На основу члана 18. став 2. и члана 33. Закона о електронском потпису („Службени гласник РС”, број 135/04),

министар за телекомуникације и информатичко друштво доноси

ПРАВИЛНИК О БЛИЖИМ УСЛОВИМА ЗА ИЗДАВАЊЕ КВАЛИФИКОВАНИХ ЕЛЕКТРОНСКИХ СЕРТИФИКАТА

Члан 1.

Овим Правилником прописују се ближи услови за издавање квалификованих електронских сертификата и начин провере њихове испуњености.

I. УСЛОВИ КОЈЕ СЕРТИФИКАЦИОНО ТЕЛО ТРЕБА ДА ИСПУНИ ЗА ИЗДАВАЊЕ КВАЛИФИКОВАНИХ СЕРТИФИКАТА

Способност за поуздано обављање услуга издавања квалификованих електронских сертификата

Члан 2.

Издавање квалификованих електронских сертификата мора бити у складу са одговарајућим међународним стандардима и препорукама, односно другим стандардима, документима и препорукама које се односе на издавање квалификованих електронских сертификата, утврђеним овим правилником.

Члан 3.

Сертификационо тело за издавање квалификованих електронских сертификата (у даљем тексту: сертификационо тело) издаје квалификоване електронске сертификате тако што формира квалификовани електронски потпис сертификата на основу свог приватног кључа и асиметричног криптографског алгоритма у складу са правилником о техничко-технолошким поступцима за формирање квалификованог електронског потписа и условима и критеријумима које треба да испуне средства за формирање квалификованог електронског потписа.

Сертификационо тело издаје квалификоване електронске сертификате корисницима у складу са документима ETSI ESI TS 101 862 „Qualified Certificate Profile”, RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile“, RFC 3280 „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” и ETSI TS 102 280 „X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons" и са обавезним садржајем дефинисаним у члану 17. Закона о електронском потпису (у даљем тексту : Закон).

Члан 4.

Сертификационо тело дужно је да обезбеди комплетне услуге сертификације које укључују следеће сервисе, и то:

1) регистрацију корисника;

2) формирање квалификованих електронских сертификата;
3) дистрибуцију квалификованих електронских сертификата корисницима;
4) управљање животним веком (обнављање, суспензија, опозив) квалификованих електронских сертификата;
5) обезбеђивање поузданог и јавно доступног сервиса за проверу статуса опозваности квалификованих електронских сертификата.

Сертификационо тело може, поред сервиса из става 1. овог члана, да обезбеди и формирање асиметричног пара кључева за кориснике, као и дистрибуцију приватног кључа и сертификата кориснику на безбедан начин, уколико је то прописано у Политици сертификације датог сертификационог тела.

Члан 5.

Сертификационо тело, пре почетка рада, утврђује Општа интерна правила пружања услуге сертификације (у даљем тексту: Општа правила) која корисницима обезбеђују довољно информација на основу којих се могу одлучити о прихватању услуга и о обиму услуга.

Општа правила Сертификационог тела уграђују се у документима:
1) Политика сертификације (Certificate Policy);
2) Практична правила пружања услуге Сертификације (Certification Practices Statement) (у даљем тексту: Практична правила).

Политика сертификације и Практична правила јесу јавни документи.

Члан 6.

Политика сертификације дефинише предмет рада сертификационог тела, док Практична правила дефинишу процесе и начин њиховог коришћења при формирању и управљању квалификованим електронским сертификатима. Политика сертификације дефинише захтеве пословања сертификационог тела, док Практична правила дефинишу оперативне процедуре у циљу испуњења тих захтева. Практична правила дефинишу начин на који сертификационо тело испуњава техничке, организационе и процедуралне захтеве пословања који су идентификовани у Политици сертификације.

Политика сертификације је мање специфичан и детаљан документ у односу на Практична правила која представљају много детаљнији опис начина пословања, као и пословне и оперативне процедуре које сертификационо тело примењује у издавању и управљању квалификованим електронским сертификатима.

Политика сертификације се дефинише независно од специфичног оперативног окружења сертификационог тела, док Практична правила дају детаљан опис организационе структуре, оперативних процедура, као и физичко и рачунарско окружење сертификационог тела.

Члан 7.

Општа правила функционисања сертификационог тела треба да буду у складу са документима RFC 3647 „Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”и ETSI TS 101 456 „Policy Requirements for Certification Authorities Issuing Qualified Certificates”.

Члан 8.

Садржај докумената Политика сертификације и Практична правила, обухвата:
1) опште одредбе о раду сертификационог тела:
   (1) појам сертификационог тела,

(2) сертификационе услуге,
(3) обухват документа Политика сертификације,
(4) обухват документа Практична правила пружања услуге сертификације,
(5) кориснике услуга сертификације;

2) уводне одредбе о Политици издавања квалификованих електронских сертификата;
3) обавезе и одговорности:
   (1) обавезе сертификационог тела,
   (2) обавезе корисника,
   (3) одговорност сертификационог тела,
   (4) одговорност корисника;
4) функционалне захтеве за рад сертификационог тела:
   (1) оперативне процедуре рада сертификационог тела,
   (2) процедуре управљања животним циклусом криптографских кључева:
      - генерисање кључа сертификационог тела,
      - процедуре чувања и формирања резервних копија кључева сертификационог тела,
      - дистрибуцију јавног кључа сертификационог тела,
      - коришћење кључа сертификационог тела,
      - крај животног циклуса кључа сертификационог тела,
      - управљање животним циклусом криптографског хардвера који се користи за генерисање квалификованих сертификата,
      - управљање кључевима корисника за идентификацију и дигиталну енвелопу,
      - процедуру припреме средстава за формирање квалификованог електронског потписа;
   (3) процедуре управљања животним циклусом сертификата:
      - методе регистрације корисника,
      - издавање сертификата,
      - дистрибуција сертификата,
      - обнављање сертификата,
      - суспензија сертификата,
      - опозив сертификата,
      - начин публикације листе опозваних сертификата;
   (4) управљање оперативним радом сертификационог тела:
      - управљање у складу са безбедносним принципима,
      - управљање и класификација најважнијих информација и података у оквиру сертификационог тела,
      - кадровски ресурси,
      - систем физичке безбедности и безбедности окружења,
      - управљање радом сертификационог тела,
      - управљање системом контроле приступа,
      - употреба и одржавање безбедних криптографских система,
      - управљање процедурама континуалног пословања у инцидентним ситуацијама,
      - престанак рада сертификационог тела,
      - усаглашеност рада са критеријумима за рад сертификационих тела која издају квалификоване електронске сертификате у складу са Законом и овим правилником,

- формирање и чување документације која се односи на квалификоване електронске сертификате;

(5) организација рада сертификационог тела.

