VENDIM
Nr. 69, datë 27.1.2016

PËR MIRATIMIN E RREGULLORES "PËR IDENTIFIKIMIN ELEKTRONIK DHE SHËRBIMET E BESUARA"

Në mbështetje të nenit 100 të Kushtetutës, të neneve 14, 19, 28, 52 e 54, të ligjit nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik", dhe të neneve 5, 17 e 35, të ligjit nr. 107/2015, "Për identifikimin elektronik dhe shërbimet e besuara",

me propozimin e ministrit të Shtetit për Inovacionin dhe Administratën Publike, Këshilli i Ministrave

VENDOSI:

1. Miratimin e rregullores "Për identifikimin elektronik dhe shërbimet e besuara", sipas tekstit të rregullores dhe aneksit 1, bashkëlidhur këtij vendimi.

2. Të gjitha subjektet që kanë filluar aktivitetin para hyrjes në fuqi të kësaj rregulloreje, brenda 30 (tridhjetë) ditëve nga data e miratimit të saj, duhet të fillojnë procedurat e regjistrimit të parashikuara në ligjin nr. 107/2015, datë 1.10.2015, "Për identifikimin elektronik dhe shërbimet e besuara", dhe në këtë rregullore.

Përjashtohen nga ky detyrim ato subjekte të regjistruara pranë Autoritetit për ofrimin e nënshkrimit elektronik, sipas ligjit nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik".

3. Vendimi nr. 525, datë 13.5.2009, i Këshillit të Ministrave, "Për miratimin e rregullores për nënshkrimin elektronik", shfuqizohet.

4. Ngarkohet Autoriteti Kombëtar për Certifikimin Elektronik për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTRI
Edi Rama

RREGULLORE
PËR IDENTIFIKIMIN ELEKTRONIK DHE SHËRBIMET E BESUARA

I. DISPOZITA TË PËRGJITHSHME

1. Objekti i rregullores

Në zbatim të ligjit nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik", dhe të ligjit nr. 107/2015, datë 1.10.2015, "Për identifikimin elektronik dhe shërbimet e besuara", kjo rregullore përcakton:

a) mënyrën e regjistrimit për ofruesit e kualifikuar të shërbimit të besuar pranë Autoritetit Kombëtar për Certifikimin Elektronik (Autoriteti);

b) kërkesat e nevojshme funksionale, teknike dhe ligjore që duhet të zotërojnë dhe të zbatojnë ofruesit e kualifikuar të shërbimit të besuar, në zbatim të neneve 19 e 28, të ligjit nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik", dhe të nenit 17, të ligjit nr. 107/2015, "Për identifikimin elektronik dhe shërbimet e besuara";

c) procedurat për shfuqizimin dhe çregjistrimin e certifikatave të kualifikuara dhe mënyrat e informimit, në zbatim të nenit 14, të ligjit nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik", dhe të nenit 15, të ligjit nr. 107/2015, "Për identifikimin elektronik dhe shërbimet e besuara";

ç) organizmat e testimit dhe të konfirmimit, në zbatim të nenit 52, të ligjit nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik", dhe nenit 33, të ligjit nr. 107/2015, "Për identifikimin elektronik dhe shërbimet e besuara";

d) njohjen dhe pranimin e identifikimit elektronik e të shërbimeve të besuara dhe produkteve të huaja, në zbatim të nenit 54, të ligjit nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik", dhe të nenit 34, të ligjit nr. 107/2015, "Për identifikimin elektronik dhe shërbimet e besuara".

2. Përkufizime

Termat e përdorur në këtë rregullore kanë të njëjtin kuptim me ata të dhënë në ligjin nr. 107/2015, "Për identifikimin elektronik dhe shërbimet e besuara".

II. REGJISTRIMI

3. Regjistrimi në Autoritet

a) Ofruesi i shërbimit të besuar regjistrohet pranë Autoritetit brenda 30 (tridhjetë) ditëve nga data e fillimit të aktivitetit dhe paraqet dokumentacionin e nevojshëm që vërteton se subjekti plotëson të gjitha kushtet e përcaktuara në ligj dhe në këtë rregullore;

b) Autoriteti ka të drejtë të kërkojë informacione shtesë apo të përgatitë 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 kualifikuar të shërbimit të besuar apo organizmat e testimit dhe të konfirmimit;

c) Regjistrimi në autoritet duhet, minimalisht,

të shoqërohet me këto të dhëna dhe dokumente:

i) emrin dhe adresën e ofruesit të kualifikuar të shërbimit të besuar;

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, sipas listës së dokumentacionit të miratuar nga Autoriteti.

ç) Formulimi i të gjithë dokumentacionit që paraqitet pranë Autoritetit duhet të jetë në përputhje me legjislacionin në fuqi në Republikën e Shqipërisë.

