



REPUBLIKA E SHQIPËRISË
KËSHILLI I MINISTRAVE

PROJEKTVENDIM

Nr.____, datë _____.2015

**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 neneve 5, 17 dhe 35 të Ligjit nr. 107/2015, datë 1.10.2015 “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 që i bashkëlidhet këtij vendimi.
2. Ngarkohet Autoriteti Kombëtar për Certifikimin Elektronik për zbatimin e këtij vendimi.
3. Vendimi i Këshillit të Ministrave Nr. 525, datë 13.5.2009, “Për miratimin e rregullores për nënshkrimin elektronik”, shfuqizohet.

Ky vendim hyn në fuqi menjëherë.

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 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 zbatojnë Ofruesit e kualifikuar të shërbimit të besuar, në zbatim të neneve 19 dhe 28 të Ligjit nr. 9880, datë 25.2.2008 “Për nënshkrimin elektronik” dhe nenit 17 të Ligjit nr. 107/2015, datë 1.10.2015 “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 nenit 15 të Ligjit nr. 107/2015, datë 1.10.2015 “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, datë 1.10.2015 “Për identifikimin elektronik dhe shërbimet e besuara”;

d) Njohjen dhe pranimin e identifikimit elektronik dhe shërbimeve të besuara dhe produkteve të huaja, në zbatim të nenit 54 të Ligjit nr. 9880, datë 25.2.2008 “Për nënshkrimin elektronik” dhe nenit 34 të Ligjit nr. 107/2015, datë 1.10.2015 “Për identifikimin elektronik dhe shërbimet e besuara”.

2. Përkufizime

Termat e përdorura në këtë Rregullore kanë të njëjtin kuptim me ato të dhëna në Ligjin nr. 107/2015, datë 1.10.2015 “Për identifikimin elektronik dhe shërbimet e besuara”.

II. RREGJISTRIMI

3. Regjistrimi në Autoritet

a) Ofruesi i shërbimit të besuar regjistrohet pranë Autoritetit brenda 30 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 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 kualifikuar të shërbimit të besuar apo Organizmat e testimit dhe 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 konform ligjeve të Republikës së 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 RSH, 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 veprimtarinë 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 ndonjë nga çështjet e përmendura në pikën 4(b) 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 dhe kriptografike e proceseve që kryen, konfirmohet pasi të ketë kaluar testimet e nevojshme nga Organizmat e testimit dhe konfirmimit;
- c) Metodat e vlerësimit të sigurisë së sistemit të përdorur duhet të bazohen në metodat e parashikuara nga standartet ISO 15408 dhe ISO 27001 (Organizata Ndërkombëtare për Standartizimet) 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 dizajnohet vetëm për këtë qëllim;
- d) Çdo sistem dhe pajisje teknike e përdorur nga Ofruesi i kualifikuar të 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 pikës 5.1 (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 çdo ndryshimi;
- e) Krijimi, ruajtja dhe përdorimi i çelësave privat 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 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;
- iv) Arkivimin e informacionit mbi punën e kryer në lidhje me lëshimin e certifikatave elektronike;
- v) Sigurimin e integritetit të të dhënave të ruajtura dhe të shkëmbyera, përfshirë çelësat kriptografik të përdorur;
- vi) Ruajtjen e çelësve privat të përdorur nga Ofruesi i kualifikuar i shërbimit të besuar;
- vii) 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;
- viii) 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 Komiteti Evropian për Standartizimet (CEN/ISSS);
 - ii) Të jetë në gjendje të përdorë protokollin OCSP (Protokolli i Statusit të Certifikatës Online);
 - 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 specializuara 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.

a.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;

a.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 a.1, më sipër;

a.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. Dokumentacion mbi 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 mbi mënyrat e kontaktimit të Ofruesit të kualifikuar të shërbimit të besuar.

Zotëruesit e certifikatave, do të njoftohen menjëherë mbi ndryshimet e detyruara e 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 përjasjen 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 kontrollet e sigurisë dhe procedurat operative për sistemet dhe mjetet e informacionit që mbështesin shërbimet 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. Konfigurimi 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 privatë, me pjesëmarrjen e njëkohëshme 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) Praktika të ofrimit të shërbimit të besuar të cilat duhet të jenë jo diskriminuese;
- d) Shërbime të 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, në përputhje me ligjin për të mbuluar detyrimet që lindin nga operacionet dhe/ose aktivitetet e tij;
- e) Politika dhe procedura për zgjidhjen me mirëkuptim të ankesave dhe mosmarrëveshjeve me klientët ose palë të tjera, rreth sigurisë të 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 kriterëve 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 pikën 4 (b), 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 audituar loget e sistemeve të Ofruesit të kualifikuar të shërbimit të besuar;
- d) përcaktojë 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 mos cënimin e veprimtarisë së Ofruesit të kualifikuar të shërbimit të besuar.