Члан 9.

Сертификационо тело демонстрира способност за обезбеђивање услуга издавања квалификованих електронских сертификата, тако што мора:

1) имати Практична правила, и у њима дефинисане процедуре, у којима се специфицира начин испуњења свих захтева за издавањем квалификованих електронских сертификата који су идентификовани у Политици сертификације;
2) учинити расположивим Практична правила свим корисницима и другим заинтересованим странама;
3) објавити свим корисницима и потенцијалним заинтересованим странама услове коришћења квалификованих електронских сертификата;
4) имати управну структуру највишег нивоа која ће имати коначну ауторизацију и одговорност за објављивање Практичних правила сертификационог тела;
5) имати управну структуру оперативног нивоа у сертификационом телу која је одговорна за исправну примену Практичних правила;
6) дефинисати процес периодичне анализе и одржавања Практичних правила;
7) имати одобрене, од стране управне структуре највишег нивоа, све измене у Практичним правилима, тј. нове верзије Практичних правила, у складу са тачком 4. овог става и, након одобравања, одмах јавно објављене у складу са тачком 2. овог става.

Члан 10.

Сертификационо тело утврђује и Посебна интерна правила рада сертификационог тела и заштите система сертификације (у даљем тексту: Посебна правила) у којима су садржани и детаљно описани поступци и мере који се примењују приликом издавања и руковања квалификованим електронским сертификатима.

Посебна правила су приватни документ и представљају пословну тајну сертификационог тела.

Члан 11.

Посебна правила садрже детаљне одредбе о:

1) систему физичке контроле приступа у поједине просторије сертификационог тела;
2) систему логичке контроле приступа рачунарским ресурсима сертификационог тела;
3) систему за чување приватног кључа сертификационог тела;
4) систему дистрибуиране одговорности при активацији приватног кључа сертификационог тела;
5) поступцима и радњама у ванредним ситуацијама (пожари, поплаве, земљотреси, друге временске непогоде, злонамерни упади у просторије или информациони систем сертификационог тела).

Члан 12.

Сертификационо тело обезбеђује поуздану организацију рада, а нарочито:

1) правила и оперативне процедуре које нису дискриминаторске;
2) доступност својих сервиса свим корисницима чије су активности у складу са објављеним Општим правилима;
3) пословање у својству правног лица у складу са одговарајућим домаћим прописима;
4) систем квалитета и систем безбедног управљања квалификованим електронским сертификатима у складу са услугама сертификације које пружа;
5) осигурање од одговорности за штету која може да проистекне у вршењу његових активности у складу са Политиком сертификације;
6) финансијску стабилност и довољне ресурсе који се захтевају у пружању услуга сертификације у складу са Политиком сертификације;
7) довољан број стално запослених на пословима сертификације са неопходним образовањем, нивоом обучености, техничким знањима и искуством;
8) ефикасно поступање у решавању жалби и спорова са корисницима или другим заинтересованим странама у вези пружања услуга сертификације;
9) независност делова сертификационог тела укључених у послове генерисања квалификованих електронских сертификата од других спољних организација у сфери пружања услуга сертификације. Посебно управна структура сертификационог тела, као и запослени са безбедносним функцијама, морају бити заштићени од било каквих финансијских и других притисака који могу утицати на поверење у услуге сертификације које пружа сертификационо тело;
10) прописно документовану структуру делова сертификационог тела повезаних са генерисањем квалификованих електронских сертификата ради обезбеђивања непристрасности у пружању услуга сертификације, у складу са Општим и Посебним правилима.

Члан 13.

Сертификационо тело је дужно да обезбеди најнижи износ осигурања од ризика одговорности за могућу штету насталу вршењем услуга издавања електронских сертификата тако да:

1. осигурана сума на коју мора бити уговорено осигурање по једном штетном догађају не може износити мање од 20.000 (двадесет хиљада) евра у динарској противвредности, подразумевајући притом као штетни догађај појединачну штету насталу употребом једног квалификованог сертификата у једном акту у правном промету;
2. укупна осигурана сума на коју мора бити уговорено осигурање од одговорности сертификационог тела кумулативно на годишњем нивоу, по свим штетним догађајима, не може бити нижа од 1.000.000 (милион) евра у динарској противвредности.

Члан 14.

Сертификационо тело обезбеђује да у случају катастрофа оперативни рад буде обновљен што је могуће пре а у складу са Општим и Посебним правилима.

У случају компромитације свог асиметричног приватног кључа, сертификационо тело:

1) престаје са издавањем квалификованих електронских сертификата;
2) информише све кориснике и друге заинтересоване стране о компромитацији приватног кључа;
3) јавно објављује информације о томе да издати квалификовани електронски сертификати, као и информације о статусу опозваности квалификованих електронских сертификата, више нису важеће;
4) врши опозив свих издатих квалификованих електронских сертификата одмах а најкасније у року од 24 часа у складу са Законом.

Безбедно и ажурно вођење регистра издатих и опозваних сертификата

Члан 15.

Сертификационо тело води ажурну, тачну и безбедну евиденцију издатих квалификованих електронских сертификата која може бити јавно доступна, осим у случајевима када власник сертификата изричито захтева да његови подаци не буду јавно доступни, или када сертификат носи ЈМБГ или лични број, а у складу са чланом 28. тачка 6. Закона.