III. KUSHTET LIGJORE, TEKNIKE, PROFESIONALE DHE FINANCIARE

4. Besueshmëria ligjore

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

a) Të jetë person juridik ose fizik i regjistruar në Republikën e Shqipërisë, sipas legjislacionit në fuqi;

b) Të mos jetë dënuar me vendim gjykate të formës së prerë për ndonjë nga veprat penale të mëposhtme:

i) vjedhje;

ii) mashtrim;

iii) korrupsion;

iv) pastrim parash;

v) pjesëmarrje në organizata kriminale;

c) Të ketë shlyer të gjitha detyrimet tatimore, duke e vërtetuar nëpërmjet dokumentacionit përkatës për këto detyrime.

ç) Të mos jetë në proces falimentimi dhe kapitalet e tij të jenë në proces konfiskimi, si dhe kur veprimtaria e tij e biznesit është e pezulluar apo është në proces për ndonjërën nga çështjet e përmendura në shkronjën "b", të pikës 4, të kësaj rregulloreje.

5. Besueshmëria teknike

5.1 Kërkesat e përgjithshme teknike që përmbush ofruesi i kualifikuar i shërbimit të besuar

a) Ofruesi i kualifikuar i shërbimit të besuar për administrimin e sigurisë aplikon metoda, që janë në përputhje me standardet e njohura ndërkombëtare për identifikimin elektronik dhe shërbimet e besuara;

b) Besueshmëria e sistemit të përdorur dhe siguria teknike e kriptografike e proceseve që kryhen, konfirmohet pasi të ketë kaluar testimet e nevojshme nga organizmat e testimit e të konfirmimit;

c) Metodat e vlerësimit të sigurisë së sistemit të përdorur duhet të bazohen në metodat e parashikuara nga standardet ISO 15408 dhe ISO 27001 (Organizata Ndërkombëtare për Standardizimet) ose më të avancuar apo metoda ekuivalente, që janë në gjendje të bëjnë vlerësimin e sigurisë;

ç) Çdo pajisje apo sistem i përdorur për certifikim nga ofruesi i kualifikuar i shërbimit të besuar për krijimin, nënshkrimin, ruajtjen dhe administrimin e certifikatave duhet të dizenjohet vetëm për këtë qëllim;

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

dh) Testimet për të verifikuar besueshmërinë e sistemeve dhe pajisjeve të përdorura nga ofruesit e shërbimit të besuar dhe të kërkuara sipas shkronjës "b", të pikës 5.1, 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 çdo ndryshimi;

e) Krijimi, ruajtja dhe përdorimi i çelësave privatë të çdo ofruesi të kualifikuar të shërbimit të besuar duhet të realizohet brenda sistemit, me një profil mbrojtjeje, në përputhje me kërkesat e sigurisë të 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;

ë) Ofruesi i shërbimit të certifikimit përdor pajisje dhe teknologji që mundësojnë 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) arkivimin e informacionit mbi punën e kryer në lidhje me lëshimin e certifikatave elektronike;

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

v) ruajtjen e çelësave privatë të përdorur nga ofruesi i kualifikuar i shërbimit të besuar;

vi) administrimin e aksesit të burimit të informacionit që lidhet me të dhënat për krijimin e identifikimit elektronik dhe shërbimeve të besuara, listën e certifikatave që janë revokuar/shfuqizuar

dhe korrespondencën zyrtare të ruajtur në sistem;

vii) krijimin dhe arkivimin e raporteve të auditit të brendshëm;

f) Çdo ofrues i kualifikuar i shërbimit të besuar duhet të kryejë nëpërmjet pajisjeve dhe teknologjisë së instaluar prej tij këto funksione:

i) të testojë identifikimin elektronik dhe shërbimet e besuara në përputhje me kërkesat teknike, të parashikuara nga Instituti Evropian i Standardeve të Telekomunikacionit (ETSI) dhe nga Komiteti Evropian për Standardizimet (CEN/ISSS);

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 rregullore, përdor standardet ndërkombëtare të organizmave të specializuar, si Instituti Evropian i Standardeve të Telekomunikacionit (ETSI), Komiteti Evropian për Standardizimet (CEN/ISSS).

5.2 Dokumentacioni teknik që duhet të zotërojë ofruesi i kualifikuar i shërbimit të besuar

A. Deklarata e praktikës dhe politika e certifikimit të shërbimit të besuar

1. Ofruesi i kualifikuar i shërbimit të besuar do të përcaktojë politikat e certifikimit dhe praktikat e duhura për shërbimet e besuara që ofron. Këto dokumente, pasi të aprovohen nga Autoriteti, publikohen dhe u komunikohen palëve të treta.

2. Ofruesi i kualifikuar i shërbimit të besuar duhet të njoftojë Autoritetin për çdo ndryshim që synon të kryejë në deklaratën e praktikës dhe politikën e certifikimit. Pas miratimit nga Autoriteti, këto dokumente vendosen menjëherë në dispozicion, sipas pikës 1.

3. Ofruesi i kualifikuar i shërbimit të besuar duhet të përcaktojë në praktikat e tij dispozita të veçanta të cilat parashikojnë ndërprerjen e shërbimit.

