ПРАВИЛНИК
О ТЕХНИЧКО-ТЕХНОЛОШКИМ ПОСТУПЦИМА ЗА ИЗРАДУ КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПОТПИСА И ДРУГИХ УСЛУГА ПОВЈЕРЕЊА И МЈЕРАМА ЗАШТИТЕ ЕЛЕКТРОНСКОГ ПОТПИСА И ДРУГИХ УСЛУГА ПОВЈЕРЕЊА.

На основу члана 8. став 4. Закона о електронском потпису Републике Српске Закона о електронском потпису Републике Српске („Службени гласник Републике Српске“, број 106/15) и члана 82. став 2. Закона о републичкој управи („Службени гласник Републике Српске“, бр. 118/08, 11/09, 74/10, 86/10, 24/12 и 121/12), министар науке и технологије доноси

ПРАВИЛНИК
О ТЕХНИЧКО-ТЕХНОЛОШКИМ ПОСТУПЦИМА ЗА ИЗРАДУ КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПОТПИСА И ДРУГИХ УСЛУГА ПОВЈЕРЕЊА И МЈЕРАМА ЗАШТИТЕ ЕЛЕКТРОНСКОГ ПОТПИСА И ДРУГИХ УСЛУГА ПОВЈЕРЕЊА.

Члан 1.

Правилником о техничко-технолошким поступцима за израду квалификованог електронског потписа и других услуга повјерења и мјерама заштите електронског потписа и других услуга повјерења (у даљем тексу: Правилник) утврђују се техничко-технолошки поступци за израду квалификованог електронског потписа и других услуга повјерења као и мјере заштите које се морају предузети приликом креирања електронског потписа и других услуга повјерења.

Члан 2.

Одредбе овог правилника које се односе на електронски потпис и квалификовани електронски потпис, сходно се примјењују и на све остале услуге повјерења уколико посебним правилником није уређено другачије.

Члан 3.

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

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

Члан 4.

(1) Структура електронског потписа базира се на актуелној верзији ETSI TS 101 733.

(2) Уз спецификацију из става 1. овог члана, у изради структуре електронског потписа преузимају се обрасци темељени на CMS (Cryptographic Message Syntax) моделу утврђеном у документу RFC 5652 те ESS (Enhanced Security Services for S/MIME) моделу утврђеном у документу RFC 2634.

(3) Електронски потпис мора садржавати основна обиљежја (атрибуте) утврђене у CMS, ESS и ETSI TS 101 733.

Члан 5.

(1) Електронски потпис користе потписник и прималац у складу са утврђеном политиком употребе потписа.

(2) Политика употребе потписа мора се исказивати у документу читљивом корисницима потписа који морају имати могућност увида у обавезе и права која произлазе из садржаја који се потписује.

(3) За потребе машинског, односно аутоматског обрађивања електронског потписа неопходно је израдити политику употребе потписа и у форматираном облику за потребе директног преузимања од стране рачунарских програма (апликација).

(4) Форматирани облик политике употребе потписа мора бити израђен примјеном обрасца ASN.1:1997 (Abstract Syntax Notation 1) и мора имати јединствену бинарно кодирану вриједност добивену кодирањем по BER (Basic Encoding Rules)/X.209 обрасцу – ISO/IEC 8825-1 ASN.1 Encoding Rules-BER.

(5) Потписник и прималац (овјерилац) морају консултовати исту политику употребе потписа ради постизања истовјетности потписа код његове израде и овјере.

(6) За несумњиву идентификацију политике употребе потписа, у потпис се мора уградити идентификатор или садржај политике употребе потписа.

Члан 6.

(1) Код система цертификације који подржавају и користе промет докумената и сарадњу рачунарских апликација у обрасцу XML (Extended Markup Language) може се прихватити и употреба електронског потписа обликованог у складу са XAdES (XML Advanced Electronic Signatures), актуелном верзијом документа ETSI TS 101 903.

(2) Приликом употребе обрасца електронског потписа из става 1. овог члана, електронски потпис мора укључивати политику употребе електронског потписа и бити израђен у систему цертификације јавних кључева.

Члан 7.

