VENDIM
Nr.525, datë 13.5.2009

PËR MIRATIMIN E RREGULLORES PËR NËNSHKRIMIN ELEKTRONIK

Në mbështetje të nenit 100 të Kushtetutës dhe të neneve 14, 19, 28, 52 e 54 të ligjit nr.9880, datë 25.2.2008 "Për nënshkrimin elektronik", me propozimin e Ministrit të Brendshëm, Këshilli i Ministrave

VENDOSI:

1. Miratimin e rregullores për nënshkrimin elektronik, sipas tekstit, që i bashkëlidhet këtij vendimi.
2. Ngarkohet Ministria e Brendshme për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTRI
Sali Berisha

RREGULLORE
PËR NËNSHKRIMIN ELEKTRONIK

I. Dispozita të përgjithshme

1. Objekti i rregullores

Në zbatim të ligjit nr.9880, datë 25.2.2008 "Për nënshkrimin elektronik", kjo rregullore përcakton:

a) Mënyrën e regjistrimit pranë autoritetit kombëtar për certifikimin elektronik (autoriteti);

b) Kërkesat e nevojshme funksionale, teknike dhe ligjore që duhet t'i zotërojnë dhe zbatojnë ofruesit e shërbimit të certifikimit, në zbatim të neneve 19 dhe 28 të ligjit;

c) Procedurat për shfuqizimin dhe çregjistrimin e certifikatave të kualifikuara dhe mënyrat e informimit, në zbatim të nenit 14 të ligjit;

d) Organizmat e testimit dhe të konfirmimit, në zbatim të nenit 52 të ligjit;

e) Njohjen dhe pranimin e nënshkrimeve elektronike dhe produkteve të huaja, në zbatim të nenit 54 të ligjit.

II. Regjistrimi

2. Regjistrimi në autoritet

a) Ofruesi i shërbimit të certifikimit regjistrohet pranë autoritetit jo më vonë se dita e fillimit të aktivitetit, dhe njëkohësisht paraqet dëshmitë e nevojshme që tregojnë se subjekti plotëson të gjitha kushtet e përcaktuara në ligj dhe në këtë rregullore.

b) Autoriteti ka të drejtë të kërkojë informacione shtesë apo përgatisë udhëzime teknike të hollësishme në lidhje me kërkesat teknike, profesionale e ligjore që përcaktohen në ligj dhe në këtë rregullore dhe, që lidhen me ushtrimin e aktivitetit nga ofruesit e shërbimit të certifikimit apo organizmit të testimit e konfirmimit.

c) Regjistrimi në autoritet duhet minimalisht të shoqërohet me këto të dhëna dhe dokumente:

i) Emrin dhe adresën e ofruesit të shërbimit të certifikimit;

ii) Dëshmitë përkatëse të fillimit të aktivitetit;

iii) Dokumentet që provojnë se plotëson kushtet ligjore, profesionale, teknike dhe financiare të përcaktuara në ligj dhe në këtë rregullore;

iv) Çdo dokument tjetër që lidhet me aktivitetin që do të kryhet.

d) Formulimi i të gjithë dokumentacionit që paraqitet pranë autoritetit duhet të jetë konform ligjeve të Republikës së Shqipërisë.

III. Kushtet ligjore, profesionale, teknike dhe financiare

3. Besueshmëria ligjore

Ofruesi i shërbimit të certifikimit që fillon aktivitetin duhet të dëshmojë se plotëson kërkesat e mëposhtme:

a) Të jetë person juridik ose fizik i regjistruar sipas legjislacionit në fuqi;

b) Të mos jetë dënuar me vendim gjykate për ndonjë nga veprat e mëposhtme:

i) Vjedhje;

ii) Mashtrim;

iii) Korrupsion;

iv) Pastrim parash;

v) Pjesëmarrje në organizata kriminale;

vi) Vepra që lidhen me veprimtaritë profesionale;

c) Të mos jetë në proces falimentimi dhe kapitalet e tij të jenë në duart e përmbaruesit ose në proces konfiskimi, si dhe kur veprimtaria e tij e biznesit është e pezulluar apo është në ndjekje ligjore për ndonjërën nga çështjet e përmendura në pikën 3(b) të kësaj rregulloreje.