B. Dokumentacioni për afatet dhe kushtet për ofrimin e identifikimit elektronik dhe shërbimeve të besuara

Ofruesi i kualifikuar i shërbimit të besuar vendos në dispozicion të aplikueseve dhe zotëruesve të produkteve që ofron të gjitha afatet dhe kushtet e nevojshme.

Këto afate dhe kushte do të specifikojnë:

a) politikat që do të aplikohen për ofrimin e shërbimit të besuar;

b) çdo kufizim në përdorimin e shërbimit;

c) detyrimet e zotëruesit të certifikatës;

ç) kufizimet në përdorimin e shërbimeve, duke përfshirë kufizimin për dëmet që lindin nga përdorimi i shërbimeve në tejkalim të këtyre kufizimeve, nëse ka;

d) legjislacionin e zbatueshëm;

dh) procedurat për ankesat dhe zgjidhjen e mosmarrëveshjeve;

e) informacionin për mënyrat e kontaktimit të ofruesit të kualifikuar të shërbimit të besuar.

Zotëruesit e certifikatave do të njoftohen menjëherë për ndryshimet e detyruara të afateve dhe kushteve.

C. Dokumenti i politikave të sigurisë së informacionit

Ofruesi i kualifikuar i shërbimit të besuar duhet të disponojë një dokument të politikave të sigurisë së informacionit, i cili përcakton përqasjen e ofruesit të kualifikuar të shërbimit të besuar për menaxhimin e sigurisë së informacionit të saj. Në veçanti:

1. Politika e sigurisë së informacionit të ofruesit të kualifikuar të shërbimit të besuar dokumentohet, zbatohet dhe mirëmbahet, duke përfshirë kontro-llet e sigurisë dhe procedurat operative për sistemet dhe mjetet e informacionit që mbështetin shërbi-met e ofruara nga ofruesi i kualifikuar i shërbimit të besuar.

2. Politika e sigurisë së informacionit e ofruesit të kualifikuar të shërbimit të besuar dhe inventari i aseteve për sigurinë e informacionit, sipas pikës 6.4, do të rishikohet në intervale të planifikuara, si dhe në çdo rast kur ndodhin ndryshime. Çdo ndryshim që do të ndikojë në nivelin e sigurisë, duhet të reflektohet në dokumentin e politikave. Konfigu-rimi i sistemeve të ofruesit të kualifikuar të shërbimit të besuar do të kontrollohet rregullisht për ndryshime të cilat shkelin politikat e sigurisë.

6. Besueshmëria profesionale

6.1 Besueshmëria e ofruesit

Ofruesi i kualifikuar i shërbimit të besuar garanton se operon në mënyrë të ligjshme dhe të besueshme duke siguruar prova se përmbush kërkesat ligjore dhe teknike të aplikueshme, sipas legjislacionit në fuqi për identifikimin elektronik dhe shërbimet e besuara. Menaxhimi dhe funksionimi i ofruesit të kualifikuar të shërbimit të besuar mbështetet në politika të besueshme, të cilat konsistojnë në:

a) organizimin në atë mënyrë që krijimi dhe lëshimi i certifikatave elektronike të jetë i ndarë nga çdo aktivitet tjetër;

b) parashikimin e kryerjes së krijimit, ruajtjes,

përdorimit dhe restaurimit të kodeve private, me pjesëmarrjen e njëkohshme të të paktën dy personave të autorizuar;

c) përcaktimin e qartë të zonës së mbrojtur fizike, ku ruhen të gjitha kodet kontrolluese dhe ku menaxhohen certifikatat e lëshuara, si dhe autorizimin e punonjësve të caktuar, që gëzojnë të drejtën e hyrjes në zonën e mbrojtur;

ç) praktikën e ofrimit të shërbimit të besuar, e cila duhet të jetë jodiskriminuese;

d) shërbimin e aksesueshëm për të gjithë aplikuesit, siç specifikohet në afatet dhe kushtet e përcaktuara nga ofruesi i kualifikuar i shërbimit të besuar;

dh) burime financiare të mjaftueshme për të mbuluar dëmet e shkaktuara në përputhje me ligjin nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik", dhe ligjin nr. 107/2015, "Për identifikimin elektronik dhe shërbimet e besuara";

e) politika dhe procedura për zgjidhjen me mirëkuptim të ankesave dhe mosmarrëveshjeve me klientët ose palë të tjera rreth sigurisë së shërbimeve apo çështje tjetër të lidhur me to.