Сертификационо тело води ажурну и безбедну евиденцију неважећих (опозваних и суспендованих) квалификованих електронских сертификата и мора за сваки сертификат који је издало, информацију о његовој валидности учинити јавно доступном.

Тачност и валидност евиденција из ст. 1. и 2. овог члана, сертификационо тело гарантује својим квалификованим електронским потписом.

Обезбеђивање тачног времена издавања и опозива сертификата

Члан 16.

За поуздано одређивање времена издавања и опозива квалификованих електронских сертификата, сертификационо тело мора обезбедити извор тачног времена који је синхронизован са извором референтног времена који одреди Министарство и објављује на веб страни Министарства.

Тачно време издавања квалификованог електронског сертификата сертификационо тело уграђује у издати квалификовани електронски сертификат.

Тачно време издавања и опозива квалификованих електронских сертификата сертификационо тело чува у евиденцији издатих и опозваних сертификата из члана 15. овог правилника.

Процедуре регистрације корисника

Члан 17.

Сертификационо тело врши регистрацију корисника, односно поуздану идентификацију и аутентикацију корисника којима издаје квалификоване електронске сертификате, у складу са чланом 28. тачка 2. Закона.

Поступке регистрације из става 1. овог члана врши овлашћени службеник сертификационог тела или регистрационог тела на удаљеној регистрационој локацији које успоставља сертификационо тело за потребе регистрације корисника.

Регистрационо тело, у смислу овог правилника, јесте организациона јединица сертификационог тела или овлашћена јединица од стране сертификационог тела за вршење послова регистрације корисника.

Члан 18.

Сертификационо тело дужно је да у поступку регистрације корисника, у складу са чл. 17. овог правилника, обезбеди да:

1) се корисник идентификује као физичко лице са специфичним атрибутима који могу означавати организациону јединицу или улогу у организацији где је запослен;
2) пре успостављања уговорног односа са корисником, јавно информише корисника на јасном и разумљивом језику о свим релевантним условима коришћења квалификованих електронских сертификата;
3) се верификује идентитет корисника у складу са важећим прописима. Под скупом података који јединствено идентификује потписника у складу са чланом 17. тачка 3. Закона подразумевају се идентификациони подаци који су садржани у идентификационим документима;
4) за поуздану проверу идентитета корисника у поступку регистрације, захтева физичко присуство корисника у сертификационом телу или у регистрационом телу;
5) ако је потребно, верификује и било који специфични атрибут корисника коме се издаје квалификовани електронски сертификат;
6) уколико се ради о физичком лицу као индивидуалном кориснику, идентитет корисника мора да буде проверен на основу законом прописаног личног идентификационог документа;
7) уколико се ради о кориснику који се идентификује као припадник правног лица или неке организације, доказ његовог идентитета мора да садржи следеће елементе, и то:
   (1) законом прописани лични идентификациони документ,
   (2) правно ваљане податке о регистрацији правног лица или организације,
   (3) доказ да је корисник овлашћен од стране тог правног лица или организације за добијање квалификованог електронског сертификата;
8) информације садржане у квалификованом електронском сертификату буду поуздане и тачне;
9) корисник мора доставити тачне и поуздане информације о физичкој адреси, или другим атрибутима, који описују како се корисник може контактирати;

10) чува све информације коришћене за верификацију идентитета корисника и документацију коришћену за идентификацију, као и било која ограничења њене важности;
11) са корисником закључи уговор који треба, нарочито, да садржи:
    (1) обавезе корисника,
    (2) обавезу корисника да користи средство за формирање квалификованог електронског потписа које обезбеђује сертификационо тело, ако је то у складу са Општим правилима,
    (3) обавезу сертификационог тела да чува податке коришћене у регистрацији корисника и све информације о животном циклусу издатог квалификованог електронског сертификата корисника. Прослеђивање ових информација трећим странама је под условима дефинисаним Политиком сертификације,
    (4) услове за публикацију сертификата,
    (5) потврду да су информације садржане у сертификату коректне;
12) уговор из тачке 11) овог става чува у року из члана 31. Закона;
13) ако асиметрични пар кључева корисника није генерисан од стране сертификационог тела, процес генерисања захтева за квалификованим електронским сертификатом у потпуности обезбеђује да корисник поседује асиметрични приватни кључ који је математички, на бази асиметричног криптографског алгоритма, повезан са јавним кључем који је презентиран за сертификацију. У том случају корисник мора обезбедити да се асиметрични пар кључева генерише искључиво у средству за формирање квалификованог електронског потписа;
14) се поштују одредбе важећих прописа којима се уређује заштита података о личности.

Кадровски ресурси и управљање оперативним радом сертификационог тела

Члан 19.

Сертификационо тело обезбеђује структуру стално запослених у складу са захтевима за поуздано и безбедно функционисање сертификационог тела које издаје квалификоване електронске сертификате на основу Закона и овог правилника.

Члан 20.

Сертификационо тело обезбеђује неопходне кадровске ресурсе, и са њима повезане предуслове, а нарочито да :
1) запослени у сертификационом телу морају да поседују експертско знање, искуство и неопходну квалификацију за услуге које сертификационо тело нуди, као и за одговарајуће пословне функције и то:
    (1) најмање 4 запослених са вишом или високом школском спремом из области информационо-комуникационих технологија и радним искуством од најмање 3 године у области одржавања и безбедности информационих система и положен најмање један од испита: CompTIA Security+, ISC2 CISSP или SANS GSEC,
    (2) најмање 2 од запослених из претходне тачке треба да има високу школску спрему и 5 година радног искуства у области информационих система и положен ISC2 CISSP испит или SANS GSEC испите у области безбедности информационих система;

