На основу члана 31. став 3. Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/17) и члана 42. став 1. члана 43. став 3. Закона о Влади („Службени гласник РС”, бр. 55/05, 71/05 – исправка, 101/07, 65/08, 16/11, 68/12 – УС, 72/12, 7/14 – УС, 44/14 и 30/18 – др. закон),

Влада доноси

УРЕДБУ

о условима за пружање квалификованих услуга од поверења

I. УВОДНЕ ОДРЕДБЕ

Предмет уредбе

Члан 1.

Овом уредбом уређују се услови за пружање квалификованих услуга од поверења.

Сви појмови који се користе у овој уредби у мушком роду, обухватају исте појмове у женском роду.

Обављање квалификованих услуга од поверења у складу са прописима стандардима и препорукама

Члан 2.

Пружалац квалификоване услуге од поверења (у даљем тексту: пружалац услуге) обавља квалификоване услуге од поверења сагласно захтевима стандарда ETSI EN 319 401 „Electronic Signatures and Infrastructures (ETSI); General Policy Requirements For Trust Service Providers” (у даљем тексту: EN 319 401) укључујући захтеве из других стандарда на које се из тог стандарда директно и индиректно упућује, као и сагласно другим стандардима, документима и препорукама које се односе на пружање квалификованих услуга од поверења, утврђеним овом уредбом и другим прописима донетим на основу Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању (у даљем тексту: Закон).

Уговор о пружању квалификованих услуга од поверења

Члан 3.

О пружању квалификоване услуге од поверења закључује се уговор између пружаоца и корисника услуге, на захтев корисника.

Садржај аката пружаоца услуге

Члан 4.

У оквиру аката из члана 31. став 2. Закона пружалац услуге, између осталог, прецизира:

1) опште услове пружања услуга;

2) политике пружања услуга;

3) практична правила за пружање услуге и

4) политике информационе безбедности.

Општи услови за пружање услуга

Члан 5.

У складу са чланом 31. став 2. тачка 1) Закона, сагласно захтевима стандарда EN 319 401 који се односе на документ из одељка „6.2 Terms and Conditions”, пружалац услуге доноси Опште услове за пружање услуга (у даљем тексту: Општи услови) који су доступни свим корисницима услуга и поуздајућим странама.

Општи услови, између осталог, одређују политике пружања услуга које се примењују и за сваку политику прецизирају следеће:

1) обавезе корисника услуга;

2) информације за поуздајуће стране;

3) ограничења у коришћењу услуге;

4) ограничења одговорности, укључујући ограничење одговорности за штету насталу при коришћењу услуге ван оквира истакнутих ограничења;

5) временски период чувања записа у дневнику догађаја који су повезани са пружањем услуге;

6) правни оквир који се примењује на пружање услуге;

7) начин решавања приговора и спорова;

8) на који начин је оцењено да се пружање услуге врши сагласно политици пружања услуге;

9) подаци за контакт пружаоца услуге;

10) гарантовани ниво доступности услуге;

11) услови техничке подршке кориснику услуга.

Корисници услуга треба да буду прецизно информисани о Општим условима пре него што закључе уговор о пружању услуга.

Поуздајуће стране треба да буду информисане о Општим условима на начин који је погодан и примењив за дату услугу.

Пружалац услуге обезбеђује јавну доступност Општих услова на свом веб сајту, на начин који обезбеђује њихову једноставну и сталну доступност.

Политика пружања услуге и практична правила за пружање услуга

Члан 6.

Политиком пружања услуга се прецизирају правила пружања квалификоване услуге од поверења.

У оквиру једне квалификоване услуге од поверења из члана 41. став 2. Закона пружалац услуге може имати једну или више политика пружања услуге које су прилагођене појединим циљним групама корисника услуга односно прилагођене одређеним захтевима везаним за безбедност.

Практична правила дефинишу оперативне процедуре и друге услове у циљу испуњења захтева одређених политиком пружања услуге, а сагласно захтевима стандарда EN 319 401 из одељка „6.1 Trust Service Practice statement".

Практична правила за пружање квалификованих услуга од поверења треба да буду јавно доступна у оквиру аката који су јасно истакнути на веб сајту пружаоца услуге.

Форма и садржај политика и практичних правила пружања услуга могу бити додатно уређени одредбама овог и других прописа којима се уређује пружање појединих услуга од поверења.