6.2 Besueshmëria e personelit

Menaxhimi dhe funksionimi i ofruesit të kualifikuar të shërbimit të besuar mbështetet në politika të cilat përcaktojnë ndarjen e detyrave dhe fushat e përgjegjësive sipas kritereve të mëposhtme:

a) Punëson staf që zotëron ekspertizën, besueshmërinë, eksperiencën dhe kualifikimet e nevojshme dhe që kanë marrë trajnim në lidhje me sigurinë dhe rregullat e mbrojtjes së të dhënave personale për shërbimet e ofruara sipas funksionit të punës;

b) Punëson personel në përputhje me shkronjën "b", të pikës 4, të kësaj rregulloreje;

c) Përcakton sanksione disiplinore për personelin, në rast të shkeljes së politikave ose procedurave të përcaktuara nga ajo;

ç) Rolet dhe përgjegjësitë e sigurisë, siç specifikohet në politikën e sigurisë së menaxhimit të ofruesit të kualifikuar të shërbimit të besuar, do të dokumentohen në përshkrimet e punës ose në dokumente të tjera të miratuara për personelin e dedikuar. Rolet e besuara, nga të cilat varet siguria e operimit të ofruesit të kualifikuar të shërbimit të besuar, duhet të identifikohen qartë. Përgjegjësitë mbi këto role janë:

i) oficerët e sigurisë janë përgjegjës për administrimin e zbatimit të praktikave të sigurisë;

ii) administratorët e sistemit janë përgjegjës për instalimin, konfigurimin dhe mirëmbajtjen e sistemeve të besueshme të ofruesit të kualifikuar të shërbimit të besuar për menaxhimin e shërbimeve;

iii) operatorët e sistemit janë përgjegjës për operimin e sistemeve të besuara në baza ditore dhe për të kryer suportin dhe rikuperimin e sistemit;

iv) audituesit e sistemit janë përgjegjës për të kontrolluar arkivat dhe për të audituar loget e sistemeve të ofruesit të kualifikuar të shërbimit të besuar;

d) Përcakton në përshkrimin e punës së punonjësve ndarjen e detyrave, aksesin e kategorizuar sipas niveleve dhe privilegjet;

dh) Siguron që personeli i roleve të besuara të mos jetë në kushtet e konfliktit të interesit, me qëllim moscenimin e veprimtarisë së ofruesit të kualifikuar të shërbimit të besuar.

6.3 Menaxhimi i aseteve

Ofruesi i kualifikuar i shërbimit të besuar siguron një nivel të duhur mbrojtjeje të aseteve, përfshirë asetet e informacionit. Gjithashtu, mban një inventar të të gjitha aseteve të informacionit dhe cakton një klasifikim në përputhje me vlerësimin e riskut.

Të gjitha asetet duhet të identifikohen dhe të inventarizohen. Ofruesi i kualifikuar i shërbimit të besuar duhet të dokumentojë rëndësinë e këtyre aseteve. Inventari i aseteve duhet të përmbajë të gjithë informacionin e nevojshëm për të rikthyer shërbimet në gjendje pune në rastin e katastrofave. Për sa më sipër, klasifikimi i informacionit duhet të dokumentohet për secilin aset. Bazuar në rëndësinë, vlerën e tij të biznesit dhe klasifikimin e sigurisë, niveli i mbrojtjes duhet të përcaktohet në proporcion të drejtë me rëndësinë e asetit.

Asetet mund të jenë të llojeve të ndryshme. Disa shembuj janë:

- Informacione: databaza, file elektronik, kontrata dhe marrëveshje, dokumentacione të sistemeve, manuale përdoruesi, materiale trajnimi, procedura operacionale dhe të suportit, planet e vazhdimësisë së biznesit, gjurmë të auditeve, informacionet e arkivuara etj.;

- Asete *software*: aplikacione, *software* të sistemit, mjete të zhvillimit *software* etj.;

- Asete fizike: pajisje kompjuterike, pajisjet e komunikacionit, mediume të lëvizshme etj.;

- Shërbimet: shërbimet kompjuterike dhe të komunikimeve, shërbime mbështetëse, si ngrohja/ftohja, elektriciteti etj.;

- Burimet njerëzore: punonjësit dhe kualifikimet e tyre, aftësitë dhe eksperienca.

Çdo aset duhet të zotërohet nga një strukturë e përcaktuar e ofruesit të kualifikuar të shërbimit të besuar. Zotëruesi i asetit duhet të jetë përgjegjës për klasifikimin e duhur të aseteve, si dhe përcaktimin e rishikimin e herëpashershëm të kufizimit dhe të klasifikimit të aksesit, duke marrë parasysh politikat e zbatueshme të kontrollit të aksesit.

6.4 Menaxhimi i mediumeve të ruajtjes së informacionit

Çdo medium trajtohet në mënyrë të sigurt, në përputhje me kërkesat e skemës së klasifikimit të informacionit. Mediumet që përmbajnë të dhëna sensitive eliminohen kur nuk janë më të nevojshme.

6.5 Kontrolli i aksesit

Aksesi në sistemin e ofruesit të kualifikuar të shërbimit të besuar duhet të jetë i limituar vetëm për individët e autorizuar. Nivelet dhe skemat e aksesit duhet të jenë në përputhje me specifikimet përkatëse në standardet e miratuara nga Instituti Evropian i Standardeve të Telekomunikacionit (ETSI) dhe nga Komiteti Evropian për Standardizimet (CEN/ISSS).