2) улоге и функције безбедности, утврђене у Општим правилима, морају бити документоване и детаљно специфициране са описима сваког радног места у сертификационом телу. Пословне функције од највишег нивоа поверљивости, од којих највише зависи безбедност функционисања сертификационог тела, морају бити посебно и јасно идентификоване;
3) запослени у сертификационом телу (стални и привремени) морају имати описе послова дефинисане са становишта раздвајања дужности и привилегија. Описи послова морају разликовати опште послове и специфичне функције сертификационог тела. Препоручује се да описи послова укључе и дефиниције захтева за специфичним вештинама и искуством која се траже од запослених;
4) запослени у управној структури сертификационог тела морају да поседују експертизу у технологији електронског потписа, да су добро упознати са безбедносним процедурама за запослене и са одговорностима у домену безбедности, као и да имају одговарајућа искуства у примени безбедних информационих система и процени ризика;
5) сви запослени у сертификационом телу са безбедносним функцијама не смеју имати сукобе интереса који могу утицати на непристрасност рада сертификационог тела;
6) безбедносне функције у сертификационом телу укључују следеће одговорности и то за :
    (1) главног администратора безбедности - свеукупну одговорност за администрирање и имплементацију безбедносних функција и процедура, као и управљање активностима на додатном унапређењу послова генерисања, опозива и суспензије квалификованих електронских сертификата,
    (2) систем администраторе – ауторизовану одговорност за инсталацију, конфигурисање и одржавање безбедних система сертификационог тела за регистрацију корисника, генерисање квалификованих електронских сертификата, обезбеђење средстава за формирање квалификованог електронског потписа за кориснике и управљање опозивом квалификованих електронских сертификата,
    (3) систем операторе - одговорност за рад безбедних система сертификационог тела у текућем раду на дневном нивоу и ауторизовану одговорност за имплементацију система за формирање резервних копија и процедуре опоравка,
    (4) систем евидентичаре - ауторизовану одговорност за прегледање и одржавање архива и лог фајлова безбедних система сертификационог тела;
7) запосленима у сертификационом телу морају бити формално додељене безбедносне функције од стране више управне структуре надлежне за безбедност;
8) сертификационо тело не сме доделити безбедносне ни управне функције особама које су осуђиване или које су на било који начин кажњаване у односу на њихову подобност за рад на одговорним функцијама. Запослени не смеју имати приступ безбедносним функцијама пре завршетка неопходних провера.

Коришћење поузданих и безбедних криптографских система

Члан 21.

Сертификационо тело мора да користи безбедне системе и производе који су заштићени од неовлашћених модификација.

Члан 22.

Сертификационо тело пре почетка обављања услуга сертификације, као и периодично, током оперативног рада, врши анализу ризика којом идентификује критичне сервисе који захтевају коришћење безбедних система и високе нивое сигурности.

Члан 23.

Сертификационо тело обезбеђује безбедно и коректно функционисање својих система, са минималним ризиком од кварова, а нарочито:

1) заштићен интегритет система сертификационог тела, као и информација, од вируса, малициозног и неауторизованог софтвера;
2) минималну штету услед могућих инцидената коришћењем процедура извештавања и одговарајућих одговора. Сертификационо тело мора да реагује брзо и координирано у циљу одговора на безбедносне инциденте и да ограничи утицај безбедносних упада;
3) безбедно коришћење меморијских медијума у складу са унапред специфицираним шемама класификације информација. Медији који садрже безбедносно осетљиве податке морају бити безбедно архивирани уколико нису у оперативном раду;
4) успостављене и имплементиране процедуре за све безбедне и административне функције-роле које имају утицај на пружање услуга сертификације. Сваки запослени из управне структуре сертификационог тела је одговоран за планирање и ефективну имплементацију Општих правила;
5) стални надзор текућих и будућих потреба за капацитетом система сертификационог тела ради обезбеђења адекватне процесне снаге и меморијских капацитета.

Члан 24.

Сертификационо тело обезбеђује да су његови асиметрични кључеви генерисани у строго контролисаним и безбедним условима, а нарочито да се:

1) генерисање асиметричних кључева врши у физички заштићеном окружењу од стране и уз минималан број ауторизованих запослених (најмање два запослена лица) за извршавање ове функције а према захтевима и процедурама дефинисаним у Практичним правилима;
2) генерисање асиметричних кључева врши у средству које:
    a. задовољава захтеве из стандарда FIPS PUB 140-2 ниво 3 и виши или
    b. CEN Workshop Agreement (CWA) 14169: „Secure Signature-Creation Device (EAL 4+)” или

c. задовољава захтеве из стандарда CEN Workshop Agreement 14167-3 „Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Modules for CSP Key Generation Services - Protection Profile (CMCKG-PP)”;

3) генерисање кључева врши коришћењем алгоритма верификованог за сврху генерисања квалификованих електронских сертификата од стране Министарства;
4) да резервне копије приватних кључева за формирање квалификованог електронског потписа квалификованих електронских сертификата имају исти или виши ниво безбедносних контрола у односу на кључеве који се оперативно користе;
5) обезбеди да су издати квалификовани електронски сертификати потписани квалификованим електронским потписом сертификационог тела.

Члан 25.

Сертификационо тело обезбеђује заштиту тајности и интегритет асиметричних приватних кључева, а нарочито:

1) чување и коришћење приватног кључа за формирање квалификованог електронског потписа у безбедном криптографском уређају који:
   a. задовољава захтеве из стандарда FIPS PUB 140-2 ниво 3 и виши или
   b. CEN Workshop Agreement (CWA) 14169: „Secure Signature-Creation Device (EAL 4+)” или
   c. задовољава захтеве из стандарда CEN Workshop Agreement 14167-3 „Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Modules for CSP Key Generation Services - Protection Profile (CMCKG-PP)”;
2) да су делови за активацију приватног кључа сертификационог тела, када се налазе изван криптографског уређаја шифровани коришћењем симетричног алгоритма и дужине кључа, верификованих за те потребе од стране Министарства, и који омогућавају поуздану одбрану од криптоаналитичких напада;
3) чување делова за активацију приватног кључа, уз обезбеђење резервних копија тих делова, и активација само од стране оних запослених који имају безбедносне функције, уз коришћење најмање двоструке контроле у физички обезбеђеном окружењу. Број запослених у сертификационом телу који су ауторизовани да извршавају ове функције мора бити минималан и мора да задовољи захтеве и процедуре дефинисане у Општим и Посебним правилима рада сертификационог тела;
4) да се мерама логичке контроле приступа онемогући неовлашћено активирање криптографског уређаја са приватним кључем сертификационог тела.