Информациона безбедност

Члан 7.

На пружаоца услуге се сходно примењују одредбе о мерама заштите из Уредбе о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја („Службени гласник РС", број 94/16) које се односе на оператора ИКТ система од посебног значаја.

Актом који утврђује политику информационе безбедности пружалац услуге треба да испуни захтеве стандарда EN 319-401 који се односе на информациону безбедност, као и да предвиди примену мера из става 1. овог члана.

Људски ресурси

Члан 8.

У складу са чланом 31. став 1. тачка 1) Закона, и сагласно захтевима стандарда EN 319 401 који се односе на људске ресурсе, пружалац услуге обезбеђује неопходне људске ресурсе, и са њима повезане предуслове.

Осигурање од одговорности за штету насталу вршењем квалификоване услуге од поверења

Члан 9.

У складу са чланом 31. став 1. тачка 2) Закона, и сагласно захтевима стандарда EN 319 401 који се односе на осигурање од одговорности, пружалац услуге обезбеђује финансијске ресурсе за осигурање од одговорности за штету насталу вршењем квалификованих услуга од поверења.

Начин осигурања, као и одговарајући износ средстава, морају бити јасно наведени у Општим условима односно политици пружања услуге и усклађени са прописаним најнижим износом осигурања из подзаконског акта донетог на основу члана 32. Закона.

Коришћење сигурних уређаја и производа

Члан 10.

Пружалац услуге је дужан да користи сигурне уређаје и производе који су заштићени од неовлашћене промене тако да гарантују техничку безбедност и поузданост процеса које подржавају, користи сигурне системе за чување података који су му поверени и проводи мере против фалсификовања и крађе података све сагласно захтевима из одељка 7 стандарда EN 319 401, као и захтевима стандарда чија примена је прописана за поједине типове услуга од поверења.

Пружалац услуге пре почетка обављања квалификованих услуга од поверења, као и периодично, током оперативног рада, врши анализу ризика којом идентификује критичне сервисе који захтевају коришћење сигурних уређаја и производа и високе нивое сигурности.

Чување релевантних информација

Члан 11.

Информације из члана 31. став 1. тачка 6) Закона, укључују податке о регистрацији корисника и информације о значајним догађајима везаним за оперативни рад пружаоца услуге, као и за управљање кључевима и сертификатима, пружалац услуге чува сагласно захтевима из одељка 7.10 стандарда EN 319 401.

План завршетка рада пружаоца услуге

Члан 12.

План завршетка пружаоца услуге из члана 31. став 1. тачка 8) Закона, пружалац услуге доноси и ажурира сагласно захтевима из одељка 7.12 стандарда EN 319 401, а имајући у виду неопходност испуњења услова из члана 36. Закона у случају издавања квалификованих електронских сертификата.

II. ИЗДАВАЊЕ КВАЛИФИКОВАНИХ ЕЛЕКТРОНСКИХ СЕРТИФИКАТА

Квалификовани електронски сертификат

Члан 13.

Одредбе ове уредбе које се односе на издавање квалификованих електронских сертификата примењују се на издавање квалификованих сертификата за електронски потпис, издавање квалификованих сертификата за електронски печат и издавање квалификованих сертификата за аутентикацију веб сајтова.

Примена стандарда ETSI EN 319 411-2

Члан 14.

Услуга издавања квалификованих електронских сертификата обавља се сагласно захтевима стандарда ETSI EN 319 411-2 „Electronic Signatures and Infrastructures (ETSI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates” (у даљем тексту:

EN 319 411-2), укључујући захтеве из других стандарда на које се из тог стандарда директно и индиректно упућује, одговарајућим међународним стандардима и препорукама, односно другим стандардима, документима и препорукама које се односе на пружање услуге издавања квалификованих електронских сертификата, утврђеним овом уредбом.

Примена индикатора политика у стандарду EN 319 411-2

Члан 15.

Приликом примене стандарда EN 319 411-2 код издавања квалификованих електронских сертификата намењених за квалификован електронски потпис узима се у обзир индикатор политике издавања сертификата „[QCP-n-qscd]”.

Приликом примене стандарда EN 319 411-2 код издавања квалификованих електронских сертификата намењених за квалификован електронски печат узима се у обзир индикатор политике издавања сертификата „[QCP-l-qscd]”.