(1) Подаци које садржи електронски потпис морају бити кодирани једним од три сљедећа обавезна обрасца кодирања: DER (Definitive Encoding Rules), Base 64, CMS (Cryptographic Message Syntax) – PKCS#7.

(2) Електронски потпис обједињује се (програмски затвара) у омотницу примјеном једног или свих сљедећих образаца: PKCS#7, ISO/IEC 9796-2 (Digital Signature Schemes), S/MIME (Secure Multipurpose Internet Mail Extensions).

(3) Сваки омот са PKCS#7 структуром мора садржавати само основни дигитални документ без заглавља или додатних обиљежја за идентификацију врсте документа.

Члан 8.

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

(2) Потписник је дужан да заштити податке за израду електронског потписа од неовлашћеног приступа, отуђивања и неправилне употребе.

(3) Заштита се мора додатно проводити примјеном лозинке, биометричким техникама или другим технологијама заштите.

Члан 9.

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

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

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

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

(5) Код израде квалификованог електронског потписа обавезно се уграђује и функција криптовања (маскирања) садржаја који се потписује (hash функција).

(6) Алгоритми који се примјењују у провођењу hash функције морају минимално бити из групе SHA-2 (Secure Hash Algorithm).

Члан 10.

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

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

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

1) податке о цертификационом тијелу које издаје квалификоване цертификате,
2) рок важаности квалификованог цертификата,
3) важаност уписа у регистру издатих квалификованих цертификата,
4) непостојање у регистру опозваних цертификата.

Члан 11.

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

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

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

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

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

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

Члан 12.

(1) Код израде квалификованог електронског потписа када се примјењује систем два (пар) криптографска кључа, дужина кључа за израду квалификованог електронског потписа мора бити дужине најмање 2048 бита, уз примјену криптографских алгоритама из класе RSA/DSA и усклађено са међународним стандардом PKCS#1 (верзија 2.2 и више).

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

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

Члан 13.

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

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

Члан 14.

Програмска опрема за израду квалификованог електронског потписа мора имати уграђене основне облике заштите у складу са документима о основним правилима заштите и сигурности средстава за израду квалификованог електронског потписа - SSCD/PP, односно EAL 4+ препорукама.

Члан 15.

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

(2) Цертификационо тијело које је примило обавјест према ставу 1. овог члана поступа у складу са интерним Правилником о поступцима цертификације.

Члан 16.

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

(2) У случајевима пружања услуга цертификације за потребе правних лица, захтјев из става 1. овог члана може се поднијети и посредством опуномоћеника.

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

(4) Цертификационо тијело које издаје квалификоване цертификате дужно је у цјелини размотрити податке који је потписник предао у захтјеву за издавање цертификата те провести физичку идентификацију потписника односно опуномоћеника у присуству истог на основу личне

карте и других релевантних докумената са фотографијом потписника (нпр. пасош) којима се потврђује истинитост података наведених у захтјеву.

Члан 17.

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

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

Члан 18.

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

(2) У случају издавања цертификата правним лицима, цертификат без приступних података се може преузети од стране опуномоћеника.

(3) Приступни подаци се достављају директно потписнику.

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

Члан 19.

Цертификат обавезно садржи сљедеће елементе:

1) серијски број (јединствен и непоновљив),
2) ознаку цертификационог тијела,
3) криптографски алгоритам примјењен код израде електронског потписа,
4) електронски потпис цертификационог тијела,
5) назив цертификационог тијела које је издало цертификат,
6) име, адресу и остале идентификационе елементе потписника неопходне за јединствену идентификацију,
7) податке неопходне за поступак овјере електронског потписа потписника на којег се односи цертификат,
8) податке за овјеру електронског потписа,
9) датум издавања и рок ваљаности цертификата,
10) једнообразни идентификациони код (Object Identifier према ASN.1) правила цертификационог тијела (ако је претходно придобио OID) по којима је креиран цертификат“.

Члан 20.

(1) Цертификат израђен примјеном обрасца X.509 v3 мора да садржи и додатне податке:

1) идентификатор кључа цертификационог тијела,
2) идентификатор кључа потписника (корисника цертификата),
3) намјене употребе кључа, основна ограничења употребе кључа,
4) политика цертификације,
5) допунски подаци о потписнику укључујући физичку/поштанску и електронску адресу и
6) поступак и мјесто приступа листи опозваних цертификата.