Члан 26.

Сертификационо тело обезбеђује да његов асиметрични јавни кључ који служи за верификацију квалификованог електронског потписа квалификованих електронских сертификата буде расположив свим корисницима и другим заинтересованим странама на начин којим се обезбеђује аутентичност и интегритет јавног кључа.

Члан 27.

Сертификационо тело мора свој асиметрични јавни кључ и локацију листе опозваних сертификата дистрибуирати корисницима и другим заинтересованим странама на сигуран начин у облику квалификованог електронског сертификата односно листе опозваних сертификата.

Члан 28.

Сертификационо тело користи свој асиметрични приватни кључ у складу са Општим и Посебним правилима, а нарочито обезбеђује:

1) да се користи искључиво за формирање квалификованог електронског потписа квалификованих електронских сертификата, као и квалификованог електронског потписа листе опозваних сертификата;
2) да се користи само у оквиру физички заштићених просторија сертификационог тела.

Члан 29.

Сертификационо тело обезбеђује да се његови асиметрични приватни кључеви не користе након истека њиховог животног циклуса, у складу са Општим и Посебним правилима.

Приватни кључеви, из става 1. овог члана, морају бити уништени на начин којим се обезбеђује да се не могу реконструисати.

Члан 30.

Сертификационо тело осигурава безбедност криптографских уређаја који се користе за генерисање и чување кључева и формирање квалификованог електронског потписа током животног циклуса уређаја, у складу са Посебним правилима , а нарочито да:

1) криптографски уређај није компромитован током транспорта;
2) криптографски уређај није компромитован за време чувања у сертификационом телу;
3) процедуре инсталације активације, креирања резервних копија и реконструкције асиметричног приватног кључа у криптографском уређају врши само уз истовремену контролу најмање два запослена са безбедносним функцијама;
4) криптографски уређај функционише коректно;
5) обезбеди да се приватни кључеви сертификационог тела који су чувани у криптографском уређају униште након краја животног циклуса кључева или уређаја.

Обезбеђење заштите од фалсификовања сертификата и тајности генерисаних кључева

Члан 31.

Сертификационо тело мора осигурати безбедан процес генерисања квалификованих електронских сертификата ради обезбеђења њихове аутентичности и интегритета.

Члан 32.

Сертификационо тело обезбеђује:

1) да се квалификовани електронски сертификати генеришу у складу са форматом дефинисаним у документима ETSI TS 101 862, RFC 3739, RFC 3280 и ETSI TS 102 280;
2) да је процедура генерисања квалификованог електронског сертификата безбедно повезана са одговарајућим процедурама регистрације корисника, обнављања сертификата уз задржавање постојећег или генерисање новог асиметричног пара кључева:
3) у случају да сертификационо тело генерише корисникове кључеве:
   (1) да је процедура генерисања квалификованог електронског сертификата безбедно повезана са процедуром генерисања асиметричног пара кључева од стране сертификационог тела,
   (2) да је приватни кључ, односно средство за формирање квалификованог електронског потписа, безбедно достављено до регистрованог корисника, а да се активациони код средства за формирање квалификованог електронског потписа овлашћеном лицу достави на безбедан начин другим путем;
4) јединственост додељеног имена кориснику у оквиру домена сертификационог тела (за време радног века сертификационог тела мора се обезбедити да корисничко име које се додели у поступку генерисања сертификата не може никада да се придружи другом кориснику);
5) тајност и интегритет регистрационих података, и то посебно у случајевима размене података са корисником или у случају размене информација између дистрибуираних компоненти сертификационог тела;
6) верификацију регистрационих података корисника које аутентиковани службеник регистрационог тела доставља сертификационом телу.

Члан 33.

Сертификационо тело обезбеђује да захтеви за обнављање квалификованих електронских сертификата и/или захтеви за издавање квалификованих електронских сертификата корисницима којима су претходни сертификати били опозвани, буду комплетни, тачни и ауторизовани.

Члан 34.

У захтеву за обнављањем сертификата, сертификационо тело мора унети ажуриране информације о кориснику и све друге измене које су претходно верификоване на исти начин као и у поступку регистрације корисника, у складу са чл. 17. и 18. овог правилника.

Сертификационо тело ће издати нови квалификовани електронски сертификат користећи претходно сертификовани јавни кључ корисника само ако је његова криптографска безбедност још увек довољна за предвиђени нови животни циклус сертификата и ако не постоје индикације да је корисников приватни кључ компромитован.

Одговорност и осигурање

Члан 35.

Сертификационо тело је одговорно да су сви сертификациони сервиси наведени у Политици сертификације конзистентни и имплементирани у складу са Практичним правилима.

Члан 36.

Пружање услуга сертификације регулише се посебним уговором између сертификационог тела и корисника, у складу са чланом 18. став 1. тачка 11) овог правилника.

Уговор из става 1. овог члана мора да утврди обавезе корисника, а нарочито да :

1) достави тачне и комплетне информације сертификационом телу у складу са процедуром регистрације дефинисаном у Политици сертификације;
2) искључиво користи свој асиметрични приватни кључ за формирање квалификованог електронског потписа у складу са уговором;
3) онемогући неовлашћен приступ свом приватном кључу;
4) уколико сам генерише асиметрични пар кључева:
   (1) за генерисање користи алгоритам верификован од стране Министарства и усаглашен за потребе формирања квалификованог електронског потписа,
   (2) користи прописану дужину кључа и прописани алгоритам за формирање квалификованог електронског потписа у складу са Правилником о техничко-технолошким поступцима за формирање квалификованог електронског потписа и критеријумима које треба да испуне средства за формирање квалификованог електронског потписа,
   (3) обезбеди да једино он поседује свој приватни кључ;
5) користи квалификовани електронски сертификат само уз квалификовани електронски потпис који је формиран средствима за формирање квалификованог електронског потписа;
6) уколико захтева квалификовани електронски сертификат од сертификационог тела које испуњава услове из члана 18. Закона и овог правилника, генерише пар кључева за формирање и проверу квалификованог електронског потписа у средству за формирање квалификованог електронског потписа које је у потпуности под његовом контролом;
7) одмах обавести сертификационо тело ако пре истека важности сертификата који је назначен у самом сертификату :
   (1) корисников приватни кључ се изгуби, украде или наступи основана сумња да је компромитован,

(2) престане контрола над коришћењем корисниковог приватног кључа из разлога компромитације активационих података (PIN код или лозинка) за средство за формирање квалификованог електронског потписа или других разлога,
(3) установи нетачност или измена садржаја квалификованог електронског сертификата;

8) прекине коришћење свог приватног кључа уколико постоји основана сумња у компромитацију кључа или контролу над активационим подацима за средство за формирање квалификованог електронског потписа.