Приликом примене стандарда EN 319 411-2 код издавања квалификованих електронских сертификата намењених за аутентикацију веб сајтова узима се у обзир индикатор политике издавања сертификата „[QCP-l-w]”.

Политика издавања сертификата и практична правила за издавање сертификата

Члан 16.

Политика пружања услуге издавања квалификованих електронских сертификата (у даљем тексту: политика издавања сертификата) дефинише захтеве које треба да испуњава услуга издавања квалификованих електронских сертификата, док практична правила за пружање услуге издавања квалификованих електронских сертификата (у даљем тексту: практична правила за издавање сертификата) дефинишу оперативне процедуре у циљу испуњења тих захтева, тј. начин на који издавалац квалификованих електронских сертификата (у даљем тексту: издавалац сертификата) испуњава техничке, организационе и процедуралне захтеве пословања који су одређени у политици издавања сертификата.

Политика издавања сертификата се дефинише независно од специфичног оперативног окружења издаваоца сертификата, док практична правила издавања сертификата дају детаљан опис организационе структуре, оперативних процедура, као и физичко и рачунарско окружење издаваоца сертификата.

Услови које треба да испуњавају политика и практична правила

Члан 17.

Политика издавања сертификата и Практична правила издавања сертификата морају бити усклађени са одредбама Закона, одредбама прописа донетих на основу Закона, као и захтевима стандарда који су тим прописима прописани да се примењују.

Политика издавања сертификата треба да испуњава захтеве из стандарда EN 319 411-2, укључујући захтеве из других стандарда на које се из тог стандарда директно и индиректно упућује, а који се односе на политику сертификата (енгл. „certificate policy”).

Практична правила за издавање сертификата треба да испуњавају захтеве из стандарда EN 319 411-2, укључујући захтеве из других стандарда на које се из тог стандарда директно и индиректно упућује, а који се односе на изјаву о правилима сертификације (енгл. „certification practice statement”).

Одредбе политике издавања сертификата као и одредбе практичних правила за издавање сертификата треба да буду структуиране у складу са стандардом RFC 3647 „Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework”.

Сервиси које обухвата услуга издавања сертификата

Члан 18.

Издавалац сертификата дужан је да обезбеди услуге издавања сертификата које укључују следеће сервисе:

1) регистрацију корисника;

2) формирање квалификованих електронских сертификата;

3) дистрибуцију квалификованих електронских сертификата корисницима;

4) управљање животним веком (као што је обнављање, суспензија, опозив) квалификованих електронских сертификата;

5) обезбеђивање поузданог и јавно доступног сервиса за проверу статуса опозваности квалификованих електронских сертификата.

Издавалац сертификата може, поред сервиса из става 1. овог члана, да припрема, испоручује или чини доступним кориснику и средства за креирање електронског потписа односно печата и друге безбедне уређаје уколико је то предвиђено политиком издавања сертификата.

Интерна правила

Члан 19.

Издавалац сертификата утврђује и посебна интерна правила рада и заштите система издавања сертификата (у даљем тексту: интерна правила) у којима су садржани и детаљно описани поступци и мере који се примењују приликом издавања и руковања квалификованим електронским сертификатима.

Интерна правила не могу бити јавна и могу представљати пословну тајну издаваоца сертификата.

Садржај интерних правила

Члан 20.

Интерна правила садрже детаљне одредбе о:

1) систему физичке контроле приступа у поједине просторије издаваоца сертификата;

2) систему логичке контроле приступа рачунарским ресурсима издаваоца сертификата;

3) систему за чување приватног кључа издаваоца сертификата;

4) систему дистрибуиране одговорности при активацији приватног кључа издаваоца сертификата;

5) поступцима и радњама у ванредним ситуацијама (нпр. пожари, поплаве, земљотреси, друге временске непогоде, злонамерни упади у просторије или информациони систем издаваоца сертификата).

Поступање у случају тешких инцидената

Члан 21.

Издавалац сертификата обезбеђује да у случају катастрофа оперативни рад буде обновљен што је могуће пре, а у складу са политиком издавања сертификата и практичним правилима за издавање сертификата.

У случају компромитације свог асиметричног приватног кључа, издавалац сертификата:

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.

Евиденција издатих сертификата

Члан 22.

Издавалац сертификата води ажурну, тачну и безбедну евиденцију издатих квалификованих електронских сертификата.