(2) Додатни подаци морају бити структурисани у складу са актуелном верзијом документа ETSI TS 101 862 – Qualified Certificate Profile и RFC 3739.

Члан 21.

Садржај квалификованог цертификата мора бити усклађен са техничком спецификацијом ETSI 101 862 (v1.2.1 – 2001-06 или новије) - Qualified Certificate Profile, и који се уједно базира на Qualified Certificate Profile обрасцу RFC 3739.

Члан 22.

(1) Сви подаци садржани у цертификату морају се кодирати путем два међуповезана модула:

1) ASN.1:1997 (Abstract Syntax Notation 1) усклађен са ISO/IEC 8824-1:1998 којим се описују подаци и

2) DER (Definitve Encoding Rules) којим се описује јединствен образац похране и размјене података.

(2) Цертификати (укључујући и јавне кључеве потписника код примјене система јавних кључева), морају бити похрањени у стандардном X.509 v3 формату и бити независни од модела система управљања базама података.

Члан 23.

Свака опрема укључена у систем цертификације мора бити у складу са општеприхваћеним и у употреби најзаступљенијим обрасцима.

Члан 24.

Свака опрема мора омогућити издвајање података електронског потписа и цертификата у један од најмање три основна обрасца:

1) DER Encoded Binary X.509 (*.cer),
2) Cryptographics Message Syntax Standard PKCS#7 Certificates (*.p7b) и
3) Personal Information Exchange Syntax Standard PKCS#12 (*.pfx).

Члан 25.

(1) Код употребе смарт картица нужна је могућност издвајања приватних кључева, цертификата и личних података у један од стандардних записа из члана 11. овог правилника.

(2) Код употребе смарт картица нужна је примјена ISO/IEC 7816 (1, 2, 3) те ISO 7816 (4, 5, 6, 7, 8, 9, 10) обрасца уједначавања облика, величине и функционалности картица и терминала за прихватање картица.

(3) Код употребе смарт картица у поступцима примјене електронских потписа и цертификата неопходна је примјена обрасца PKCS#15 записа криптокључева, цертификата и других података (PKCS#15 smart card file format).

(4) Уређаји/терминали за читање и писање записа на смарт картице, морају у окружењу персоналних рачунара имати подршку за техничке обрасце PCMCIA и PC/SC.

(5) Уређаји за израду, похрану и употребу података за израду електронског потписа и овјеру електронског потписа и цертификата у облику кључева и других облика (токени) морају осигурати прикључак на стандардне корисничке интерфејсе: RS232, USB, Firewire, PCMCIA, Bluetooth.

Члан 26.

Записи и електронски потписи израђени једном опремом, примјеном било којег од одабраних образаца, морају бити читљиви примјеном друге опреме уз претпоставку истовјетног алгоритма потписивања (DSS/DSA) или криптовања (PKCS#1-RSA).

Члан 27.

(1) Сваки систем цертификације који пружа услуге цертификације мора бити у непрекидном раду и јавно доступан путем телекомуникацијског система.

(2) Систем серитификације обухвата једну или више сљедећих услуга:

1) услуге регистрације корисника цертификата,
2) услуге издавања, доставе, чувања и опозива цертификата,
3) услуге управљања и чувања кључева,
4) услуге чувања потписаних записа и
5) услуге електронских именика.

Члан 28.

(1) Сваки систем цертификације мора прихватити (имати систем цертификације који мора прихватити) улазне податке у PKCS обрасцу, кодираном у DER и PEM облику.

(2) Сваки систем цертификације мора прихватати (имати систем цертификације који може управљати) минимални скуп X.509 v3 додатних атрибута у цертификатима.

Члан 29.

(1) Издати цертификат се опозива

1) истеком рока на који је издат, односно на дан престанка важења,
2) на захтјев потписника,
3) на службени захтјев суда, односно органа државне управе односно правног лица код којег је потписник запослен у тренутку подношења захтјева за опозив цертификата,
4) на захтјев цертификационог тијела у случајевима неиспуњавања техничких услова, односно ако се при употреби електронског потписа не поступа на прописан начин.