Члан 37.

Заинтересоване стране које користе квалификоване електронске сертификате имају обавезу да:

1) провере важност и исправност статуса суспензије или опозива квалификованог електронског сертификата коришћењем статусних информација које је одговарајуће сертификационо тело јавно публиковало (у зависности од Општих правила и примењених механизама за публиковање информација о статусу опозива квалификованих електронских сертификата постоји могућност кашњења до једног дана у ажурирању статусних информација);
2) узму у обзир сва ограничења у коришћењу квалификованог електронског сертификата која су назначена у самом сертификату или публикована у Општим правилима.

Члан 38.

Сертификационо тело обезбеђује финансијске ресурсе за осигурање од ризика и одговорности за могућу штету насталу вршењем услуга издавања квалификованих електронских сертификата у складу са Законом и овим правилником.

Начин осигурања из става 1. овог члана, као и одговарајући износ средстава, морају бити јасно наведени у Општим правилима рада.

Чување свих релевантних информација

Члан 39.

Сертификационо тело мора да обезбеди чување свих релевантних информација које се тичу квалификованих електронских сертификата у временском периоду дефинисаном у складу са Законом и Општим правилима, и то посебно у циљу обезбеђења доказа о извршеној сертификацији за правне сврхе.

Информације из става 1. овог члана, укључују податке о регистрацији корисника и информације о значајним догађајима везаним за оперативни рад сертификационог тела, као и за управљање кључевима и сертификатима.

Члан 40.

Сертификационо тело обезбеђује:

1) тајност и интегритет текућих и архивираних записа о квалификованим електронским сертификатима;

2) комплетно и поуздано архивирање информација о квалификованим електронским сертификатима у складу са објављеним Општим правилима;
3) да су записи у вези квалификованих електронских сертификата, као и регистрационе и друге информације о кориснику, расположиви за потребе правних послова као доказ извршене сертификације;
4) поуздано архивирање тачног времена значајних догађаја у сертификационом телу;
5) да се информације у вези квалификованих електронских сертификата чувају онолико времена колико је потребно да се користе у правним пословима везаним за електронске потписе;
6) евидентирање свих догађаја на начин да се не могу лако обрисати или уништити (изузев у циљу преноса на дуготрајне медије за чување) у оквиру временског периода у коме се морају чувати;
7) документовање специфичних догађаја и података који треба да се евидентирају;
8) евидентирање свих догађаја који се односе на регистрацију корисника, укључујући и захтеве за обнављањем сертификата, а нарочито:
   (1) тип идентификационог документа који је презентован од стране корисника,
   (2) јединствени идентификациони податак о кориснику преузет из идентификационог документа,
   (3) место чувања копија апликативних и идентификационих докумената, укључујући и потписан Уговор са корисником,
   (4) специфичне елементе из Уговора са корисником,
   (5) идентитет службеника регистрационог тела који је извршио регистрацију корисника,
   (6) податке о методи која је коришћена за валидацију идентификационих докумената,
   (7) име сертификационог тела које је примило регистрационе информације и/или име регистрационог тела које је послало информације;
9) заштиту приватности података корисника;
10) евидентирање свих догађаја у вези са животним циклусом кључева сертификационог тела;
11) евидентирање свих догађаја у вези са животним циклусом квалификованих електронских сертификата;
12) евидентирање свих догађаја у вези са животним циклусом кључева којима управља сертификационо тело, укључујући и корисничке кључеве ако су генерисани у сертификационом телу;
13) евидентирање свих догађаја који се односе на припрему средстава за формирање квалификованог електронског потписа;
14) да се сви захтеви и извештаји који се односе на процедуру опозива сертификата евидентирају, укључујући и све одговарајуће активности.

Члан 41.

Сертификационо тело обезбеђује минималну могућу штету корисницима и другим заинтересованим странама у случају његовог престанка рада и континуирано чување података које се захтева у правним процедурама као доказ извршене услуге сертификације, а нарочито :

1) пре престанка пружања услуга сертификације, извршава следеће активности:

(1) информише све кориснике и друге заинтересоване стране о престанку рада,
(2) уништава, или потпуно онемогућава коришћење, својих асиметричних приватних кључева који су коришћени за формирање квалификованог електронског потписа квалификованих електронских сертификата;

2) обезбеђује неопходна финансијска средства за реализацију захтева из тачке 1) овог става;
3) Општим правилима дефинише процедуру престанка рада, која обухвата :
(1) обавештавање заинтересованих страна,
(2) евентуални пренос обавеза другим сертификационим телима,
(3) процедуру опозива издатих квалификованих електронских сертификата којима није истекао рок важности, и пренос листи опозваних сертификата другом сертификационом телу.

Обезбеђивање безбедних услова за кориснике за које се генеришу подаци за формирање квалификованог електронског потписа

Члан 42.

Сертификационо тело може, уз услуге из члана 4. овог правилника, а у складу са својим Општим и Посебним правилима, да обезбеди и средство за формирање квалификованог електронског потписа корисницима и придружену лозинку (или PIN код) за активацију средства, као и њихову безбедну дистрибуцију до корисника.

Члан 43.

Сертификационо тело обезбеђује да су кључеви корисника које оно генерише, генерисани безбедно и да је осигурана тајност приватног кључа корисника све до његове доставе кориснику и да при испоруци само корисник има приступ свом приватном кључу.