6.6 Kontrollet kriptografike

Kontrollet e sigurisë do të zbatohen për menaxhimin e çdo çelësi kriptografik dhe/ose pajisjeje kriptografike, duke u bazuar në standardet e përcaktuara dhe përputhshmërinë me kërkesat për nivelin e sigurisë që këto pajisje ofrojnë gjatë gjithë ciklit të tyre të jetës.

6.7 Siguria fizike dhe mjedisore

Ofruesi i kualifikuar i shërbimit të besuar kontrollon aksesin fizik për komponentët e sistemit, siguria e të cilëve është kritike për shërbimet e besuara dhe minimizon riskun e lidhur me sigurinë fizike. Komponentët e sistemit dhe standardet për sigurinë fizike e mjedisore përcaktohen në dokumente politikash, në përputhje me specifikimet përkatëse në standardet e miratuara nga Instituti Evropian i Standardeve të Telekomunikacionit (ETSI) dhe nga Komiteti Evropian për Standardizimet (CEN/ISSS).

6.8 Siguria e operacioneve

Ofruesi i kualifikuar i shërbimit të besuar përdor sisteme të besuara dhe produkte të mbrojtura nga modifikimet dhe garanton sigurinë teknike e besueshmërinë e procesit. Mënyra e përdorimit dhe e mbrojtjes së tyre përcaktohet në aneksin nr. 1, bashkëlidhur kësaj rregulloreje, në përputhje me specifikimet përkatëse në standardet e miratuara nga Instituti Evropian i Standardeve të Telekomunikacionit (ETSI) dhe nga Komiteti Evropian për Standardizimet (CEN/ISSS).

6.9 Siguria e rrjetit

Ofruesi i kualifikuar i shërbimit të besuar zbaton legjislacionin përkatës për mbrojtjen e rrjetit dhe të sistemit nga sulmet e mundshme, si dhe përcakton politika për mbrojtjen e tyre, në përputhje me specifikimet përkatëse në standardet e miratuara nga Instituti Evropian i Standardeve të Telekomunikacionit (ETSI) dhe nga Komiteti Evropian për Standardizimet (CEN/ISSS).

6.10 Menaxhimi i incidenteve

Ofruesi i kualifikuar i shërbimit të besuar ngre sistemin e monitorimit të proceseve të teknologjisë së informacionit në lidhje me aksesin në sistem, me qëllim menaxhimin e incidenteve. Mënyra e funksionimit të këtij sistemi përcaktohet në aneksin nr. 1, bashkëlidhur kësaj rregulloreje, në përputhje me specifikimet përkatëse në standardet e miratuara nga Instituti Evropian i Standardeve të Telekomunikacionit (ETSI) dhe nga Komiteti Evropian për Standardizimet (CEN/ISSS).

6.11 Ruajtja e të dhënave dhe mbledhja e provave

Ofruesi i kualifikuar i shërbimit të besuar ruan të gjithë informacionin në lidhje me të dhënat e gjeneruara gjatë proceseve të punës, në veçanti për qëllimin e marrjes së provave në procedime ligjore dhe për qëllimin e sigurimit të vazhdueshmërisë së shërbimit, në përputhje me ligjin nr. 9887, datë 10.3.2008, "Për mbrojtjen e të dhënave personale".

Procedurat për ruajtjen e të dhënave dhe mbledhjen e provave përcaktohen në dokumentin e politikave, të hartuar e të miratuar nga ofruesi i kualifikuar i shërbimit të besuar, në përputhje me legjislacionin shqiptar dhe me specifikimet përkatëse në standardet e miratuara nga Instituti Evropian i Standardeve të Telekomunikacionit (ETSI) dhe nga Komiteti Evropian për Standardizimet (CEN/ISSS) KE.

6.12 Menaxhimi i vazhdueshmërisë së punës

Ofruesi i kualifikuar i shërbimit të besuar ka detyrimin 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.

Në rast katastrofash, përfshirë kompromet imin e çelësit privat të nënshkrimit *root key* ose të kredencialeve të aksesit në sistemet

që mundësojnë ofrimin e shërbimeve të besuara, ofruesi i kualifikuar i shërbimit të besuar ka detyrimin të garantojë vazhdueshmërinë e punës dhe rikuperimin e të dhënave.

6.13 Vlerësimi i riskut

Ofruesi i kualifikuar i shërbimit të besuar, pasi identifikon, analizon dhe vlerëson riskun në ofrimin e shërbimit të besuar, përfshirë çështjet e menaxhimit dhe ato teknike, aplikon masat e duhura të trajtimit të riskut. Masat e trajtimit të riskut duhet të garantojnë se niveli i sigurisë është në përpjesëtim të drejtë me shkallën e riskut.

Ofruesi i kualifikuar i shërbimit të besuar përcakton të gjitha kërkesat e sigurisë dhe procedurat operacionale, që janë të nevojshme për të zbatuar masat e trajtimit të riskut të përzgjedhura, të cilat janë të dokumentuara në politikën e sigurisë së informacionit dhe deklaratën e praktikës së shërbimit të besuar. Vlerësimi rishikohet dhe përditësohet vazhdimisht.

