РЕПУБЛИКА СРПСКА
ВЛАДА
МИНИСТАРСТВО НАУКЕ И ТЕХНОЛОГИЈЕ

ПРАВИЛНИК
О ТЕХНИЧКИМ ПРАВИЛИМА ЗА ОСИГУРАЊЕ ПОВЕЗАНОСТИ ЕВИДЕНЦИЈА ИЗДАТИХ И ОПОЗВАНИХ ЦЕРТИФИКАТА ОД ЦЕРТИФИКАЦИОНИХ ТИЈЕЛА У РЕПУБЛИЦИ СРПСКОЈ

Бања Лука, јули 2009. године

На основу члана 34. став 2. Закона о електронском потпису Републике Српске („Службени гласник Републике Српске“, број 59/08) и члана 82. став 2. Закона о републичкој управи („Службени гласник Републике Српске“, број 118/08), министар науке и технологије д о н о с и

ПРАВИЛНИК О ТЕХНИЧКИМ ПРАВИЛИМА ЗА ОСИГУРАЊЕ ПОВЕЗАНОСТИ ЕВИДЕНЦИЈА ИЗДАТИХ И ОПОЗВАНИХ ЦЕРТИФИКАТА ОД ЦЕРТИФИКАЦИОНИХ ТИЈЕЛА У РЕПУБЛИЦИ СРПСКОЈ

I ОПШТЕ ОДРЕДБЕ

Члан 1.

Овим Правилником утврђују се техничка правила и услови за осигурање повезаности евиденција издатих и опозваних цертификата цертификационих тијела у Републици Српској.

II ЕЛЕКТРОНСКИ ПОТПИС

Члан 2.

(1) Структура електронског потписа базира се на ETSI TS 101 733 V1.5.1. (2003-12) – Electronic signature formats, односно ETSI TS 101 733 V1.4.0. (2002-09) за постојеће системе цертификације, као спецификацији образаца (формата) електронског потписа.

(2) Уз спецификацију из става 1. овог члана, у изради структуре електронског потписа преузимају се образци темељени на CMS (Cryptographic Message Syntax) моделу утврђеном у документу RFC 3852 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 V1.5.1.

Члан 3.

(1) Електронски потпис мора бити уградив у све расположиве облике рачунарских записа.

(2) За потребе аутоматског препознавања врсте потписаних података може се користити образац MIME-encapsulated message (Multipurpose Internet Mail Extensions - RFC-1341).

Члан 4.

(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 произилазе 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 користити 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.

(7) Код рачунарских апликација које користе велики број историодних докумената с једном политиком употребе електронског потписа допуштено је унапријед дефинисати уградњу те политике у електронски потпис или је уградити у апликацију.

Члан 5.

Потписнику у процесу потписивања мора бити представљен и опис процедуре (поступка) потписивања у читљивом облику с најмање сљедећим скупом података:

а) упозорење – садржај правних и других чињеница повезаних с потписивањем, мора бити исказан прије чина потписивања,

б) изјава потписника – о прихватању политике употребе потписа и сазнања о садржају који потписује,

в) потписни скуп података – дио је електронског потписа и додаје се потписаном електронском запису; садржи име потписника, вријеме и мјесто потписивања и разлог/сврху потписивања.

Члан 6.

Сваки електронски потпис мора садржавати јединствени идентификатор (име потписника) који мора бити криптографски заштићен.

Члан 7.

(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) документом ETSI TS 101 903 V1.2.2. (2004-04)

(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 8.

(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.

III ЦЕРТИФИКАТ

Члан 9.

Структура цертификата базира се на обрасцу ITU X.509 v3 и укључује као обавезне садржи сљедеће дијелове:

а) верзију обрасца X.509,

б) серијски број,

в) једнозначни идентификациони код (Object Identifier према ASN.1) Општих правила цертификационог тијела (ako је претходно придобио OID),

г) ознаку (ID) алгоритма израде електронског потписа (SHA1/RSA, MD5/RSA)

д) име издаваоца цертификата – по структури утврђеној у обрасцу X.500,

ђ) период важења цертификата,

е) име потписника (корисника) цертификата – по структури утврђеној у обрасцу X.500,

ж) подаци о јавном кључу потписника,

з) јединствени идентификатор издаваоца цертификата,

и) јединствени идентификатор корисника (потписника) цертификата,

ј) додатни атрибути (проширење основног скупа атрибута), у складу са чланом 10 овог Правилника.

к) електронски потписане претходне податке од стране издаваоца цертификата.

Члан 10.

(1) Цертификат израђен примјеном обрасца X.509v3 мора садржавати и додатне атрибуте (проширење).

(2) Обвезни скуп додатних атрибута је:

а) идентификатор кључа цертификационог тијела,

б) идентификатор кључа потписника (корисника цертификата),

в) намјене употребе кључа,

г) политика цертификације,

д) допунски подаци о потписнику укључујући физичку/поштанску и електронску адресу

ђ) поступак и мјесто приступа листи опозваних цертификата.