Члан 44.

Сертификационо тело обезбеђује да:
1) се асиметрични пар корисничких кључева генерише коришћењем алгоритма који је прописан да задовољи захтеве који се примењују за квалификоване електронске потписе;
2) су асиметрични кључеви корисника прописане дужине и коришћени у прописаном асиметричном криптографском алгоритму у циљу да се задовоље прописани захтеви за имплементацијом квалификованог електронског потписа.

Члан 45.

Уколико сертификационо тело обезбеђује средства за формирање квалификованог електронског потписа за кориснике, то чини на безбедан начин а нарочито обезбеђује да :
1) припрема средства за формирање квалификованог електронског потписа мора бити безбедно контролисана од стране сертификационог тела;

2) средства за формирање квалификованог електронског потписа морају бити безбедно чувана и дистрибуирана;
3) деактивирање и реактивирање средстава за формирање квалификованог електронског потписа мора бити безбедно контролисано од стране сертификационог тела;
4) уколико средства за формирање квалификованог електронског потписа имају придружене активационе податке (PIN код или лозинка) исти морају бити безбедно припремљени и дистрибуирани одвојено у односу на средство за формирање квалификованог електронског потписа. Одвојено слање може бити обезбеђено или доставом у различито време или на различити начин.

Члан 46.

Сертификационо тело које издаје квалификоване сертификате и које обезбеђује средство за формирање квалификованог електронског потписа (SSCD) корисницима мора да гарантује тајност идентификационих података (PIN код, лозинка), након што се угради у иста.

Лице кога је овластило сертификационо тело које издаје квалификоване сертификате и које обезбеђује корисницима SSCD и мора исте лично да уручи идентификованом кориснику и да од корисника узме потврду уручења у писаном облику са својеручним потписом или у електронском облику са квалификованим електронским потписом датог корисника. Издати квалификовани сертификат датом кориснику не сме да буде са могућношћу верификације, као и са могућношћу расположивости трећим лицима уз допуштење корисника, све док корисник не потврди пријем SSCD уређаја и одговарајућих идентификационих података.

Системи физичке заштите уређаја, опреме и података и сигурносна решења заштите од неовлашћеног приступа

Члан 47.

Сертификационо тело обезбеђује контролу физичког приступа својим безбедносно критичним ресурсима, као и минимизацију ризика у приступу својим кључним елементима.

Члан 48.

Сертификационо тело обезбеђује да :

1) се физички приступ просторијама у којима се обавља генерисање квалификованих електронских сертификата, припрема средстава за формирање квалификованог електронског потписа и управљање процедуром опозива сертификата, ограничи само на поуздано ауторизоване особе;
2) су имплементиране неопходне мере у циљу избегавања губитака, оштећења или компромитовања кључних ресурса и елиминисање могућности прекида пословних активности;
3) се имплементирају одговарајуће мере за спречавање компромитовања или крађе информација и/или уређаја за процесирање информација;
4) су просторије у којима се врши генерисање квалификованих електронских сертификата, припрема средстава за формирање квалификованог електронског потписа и управљање опозивом, такве да

се оперативни рад у њима одвија у окружењу које обезбеђује физичку заштиту сертификационих сервиса и ресурса од компромитације проузроковане неауторизованим приступом систему и подацима;
5) је физичка заштита успостављена креирањем јасно дефинисаних безбедносних периметара (тј. физичких баријера) којима се штите процеси генерисања квалификованих електронских сертификата, обезбеђења средстава за формирање квалификованог електронског потписа и управљање опозивом. Било који део пословне зграде који се дели са другим организацијама мора бити изван ових периметара;
6) су имплементиране одговарајуће физичке мере и контроле безбедносног окружења у циљу заштите просторија и системских елемената сертификационог тела;
7) су имплементиране одговарајуће мере у циљу заштите уређаја, информација, меморијских медија и софтвера од отуђивања са локације без прописне ауторизације;
8) се и друге специфичне безбедносне функције могу применити у оквиру истог безбедног простора који обезбеђује приступ само ауторизованим запосленим особама.

Члан 49.

Сертификационо тело обезбеђује да је приступ систему сертификације ограничен искључиво на поуздано ауторизоване особе, а нарочито обезбеђује:
1) имплементацију контрола на мрежном нивоу у циљу заштите интерне мреже сертификационог тела од екстерних мрежних домена којима може приступити трећа страна, уз забрану свих протокола и приступа који се не користе у оперативном раду сертификационог тела;
2) поуздану заштиту осетљивих података, који укључују и податке о регистрацији корисника, током проласка кроз делове мреже који нису безбедни;
3) ефикасну и поуздану администрацију корисничких приступа (укључујући операторе, администраторе и било које специфичне кориснике који имају директан приступ систему) у циљу одржавања безбедности система, укључујући и управљање налозима корисника, евидентирање и могућност модификације и забране приступа;
4) строго ограничен приступ информацијама и апликативним функцијама система у складу са Општим и Посебним правилима и политиком контроле приступа, идентификованом у њима, као и довољну рачунарско-безбедносну контролу у циљу раздвајања безбедних функција - рола у систему које су идентификоване у Општим правилима, укључујући раздвајање функција администратора безбедности и оператера, а посебно рад са корисничким програмима за управљање системом мора бити посебно ограничено и строго контролисано;
5) поуздану идентификацију и аутентикацију запослених у сертификационом телу пре коришћења критичних операција везаних за процедуре управљања сертификатима;
6) евидентирање свих активности запослених у сертификационом телу на основу одговарајућих корисничких налога и лог фајлова, који су потписани квалификованим електронским потписом;
7) поуздану заштиту безбедносно осетљивих података, који укључују и регистрационе податке корисника, од неауторизованог приступа на

основу поновног коришћења претходно обрисаних или архивираних података;

8) да се локалне мрежне компоненте (рутери и сл.) чувају у физички заштићеном окружењу и да се њихова конфигурација периодично контролише у циљу испитивања усклађености са захтевима специфицираним у Општим и Посебним правилима;
9) уређаје за континуално мониторисање и алармирање (системи за детекцију напада и системи за мониторисање контроле приступа и аларма) за појачану детекцију, регистрацију и реакцију на било какав неауторизовани и/или нерегуларни покушај приступа ресурсима која се користе за пружање услуга сертификације;
10) да апликација за дистрибуцију сертификата мора применити систем логичке контроле приступа у циљу спречавања покушаја додавања или брисања одговарајућих сертификата и модификације других придружених информација;
11) да апликација за добијање статуса опозива сертификата примењује систем логичке контроле приступа у циљу спречавања покушаја модификације информација о статусу опозива сертификата.