Издавалац сертификата води ажурну и безбедну евиденцију неважећих (опозваних и суспендованих) квалификованих електронских сертификата и мора за сваки сертификат за који је издао информацију о његовој валидности учинити јавно доступном путем сервиса за проверу статуса опозваности електронских сертификата.

Утврђивање времена издавања сертификата

Члан 23.

За поуздано одређивање времена издавања и опозива квалификованих електронских сертификата, издавалац сертификата мора обезбедити извор тачног времена који је синхронизован са извором референтног времена који одреди министарство надлежно за

послове информационог друштва (у даљем тексту: Министарство) и објављује на веб сајту Министарства.

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

Тачно време издавања и опозива квалификованих електронских сертификата издавалац сертификата чува у евиденцији издатих и опозваних сертификата из члана 22. ове уредбе.

Регистрација корисника

Члан 24.

Пре издавања квалификованог електронског сертификата издавалац квалификованих електронских сертификата врши регистрацију корисника у оквиру које поуздано утврђује идентитет корисника којима издаје квалификовани електронски сертификат, као и проверу свих других података који ће бити садржани у сертификату у складу са чланом 33. Закона.

Поступке регистрације из става 1. овог члана врши овлашћени службеник издаваоца квалификованих електронских сертификата или регистрационог тела на удаљеној регистрационој локацији које успоставља издавалац сертификата за потребе регистрације корисника.

Регистрационо тело, у смислу ове уредбе, јесте организациона јединица издаваоца сертификата или друго правно лице које је од стране издаваоца сертификата овлашћено за вршење послова регистрације корисника односно одговарајућа организациона јединица таквог правног лица.

Асиметрични криптографски кључеви

Члан 25.

Подаци за креирање електронског потписа односно печата и подаци за валидацију електронског потписа односно печата технички се реализују као асиметрични пар криптогафских кључева кога чине асиметрични приватни и асиметрични јавни кључ, при чему асиметрични приватни кључ представља податке за креирање електронског потписа односно печата, а асиметрични јавни кључ представља податке за валидацију електронског потписа односно печата.

Услови за поступак регистрације корисника

Члан 26.

Издавалац сертификата је дужан да при регистрацији корисника обезбеди:

1) да пре успостављања уговорног односа са корисником, јавно информише корисника на јасном и разумљивом језику о свим релевантним условима коришћења квалификованих електронских сертификата;

2) да се, уколико се корисник идентификује као физичко лице, утврди и провери идентитет корисника на бази исправе која на основу закона служи за утврђивање идентитета, и то:

(1) уз физичко присуство, а на основу личне карте, путне исправе, стране путне исправе, путне исправе за странце или личне карте за странце или

(2) путем јавне исправе која служи као средство идентификације на даљину у складу са законом;

3) да се, уколико се корисник идентификује као правно лице:

(1) у складу са тачком 2) овог става утврди и провери идентитет овлашћеног лица корисника које у име корисника захтева издавање квалификованог електронског сертификата;

(2) провери овлашћење на бази акта корисника којим се овлашћено лице овлашћује да у име корисника захтева издавање квалификованог електронског сертификата;

(3) провере подаци о кориснику као правном лицу на бази увида у податке Агенције за привредне регистре или на бази акта надлежног органа о регистрацији правног лица;

4) да се, уколико се корисник идентификује као физичко лице које је припадник правног лица или неке организације, након поступка из тачке 2), овог става исказана припадност провери на бази:

(1) доказа да је корисник овлашћен од стране тог правног лица или организације за добијање квалификованог електронског сертификата у коме се исказује припадност правном лицу односно организацији;

(2) увида у податке Агенције за привредне регистре или на бази акта надлежног органа о регистрацији правног лица односно организације;

5) да се, уколико се корисник идентификује са додатним специфичним атрибутима, као што је ознака организационе јединице или улога у организацији где је запослен, проверава тачност информација које су исказана у таквим атрибутима;

6) проверу да ли је уредно регистрован назив интернет домена садржан у квалификованом електронском сертификату, у случају издавања квалификованог сертификата за аутентикацију веб сајта;

7) да информације садржане у квалификованом електронском сертификату буду поуздане и тачне;

8) да се од корисника прибаве тачне и поуздане информације о физичкој адреси, или другим атрибутима, који описују како се корисник може контактирати;

