"Службени гласник РС", бр. 26/2008, 13/2010

На основу члана 11. Закона о електронском потпису ("Службени гласник РС", број 135/04),

Министар за телекомуникације и информатичко друштво доноси

ПРАВИЛНИК

о техничко-технолошким поступцима за формирање квалификованог електронског потписа и критеријумима које треба да испуне средства за формирање квалификованог електронског потписа

Члан 1.

Овим правилником прописују се техничко-технолошки поступци за формирање квалификованог електронског потписа и критеријуми које треба да испуне средства за формирање квалификованог електронског потписа.

Члан 2.

Техничко-технолошки поступци за формирање квалификованог електронског потписа, као и критеријуми које треба да испуњавају средства за формирање и проверу квалификованог електронског потписа морају бити у складу са одговарајућим међународним стандардима и препорукама, односно другим стандардима, документима и препорукама, које се односе на формирање и проверу квалификованог електронског потписа, утврђеним овим правилником.

Члан 3.

Квалификовани електронски потпис, поред услова из члана 7. Закона о електронском потпису (у даљем тексту: Закон), мора да задовољи и следеће ближе услове, и то:

1) да је формиран применом средства за формирање квалификованог електронског потписа (SSCD);

2) да се проверава на основу квалификованог електронског сертификата потписника - који је валидан у тренутку формирања квалификованог електронског потписа.

Члан 4.

Квалификовани електронски потпис формира се применом једног од стандардизованих асиметричних криптографских алгоритама, и то:

1) RSA (Rivest Shamir Adleman) применом стандарда PKCS#1 уз минималну дужину RSA модулуса n од 1024 бита;

2) DSA (Digital Signature Algorithm) са минималним дужинама параметара p и q од 1024 и 160 бита, респективно;

3) ECDSA (Elliptic Curve Digital Signature Algorithm) са минималним дужинама параметара p и q од 192 и 160 бита, респективно.

Члан 5.

При формирању квалификованог електронског потписа примењују се и hash функције за добијање отисака поруке фиксне величине (најмање 160 бита).

Hash функције из става 1. овог члана реализују се применом стандардизованих hash алгоритама, и то:

1) SHA-1 (Secure Hash Algorithm) - hash вредност величине 160 бита;

2) RIPEMD-160 - hash вредност величине 160 бита;

3) SHA-224, SHA-256, SHA-384 и SHA-512.

Члан 6.

Скуп стандардних алгоритама из чл. 4. и 5. овог правилника комбиновани са захтевима у вези избора параметара, као и листа стандардних комбинација примењених алгоритама у форми алгоритамских веза ("signature suites"), морају бити у складу са документом ETSI ESI SR 002 176 "Algorithms and Parameters for Secure Electronic Signatures".

Члан 7.

Средство за формирање квалификованог електронског потписа мора имати својства која омогућавају накнадну уградњу нових алгоритама у складу са даљим развојем криптографских техника и стандарда.

Члан 8.

Потписана електронска документа квалификованим електронским потписом размењују се у формату докумената у којима су уграђени основни подаци о поступку, алгоритму и квалификованом електронском сертификату потписника, како би прималац електронског документа могао проверити квалификовани електронски потпис на бази усаглашене технологије и поступака.

Члан 9.

Формат електронског документа који је потписан квалификованим електронским потписом мора бити усклађен са неким од докумената: PKCS#7 препорука, RFC 3852 "Cryptographic Message Syntax (CMS)", ETSI ESI TS 101 733 "CMS Advanced Electronic Signatures (CAdES)", RFC 3275 XMLDSIG, ETSI ESI TS 101 903 "XML Advanced Electronic Signatures (XAdES)" или ETSI ESI TS 102 778, PDF Advanced Electronic Signatures (PAdES)".

Члан 10.

Квалификовани електронски сертификат мора бити усклађен са препоруком ITU-T X.509 и 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 Revocation List (CRL) Profile" и ETSI TS 102 280 "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".

Поступци за формирање квалификованог електронског потписа треба да буду у складу са документом ETSI ESI TR 102 272 "ASN.1 format for signature policies" или са документом ETSI ESI TR 102 038 "XML format for signature policies".

Члан 11.

Поље "subject" квалификованог електронског сертификата мора да има атрибут "commonName".

У атрибут "commonName" треба да је уписано пуно име и презиме потписника, јединствени идентификатор потписника унутар сертификационог тела и опционо ЈМБГ. Подаци се уписују следећим редом: име, размак, презиме, размак, јединствени идентификатор унутар сертификационог тела и на крају, опционо, цртица и ЈМБГ. За атрибут "commonName" треба користити UTF8String кодирање, тако да сва слова из имена и презимена буду верно представљена одговарајућим карактерима.

Сертификационо тело је дужно да кориснику јасно стави до знања да ли ће сертификат садржати ЈМБГ.

Сертификати који се користе у општењу органа, општењу органа и странака, достављању и изради одлуке органа у електронском облику у управном, судском и другом поступку пред државним органом, треба да садрже ЈМБГ. Сертификате који садрже ЈМБГ или лични број сертификационо тело не сме учинити јавно доступним.

