РЕПУБЛИКА СРПСКА
ВЛАДА
МИНИСТАРСТВО НАУКЕ И ТЕХНОЛОГИЈЕ

ПРАВИЛНИК О МЈЕРАМА И ПОСТУПЦИМА УПОТРЕБЕ, ЗАШТИТЕ И СРЕДСТАВА ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА И КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПОТПИСА И СИСТЕМА ЦЕРТИФИКАЦИЈЕ И ОБАВЕЗНОГ ОСИГУРАЊА ПРУЖАЛАЦА УСЛУГА ИЗДАВАЊА КВАЛИФИКОВАНИХ ЦЕРТИФИКАТА

Бања Лука, јули 2009. године

На основу члана 7. став 2., члана 11. став 4. и члана 32. став 2. Закона о електронском потпису Републике Српске („Службени гласник Републике Српске“, број 59/08) и члана 82. став 2. Закона о републичкој управи („Службени гласник Републике Српске“, број 118/08), министар науке и технологије д о н о с и

ПРАВИЛНИК
о мјерама и поступцима употребе, заштите и средстава за израду електронског потписа и квалификованог електронског потписа и система цертификације и обавезног осигурања пружалаца услуга издавања квалификованих цертификата

I ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Овим Правилником утврђују се мјере, поступци и облици заштите електронског потписа и квалификованог електронског потписа, средстава за израду електронског потписа, заштите система цертификације и података о потписницима, поступци провјере идентитета потписника приликом давања електронских цертификата, као и најнижи износ обавезног осигурања изражен у новцу за коју се осигурава ризик од одговорноси за штете који се код пружалаца услуга цертификације који издају квалификоване цертификате појављује као обавезно осигурање.

II ЕЛЕКТРОНСКИ ПОТПИС

Члан 2.

(1) Потписник израђује и користи електронски потпис и квалификовани електронски потпис у складу са општим условима садржаним у чл. 12. и 17. Закона о електронском потпису Републике Српске (у даљем тексту Закон) и овом Правилнику.

(2) Потписник у случајевима коришћења услуга цертификације израђује и користи електронски потпис и у складу са условима које је прихватио од цертификационог тијела.

Члан 3.

(1) Подаци за израду електронског потписа чине саставни дио електронског потписа.

(2) Потписник је дужан да заштити податке за израду електронског потписа од неовлашћеног приступа, отуђивања и неправилне употребе. Заштита се мора додатно проводити примјеном лозинке, биометричким техникама или другим технологијама заштите.

Члан 4.

(1) Подаци за израду електронског потписа морају се у потпуности разликовати од података за овјеру електронског потписа.

(2) Поступак израде електронског потписа не смије измјенити податке који се потписују нити спријечити приказ тих података потписнику прије чина потписивања.

(3) Потписник у електронски потпис уграђује основне податке о поступку, алгоритму и садржају потписа како би прималац (корисник електронског потписа) могао овјерити потпис на основу исте или одговарајуће технологије и поступака.

(4) Квалификовани електронски потпис мора се израђивати примјеном стандардизованих алгоритама из групе RSA (rsagen1) или DSA (dsagen1).

(5) Код израде квалификованог електронског потписа обавезно се уграђује и функција криптовања (маскирања) садржаја који се потписује (hash функција). Алгоритми који се примјењују у провођењу hash функције морају бити из групе SHA-1 (Secure Hash Algorithm) односно RIPEMD 160.

Члан 5.

(1) Корисник електронског потписа проводи овјеру електронског потписа у складу са упутствима потписника.

(2) Ако је уз потпис уграђен и цертификат, овјеру проводи у складу са упутствима цертификационог тијела које је издало цертификат, односно другог цертификационог тијела које пуноправно одговара и признаје цертификат.