6.14 Ndërprerja e shërbimeve të ofruesit të kualifikuar të shërbimit të besuar

a) Në rastet e ndërprerjes së veprimtarisë së ofruesit të kualifikuar të shërbimit të besuar duhet të sigurohet në vazhdimësi mirëmbajtja e vazhduar e informacionit për të verifikuar vlefshmërinë e identifikimit elektronik apo shërbimeve të besuara të ofruara para ndërprerjes së veprimtarisë. Procedurat për ndërprerjen e veprimtarisë përcaktohen në një plan të përditësuar, i cili duhet të përmbajë:

i) procedurat për garantimin e vazhdimësisë së statusit të revokimit;

ii) arkivin e logove të eventeve për periudhën e ofrimit të veprimtarisë, OCSP;

iii) informimin e të gjithë zotëruesve të produkteve dhe shërbimeve, ofrimi i të cilave do të ndërpritet prej ofruesit të kualifikuar të shërbimit të besuar;

iv) detyrimet që transferohen te një ofrues i kualifikuar i shërbimit të besuar, me qëllim mbajtjen e gjithë informacionit të nevojshëm dhe sigurimin e provave të funksionimit të ofruesit të kualifikuar të shërbimit të besuar që ka ndërprerë veprimtarinë;

v) mënyrën e asgjësimit apo të revokimit të çelësave privatë, duke përfshirë edhe kopjet sekondare të tyre, në mënyrë të tillë që çelësat privatë të mos aksesohen dhe të përdoren më tej;

b) Ofruesi i kualifikuar i shërbimit të besuar përcakton një plan për të mbuluar kostot e nevojshme për të përmbushur këto kërkesa minimale;

c) Ofruesi i kualifikuar i shërbimit të besuar mban ose transferon te një palë e besuar çelësin e tij publik ose certifikatat e kualifikuara, të lëshuara deri në përmbushjen e detyrimeve të maturuara gjatë ushtrimit të veprimtarisë.

7. Besueshmëria financiare

a) Ofruesi i kualifikuar i shërbimit të besuar demonstron se disponon garancitë e nevojshme financiare, që bëjnë të mundur mbulimin e përgjegjësive ligjore, që rrjedhin nga neni 41, i ligjit nr. 9880, datë 25.2.2008, "Për nënshkrimin elektronik", dhe neni 29, i ligjit nr. 107/2015, "Për identifikimin elektronik dhe shërbimet e besuara". Garancia minimale financiare duhet të jetë 100 (njëqind) milionë lekë;

b) Vlera e garancisë e përcaktuar në shkronjën "a", të pikës 7, 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 shkronjën "a", të pikës 7, ofruesi i kualifikuar i shërbimit të besuar 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 (pesë) 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 (dhjetë) milionë lekë, kur certifikata e kualifikuar është e pakufizuar dhe universale.

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

8. Detyrimi për informim Ofruesi i kualifikuar i shërbimit të besuar është i detyruar të informojë aplikuesit për certifikatë të kualifikuar, në lidhje me:

a) mjetet e sigurta të krijimit të identifikimit elektronik edhe për shërbimin e besuar dhe masat që merren në rast të humbjes ose dyshimit për përvetësim të këtyre mjeteve;

b) mjetet e ruajtjes dhe sqarime për konfidencialitetin e të dhënave personale të përdorura;

c) masat e sigurisë që aplikon ofruesi i kualifikuar i shërbimit të besuar për mbrojtjen nga aksesi i paautorizuar i mjeteve të krijimit të identifikimit elektronik edhe për shërbimin e besuar, si dhe të drejtat e aplikuesit si subjekt i të dhënave personale;

ç) kufizimet e mundshme që do të ketë certifikata e kualifikuar;

d) njoftimin se përdorimi i certifikatës së kualifikuar është vullnetar;

dh) njoftimin për procedurën e revokimeve;

e) njoftimin për mënyrat e zgjidhjes se mosmarrëveshjeve dhe ankesave.

Informacioni i paraqitur sipas kësaj shkronje 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 TË KONFIRMIMIT

9. 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 ofruesit të kualifikuar të shërbimit të besuar, me pajisjet dhe proceset, që lidhen me shërbimin e certifikimit të kualifikuar, të njohura nga praktika më e mirë ndërkombëtare apo organizma të standardizimit në këtë fushë;

ii) organizmi i testimit dhe të konfirmimit dhe personeli që punëson, plotëson të gjitha kërkesat e parashikuara në shkronjën "b", të pikës 4, të 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 nga ana e tyre;

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

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

vi) 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 shkronjën "a", në pikën 9, si dhe të publikojë një listë të përditësuar të organizmave të testimit e të konfirmimit;

c) Autoriteti mund të njohë organizmat e testimit e të konfirmimit për të gjitha ose për një pjesë të proceseve apo përbërësve që lidhen me identifikimin elektronik edhe shërbimin e besuar;