Члан 12.

Поступак провере квалификованог електронског потписа обухвата и поступак провере квалификованог електронског сертификата потписника, који се састоји од:

1) провере рока важности датог сертификата;

2) провере података о сертификационом телу које је издало квалификовани електронски сертификат потписника;

3) провере да ли се дати сертификат налази на листи опозваних сертификата.

Могуће је извршити и додатне провере у односу на став 1. овог члана уколико је то дефинисано у Правилима надлежног сертификационог тела које је издало квалификовани електронски сертификат.

Члан 13.

Формирање и провера квалификованог електронског потписа се врши применом:

1) средства за формирање квалификованог електронског потписа (SSCD);

2) безбедне апликације за формирање и проверу квалификованог електронског потписа (SSCA и SSVA, респективно);

3) техничких компонената сертификационих тела;

4) квалификованог електронског сертификата.

Члан 14.

Средства за формирање квалификованог електронског потписа, поред услова из члана 8. Закона, морају да испуне следеће критеријуме, и то:

1) да се подаци за формирање квалификованог електронског потписа генеришу у самом средству за формирање квалификованог електронског потписа и да га никад не напуштају;

2) да се квалификовани електронски потпис формира у самом средству за формирање квалификованог електронског потписа;

3) да се обезбеди коришћење средства за формирање квалификованог електронског потписа искључиво од стране потписника уз претходно реализовану поуздану процедуру аутентикације;

4) да средство мора бити такво да је потписник у могућности да га користи у различитим апликацијама и информатичко-технолошким окружењима.

Члан 15.

Безбедна апликација за израду квалификованог електронског потписа (SSCA - Secure Signature Creation Application) се користи заједно и неодвојиво од SSCD.

SSCA у себи може да садржи и безбедну апликацију за проверу квалификованог електронског потписа (SSVA - Secure Signature Verification Application) и валидацију квалификованог електронског сертификата потписника, као и приказ резултата.

Члан 16.

Техничке компоненте из делатности сертификационих тела јесу софтверски и хардверски производи који:

1) креирају податке за формирање квалификованог електронског потписа и преносе их у одговарајући хардверски уређај са карактеристикама које су у складу са овим правилником, или их генеришу директно на датом хардверском уређају;

2) чине расположивим квалификоване сертификате корисника (уз сагласност корисника и без ЈМБГ-а и личног броја) и статусе сертификата, односно листе опозваних сертификата за накнадну верификацију и проверу статуса опозваности и, ако је потребно, за преузимање од стране заинтересованих страна.

Члан 17.

Средство за формирање квалификованог електронског потписа (SSCD) из члана 14. овог правилника мора бити у складу са једним од следећих стандарда:

1) преферирано CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)";

2) FIPS 140-2 (Federal Information Processing Standard) нивоа 2 или виших.

Члан 18.

Апликација за израду квалификованог електронског потписа (SSCA) из члана 15. став 1. овог правилника треба да буде у складу са следећим стандардом CEN Workshop Agreement 14170 "Security requirements for signature creation applications".

Члан 19.

Апликација за проверу квалификованог електронског потписа (SSVA) из члана 15. став 2. овог правилника треба да буде у складу са следећим стандардом CEN Workshop Agreement 14171 "General guidelines for electronic signature verification".

Члан 20.

Техничке компоненте сертификационог тела из члана 16. овог правилника морају бити у складу са следећим стандардима:

1) За генерисање асиметричних криптографских кључева у сертификационом телу у складу са неким од стандарда:

(1) 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) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)",

(3) FIPS 140-2 (Federal Information Processing Standard) нивоа 3 или виши;

2) За генерисање квалификованих сертификата у складу са неким од стандарда:

(1) CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection profile (MCSO-PP)",

(2) CEN Workshop Agreement 14167-4: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic Module for CSP Signing Operations - Protection profile (CMCSO-PP)",

(3) CEN Workshop Agreement (CWA) 14169: "Secure Signature-Creation Device (EAL 4+)",

(4) FIPS 140-2 (Federal Information Processing Standard) нивоа 3 или виши.

Члан 21.

Програмска опрема и поступци применом којих се врши провера квалификованог електронског потписа морају у потпуности онемогућити добијање података за формирање квалификованог електронског потписа помоћу података за његову проверу.

Члан 22.

Потписник је дужан да заштити податке за формирање квалификованог електронског потписа од неовлашћеног приступа, отуђивања и неправилне употребе.

Заштита из става 1. овог члана додатно обухвата примену лозинки или ПИН кодова, биометријских поступака или других заштитних техника.

Члан 23.

Ступањем на снагу овог правилника престаје да важи Правилник о техничко-технолошким поступцима за формирање квалификованог електронског потписа и критеријумима које треба да испуне средства за формирање квалификованог електронског потписа ("Службени гласник РС", бр. 48/05, 82/05 и 116/05).

Члан 24.

Овај правилник ступа на снагу осмог дана од дана објављивања у "Службеном гласнику Републике Србије".

Број 110-00-00015/2008-01
У Београду, 10. марта 2008. године

Министар,
др **Александра Смиљанић**, с.р.