(3) Корисник приликом овјере квалификованог електронског потписа мора провјерити уз податке о потписнику и:

а) податке о цертификационом тијелу које издаје квалификоване цертификате,

б) рок ваљаности квалификованог цертификата

в) ваљаност уписа у регистру издатих квалификованих цертификата

г) непостојање у регистру опозваних цертификата.

III СРЕДСТВА ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА

Члан 6.

(1) Потписник је дужан заштитити средство за израду електронског потписа од неовлашћеног приступа, крађе и оштећивања.

(2) У случајевима када средство за израду електронског потписа садржи и цертификат те електронски потпис цертификационог тијела које је издало цертификат, потребно је средство за израду електронског потписа ускладити са захтјевима за заштиту и сигурност терминалне опреме за израду квалификованог електронског потписа.

(3) Усклађивање из става 2. овог члана мора се проводити примјеном заједничких међународних образаца заштите средстава за израду квалификованог електронског потписа од којих се примјењују сљедећи:

а) ISO/IEC 15408-1:1999 - општи систем мјера заштите уређаја и опреме који су заједнички прихватили међународно (ISO) и европско (IEC) тијело у домену стандардизације којим је дефинисан скуп услова за функционалност и сигурност средстава за израду електронских потписа у документу - Common Criteria 2.1 (for Information Technology Security Evaluation) у секцији EAL 4+ (5) – (Evaluation Assurance Level) којом се посебно утврђују безбједности захтјеви на највишем нивоу којима мора одговарати дјеловање средстава за израду квалификованих електронских потписа (SOF-high),

б) CEN/ISSS SSCD-PP (Secure Signature Creation Device-Protection Profile) – општи образац заштите средстава који је Европска унија прихватила на основу препорука садржаних у Директиви о електронском потпису (Directive 1999/93) у додатку II којим се детаљно описују захтјеви које мора испуњавати средство за израду квалификованог електронског потписа кроз документ CWA (CEN Workshop Agreement) 14169,

в) општи образац за безбједност криптографских модула FIPS 140-1, ниво 1., пожељно 2. (америчко тијело за стандардизацију National Institute of Standards and Technology – Federal Information Processing Standard).

Члан 7.

(1) Код израде квалификованог електронског потписа када се примјењује систем два (пар) криптографска кључа, дужина кључа за израду квалификованог електронског потписа мора бити дужине најмање 1024 бита, уз примјену криптографских алгоритама из класе RSA/DSA и усклађено са међународним стандардом PKCS#1 (верзија 2.1 и више).

(2) Криптографски модули морају се заснивати на алгоритмима и параметрима који чине радно окружење израде квалификованог електронског потписа на основу тренутно важећих образаца уграђених у документу Algorithms and Paramaters for Secure Electronic Signatures (верзија 2.1, 2001-10) којег за потребе Европске уније израђује EESSI/SG (European Electronic Signatures Standardisation Inititiative/Steering Group).

(3) Код уграђивања криптографских алгоритама у средство за израду квалификованог електронског потписа потребно је осигурати модуларност којом се омогућава накнадно уграђивање нових алгоритама.

Члан 8.

(1) Програмска опрема којом се проводи овјера елетронског потписа мора у потпуности онемогућити могућност откривања података за израду електронског потписа помоћу података за овјеру истог.

(2) Програмска опрема која генерише податке за израду еалектронског потписа мора заштитити те податке од нежељеног или неовлашћеног приступа примјеном постојеће технологије.

Члан 9.

Програмска опрема за израду квалификованог електронског потписа мора имати уграђене основне облике заштите у складу са документима о основним правилима заштите и сигурности средстава за израду квалификованог електронског потписа - SSCD/PP, односно EAL4+ препорукама.

Члан 10.

(1) Потписник који изгуби или му је отуђено средство за израду електронског потписа те у случајевима када му је онемогућен приступ подацима за израду електронског потписа, дужан је о томе одмах обавјестити цертификационо тијело, односно његову надлежну службу.