6.3 Menaxhimi i aseteve

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

6.4 Menaxhimi i medimeve të ruajtjes së informacionit

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

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 Instituti Evropian i Standardeve të Telekomunikacionit (ETSI) dhe Komiteti Evropian për Standartizimet (CEN/ISSS).

6.6 Kontrollat kriptografike

Kontrollet e sigurisë do të zbatohen për menaxhimin e çdo çelësi kriptografik dhe/ose pajisje kriptografike, duke u bazuar në standardet e përcaktuara dhe përputhshmërinë me kërkesat mbi 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. Komponentet e sistemit dhe standardet mbi sigurinë fizike dhe mjedisore, përcaktohen në dokumente politikash në përputhje me specifikimet përkatëse në standardet e miratuara nga Instituti Evropian i Standardeve të Telekomunikacionit (ETSI) dhe Komiteti Evropian për Standartizimet (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 dhe besueshmërinë e procesit. Mënyra e përdorimit dhe 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 Komiteti Evropian për Standartizimet (CEN/ISSS).

6.9 Siguria e rrjetit

Ofruesi i kualifikuar i shërbimit të besuar zbaton legjislacionin përkatës për mbrojtjen e rrjetit dhe 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 Komiteti Evropian për Standartizimet (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 Komiteti Evropian për Standartizimet (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 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 Komiteti Evropian për Standartizimet (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 komprometimin 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) arkivën e logeve të eventeve për periudhën e ofrimit të veprimtarisë, *OCSP*;
 - iii) informimin e të gjithë zotëruesve të produkteve dhe shërbimeve ofrimi i të cilëve do ndërpritet prej Ofruesit të kualifikuar të shërbimit të besuar;

iv) detyrimet që transferohen tek 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 revokimit të çelësave privat, duke përfshirë edhe kopjet sekondare të tyre, në mënyrë të tillë që çelësat privat 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 tek 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, datë 1.10.2015 “Për identifikimin elektronik dhe shërbimet e besuara”. Garancia minimale financiare duhet të jetë 100 (njëqind) milionë lekë;

b) Vlera e garancisë e përcaktuar në pikën 7 (a) të kësaj Rregulloreje mbulohet me një depozitë ose garanci bankare, apo policë sigurimi pa kusht, të lëshuar nga një shoqëri e liçencuar 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 7 (a), 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 msipërme 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:

i) Mjetet e sigurta të krijimit të identifikimit elektronik edhe shërbimit të besuar dhe masat që merren në rast të humbjes ose dyshimit për përvetësim të këtyre mjeteve;

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

iii) Masat e sigurisë që aplikon Ofruesi i kualifikuar i shërbimit të besuar për mbrojtjen nga aksesit i paautorizuar të mjeteve të krijimit të identifikimit elektronik edhe shërbimit të besuar;

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 se 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

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 standartizimit në këtë fushë;

ii) Organizmi i testimit dhe konfirmimit dhe personeli që punëson, plotëson të gjitha kërkesat e parashikuara nga pika 4 (b) 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) 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 9 (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 identifikimin elektronik edhe shërbimin e besuar;

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

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

dh) Konfliktet mes Organizmave të Testimit e 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 mirëqënë nga Autoriteti dhe nuk ndërpritet, por afatet e inspektimit nga Autoriteti përgjysmohen.

10. Përrjashtimet

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 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 107/2015, datë 1.10.2015 “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 të pasqyrojë:

i) Statusin e çdo certifikate;

ii) Të paktën datën, kohën dhe kodin e identifikimit të certifikatave të revokuara/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, datë 1.10.2015 “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 së ai plotëson të gjitha kërkesat e nivelit të sigurisë dhe 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 rregjistrin 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

16. Të gjithë 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 Ligjin nr. 107/2015, datë 1.10.2015 “Për identifikimin elektronik dhe shërbimet e besuara” dhe në këtë Rregullore.

Përfshihen 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”.