



ORDIN nr. 888 din 5 septembrie 2011

pentru modificarea și completarea Ordinului ministrului comunicațiilor și societății informaționale nr. 473/2009 privind procedura de acordare, suspendare și retragere a deciziei de acreditare a furnizorilor de servicii de certificare

(Publicat în Monitorul Oficial cu numărul 717 din data de 12 octombrie 2011)

Având în vedere prevederile art. 36 și 37 din Legea nr. 455/2001 privind semnătura electronică, precum și ale art. 16-20 din Normele tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, aprobate prin Hotărârea Guvernului nr. 1.259/2001, cu modificările ulterioare,

în temeiul art. 4 alin. (1) pct. 55 și al art. 6 alin. (6) din Hotărârea Guvernului nr. 12/2009 privind organizarea și funcționarea Ministerului Comunicațiilor și Societății Informaționale, cu modificările și completările ulterioare,

ministrul comunicațiilor și societății informaționale emite prezentul ordin.

Art. I

Ordinul ministrului comunicațiilor și societății informaționale nr. 473/2009 privind procedura de acordare, suspendare și retragere a deciziei de acreditare a furnizorilor de servicii de certificare, publicat în Monitorul Oficial al României, Partea I, nr. 411 din 16 iunie 2009, cu modificările și completările ulterioare, se modifică și se completează după cum urmează:

1. La articolul 1, alineatul (2) se modifică și va avea următorul cuprins:

"(2) Prezentul ordin stabilește condițiile, conținutul, durata de valabilitate și condițiile suspendării deciziei de acreditare a furnizorilor de servicii de certificare."

2. Articolul 3¹ se modifică și va avea următorul cuprins:

"Art. 3¹

În vederea acreditării, furnizorul de servicii de certificare trebuie să facă dovada:

a) utilizării a cel puțin 5 persoane angajate în baza unor contracte individuale de muncă cu normă întreagă sau prin încheierea de contracte de prestări de servicii cu societăți comerciale ori persoane fizice autorizate.

Persoanele implicate în generarea și gestionarea de certificate trebuie:

(i) să dețină diplomă de absolvire a unei forme de învățământ superior de lungă durată, eliberată de o instituție de învățământ superior acreditată, având înscrisă una dintre următoarele specializări: automatică, calculatoare, informatică, matematică, fizică, cibernetică, electronică; sau

(ii) să dețină diplomă de masterat în una dintre specializările menționate la pct. (i).

Angajații implicați în generarea și gestionarea de certificate trebuie să aibă cunoștințe în domeniul securității informatice, dovedite prin studii universitare sau postuniversitare în acest domeniu ori prin deținerea cel puțin a uneia dintre certificările ISO/IEC 27001, CISA, CISM, LPT sau CISSP recunoscute la nivel internațional. Orice modificare a schemei de personal va fi notificată către autoritate în termen de 10 zile lucrătoare de la producerea acesteia;

b) utilizării unei scheme de personal care să asigure un flux continuu de emitere, suspendare și revocare a certificatelor și segregarea rolurilor angajaților, asigurând acoperirea cel puțin a următoarelor roluri: operator pentru gestionarea cererilor de certificare (cel puțin două persoane),



operator pentru verificarea cererilor și emiterea certificatelor (cel puțin două persoane), administrator al sistemului de certificare, administrator de securitate și auditor intern. Schema de personal va fi înaintată autorității;

c) utilizării unei arhitecturi distribuite a sistemului de certificare și sistemului de înregistrare, separând logic și fizic funcționalitățile publice: înregistrarea cererilor de certificate, registrul de certificate și validarea cererilor de emitere a certificatelor. Furnizorul trebuie să dovedească disponibilitatea lunară de 99,98% a soluției de emitere, publicare și validare a certificatelor, precum și a registrului de certificare. Disponibilitatea reprezintă capacitatea sistemelor informatice ale furnizorului de a se afla în stare de funcționare în orice moment din intervalul de observație de o lună calendaristică. Disponibilitatea se calculează după formula:

$$D = [(T_o - T_i) / T_o] * 100[\%],$$

unde:

T_o = durata unei luni calendaristice, aproximată la 30 de zile * 24 de ore * 60 de minute = 43.200 de minute;

T_i = durata însumată a întreruperilor de serviciu în minute.

Arhitectura tehnică și dovada îndeplinirii condițiilor de disponibilitate a soluției vor fi înaintate autorității;

d) deținerii sau utilizării unui sediu de rezervă pentru continuarea operațiunilor în cazul apariției unui eveniment care să împiedice utilizarea sediului principal. Sediul de rezervă trebuie să răspundă aceluiași condiții tehnice ca și sediul principal și să parcurgă aceleași proceduri de audit. Documentația privind sediul de rezervă și rapoartele de audit vor fi înaintate autorității;

e) certificărilor legate de sistemul de management al calității și management al securității informaționale, certificate în conformitate cu standardele ISO 9001 și, respectiv, ISO 27001 sau Standardele naționale de protecție a informațiilor clasificate definite prin Hotărârea Guvernului nr. 585/2002 ori ultimele versiuni ale acestora sau standardele care le înlocuiesc. Rapoartele de audit vor fi înaintate autorității."