(2) Цертификационо тијело које је примило обавјест према ставу 1. овог члана проводи увид у поступак опозива издатог цертификата и даље поступа по утврђеним правилима опозивања издатих цертификата, а у складу са интерним Правилником о поступцима цертификације на основу којег пружа услугу цертификације.

IV СИСТЕМ ЦЕРТИФИКАЦИЈЕ

Члан 11.

(1) 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 документ „Општа правила пружања услуга цертификације“.

(3) Цертификационо тијело које издаје квалификоване цертификате мора донијети и посебна унутрашња правила о поступцима издавања цертификата и заштите система цертификације у којем су садржани и детаљно описани поступци и мјере које примјењује приликом издавања и руковања цертификатима.

Члан 12.

(1) Општа правила пружања услуга цертификације као и Правилник о поступцима цертификације требају бити структуисани по RFC 2527, односно међународно прихваћеном обрасцу ETSI TS 101 456 – Policy Requirements for Certification Authorities Issuing Qualified Certificates.

(2) Обавезан садржај документације коју цертификационо тијело мора израдити прије почетка обављања услуга цертификације обухвата:

Назив секције	Садржај секције
1. Уводне напомене и детаљни подаци	Опис услуга Идентификациони подаци Корисници и подручје примјене услуга Подаци о сједишту
2. 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)
3. Идентификација и потврда идентитета корисника	Регистрација потписника Планско обнављање цертификата Обнављање након опозива Захтјев за опозив цертификата
4. 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
5. Контрола безбједности опреме, поступака и особља	Контрола простора, опреме и средстава Контрола поступака и провођење радних задатака Контрола особља – број запослених, стручност, овлашћења
6. 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
7. Садржај цертификата и листа опозваних цертификата	Садржај (образац) цертификата Садржај листе опозваних цертификата
8. Управљање документацијом	Поступци код промјене садржаја документације Објављивање документације Поступци прихватања/одобравања документације

Члан 13.

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

(2) Интерна правила дјеловања система цертификације уређују допунски:

а) поступке приступа и кретања кроз пословни простор цертификационог тијела,

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

в) поступци и радње у ванредним ситуацијама, посебно код пожара и других непогода, непредвидивих упрада у физички простор (сједиште) цертификационог тијела, односно упада у информациони систем,

г) правила вођења евиденције о присуству запослених у систему цертификације, приступа систему цертификације.

Члан 14.

(1) 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.

(2) Ако одговорно лице у року од седам дана није у могућности да отклони одступања, поступак се може повјерити трећем лицу у сврху арбитраже коју прихватају стране у спору.

(3) Ако арбитража није могућа, стране покрећу поступак пред надлежним судом.

Члан 15.

(1) Цертификационо тијело које издаје квалификоване цертификате мора примјењивати смјернице Европске уније те Европске норме (ЕН) које се односе на поступке осигуравања и заштите опреме и простора.

(2) Цертификационо тијело које издаје квалификоване цертификате 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. 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 16.

(1) Цертификационо тијело које издаје квалификоване цертификате 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, цертификационо тијело које издаје квалификоване цертификате може обавити уз одговарајуће учешће запослених код произвођача те опреме и уз помоћ њихове опреме.

Члан 17.

(1) Цертификационо тијело које издаје квалификоване цертификате мора за обављање услуга цертификације имати пословни простор у свом власништву или у најму на рок од најмање годину дана од дана подношења захтјева. Пословни простор мора бити задовољавајуће величине за смјештај опреме и рад особља које обавља услуге цертификације.

(2) Цертификационо тијело које издаје квалификоване цертификате мора послове генерисања криптографских кључева и израде цертификата проводити у специјализованом простору издвојеном за ту намјену.

(3) Приступ простору у којем се спроводе радње из става 2. овог члана могу имати само овлашћене особе, и о сваком приступу простору се мора водити одговарајућа евиденција.

Члан 18.

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

Члан 19.

