографских кључева и израде цертификата проводити у специјализованом простору издвојеном за ту намјену.

(4) Приступ простору у којем се спроводе радње из става 3. овог члана могу имати само овлашћене особе, и о сваком приступу простору се мора водити одговарајућа евиденција.

Члан 9.

(1) Цертификационо тијело мора за машинску и програмску опрему којом обавља услуге цертификације примјењивати домаће норме, норме Европског института за телекомуникационе норме (ETSI), те одлуке и препоруке RFC групе, као и ISO протоколе и норме.

(2) Цертификационо тијело мора обезбједити физичку заштиту машинске опреме те проводити стални надзор приступа рачунарским ресурсима и физичком простору гдје су смјештени ресурси система цертификације.

(3) Приступ се може проводити искључиво уз присуство најмање два овлашћена лица који имају приступ информационом систему цертификационог тијела.

(4) Квалификовано цертификационо тијело мора обезбједити да само лица која раде у систему цертификације имају приступ простору гдје се налазе ресурси система цертификације.

Члан 10.

Информациони систем Квалификованог цертификационог тијела мора за основу имати софтверску и хардверску инфраструктуру намјењену искључиво за послове цертификације.

Члан 11.

(1) Квалификовано цертификационо тијело мора опрему за овјеру и дјеловање система цертификације ускладити са техничким стандардом FIPS 140-2, односно са најбољим праксама из ISO/IEC 15408-1:2009 норми.

(2) Квалификовано цертификационо тијело мора поступке и облике заштите система за цијело вријеме пружања услуга цертификације усклађивати са тренутно важећим препорукама и нормама у области заштите и безбједности дјеловања информационих средстава и система.

Члан 12.

(1) Особље запослено у систему цертификације спроводи послове и оперативне задатке у систему цертификације кроз одвојене организационе јединице (службе, одјељења и слично) за управљање информационим системом, системом управљања цертификатима, пословима заштите и контроле те пословима правне заштите и надзора дјеловања цертификационог система.

(2) Квалификовано цертификационо тијело мора у сталном радном односу имати:

1) најмање два стручњака са високом стручном спремом техничког, природноматематичког или информатичког усмјерења, специјализованих за рад са криптографским технологијама,

2) најмање два стручњака, минимално средње стручне спреме, специјализована за рад на заштити рачунарских система и информационих система, обучена за рад са системима за издавање, опозив и одржавање електронских цертификата,

3) најмање једног дипломираног правника са познавањем система заштите личних података, употребе и правне примјене електронског потписа.

Члан 13.

(1) Запослено особље цертификационог тијела мора имати стручна знања у раду са технологијом цертификације, као и за поступке заштите рачунарске опреме и програма у примјењеном систему цертификације те осигурано трајно усавршавање знања и вјештина потребних за рад у систему цертификације.

(2) Запосленици код једног цертификационог тијела не смију бити у радном односно пословном односу са другим цертификационом тијелом.

Члан 14.

(1) Цертификационо тијело мора располагати финансијским ресурсима који осигуравају несметано пружање услуга цертификације независно од броја корисника услуга и за цијело вријеме обављања дјелатности.

(2) Цертификационо тијело мора имати властити пословни рачун и гаранцију пословне банке на текуће пословање видљиво кроз јавно доступан годишњи пословни извјештај.

Члан 15.

Цертификационо тијело мора осигурати јединственост података за овјеру електронског потписа на начин који омогућава недвосмислено утврђивање (идентитета) потписника.

Члан 16.

(1) Квалификовано цертификационо тијело дужно је израдити јединствени систем заштите и сигурности обављања услуга.

(2) У сврху извођења и одржавања јединственог система заштите и сигурности обављања услуга цертификације Квалификовано цертификационо тијело израђује интерни Правилник о провођењу заштите система цертификације.

Члан 17.

(1) Квалификовано цертификационо тијело мора прије почетка обављања услуга, након значајнијих промјена у систему за вријеме обављања услуга, те редовно сваке године проводити на основу израђеног Правилника о провођењу заштите система цертификације, провјеру свих дијелова система у односу на сигурност, поузданост и квалитет дјеловања.

(2) Највећи временски размак између два поступка провјере не може бити дужи од једне године.

(3) Квалификовано цертификационо тијело може наставити пружати услуге цертификације ако се утврди да је систем усклађен са захтјевима садржаним у Правилнику о провођењу заштите система цертификације.

Члан 18.