9) чување свих информација коришћених за верификацију идентитета корисника и документације коришћене за идентификације, као и било која ограничења њене важности;

10) да се са корисником закључи уговор који треба, нарочито, да садржи:

(1) обавезе корисника,

(2) обавезе корисника које се односе на коришћење квалификованог средства за формирање електронског потписа односно печата, уколико се кориснику издаје такво средство,

(3) обавезу издаваоца сертификата 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 одговарајућом политиком издавања сертификата,

(4) услове за публикацију сертификата,

(5) потврду да су информације садржане у сертификату коректне;

11) уговор из тачке 10) овог става се чува у року из члана 45. Закона;

12) осим код издавања квалификованог сертификата за аутентикацију веб сајта, да, уколико асиметрични пар кључева корисника није генерисан од стране тела за издавање квалификованих електронских сертификата, 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 квалификованом средству за креирање електронског потписа односно печата;

13) да се поштују одредбе важећих прописа којима се уређује заштита података о личности.

Додатни услови за уговор код сертификата за електронски потпис и печат

Члан 27.

У случају издавања квалификованог сертификата за електронски потпис или печат, уговор из члана 26. става 1. тачка 10) ове уредбе, у оквиру утврђивања обавеза корисника из члана 26. став 1. тачка 10) подтачка (1) ове уредбе, мора да укључи обавезе корисника да:

1) достави тачне и комплетне информације издаваоцу сертификата у складу са процедуром регистрације дефинисаном у политици издавања сертификата у складу са овом уредбом;

2) искључиво користи свој асиметрични приватни кључ за формирање квалификованог електронског потписа односно печата у складу са уговором;

3) онемогући неовлашћен приступ свом приватном кључу;

4) уколико корисник сам генерише асиметрични пар кључева:

(1) користи квалификовано средство за креирање електронског потписа односно печата које је уписано у Регистар квалификованих средстава за креирање електронских потписа и електронских печата,

(2) користи прописану дужину кључа и алгоритам у складу са прописима донетим на основу Закона,

(3) обезбеди да једино он поседује свој приватни кључ;

5) одмах обавести издаваоца сертификата 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 (ПИН код или лозинка) за средство за формирање квалификованог електронског потписа или других разлога,

(3) установи нетачност или измена садржаја квалификованог електронског сертификата;

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

Издавање квалификованог електронског сертификата претходно регистрованом кориснику

Члан 28.

Корисник који има важећи квалификовани електронски сертификат за електронски потпис или печат може од стране истог пружаоца услуга захтевати издавање новог квалификованог електронског сертификата за електронски потпис односно печат без поновне регистрације (у даљем тексту: поновно издавање сертификата) уколико је то предвиђено политиком издавања сертификата која се примењује.

Политика издавања сертификата из става 1. питања поновног издавања сертификата уређује сагласно захтевима стандарда ETSI EN 319 411-1. „Electronic Signatures and Infrastructures (ETSI)”, одељку 6.3.6 „Certificate renewal”.

Захтев за поновно издавање сертификата корисник потписује квалификованим електронским потписом односно печатом на бази сертификата из става 1. овог члана.

Приликом поновног издавања сертификата сходно се примењују одредбе члана 26. ове уредбе прим чему није потребна поновна идентификација корисника из члана 26. став 1. тачка 2) ове уредбе односно идентификација овлашћеног лица из члана 26. став 1. тачка 3) подтачка (1) ове уредбе уколико се подаци о кориснику односно овлашћеном лицу нису променили.

Људски ресурси које запошљава издавалац сертификата

Члан 29.

Издавалац сертификата обезбеђује неопходне људске ресурсе, и са њима повезане предуслове, а поред услова из члана 8. ове уредбе нарочито треба да обезбеди:

1) да запослени код издаваоца сертификата морају да поседују експертско знање, искуство и неопходну квалификацију за услуге које издавалац сертификата нуди, као и за одговарајуће пословне функције, и то:

(1) најмање два запослена са вишом или високом школском спремом из области информационо-комуникационих технологија и радним искуством од најмање три године у области одржавања и безбедности информационих система и положен најмање један од испита: CompTIA Security+, ISC2 CISSP или SANS GSEC, као и да запослени редовно, а најмање једном годишње похађају обуке и семинаре у циљу обнављања знања о новим безбедносним претњама и актуелним безбедносним процедурама,