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

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

(3) Цертификационо тијело које издаје квалификоване цертификате мора обезбједити да само лица која раде у систему цертификације имају приступ простору гдје се налазе ресурси система цертификације.

Члан 20.

Информациони систем цертификационог тијела које издаје квалификоване цертификате мора за основу имати софтверску и хардверску инфраструктуру намјењену искључиво за послове цертификације.

Члан 21.

(1) Цертификационо тијело које издаје квалификоване цертификате мора опрему за овјеру и дјеловање система цертификације ускладити са техничким стандардом FIPS 140-1 (горњи ниво), односно са утврђеним заједничким обрасцем заштите програмско-техничке и информационе опреме и система »Common Criteria 2.1« базираном на ISO 15408-1:1999 норми.

(2) Цертификационо тијело које издаје квалификоване цертификате 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 22.

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.

Члан 23.

Цертификационо тијело које издаје квалификоване цертификате мора у сталном радном односу имати:

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

б) најмање три високообразована стручњака техничког усмјерења за заштиту рачунарских система и информационих база те са искуством у раду са системима за издавања, опозива и одржавања цертификата,

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

Члан 24.

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.

Члан 25.

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

Члан 26.

(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 27.

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

Члан 28.

(1) Лице које тражи услугу цертификације (потписник), лично у пријемној служби цертификационог тијела подноси захтјев за издавање цертификата.

(2) Потписник мора осигурати тачност и исправност података у захтјеву и за то сноси правну и материјалну одговорност.

(3) Цертификационо тијело које издаје квалификоване цертификате дужно је у цјелини размотрити податке који је потписник предао у захтјеву за издавање цертификата те провести физичку идентификацију потписника у присуству истог на основу личне карте и других релевантних докумената са фотографијом потписника (нпр. пасош) којима се потврђује истинитост података наведених у захтјеву.

Члан 29.

(1) Подаци исправних и одобрених захтјева за издавање цертификата архивирају се у информационом систему цертификационог тијела.

(2) Садржај цертификата уписује се у Регистар изданих цертификата.

Члан 30.

(1) Потписник којем је одобрено издавање цертификата мора лично код цертификационог тијела или на другом за те послове одређеном мјесту преузети идати цертификат.

(2) Издавање цертификата искључиво обавља лице стално запослено код цертификационог тијела и овлашћено за те послове.

Члан 31.

(1) Садржај квалификованог цертификата мора бити усклађен са техничком спецификацијом ETSI 101 862 (v1.2.1 – 2001-06 или новије) - Qualified Certificate Profile, и који се уједно базира на Qualified Certificate Profile обрасцу RFC 3039.

(2) Цертификат обавезно садржи сљедеће елементе:

а) серијски број (јединствен и непоновљив),

б) ознаку цертификационог тијела,

в) криптографски алгоритам примјењен код израде електронског потписа,

г) електронски потпис цертификационог тијела,

д) назив цертификационог тијела које је издало цертификат,

ђ) име, адреса и остали идентификациони елементи потписника неопходни за јединствену идентификацију,

е) подаци неопходни за поступак овјере електронског потписа потписника на којег се односи цертификат.

ж) подаци за овјеру електронског потписа,

з) датум издавања и рок ваљаности цертификата,

и) једнообразни идентификациони код (Object Identifier према ASN.1) Општих правила цертификационог тијела (ако је претходно придобио ОИД)

Члан 32.

(1) Издати цертификат се опозива

а) истеком рока на који је издат, односно на дан престанка важења,

б) на захтјев потписника,

в) на службени захтјев суда, односно органа државне управе односно правног лица код којег је потписник запослен у тренутку подношења захтјева за опозив цертификата

г) на захтјев цертификационог тијела у случајевима неиспуњавања техничких услова, односно ако се при употреби електронског потписа не поступа на прописан начин

(2) Опозвани цертификати се уписују у листу опозваних цертификата која мора бити доступна свим субјектима који имају приступ услугама цертификационог тијела.