(3) Додатни атрибути (проширење) морају бити структурисани у складу са документом ETSI TS 101 862 v1.3.2 (2004-06) – Qualified Certificate Profile и RFC 3739, који осигуравају међуповезаност квалификованих цертификата.

Члан 11.

(1) Образац и садржај квалификованих цертификата у складу са одрадбама Закона о електронском потпису Републике Српске (у даљем тексту: Закон) и смјерницама Европске уније утврђени су документом ETSI TS 101 862 V1.3.2 (2004-06) Qualified Certificate Profile.

(2) Примјена цертификата у интернет окружењу базира се на обрасцу RFC 2459 изведеном из X.509v3. Ту се придружују и сљедећи додатни обрасци:

а) RFC 3850 – S/MIME v3 Certificate Handling

б) RFC 3851 – S/MIME v3 Message Specification

в) RFC 3739 – Qualified Certificates Profiles.

Члан 12.

(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,

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.509v3 формату и бити независни о моделу система управљања базама података.

IV ОПРЕМА

Члан 13.

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

Члан 14.

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

а) DER Encoded Binary X.509 (*.cer)

б) Cryptographics Message Syntax Standard PKCS#7 Certificates (*.p7b)

в) Personal Information Exchange Syntax Standard PKCS#12 (*.pfx).

Члан 15.

(1) Код употребе смарт картица нужна је могућност издвајања приватних кључева, цертификата и личних података у један од стандардних записа из члана 14. 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 електронскох 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 i 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 (tokeni) морају осигурати прикључак на стандардне корисничке интерфејсе RS232, USB, Firewire, PCMCIA, Bluetooth.

Члан 16.

Опрема корисника система цертификације мора омогућити најмање сљедеће радње:

а) слање и примање електронски потписаних садржаја,

б) провјеравање примљених цертификата путем листе опозваних цертификата,

в) провјеравање примљених цертификата путем најмање три нивоа,

г) примање и слање критпованих запииса,

д) употребу и провјеру квалификованих цертификата,

ђ) употребу смарт картица и других медија за криптографска обраду.

Члан 17.

(1) Код употребе опреме у рачунарском окружењу, нужна је употреба API (Application Program Interface) програмских склопова којима се мора осигурати кориштење било које врсте смарт картица, PCMCIA (Personal Computer Memory Card International Association) модула, токена и других уређаја.

(2) Опрема са уграђеним API програмским склоповима мора извршавати:

а) израду електронског потписа,

б) овјеру електронског потписа,

в) обликовање података,

г) комуникацију уређаја и података.

(3) API програмски склопови морају се базирати на сљедећим криптографским обрасцима:

а) CRYPTOKI – BSAFE/PKCS (RSA) за уградњу у уређаје и програме,

б) IDUP-API (Independent Data Unit Protection) за уградњу у уређаје,

в) GSS-API (General Security Services) за уградњу у програме.

(4) Код употребе картица Fortezza нужна је примјена RFC 2876 (Use of the KEA and SKIPJACK Algorithms in CMS) обрасца повезивања процеса криптовања и процеса потписивања.

Члан 18.

(1) Свака опрема мора омогућити употребу најмање три основна сигурносна обрасца за израду и овјеру електронског потписа и израду критпованих записа:

а) Microsoft Crypto API,

б) Netscape Security Framework,

в) Entrust PKI.

(2) Опрема било које намјене, укључена у систем цертификације мора осигурати међудјеловање путем интерфејса PKCS#11 (Public Key Cryptographic Standard 11/Cryptographic Token Interface Standard – Cryptoki) независно о врсти уређаја и медија којима се израђује, користи или овјерава електроснки потпис.

(3) Записи, подаци и криптоелементи уграђени у уређаје морају бити усклађени са обрасцем PKCS#15 (Cryptographic Token Information Format), и осигурати примјену уређаја независно од врсте интерфејса израђеног у складу са обрасцем PKCS#11.

Члан 19.

(1) 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).

(2) Опрема која се користи у систему квалификованих цертификата мора бити у складу са FIPS PUB 104-1 Validation of Cryptographic Modules обрасцу сигурности уређаја, програма и записа.

Члан 20.

Свака опрема која укључује биометријске методе идентификације потписника може бити примјењена ако се придружи систему цертификације X.509 , те ако се јединствено идентификује средство за израду електронског потписа на тај начин да се гарантује да биометријски узорак може бити кориштен само с тим средством.

V СИСТЕМ ЦЕРТИФИКАЦИЈЕ

1. Услуге цертификације

Члан 21.

(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:

а) услуге регистрације корисника цертификата,
б) услуге издвања, доставе, чувања и опозива цертификата,
в) услуге управљања и чувања кључева,
г) услуге чувања потписаних записа,
д) услуге електронских именика.

Члан 22.

(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 23.

(1) Сваки систем цертификације мора осигурати повезаност са другим системима цертификације.