(2) најмање два запослена са високом школском спремом и пет година радног искуства у области информационих система и положен најмање један од испита: ISC2 CISSP испит или SANS GSEC, као и да запослени редовно, а најмање једном годишње похађају обуке и семинаре у циљу обнављања знања о новим безбедносним претњама и актуелним безбедносним процедурама;

2) улоге и функције безбедности, утврђене у политици издавања сертификата и практичним правилима за издавање сертификата, морају бити документоване и детаљно специфициране са описима сваког радног места код издаваоца сертификата. Пословне функције од највишег нивоа поверљивости, од којих највише зависи безбедност издавања квалификованих електронских сертификата, морају бити посебно и јасно идентификоване;

3) запослени и радно ангажовани код издаваоца сертификата морају имати описе послова дефинисане са становишта раздвајања дужности и привилегија. Описи послова морају разликовати опште послове и специфичне функције издаваоца квалификованих електронских сертификата. Препоручује се да описи послова укључе и дефиниције захтева за специфичним вештинама и искуством која се траже од запослених;

4) запослени у управљачкој структури издаваоца квалификованих електронских сертификата морају да поседују експертизу у технологији инфраструктуре јавних кључева и 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 код издаваоца сертификата са безбедносним функцијама не смеју имати сукобе интереса који могу утицати на непристрасност рада у оквиру издавања квалификованих електронских сертификата;

6) безбедносне функције код издаваоца сертификата укључују следеће улоге:

(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 издаваоца квалификованих електронских сертификата 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 издаваоца сертификата 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 издаваоца сертификата;

7) запосленима код издаваоца сертификата морају бити формално додељене безбедносне функције од стране више управљачке структуре надлежне за безбедност;

8) издавалац сертификата не сме доделити безбедносне ни управљачке 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.

Управљање сопственим асиметричним кључевима

Члан 30.

Издавалац сертификата обезбеђује да су асиметрични кључеви које користи у свом раду 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 за издавање сертификата;

2) генерисање асиметричних кључева врши у средству које:

(1) је поуздан систем по EAL4 или вишем нивоу, у складу са стандардом ISO/IEC 15408 (делови 1 до 3) „Information technology – Security techniques – Evaluation criteria for IT security” и испуњава захтеве из стандарда ISO/IEC 19790:2012

„Information technology – Security techniques – Security requirements for cryptographic modules” или

(2) испуњава захтеве стандарда FIPS PUB 140-2 (2001) „Security Requirements for Cryptographic Modules” ниво 3;

3) да резервне копије приватних кључева за електронско потписивање квалификованих електронских сертификата имају исти или виши ниво безбедносних контрола у односу на кључеве који се оперативно користе.

Чување података

Члан 31.

Издавалац сертификата 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 политиком издавања сертификата и практичним правилима за издавање сертификата;

3) да су записи у вези квалификованих електронских сертификата, као и регистрационе и друге информације о кориснику, расположиви за потребе правних послова као доказ извршеног издавања сертификата;

4) поуздано архивирање тачног времена значајних догађаја код издаваоца сертификата;

5) да се информације у вези квалификованих електронских сертификата чувају онолико времена колико је потребно да се користе у правним пословима везаним за употребљене сертификате;

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 идентификационе исправе која је презентована од стране корисника односно овлашћеног лица правног лица,

(2) подаци о кориснику преузети из идентификационих исправа,

(3) место чувања копија апликативних докумената и идентификационих аката, 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 аката,

(7) име издаваоца сертификата 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 издаваоца сертификата;

11) евидентирање свих догађаја у вези са животним циклусом квалификованих електронских сертификата;

12) евидентирање свих догађаја у вези са животним циклусом кључева којима управља издавалац сертификата, укључујући и корисничке кључеве ако су генерисани од стране издаваоца сертификата;

13) евидентирање свих догађаја који се односе на припрему квалификованих средстава за креирање електронског потписа;

14) да се сви захтеви и извештаји који се односе на процедуру опозива сертификата евидентирају, укључујући и све одговарајуће активности.

Поступање код престанка рада

Члан 32.

Издавалац сертификата 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 издавања квалификованих електронских сертификата, 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) Политиком издавања сертификата и Практичним правилима за издавање сертификата дефинише процедуру престанка рада, која обухвата:

(1) обавештавање заинтересованих страна,

(2) евентуални пренос обавеза другим издаваоцима сертификата,

(3) процедуру опозива издатих квалификованих електронских сертификата којима није истекао рок важности и пренос листи опозваних сертификата другом издаваоцу сертификата.