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

(3) Листа опозваних цертификата обликује се у складу са стандардом X.509 v2

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

Члан 30.

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

1) редни број радне верзије листе,
2) криптографски алгоритам коришћен при изради електронског потписа цертификационог тијела,
3) електронски потпис цертификационог тијела,
4) назив цертификационог тијела,
5) датум израде листе.

(2) Сваки опозван цертификат у Листи опозваних цертификата садржи:
1) серијски број додјељен цертификату код издавања
2) датум опозива (од којег цертификат није важећи).

Члан 31.

Сваки систем цертификације мора омогућити тренутан и несметан увид у листу опозваних цертификата код потврђивања ваљаности (од стране примаоца електронски потписаног садржаја) цертификата које је издао.

Члан 32.

(1) Цертификационо тијело утврђује временску ваљаност издатог квалификованог цертификата, односно рок до када се признаје важење издатог цертификата.
(2) Рок из става 1. овог члана за квалификоване цертификате мора се утврдити у трајању до пет година.

Члан 33.

(1) Подаци о потписницима, издати цертификати, листе опозваних цертификата као и технички подаци настали биљежењем рада система цертификације, морају се архивирати на медије који осигуравају трајност записа од најмање 20 година.
(2) У сврху чувања записа морају се израдити и сигурносне копије које морају бити смјештене на другој локацији, издвојено од система цертификације у употреби.

Члан 34.

(1) Архивирани подаци морају се чувати и заштитити од неовлаштеног приступа и могућих губитака у запису.
(2) Цертификационо тијело које издаје квалификоване цертификате мора у сврху очувања читкости и исправности записа на медијима, проводити поступке провјере и по потреби, освјеживање записа на медијима најмање два пута годишње.

Члан 35.

(1) Потписник може затражити код цертификационог тијела повремено провјеравање података за израду те података за овјеру електронског потписа.
(2) Потписник захтјев за провјеру према ставу 1. овог члана подноси лично код цертификационог тијела, а може и у електронском облику ако је такав захтјев исправно електронски постписан од стране подносиоца захтјева.

Члан 36.

(1) Цертификационо тијело које издаје квалификоване цертификате мора податке за израду свог електронског потписа одвојено распоредити на најмање два лица која заједно израђују електронски потпис.
(2) Цертификационо тијело које издаје квалификоване цертификате мора податке за израду свог електронског потписа физички и електронски заштитити у складу са утврђеним правилима и стандардима у сврху спрјечавања физичког или електронског приступа од стране неовлаштених лица.

Члан 37.

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

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

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

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

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

Члан 38.

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

Члан 39.

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

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

Члан 40.

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

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

Члан 41.

(1) Сви потписници и цертификациона тијела система цертификације уписују се у електронске именике, тј. базе података обликоване у складу са окружењем X.500 и примјеном обрасца DAP (Directory Access Protocol).

(2) Сваки електронски именик мора да садржи двије групе података:

1) јединични скуп података о цертификационом тијелу, његово једнозначно име (DN), његов цертификат и податке о листи опозваних цертификата и

2) јединични скуп података о потписницима, гдје сваког потписника дефинише његово једнозначно име (DN) и његов цертификат.

(3) Називи цертификационих тијела у електронском именику (DN) кодирају се по обрасцу ASN.1 и морају бити изражени са сљедећом минималном листом атрибута:

1) име цертификационог тијела у именику – CommonName,
2) име организационе јединице – OrganizationalUnitName,
3) име правног лица – OrganizationName,
4) мјесто/адреса – LocalityName и
5) држава – CountryName, односно адекватна доменска компонента (DC) у случају да електронски именик не подржава поље "држава"

(4) Све информације унутар електронског именика морају бити вјеродостојно приказане, што подразумијева употребу адекватног система кодовања (нпр. UTF-8).

Члан 42.

Ступањем на снагу овог Правилника престаје да важи Правилник о техничким правилима за осигурање повезаности евиденција издатих и опозваних цертификата цертификационих тијела у Републици Српској (цертификата („Службени гласник Републике Српске", број 127/11).

Члан 43.

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

Број:
Датум:

МИНИСТАР
Проф. др Јасмин Комић