Квалификовано цертификационо тијело мора за послове заштите система цертификације запослити квалификована лица за сљедеће послове заштите:

1) контрола физичког приступа рачунарској опреми,
2) уградња и конфигурација програмског склопа заштите као и системско мијењање криптографских кључева,
3) анализа рада у свим фазама рада, биљежење и архивирање тих података те обавјештавање,
4) управљачке функције и операције отклањања проблема у функционисању прописаних мјера заштите,
5) извјештавање о покушајима нарушавања прописаних мјера заштите те идентификација субјеката који проводе нарушавање.

Члан 19.

Провјера се мора провести најмање за ова подручја:

1) систем цертификације (информацијски систем),
2) технологија криптозаштите,
3) радни простор те рачунарска и мрежна опрема,
4) релевантни законски и други прописи у Републици Српској и Европи

Члан 20.

(1) Квалификовано цертификационо тијело мора рад са рачунаром и програмском опремом повјерити само лицима обученим за руковање опремом уграђеном у систем цертификације.

(2) Квалификовано цертификационо тијело мора физички приступ рачунарском систему којим се проводе услуге цертификације омогућити само оперативним запосленицима који изравно раде са рачунарским системом.

(3) Лица која чисте простор у коме се налази рачунарски систем, могу то радити искључиво у вријеме присуства оперативних лица.

(4) У случају неовлаштеног приступа рачунарској и програмској опреми односно информационом систему, цертификационо тијело мора зауставити нормалан рад и проводити мјере предвиђене за рад у ванредним околностима све до потпуног откривања узрока те отклањања могућих штета.

(5) Централни рачунарски систем мора имати осигурано трајно напајање енергијом уз потребно радно окружење као што је степен влажности и топлоте, дозвољен степен зрачења и остале вриједности специфичне за рачунарски систем у употреби.

(6) Рачунарски систем мора бити смјештен на мјесту које је осигурано од поплаве уз адекватну противпожарну заштиту.

Члан 21.

(1) Квалификовано цертификационо тијело дужно је осигурати ризик од одговорности за штете које настану обављањем услуга цертификације.

(2) Осигурање садржано у ставу 1. овог члана представља обавезно осигурање.

(3) Најнижи износ на који Квалификовано цертификационо тијело, изузев носиоца послова електронске цертификације за органе републичке управе, мора осигурати одговорност за штете износи 500.000 конвертибилних марака (КМ).

Члан 22.

Ступањем на снагу овог Правилника престаје да важи Правилник о мјерама заштите електронског потписа и квалификованог електронског потписа, најнижем износу обавезног осигурања и примјени организационих и техничких мјера заштите цертификата („Службени гласник Републике Српске“, број 88/09, 127/11).

Члан 23.

Овај Правилник ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Српске“.

Број:
Датум:

МИНИСТАР
Проф. др Јасмин Комић

Прилог 1.

Назив секције	Садржај секције
Уводне напомене и детаљни подаци	Опис услуга Идентификациони подаци Корисници и подручје примјене услуга Подаци о сједишту
Опште одредбе	Обавезе овјериоца, потписника и корисника Одговорност Финансијска одговорност Усклађеност са законом Накнада за услуге Објава и репозиторијум цертификата Провјера усклађености Повјерљивост и тајност (пословања и података) Заштита интелектуалне својине (ауторско дјело)
Идентификација и потврда идентитета корисника	Регистрација потписника Планско обнављање цертификата Обнављање након опозива Захтјев за опозив цертификата
Основна правила у раду са цертификатима	Примање захтјева за издавање цертификата Издавање цертификата Достављање/прихват цертификата Опозив цертификата Поступци провјере безбједносних мјера Архивирање цертификата и података Замјена цертификата Поступци отклањања посљедица изазваних штетом и незгодама Престанак рада/пружања услуга
Контрола безбједности опреме, поступака и особља	Контрола простора, опреме и средстава Контрола поступака и провођење радних задатака Контрола особља – број запослених, стручност, овлашћења
Контрола техничке сигурности рада система цертификације	Израда властитог цертификата Заштита података за израду властитог електронског потписа Управљање подацима за израду електронског потписа Подаци за приступ потпису овјериоца Контрола безбједности рачунарског система Контрола безбједности радног вијека система Контрола безбједности мрежног система

	Контрола безбједности криптографских модула
Садржај цертификата и листа опозваних цертификата	Садржај (образац) цертификата Садржај листе опозваних цертификата
Управљање документацијом	Поступци код промјене садржаја документације Објављивање документације Поступци прихватања/одобравања документације