Информације о условима издавања и коришћења сертификата

Члан 50.

Сертификационо тело обезбеђује да су све потребне информације о условима издавања и коришћења квалификованих електронских сертификата расположиве корисницима и другим заинтересованим странама.

Члан 51.

Сертификационо тело обезбеђује расположивост информација и података о свом пословању, и то :

1) Општа правила сертификационог тела која су тренутно важећа;
2) ограничења у коришћењу Општих правила;
3) обавезе корисника;
4) информације о начину провере важности квалификованих електронских сертификата, укључујући и захтеве за проверу статуса опозива сертификата;
5) ограничења одговорности која укључују случајеве за које сертификационо тело прихвата (или одбија) одговорност;
6) временски период чувања регистрационих информација корисника;
7) временски период чувања лог фајлова за евидентирање;
8) процедуре за решавање жалби и спорова;
9) правни систем који се примењује.

Сертификационо тело обезбеђује да су информације из става 1. овог члана непрекидно расположиве коришћењем једноставних видова комуникације (Интернет и сл.) са обезбеђеним интегритетом током времена, да се могу преносити електронским путем и да су приказане на потпуно разумљив начин.

Систем управљања сертификатима

Члан 52.

Сертификационо тело обезбеђује увид у издате, опозване и суспендоване квалификоване електронске сертификате свим корисницима и другим заинтересованим странама, у складу са Законом, при чему се увид односи само на статус валидности сертификата, а не и на садржај самих сертификата.

Члан 53.

Сертификационо тело обезбеђује :

1) да је издати квалификовани електронски сертификат расположив кориснику коме је сертификат издат;
2) да су квалификовани електронски сертификати расположиви трећим лицима само у оним случајевима за које је добијен пристанак корисника и када сертификат нема на себи ЈМБГ или лични број, а у складу са Општим правилима сертификационог тела;
3) расположивост информација о условима издавања и коришћења квалификованих електронских сертификата свим заинтересованим странама у систему и да се примењени услови могу лако идентификовати за дати сертификат;
4) да су информације наведене под тач. 2) и 3) овог става расположиве 24 часа на дан, седам дана у седмици. Након пада система, или делимичног губитка могућности за обезбеђење сервиса, сертификационо тело мора да примени све расположиве мере да овај информациони сервис буде поново активан што пре, али најкасније до истека рока предвиђеног у Општим правилима.

II. НАЧИН ПРОВЕРЕ ИСПУЊЕНОСТИ УСЛОВА ЗА ИЗДАВАЊЕ КВАЛИФИКОВАНИХ ЕЛЕКТРОНСКИХ СЕРТИФИКАТА

Члан 54.

Проверу испуњености услова за издавање квалифкованих електронских сертификата (у даљем тексту: акредитација) Министарство врши у поступку разматрања захтева сертификационог тела за упис у Регистар сертификационих тела која издају квалификоване електронске сетртификате.

Члан 55.

Процедура акредитације обухвата:

1) проверу Општих правила и Посебних правила рада сертификационог тела (CP, CPS и интерна правила рада) и њихове усклађености са Законом и подзаконским општим актима;
2) атестирање и сертификацију техничких и безбедносних компонената које користи сертификационо тело за генерисање асиметричних кључева и издавање квалификованих сертификата.

Провера испуњености критеријума оперативног рада сертификационог тела

Члан 56.

Провера оперативног рада сертификационог тела обухвата:

1) процедуру регистрације корисника коме се издаје квалификовани електронски сертификат;
2) процедуру припреме захтева за издавањем квалификованог електронског сертификата у регистрационом ауторитету;
3) процедуру достављања захтева до сертификационог тела;
4) процедуру генерисања квалификованог електронског сертификата;
5) коришћење безбедних система за чување података за генерисање квалификованих електронских потписа;
6) коришћење безбедних хардверских средстава за формирање квалификованог електронског потписа (хардверски модули заштите (HSM – Hardware Security Module));
7) процедуру достављања квалификованог електронског сертификата, уређаја за генерисање електронског потписа и идентификационих података корисницима;
8) процедуру опозива сертификата;
9) процедуру обнављања сертификата;
10) процедуру суспензије сертификата;
11) начин публикације листе опозваних и суспендованих сертификата;
12) системе физичке контроле приступа у просторије сертификационог тела;
13) системе логичке контроле приступа рачунарским ресурсима сертификационог тела;
14) систем за јавно публиковање основних информација о пружању услуга сертификације, као и Општих правила рада сертификационог тела.

Провера техничких и безбедносних компоненти које користи сертификационо тело

Члан 57.

Провера техничких и безбедносних компоненти које користи сертификационо тело обухвата:

1) реализацију системских захтева безбедности;
2) издавање (дигитално потписивање) квалификованих електронских сертификата применом квалификованог електронског потписа;
3) безбедно генерисање кључева сертификационог тела.

Члан 58.

Оперативни рад сертификационог тела мора да буде усклађен стандардом CEN Workshop Agreement 14167-1 (March 2003) „Security Requirements for Trustworthy Systems Managing Sertificates for Electronic Signatures - Part 1: System Security Requirements”.

Члан 59.

Ступањем на снагу овог Правилника престаје да важи Правилник о ближим условима за издавање квалификованих електронских сертификата („Службени гласник РС”, бр. 48/05, 82/05, 116/05).

Члан 60.

Овај Правилник ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.

Број: 110-00-00014/2008-01
У Београду, 10. марта 2008. године

М И Н И С Т А Р

др Александра Смиљанић