3. Articolul 3² se modifică și va avea următorul cuprins:

"Art. 3²

(1) Orice furnizor de servicii de certificare calificată poate solicita inițierea procedurii de acreditare prin bifarea opțiunii din anexa nr. 2 la Normele tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, aprobate prin Hotărârea Guvernului nr. 1.259/2001, cu modificările ulterioare.

(2) Procedura de acreditare poate fi inițiată numai după începerea activității de furnizare de servicii de certificare calificată și actualizarea registrului. Procedura de acreditare este prevăzută în anexa nr. 4, care face parte integrantă din prezentul ordin."

4. Articolul 3³ se modifică și va avea următorul cuprins:

"Art. 3³

Pentru instituțiile din domeniul apărării, ordinii publice și siguranței naționale care emit certificate calificate ce urmează a fi folosite exclusiv pentru nevoi proprii și ale căror sisteme de generare, evidență și distribuție fac parte dintr-un sistem informatic acreditat pentru gestionarea informațiilor clasificate secret de stat, cuantumul garanției se stabilește anual, prin decizia autorității de reglementare și supraveghere specializate în domeniu, la propunerea conducerii instituțiilor respective, proporțional cu prejudiciile create în anul anterior, stabilite prin decizii judecătorești definitive. Extensia certificatului va conține mențiuni referitoare la limitări privind utilizarea."

5. Articolul 3⁴ se modifică și va avea următorul cuprins:



"Art. 3⁴

(1) Furnizorul va notifica autoritatea în legătură cu orice modificare a soluției tehnice sau a procedurilor de lucru. Notificarea va fi însoțită de opinia auditorului intern al furnizorului, opinie din care să rezulte faptul că furnizarea serviciilor de certificare se face în continuare cu respectarea standardelor în domeniu și a legislației în vigoare.

(2) Notificarea prevăzută la alin. (1) se va face cu 10 zile înainte de data la care modificările specificate la alin. (1) devin operaționale sau în cazul unor urgențe ori evenimente neprevăzute, justificate, în termen de maximum 24 de ore de la efectuarea modificărilor.

(3) În urma notificării adresate de către furnizor autorității, dacă se consideră că modificările efectuate afectează major procesul de furnizare a serviciilor de certificare, în sensul nerespectării standardelor în domeniu sau a legislației în vigoare, autoritatea poate solicita reînnoirea acreditării.

(4) Furnizorul acreditat va testa anual nivelul de securitate al sistemului informatic. În urma testării, acesta trebuie să înainteze către autoritate un raport de testare de securitate (test de penetrare) a întregului sistem informatic utilizat pentru furnizarea de servicii de certificare. Testele vor fi realizate de personal specializat, echipa de testare fiind compusă din minimum un expert în teste de penetrare cu certificare (LPT sau echivalent) și un auditor certificat în auditarea sistemelor informatice (CISA). Testele de penetrare vor fi realizate atât din exteriorul sistemului, cât și din interiorul acestuia, pe baza unor metodologii recunoscute la nivel internațional. Raportul de testare va conține toate testele efectuate, vulnerabilitățile identificate, precum și nivelul de risc asociat acestora. În urma raportului de testare, autoritatea va putea solicita furnizorului implementarea măsurilor de securitate în vederea reducerii nivelului de risc.

(5) Instituțiile care emit certificate calificate ce urmează a fi folosite exclusiv pentru nevoi proprii și ale căror sisteme de generare, evidență și distribuție fac parte dintr-un sistem informatic acreditat pentru gestionarea informațiilor clasificate secret de stat vor realiza testele de penetrare și auditul de securitate cu personal propriu care deține cunoștințe în domeniul securității informatice, dovedite prin studii universitare sau postuniversitare în acest domeniu, având o experiență de cel puțin 5 ani în domeniul securității sistemelor informatice. Testele de penetrare vor fi realizate atât din exteriorul sistemului, cât și din interiorul acestuia, pe baza unor metodologii recunoscute la nivel internațional. Raportul de testare va conține toate testele efectuate, vulnerabilitățile identificate, precum și nivelul de risc asociat acestora. În urma raportului de testare, autoritatea va putea solicita instituției implementarea măsurilor de securitate în vederea reducerii nivelului de risc."

6. Articolul 3⁵ se abrogă.

7. Articolul 3⁶ se modifică și va avea următorul cuprins:

"Art. 3⁶.