(2) Сваки систем цертификације мора омогућити директну комуникацију са потписницима укљученим у систем цертификације, независно којем систему цертификације припадају.

Члан 24.

(1) Поступак повезивања система цертификације базира се на примјени договорених образаца за сљедећа подручја:

а) цертификати,
б) поруке,
в) размјена цертификата и порука,
г) пренос цертификата и порука.

(2) Цертификат има договорени обавезни формат утврђен путем обрасца X.509v3.

(3) Поруке укључују:

а) упите за издавање цертификата који се исказују путем обрасца PKCS#10

б) непотписане/потписане криптоване поруке које се исказују путем обрасца PKCS#7

в) групне податке о потписнику који се исказују путем обрасца PKCS#12 (Personal Information Exchange Syntax).

(4) Размјена цертификата и порука има договорени обавезни образац CMC (Certificate Management Messages over CMS), при чему се упит за издавање цертификата темељи на потписаној PKCS#10 обликованој поруци, а одговор (цертификат) на PKCS#7 непотписаној или CMS потписаној поруци.

(5) Системи цертификације који имају могућност технолошке подршке могу користити и CMP (Certificate Management Protocols).

(6) Пренос цертификата и порука проводи се путем телекомуникацијских система уз обавезну употребу обрасца S/MIME (Secure Multipurpose Internet Mail Extensions), односно обрасца SSL (Secure Socket Layer).

2. Провјера цертификата путем листе опозваних цертификата

Члан 25.

(1) Опозвани цертификати морају се уписати у листу опозваних цертификата која мора бити доступна свим субјектима који имају приступ систему цертификације.

(2) Листа опозваних цертификата обликује се у складу са обрасцем X.509; The Directory; Authentication Framework и документом RFC 2459; PKI Certificate and CRL Profile.

Члан 26.

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

а) редни број радне верзије листе,
б)криптографски алгоритам кориштен при изради електронског потписа цертификационих тијела,
в) електронски потпис цертификационог тијела,
г) име цертификационог тијела,
д) датум израде листе.

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

а) серијски број додјељен цертификату код издавања,
б) датум опозива (од када цертификат није више важећи).

Члан 27.

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

3. Електронски именици

Члан 28.

(1) Сви потписници и субјекти система цертификације уписују се у електронске именике.

(2) Услуге електронских именика темеље се на примјени обрасца ITU-T X.500:2001 (Directory Service) – ISO/IEC 9594:2001 путем јединствене структуре (DIT-Directory Information Tree).

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

а) име субјекта у именику (физичко, правно лице) ime subjekta u imeniku – CommonName,
б) име организационе јединице– OrganizationalUnitName,
в) име правног лица – OrganizationName,
г) мјесто/адреса – LocalityName,
д) држава – CountryName (Имена и ознаке у складу са обрасцем ISO 3166-1:1997+Alpha 2).

(4) Садржај електронског именика мора бити израђен примјеном обрасца кодирања ISO/IEC 10646 – 1:2000 Universal Multiple Octet Coded Character Set (UCS) – Basic Multiple Plane (BMP), односно у складу са обрасцем UTF-8 о окружењу Unix, Linux и сродних операционих система.

Члан 29.

(1) Приступ садржајима електронских именика мора бити обликован у складу са окружењем X.500 и примјеном обрасца DAP (Directory Access Protocol).

(2) Системи цертификације могу, ради једноставнијег пружања услуга електронских именика користити LDAPv3/RFC 4510 (Lightweight Directory Access Protocol) образац обликовања и приступа електроснким именицима.

(3) LDAP електронски именици могу бити садржајно ограничени за један систем цертификације.

(4) Сваки систем цертификације мора осигурати прослијеђивање упита у електронске именике других сиситема цертификације.

(5) Прослијеђивање упита може се проводити употребом властитог електронског именика или усмјеравањем упита пружаоцу именичких услуга који за њега води електронски именик.

(6) Повезивање електронских именика који користе образац LDAP мора се проводити примјеном обрасца LDUP (LDAP Duplication/Replication/Update Protocol), путем два темељна модула:

а) Replication Information Model:2003

б) Replication Update Protocol:2003.

(7) Повезивање електронских именика који користе образац X.500 мора се проводити примјеном обрасц DISP (Directory Information Shadowing Protocol), путем примјене договорене структуре DIT (Directory Information Tree) обједињене обрасцима ISO 9594 односно X.520:1988 (Selected Attribute Types) и X.521:1988 (Selected Object Classes).

(8) Повезивање рачунарских система који пружају услуге електронских именика мора се проводити примјеном обрасца X.518:1993 којимк се дефинише образац повезивања DSP (Directory System Protocol).

Члан 30.

Сваки електронски именик мора садржавати двије групе података:

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

б) јединични скуп података о потписнику, његово једнозначно име (DN) и његов цертификат.

VI ЗАВРШНЕ ОДРЕДБЕ

Члан 31.

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

Број:
Датум:

МИНИСТАР
Бакир др Ајановић