4. Besueshmëria profesionale

Ofruesi i shërbimit të certifikimit demonstron se zotëron aftësitë organizativo-profesionale dhe personelin e përshtatshëm sipas kërkesave që përcaktohen në vijim:

a) Për zotërimin e aftësive organizativo-profesionale, ofruesi i shërbimit të certifikimit duhet:

i) të organizohet në atë mënyrë që krijimi dhe lëshimi i certifikatave apo nënshkrimeve elektronike të avancuara të jetë i ndarë nga çdo aktivitet tjetër i tij;

ii) të parashikojë dhe dokumentojë me shkrim të gjitha masat e detajuara në lidhje me sigurinë, në përmbushje të kërkesave ligjore dhe standardeve të sigurisë;

iii) të hartojë procedura për të vlerësuar dhe për të siguruar besueshmërinë e personelit;

iv) të hartojë procedura për të vlerësuar dhe për të siguruar vazhdimësinë e aktivitetit në rastet e emergjencave që vijnë nga fatkeqësitë natyrore, gabimi njerëzor, ndërhyrjet e qëllimshme;

v) të parashikojë që krijimi ruajtja, përdorimi dhe restaurimi i kodeve private të kryhet me pjesëmarrjen e njëkohshme e të paktën dy punonjësve të autorizuar;

vi) të përcaktojë qartë zonën e mbrojtur fizike, ku ruhen të gjitha kodet kontrolluese dhe ku menaxhohen certifikatat e lëshuara, si dhe të autorizojë punonjës të caktuar, që gëzojnë të drejtën e hyrjes në zonën e mbrojtur.

b) Për zotërimin e personelit të besueshëm ofruesi i shërbimit të certifikimit duhet:

i) të punësojë personel të specializuar në fusha të tilla si: shkencë kompjuterike, informatikë, kriptografi;

ii) të punësojë personel, që i përmbush kërkesat e pikës 3(b) të kësaj rregulloreje;

iii) të përgatisë përshkrime të qarta pune që nga koha e fillimit të aktivitetit për disa funksione minimalisht të nevojshme dhe të ndara, siç janë administratori i sistemit, administratori i sigurisë, operatori i përditshëm i sistemit dhe mbikëqyrja e administrimit të dosjeve dhe arkivave, që përmbajnë të dhëna për operacionet që kryhen nga sistemi.

5. Besueshmëria teknike

a) Ofruesi i shërbimit të certifikimit për administrimin e sigurisë aplikon metoda, që janë në përputhje me standardet e njohura ndërkombëtare;

b) Besueshmëria e sistemit të përdorur dhe siguria teknike dhe kriptografike e proceseve që kryen, konfirmohen pasi të kenë kaluar testimet e nevojshme, nga organizmat e përcaktuar në nenin 52 të ligjit dhe në këtë rregullore;

c) Metodat e vlerësimit të sigurisë së sistemit të përdorur duhet të bazohen në metodat e parashikuara nga standardet ISO 15408 (Organizata Ndërkombëtare për Standardizimet) ose më të avancuara, apo metoda ekuivalente, që janë në gjendje të bëjnë vlerësimin e sigurisë;

d) Çdo pajisje apo sistem i përdorur për certifikim nga ofruesit e shërbimit për krijimin, nënshkrimin, ruajtjen dhe administrimin e certifikatave duhet të disenjohen vetëm për këtë qëllim;

e) Çdo sistem dhe pajisje teknike e përdorur nga ofruesi i shërbimit të certifikimit për ofrimin e shërbimit për krijimin, ruajtjen dhe administrimin e certifikatave projektohet për t'u përdorur vetëm për këtë qëllim, dhe për asnjë tjetër;

f) Testimet për të verifikuar besueshmërinë e sistemeve dhe pajisjeve të përdorura nga ofruesit e shërbimit të certifikimit dhe të kërkuara sipas pikës 5 (b) të kësaj rregulloreje, bëhen

normalisht çdo 2(dy) vjet dhe sa herë që ka ndryshime në sistem, të cilat kërkojnë verifikimin e ruajtjes së besueshmërisë pas ndryshimeve;

g) Krijimi, ruajtja dhe përdorimi i çelësave privatë të çdo ofruesi të shërbimit të certifikimit duhet të realizohen brenda sistemit, me një profil mbrojtjeje në përputhje me kërkesat e sigurisë së nivelit EAL 3 (Vlerësimi i nivelit të garancisë) të vlerësimit të sigurisë ose më i avancuar, në përputhje me standardin ISO 15408 ose specifikime të tjera me nivele ekuivalente të sigurisë;