(3) Листа опозваних цертификата мора се тренутно обновити код сваке настале измјене, односно ако није било промјена, најдуже до тридесет дана.

Члан 33.

(1) Листа опозваних цертификата мора садржавати најмање сљедеће елементе:

а) редни број радне верзије листе,

б) криптографски алгоритам коришћен при изради електронског потписа цертификационог тијела,

в) електронски потпис цертификационог тијела,

г) назив цертификационог тијела,

д) датум израде листе.

(2) Сваки опозван цертификат у Листи опозваних цертификата садржи:

а) серијски број додјељен цертификату код издавања

б) датум опозива (од којег цертификат није важећи).

Члан 34.

(1) Цертификационо тијело утврђује временску ваљаност издатог квалификованог цертификата, односно рок до када се признаје важење издатог цертификата.

(2) Рок из става 1. овог члана за квалификоване цертификате мора се утврдити у трајању до пет година.

Члан 35.

(1) Подаци о потписницима, издати цертификати, листе опозваних цертификата као и технички подаци настали биљежењем рада система цертификације, морају се архивирати на медије који осигуравају трајност записа од најмање 20 година.

(2) У сврху чувања записа морају се израдити и сигурносне копије које морају бити смјештене на другој локацији, издвојено од система цертификације у употреби.

Члан 36.

(1) Архивирани подаци морају се чувати и заштитити од неовлаштеног приступа и могућих губитака у запису.

(2) Цертификационо тијело које издаје квалификоване цертификате мора у сврху очувања читкости и исправности записа на медијима, проводити поступке провјере и по потреби, освјеживање записа на медијима најмање два пута годишње.

Члан 37.

(1) Потписник може затражити код цертификационог тијела повремено провјеравање података за израду те података за овјеру електронског потписа.

(2) Потписник захтјев за провјеру према ставу 1. овог члана подноси лично код цертификационог тијела, а може и у електронском облику ако је такав захтјев исправно електронски постписан од стране подносиоца захтјева.

Члан 38.

(1) Цертификационо тијело које издаје квалификоване цертификате мора податке за израду свог електронског потписа одвојено распоредити на најмање два лица која заједно израђују електронски потпис.

(2) Цертификационо тијело које издаје квалификоване цертификате мора податке за израду свог електронског потписа физички и електронски заштитити у складу са утврђеним правилима и стандардима у сврху спрјечавања физичког или електронског приступа од стране неовлаштених лица.

Члан 39.

(1) Цертификационо тијело мора податке о потписницима прикупљати, похрањивати, користити и брисати у складу са одговарајућим прописима о заштити личних података и поштовања и заштите приватности корисника система цертификације.

(2) Подаци о потписнику могу се придобивати искључиво лично од самог потписника и у обиму односно садржају потребном за поступак издавања цертификата.

(3) Потписник има право увида у податке који се о њему воде код цертификационог тијела у сврху провјере или потребних допуна односно исправки.

(4) Захтјев за увид у податке може се доставити и у електронском облику и потписан електронским потписом подносиоца захтјева.

(5) Цертификационо тијело мора доставити тражене податке најкасније у року од пет радних дана од дана примања захтјева.

Члан 40.

(1) Цертификационо тијело не смије пружати повјерљиве податке осим у случајевима кад то тражи суд или републичко тужилаштво.

(2) Лице које код цертификационог тијела проводи провјеру рада система цертификације, има право увида у повјерљиве податке изузев у криптографске податке (подаци за израду и овјеру електронског потписа пружаоца услуга цертификације), али их не смије износити изван система нити објављивати у извјештајима.

(3) Уговором се додатно обавезује на држање у потпуној тајности повјерљивих података у које је имао увид за вријеме поступака провјере рада система цертификације.