ç) Organizmi i testimit dhe i konfirmimit duhet, që para fillimit të shërbimeve të testimit dhe i konfirmimit, të bëjë të njohur tarifat që do të aplikohen ndaj ofruesve të kualifikuar të shërbimit të besuar;

d) Organizmi i testimit dhe i 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;

dh) Konfliktet mes organizmave të testimit e të konfirmimit dhe ofruesve të kualifikuar të shërbimit të besuar zgjidhen me ndërhyrjen e Autoritetit ose/dhe në rrugë gjyqësore;

e) Në rastet kur pranë Autoritetit nuk rezulton asnjë organizëm testimi dhe konfirmimi i regjistruar, aktiviteti i ofruesit të kualifikuar të shërbimit të besuar quhet i mirëqenë nga Autoriteti dhe nuk ndërpritet, por afatet e inspektimit nga Autoriteti përgjysmohen.

10. Përjashtimet

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

V. SHFUQIZIMI, REVOKIMI DHE INFORMIMI I PALËVE

11. 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", dhe në ligjin nr. 107/2015, "Për identifikimin elektronik dhe shërbimet e besuara".

12. Veprimet që shoqërojnë revokimin/-shfuqizimin

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

b) Ofruesi i kualifikuar i shërbimit të besuar mundëson pezullimin e menjëhershëm të

certifikatës, deri në daljen dhe verifikimin ose jo të shkaqeve për revokimin apo shfuqizimin e certifikatës;

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

ç) Ofruesi i kualifikuar i shërbimit të besuar siguron shërbim të vazhdueshëm për revokimin e certifikatës, 24 orë 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 kualifikuar i shërbimit të besuar verifikon nëse kërkesa është paraqitur nga një person që ka të drejtë ligjore për këtë gjë;

d) 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;

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

i) të pasqyrojë statusin e çdo certifikate;

ii) të pasqyrojë të paktën datën, kohën dhe kodin e identifikimit të certifikatave të revokuara/të shfuqizuara;

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

VI. NËNSHKRIMET DHE PRODUKTET E HUAJA

13. 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", ligji nr. 107/2015, "Për identifikimin elektronik dhe shërbimet e besuara", dhe kjo rregullore.

14. Procedurat për njësimin e certifikatave dhe produkteve të huaja

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

b) Dokumentacioni që i përket ofruesit të kualifikuar të shërbimit të besuar të huaj duhet të jetë i konfirmuar nga Autoriteti i vendit të origjinës se ai plotëson të gjitha kërkesat e nivelit të sigurisë dhe të vlerësimit, siç e përcakton ligji dhe kjo rregullore. Në çdo rast, ofruesi i kualifikuar i shërbimit të besuar përgjigjet për sigurinë e produkteve dhe certifikatave të huaja të lëshuara që përdoren në vendin tonë, si dhe për pasojat që mund të vijnë nga mospërmbushjet e detyrimeve nga ky ofrues;

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.

ANEKS I

1. Siguria e operacioneve

Ofruesi i kualifikuar i shërbimit të besuar duhet të përdorë sisteme dhe produkte që janë të mbrojtura kundër modifikimeve dhe garantojnë sigurinë teknike dhe besueshmërinë e proceseve të mbështetura në to. Në veçanti:

a) Një analizë e kërkesave të sigurisë duhet të kryhet gjatë dizenjimit dhe fazës së specifikimeve të çdo projekti të zhvillimit të sistemeve nga Ofruesi i kualifikuar i shërbimit të besuar, për të garantuar sigurinë në sistemet e Teknologjisë së Informacionit.

b) Integriteti i sistemeve dhe informacionit duhet të mbrohet kundër viruseve, programeve keqdashëse dhe atyre të paautorizuara.

c) Mediumet e përdorura brenda sistemeve duhet të trajtohen në mënyrë të sigurt për t'i mbrojtur ato nga dëmtimi, vjedhja, dhe aksesi i paautorizuar.

d) Procedurat e menaxhimit të mediumeve duhet t'i mbrojnë ato kundër vjetërimit dhe përkeqësimit të mediumeve brenda periudhës kohore që të dhënat janë të nevojshme për t'u ruajtur.

e) Procedurat duhet të përcaktohen dhe të zbatohen për të gjitha rolet e besuara dhe administrative që ndikojnë në sigurinë e sistemeve dhe shërbimeve.

f) Ofruesi i kualifikuar i shërbimit të besuar duhet të specifikojë dhe të zbatojë procedura të tilla që të garantojë se *security patches* aplikohen brenda një kohe të arsyeshme pasi ato janë bërë të disponueshme. Një *security patch* nuk duhet të aplikohet nëse do të paraqiste dobësi ose paqëndrueshmëri të mëtejshme që do të shmangnin përfitimet e aplikimit të tyre. Arsyeja për mos aplikimin e *security patches* duhet të dokumentohet.