h) Ofruesi i shërbimit të certifikimit përdor pajisje dhe teknologji që mundëson realizimin e funksioneve bazë si më poshtë:

i) testimin për të provuar origjinën e informacionit të marrë dhe të shkëmbyer;

ii) testimin e integritetit të mesazheve të shkëmbyera;

iii) nënshkrimin e mesazheve të shkëmbyera;

iv) arkivimin e informacionit mbi punën e kryer dhe nënshkrimeve elektronike;

v) sigurimin e integritetit të të dhënave të ruajtura dhe të shkëmbyera, përfshirë çelësat kriptografikë të përdorur;

vi) ruajtjen e çelësave privatë të përdorur nga ofruesi i shërbimit të certifikimit;

vii) administrimin e aksesit të burimit të informacionit që lidhet me të dhënat për krijimin e nënshkrimit të avancuar, listën e certifikatave që janë mbyllur dhe korrespondenca zyrtare e ruajtur në sistem;

viii) krijimin dhe arkivimin e rekordeve të auditit të brendshëm.

i) Çdo ofrues i shërbimit të certifikimit duhet të kryejë nëpërmjet pajisjes dhe teknologjisë së instaluar prej tij këto funksione:

i) të testojë nënshkrimet elektronike të avancuara në përputhje me kërkesat teknike për nënshkrimet elektronike të parashikuara nga CEN/ISSS (Komiteti Europian për Standardizimet);

ii) të jetë në gjendje të përdorë protokollin OCSP (Protokolli i Statusit të Certifikatës On-line);

iii) ofruesi i shërbimit të certifikimit për standardet e pajisjeve dhe teknologjisë, që nuk janë përcaktuar në këtë rrregullore, përdor standardet ndërkombëtare të organizmave të specializuara si Instituti Europian i Standardeve të Telekomunikacionit (ETSI), Komiteti Europian për Standardizimet (CEN/ISSS).

6. Besueshmëria financiare

a) Ofruesi i shërbimit të certifikimit demonstron se disponon garancitë e nevojshme financiare, që bëjnë të mundur mbulimin e përgjegjësive ligjore, që rrjedhin nga neni 41 i ligjit. Garancia minimale financiare duhet të jetë 100 milionë lekë;

b) Vlera e garancisë e përcaktuar në pikën 6(a) të kësaj rregulloreje mbulohet me një depozitë ose garanci bankare, apo policë sigurimi pa kusht, të lëshuar nga një shoqëri e licencuar në fushën e sigurimeve dhe që mbulon edhe këtë kategori shërbimi. Garancitë financiare duhet të jenë të vlefshme përgjatë gjithë kohës së aktivitetit të ofruesit të shërbimit dhe duhet të mbulojnë të gjitha ngjarjet e siguruara;

c) Pavarësisht nga garancia financiare e parashikuar në pikën 6(a), ofruesi i shërbimit për çdo certifikatë të kualifikuar të lëshuar, duhet të sigurohet nga dëmet që mund t'i vijnë zotëruesit të nënshkrimit nga shkeljet e ligjit apo mosfunksionimi si duhet i produktit të tij, si më poshtë:

i) Deri në 5 milionë lekë për çdo dëm të shkaktuar, kur certifikata e kualifikuar është e kufizuar në disa veprime financiare apo kufizime të tjera të përcaktuara nga palët;

ii) Deri në 10 milionë lekë, kur certifikata e kualifikuar është e pakufizuar dhe universale.

Kërkesat e mësipërme nuk e ndalojnë ofruesin e shërbimit të certifikimit që në mënyrë vullnetare të ofrojë polica sigurimi me vlera më të larta se ato të parashikuara në këtë pikë.

7. Detyrimi për informim

Në zbatim të nenit 32 të ligjit, ofruesi i shërbimit të certifikimit është i detyruar t'i informojë aplikuesit për certifikatë të kualifikuar në lidhje me:

i) Mjetet e prodhimit e të ruajtjes së nënshkrimit dhe masat që merren në rast të humbjes ose dyshimit për përvetësim të certifikatës së kualifikuar;

ii) Mjetet e ruajtjes dhe sqarime për konfidencialitetin e të dhënave personale të përdorura;

iii) Masat e sigurisë që aplikon ofruesi i shërbimit të certifikimit për ruajtjen e nënshkrimit

elektronik;

iv) Kufizimet e mundshme që do të ketë certifikata e kualifikuar;

v) Njoftimin se përdorimi i certifikatës së kualifikuar është vullnetar;

vi) Njoftimin mbi procedurën e revokimeve;

vii) Njoftimin mbi mënyrat e zgjidhjes së mosmarrëveshjeve dhe ankesave.