V ОПШТИ ПОСТУПЦИ ЗАШТИТЕ СИСТЕМА ЦЕРТИФИКАЦИЈЕ

Члан 41.

(1) Цертификационо тијело које издаје квалификоване цертификате дужно је израдити јединствени систем заштите и сигурности обављања услуга.

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

Члан 42.

(1) Цертификационо тијело које издаје квалификоване цертификате 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.

Члан 43.

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 44.

(1) Цертификационо тијело које издаје квалификоване цертификате мора за послове заштите система цертификације запослити квалификована лица за сљедеће послове заштите:

а) контрола физичког приступа рачунарској опреми,

б) уградња и конфигурација програмског склопа заштите као и системско мјењање криптографских кључева,

в) анализа рада у свим фазама рада, биљежење и архивирање тих података те обавјештавање,

г) управљачке функције и операције отклањања проблема у функционисању прописаних мјера заштите,

д) извјештавање о покушајима нарушавања прописаних мјера заштите те идентификација субјеката који проводе нарушавање.

Члан 45.

Провјера се мора провести најмање за ова подручја:

а) систем цертификације (информацијски систем)

б) технологија криптизаштите

в) радни простор те рачунарска и мрежна опрема

г) релевантни законски и други прописи у Републици Српској и Европи

Члан 46.

(1) Цертификационо тијело које издаје квалификоване цертификате мора систем цертификације и информациони систем ускладити са захтјевима сигурности дјеловања информационих система у складу са обрасцем ISO/IEC 17799:2000 (Code of Practice for Information Security Menagement) те BS 7799-2:1999 (British Standard for Information Security Menagement – Specification for Information Security Menagement System).

(2) Систем цертификације мора садржавати одвојене радне групе при чему лица која раде на пословима управљања рачунарским системом не могу радити послове издавања и опозива цертификата.

Члан 47.

(1) Сви подаци за израду квалификованог електронског потписа пружаоцу услуга цертификације морају бити криптографски заштићени уз примјену:

а) средстава за израду квалификованог електронског потписа у складу са FIPS 140-1 (горњег нивоа) те којима је могућа употреба посебних приступних техника за рад са подацима за израду електронског потписа

б) података за израду потписа примјеном RSA или DSA алгоритма дужине најмање 2048 bita односно одговарајућег нивоа Elliptic Curve алгоритма, те SHA-1 или RIPEMD - 160 алгоритма за криптовање садржаја.

в) криптографских алгоритама (3DES алгоритма - 128 bitni или AES техника) у сврху заштите приступа подацима.

Члан 48.

(1) Цертификационо тијело мора податке за израду свог електронског потписа чувати у најмање два примјерка на одвојеним локацијама у за то намјенски уређеном простору заштићеном од оштећења у случају пожара, поплаве и других штетних утицаја, те осигурати раздвајање основног скупа података за израду електронског потписа у најмање два дијела.

(2) Расположивост података за израду квалификованог електронског потписа цертификационог тијела које издаје квалификоване цертификате мора бити једнократна и то за вријеме израде електронског поптиса и мора престати након сваке израде електронског потписа.

Члан 49.

(1) Цертификационо тијело које издаје квалификоване цертификате мора рад са рачунаром и програмском опремом повјерити само лицима са високом стручном спремом и специјалистичких знања у руковању опремом уграђеном у систем цертификације.

(2) Цертификационо тијело које издаје квалификоване цертификате 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.

VI ПОСЕБНЕ ОДРЕДБЕ

Члан 50.

(1) Цертификационо тијело које издаје квалификоване цертификате 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 цертификационо тијело које издаје квалификоване цертификате, изузев носиоца послова електронске цертификације за органе државне управе, мора осигурати одговорност за штете износи 500.000 конвертибилних марака (КМ).

VII ЗАВРШНЕ ОДРЕДБЕ

Члан 51.

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

Број:
Датум:

МИНИСТАР
Бакир др Ајановић