2. Menaxhimi i incidenteve

Të përgjithshme

Aktivitetet e sistemit në lidhje me aksesin në sistemet IT, përdoruesi i sistemeve IT, dhe kërkesat e shërbimit do të monitorohen. Në veçanti:

a) Aktivitetet e monitorimit duhet të marrin parasysh sensitivitetin e çdo informacioni të mbledhur ose të analizuar.

b) Aktivitetet anormale të sistemit që tregojnë një shkelje potenciale të sigurisë, duke përfshirë ndërhyrjen në rrjetin e Ofruesit të kualifikuar të shërbimit të besuar, do të zbulohen dhe raportohen si emergjenca.

c) Sistemi IT i Ofruesit të kualifikuar të shërbimit të besuar do të monitorojë ngjarjet e mëposhtme:

i. Ndezja dhe fikja e funksioneve të logimit; dhe

ii. Vlefshmëria dhe përdorueshmëria e shërbimeve (*services*) thelbësore në rrjet dhe sistem.

d) Ofruesi i kualifikuar i shërbimit të besuar do të veprojë menjëherë dhe në mënyrë të koordinuar që t'i përgjigjet incidenteve dhe të kufizojë impaktin e shkeljes së sigurisë. Ofruesi i kualifikuar i shërbimit të besuar do të caktojë personelin me rol të besuar që të ndjekë të gjitha alarmet e ngjarjeve të një sigurie potencialisht kritike dhe të garantojë që incidentet përkatëse raportohen në përputhje me procedurat e tij të brendshme.

e) Ofruesi i kualifikuar i shërbimit të besuar do të përcaktojë procedura për të njoftuar palët e interesuara në përputhje me rregullat e çdo shkelje sigurie ose humbje të integritetit që ka një impakt të rëndësishëm në shërbimet e besuara të sigurta dhe mbi të dhënat personale të ruajtura në to.

f) Në rastet kur shkelja e sigurisë ose humbja e integritetit ka efekte kundrejt personit fizik ose juridik të cilit i është ofruar shërbimi, Ofruesi i kualifikuar i shërbimit të besuar do të njoftojë gjithashtu personin fizik ose juridik për shkeljen e sigurisë ose humbjen e integritetit pa vonesa.

g) Raportet e auditit do të analizohen dhe rishikohen rregullisht, për të evidentuar prova të aktivitetit keqdashës dhe njoftuar personelin për ngjarje të mundshme kritike të sigurisë.

h) Pas zbulimit të një cënueshmërie që nuk është adresuar më parë, Ofruesi i kualifikuar i shërbimit të besuar do të marrë masa e duhura për ndreqjen e saj, brenda një periudhe të arsyeshme kohore. Nëse kjo nuk është e mundur, Ofruesi i kualifikuar i shërbimit të besuar do të krijojë dhe zbatojë një plan për të ulur cënueshmërinë kritike ose do të dokumentojë bazën faktike për përcaktimin se cënueshmëria nuk kërkon ndreqje.

i) Raportime të incidentit dhe procedura përgjegjëse do të përdoren në mënyrë që dëmi nga incidentet e sigurisë dhe keqfunksionimi të minimizohet.

3. Kontrolli i aksesit

Aksesi në sistemin e Ofruesit të kualifikuar të shërbimit të besuar do të jetë i mundur vetëm për personat e autorizuar. Në veçanti:

a) Kontrollet do të mbrojnë *domainet* e rrjetit të brendshëm nga aksesi i paautorizuar duke përfshirë aksesin nga zotëruesit dhe palët e treta. *Firewall-et* duhet të konfigurohen në mënyrë të tillë, për të parandaluar të gjitha protokollet dhe akseset që nuk nevojiten për funksionet e Ofruesit të kualifikuar të shërbimit të besuar.

b) Ofruesi i kualifikuar i shërbimit të besuar do të administrojë aksesin e përdoruesve, operatorëve, administratorëve dhe audituesve të sistemit. Administrimi do të përfshijë menaxhimin e llogarisë së përdoruesit, auditimin, modifikimin kohë pas kohe dhe heqjen e aksesit.

c) Aksesi tek informacioni dhe zbatimi i funksioneve të sistemit do të kufizohet në përputhje me politikat e kontrollit të aksesit. Sistemi do të sigurojë kontrolle të mjaftueshme të sigurisë kompjuterike, të roleve të besuara të identifikuara në praktikat e Ofruesit të kualifikuar të shërbimit të besuar, duke përfshirë ndarjen e administrimit të sigurisë dhe funksionet e zbatimit. Veçanërisht, përdorimi i programeve mbështetëse do të kufizohet dhe kontrollohet.

a) Personeli i Ofruesit të kualifikuar të shërbimit të besuar do të identifikohet dhe autentifikohet përpara përdorimit të funksioneve kritike të lidhura me shërbimet. Personeli do të jetë përgjegjës për aktivitet e kryera.

f) Të dhënat sensitive do të mbrohen kundër zbulimit nëpërmjet mjeteve të ripërdorshme të ruajtjes së të dhënave.