Informacioni i paraqitur sipas kësaj pike, duhet të jetë hartuar në mënyrë të kuptueshme për klientët dhe t'i bëhet i ditur çdo pale të interesuar.

IV. Organizmat e testimit dhe konfirmimit

8. Njohja si organizëm testimi e konfirmimi

a) Organizëm testimi dhe konfirmimi njihet çdo organ që plotëson kushtet e mëposhtme:

i) Zotëron të gjitha certifikatat apo njohuritë e nevojshme që lidhen me certifikimin e ofruesve të shërbimit të certifikimit, me pajisjet dhe proceset, që lidhen me shërbimin e certifikimit të avancuar, të njohura nga praktika më e mirë ndërkombëtare apo organizma të standardizimit në këtë fushë;

ii) Plotëson të gjitha kërkesat e parashikuara nga pika 3 e kësaj rregulloreje;

iii) Nuk ka konflikt interesi dhe personeli i tij nuk është përfshirë në ndonjë aktivitet që mund të ndikojë në vlerësimin profesional dhe të pavarur të tyre;

iv) Zotëron pavarësi financiare në mbulimin e aktivitetit përkatës;

v) Siguron transparencë të plotë për aktivitetin që kryen dhe disponon raporte të hollësishme për çdo aktivitet të kryer;

vi) Disponon personel dhe mjete të nevojshme në lidhje me fushën apo aktivitetin specifik teknik që do të certifikojë;

vii) Garanton konfidencialitetin e informacionit të marrë gjatë ushtrimit të detyrës dhe gatishmërinë për t'ia vënë në dispozicion autoritetit kurdoherë që ndërpret aktivitetin në fjalë.

b) Autoriteti duhet të hartojë një listë të plotë të kërkesave specifike për çdo kusht të përcaktuar në pikën 8(a), si dhe të publikojë një listë të përditësuar të organizmave të testimit e konfirmimit;

c) Autoriteti mund të njohë organizmat e testimit e konfirmimit për të gjithë ose për një pjesë të proceseve apo përbërësve që lidhen me nënshkrimin elektronik;

d) Organizmi i testimit dhe konfirmimit duhet të paktën para fillimit të shërbimeve të testimit dhe konfirmimit të bëjë të njohur tarifat që do të aplikohen ndaj ofruesve të shërbimit të certifikimit;

e) Organizmi i testimit dhe konfirmimit certifikon me shkrim ose hedh poshtë plotësisht ose pjesërisht subjektin e kontrolluar. Konkluzionet i bëhen të ditura autoritetit në afatet e përcaktuara nga ky i fundit;

f) Konfliktet mes organizmave të testimit e konfirmimit dhe ofruesve të shërbimit të certifikimit zgjidhen me ndërhyrjen e autoritetit ose/dhe në rrugë gjyqësore;

g) Në rastet, kur pranë autoritetit nuk rezulton asnjë organizëm testimi dhe konfirmimi i regjistruar, aktiviteti i ofruesit të shërbimit të certifikimit quhet i mirëqenë dhe nuk ndërpritet, por afatet e raportimit dhe inspektimi nga autoriteti përgjysmohen.

9. Përjashtimet

Bëjnë përjashtim nga vlerësimi produktet e huaja të shoqëruara me deklaratën e prodhuesit, që vërteton përmbushjen e standardeve teknike ndërkombëtare të konfirmuara këto nga organizmat e testimit dhe konfirmimit në vendin e origjinës.

V. Shfuqizimi, revokimi dhe informimi i të tretëve

10. Shfuqizimi dhe revokimi i certifikatave

Shfuqizimi dhe revokimi i certifikatave bëhet në rastet e parashikuara në ligjin nr.9880, datë 25.2.2008 "Për nënshkrimin elektronik".