Квалификовано средство које обезбеђује издавалац

Члан 33.

Уколико издавалац квалификованог сертификата за електронски потпис или печат обезбеђује квалификована средства за формирање електронског потписа односно печата за кориснике, то чини на безбедан начин а нарочито обезбеђује да:

1) припрема средства мора бити безбедно контролисана од стране издаваоца сертификата;

2) средства морају бити безбедно чувана и дистрибуирана;

3) деактивирање и реактивирање средстава мора бити безбедно контролисано од стране издаваоца сертификата;

4) уколико средства имају придружене активационе податке (PIN код или лозинка) исти морају бити безбедно припремљени и дистрибуирани одвојено у односу на средство. Одвојено слање може бити обезбеђено или доставом у различито време или на различити начин.

Уручење квалификованог средства

Члан 34.

Издавалац квалификованог сертификата за електронски потпис који корисницима испоручује квалификовано средство за формирање електронског потписа корисницима мора да гарантује тајност активационих података (PIN код, лозинка), након што се угради у иста.

Лице кога је овластио издавалац сертификата из става 1. овог члана корисницима лично уручује квалификовано средство за формирање електронског потписа и том приликом од корисника узима потврду уручења у писаном облику са својеручним потписом или у електронском облику са квалификованим електронским потписом датог корисника.

Издати квалификовани електронски сертификат не сме да буде са могућношћу верификације, као и са могућношћу расположивости трећим лицима уз допуштење корисника, све док корисник коме је сертификат издат не потврди пријем квалификованог средства за формирање електронског потписа и одговарајућих активационих података.

III. УПРАВЉАЊЕ КВАЛИФИКОВАНИМ СРЕДСТВОМ ЗА КРЕИРАЊЕ ЕЛЕКТРОНСКОГ ПОТПИСА ОДНОСНО ПЕЧАТА

Основне одредбе о услузи управљања квалификованим средством

Члан 35.

Услугу управљања квалификованим средством за креирање електронског потписа односно печата може да обавља само издавалац квалификованих електронских сертификата као додатну услугу за кориснике којима издаје квалификоване електронске сертификате.

При издавању квалификованог електронског сертификата из става 1. овог члана издавалац сертификата генерише асиметричан пар кључева и обезбеђује квалификовано средство за креирање електронског потписа односно печата које постаје доступно кориснику путем услуге управљања квалификованим средством за креирање електронског потписа односно печата.

Квалификовано средство за креирање електронског потписа односно печата из става 2. овог члана мора бити уписано у Регистар квалификованих средстава за креирање електронских потписа и електронских печата као средство које је предвиђено да користи путем услуге управљања квалификованим средством за креирање електронског потписа односно печата.

Политика и практична правила за пружање услуге управљања квалификованом средством

Члан 36.

Политика пружања услуге управљања средством за креирање електронског потписа је саставни део одговарајуће политике издавања сертификата.

Практична правила за пружање услуге управљања средством за креирање електронског потписа односно печата су саставни део одговарајућих практичних правила за издавање сертификата.

Искључива контрола корисника над асиметричним приватним кључем

Члан 37.

Услуга управљања квалификованим средством за креирање електронског потписа односно печата мора да буде заснована на политици пружања услуге, практичним правилима за пружање услуге, интерним правилима и техничком решењу којима се обезбеђује да корисник има искључиву контролу над својим асиметричним приватним кључем, као и да се потписивање односно печатирање коришћењем тог асиметричног приватног кључа може извршити искључиво под контролом корисника чији је то приватни кључ.

Услови за аутентикацију

Члан 38.

За аутентикацију корисника приликом коришћења услуге управљања средством за креирање електронског потписа односно печата користи се шема електронске идентификације која испуњава услове за шему електронске идентификације средњег нивоа поузданости.

Уколико је шема електронске идентификације из става 1. овог члана делом или у целини поверена трећем лицу, тада одговарајућа услуга електронске идентификације мора бити регистрована за средњи или висок ниво поузданости у складу за Законом.

IV. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 39.

Ова уредба ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.

05 број 110-3793/2018-1

У Београду, 10. маја 2018. године

Влада

Председник,

Ана Брнабић, с.р.