11. Veprimet që shoqërojnë revokimin/shfuqizimin

a) Një certifikatë e revokuar/shfuqizuar nuk mund të hyjë më në përdorim në asnjë rrethanë.

b) Ofruesi i shërbimit të certifikimit mundëson pezullimin e menjëhershëm të certifikatës, deri në daljen dhe verifikimin ose jo të shkaqeve për revokimin apo shfuqizimin e certifikatës.

c) Ofruesi i shërbimit të certifikimit njofton menjëherë zotëruesin e certifikatës elektronike rreth pezullimit/revokimit të certifikatës përkatëse dhe evidenton kryerjen e njoftimit në kohë.

d) Ofruesi i shërbimit të certifikimit siguron shërbim të vazhdueshëm për revokimin e

certifikatës 24 orë në ditë, çdo ditë të javës, duke përfshirë edhe ditët e pushimeve, në mënyrë që mbajtësi i certifikatave të kualifikuara ose/dhe personat e autorizuar ligjërisht prej tyre, mund të dorëzojnë një kërkesë revokimi apo autoriteti lëshon një urdhër shfuqizimi. Në çdo rast, para revokimit, ofruesi i shërbimit të certifikimit verifikon nëse kërkesa është paraqitur nga një person që ka të drejtë ligjore për këtë gjë.

e) Kërkesa për revokim të certifikatës së kualifikuar përpunohet menjëherë. Ofruesi i shërbimit siguron mjete të përshtatshme komunikimi elektronik dhe informon zotëruesit e certifikatave për këtë, përfshirë edhe numrat e telefonit, faksit apo çdo mjet tjetër.

f) Ofruesi i shërbimit të certifikimit siguron shërbimin për dhënien e informacionit rreth statusit të certifikatave (të vlefshme/të revokuara/shfuqizuara), gjatë gjithë kohës 24 orë në ditë, 7 ditë në javë, duke përfshirë edhe ditët e pushimit. Ky informacion duhet të pasqyrojë:

i) Statusin e çdo certifikate;

ii) Të paktën datën, kohën dhe kodin e identifikimit të certifikatave të evokuara/shfuqizuara;

iii) Të jetë i hapur dhe pa pagesë për përfituesit e certifikatave ose dhe palët e treta.

VI. Nënshkrimet dhe produktet e huaja

12. Njohja e certifikatave të huaja

Nënshkrimet elektronike dhe produktet e huaja për nënshkrimet elektronike njihen dhe zbatohen në përputhje me aktmarrëveshjet e lidhura nga Republika e Shqipërisë me shtetet e huaja për pranimin e tyre dhe shkëmbimin e të dhënave, kur gëzojnë minimalisht besueshmërinë teknike dhe sigurinë që parashikon ligji nr.9880, datë 25.2.2008 “Për nënshkrimin elektronik” dhe kjo rregullore.

13. Procedurat për njësimin e certifikatave dhe produkteve të huaja

a) Produktet dhe certifikatat e kualifikuara, të lëshuara nga një ofrues i shërbimit të certifikimit që vepron në një shtet të huaj, me të cilin Republika e Shqipërisë ka nënshkruar marrëveshje, njihen vetëm pasi ofruesi i shërbimit të certifikimit lokal do të dorëzojë në autoritet të gjithë dokumentacionin që kërkohet për njohjen e certifikatës së kualifikuar sipas ligjit dhe kësaj rregulloreje.

b) Dokumentacioni që i përket ofruesit të shërbimit të certifikimit të huaj duhet të jetë i konfirmuar nga autoriteti i vendit të origjinës se ai plotëson të gjitha kërkesat e nivelit të sigurisë dhe vlerësimit siç e përcakton ligji dhe kjo rregullore. Në çdo rast, ofruesi i shërbimit të certifikimit përgjigjet për sigurinë e certifikimeve të huaja që ai kërkon të përdorë në vendin tonë, si dhe për pasojat që mund të vijnë nga keqkuptimi i tyre.

c) Autoriteti publikon në regjistrin e përditësuar të certifikatave, kodet publike për verifikimin e certifikatave, të lëshuara nga ofruesit e shërbimit të huaj të njohura në Republikën e Shqipërisë.

VII. Dispozita kalimtare

14. Të gjitha ato subjekte që kanë filluar aktivitetin para hyrjes në fuqi të kësaj rregulloreje, brenda 30 ditëve nga miratimi i saj duhet të fillojnë procedurat e regjistrimit të parashikuara në ligj dhe në këtë rregullore.