Verificarea informațiilor din cererea de eliberare a certificatului va fi realizată atât la înregistrarea cererii, cât și la emiterea certificatului, în conformitate cu prevederile art. 19 din Legea nr. 455/2001 privind semnătura electronică."

8. Articolul 3⁷ se modifică și va avea următorul cuprins:

"Art. 3⁷

Autoritatea poate dispune suspendarea activității furnizorului de servicii de certificare până la încetarea cauzelor care au determinat luarea măsurii și în următoarele situații:

1. furnizorul nu îndeplinește cerințele privind personalul sau nu anunță modificarea schemei de personal, așa cum este prevăzut la art. 3¹ lit. a) și b);
2. furnizorul nu asigură disponibilitatea soluției sau nu anunță modificările tehnice, așa cum este prevăzut la art. 3¹ lit. c) și art. 3⁴;



3. furnizorul nu mai îndeplinește cerințele tehnice definite la art. 3¹ lit. d) și e)."

9. Articolul 3⁸ se modifică și va avea următorul cuprins:

"Art. 3⁸

În cazurile prevăzute la art. 3⁷, autoritatea are dreptul de a emite pretenții asupra scrisorii de garanție bancară sau a poliței de asigurare, în limita prejudiciului."

10. După anexa nr. 3 se introduce o nouă anexă, anexa nr. 4, al cărei cuprins este prevăzut în anexa la prezentul ordin.

Art. II

Prevederile prezentului ordin intră în vigoare la 30 de zile de la publicarea sa în Monitorul Oficial al României, Partea I.

**MINISTRUL COMUNICAȚIILOR ȘI SOCIETĂȚII INFORMAȚIONALE,
VALERIAN VREME**

**ANEXĂ: PROCEDURĂ DE ACREDITARE**

(Anexa nr. 4 la Ordinul nr. 473/2009)

Numărul activității	Descrierea activității	Durata activității	Numărul activității precedente
1.	Procedura de acreditare	55 de zile	
2.	I. Cererea furnizorului	3 zile	
3.	Cererea furnizorului de servicii de certificare (FSC) circulă de la registratură până la Direcția generală pentru politici și programe în domeniul societății informaționale (DGPPSI).	o zi	
4.	Ministerul Comunicațiilor și Societății Informaționale (MCSI) verifică numai documentația transmisă de furnizor. În cazul în care furnizorul nu a transmis documentația, aceasta este solicitată.	două zile	3
5.	II. Procesul de alegere a auditorului	27 de zile	
6.	Desemnarea echipei responsabile cu îndeplinirea procesului de acreditare, formată din reprezentanți ai DGPPSI	două zile	2
7.	Stabilirea de către MCSI a condițiilor de calificare a auditorilor	două zile	2
8.	Aprobarea procedurii cu tot ce cuprinde	două zile	7
9.	Publicarea anunțului MCSI referitor la lansarea procedurii de selecție a auditorilor	o zi	8
10.	Primirea ofertelor	5 zile	9
11.	Verificarea îndeplinirii condițiilor de către auditorii care participă la procesul de calificare	5 zile	10
12.	Desemnarea auditorului	12 zile	11
13.	Raportul comisiei, inclusiv lista care trebuie aprobată	două zile	
14.	Aprobarea listei	două zile	13
15.	Comunicarea listei	o zi	14
16.	Primirea răspunsului	două zile	15
17.	Desemnarea auditorului prin ordin al ministrului comunicațiilor și societății informaționale (conform modelului din anexa nr. 2 la Ordinul ministrului comunicațiilor și societății informaționale nr. 473/2009 privind procedura de acordare, suspendare și retragere a deciziei de acreditare a furnizorilor de servicii de certificare, cu modificările și completările ulterioare)	3 zile	16
18.	Comunicarea ordinului	două zile	17
19.	III. Realizarea auditului	15 zile	
20.	Efectuarea auditului și transmiterea raportului și opiniei de audit către MCSI	15 zile	18



21.	IV. Evaluarea și decizia acreditării	10 zile	
22.	DGPPSI va primi rezultatul auditului efectuat asupra FSC	o zi	20
23.	MCSI respinge cererea de acreditare în urma analizei raportului de audit, precum și în cazul unei opinii de audit exprimate cu rezerve.	4 zile	22
24.	În cazul unor observații referitoare la raportul de audit prezentat, MCSI le va comunica atât furnizorului de servicii de certificare, cât și auditorului, în termen de 5 zile de la prezentarea raportului.	4 zile	22
25.	În termen de 10 zile de la prezentarea opiniei de audit favorabile, MCSI emite decizia de acreditare și înscrie în registru mențiunea privind acreditarea FSC.	9 zile	22
26.	Acreditarea se face prin ordin al ministrului comunicațiilor și societății informaționale, forma și conținutul ordinului de acreditare fiind prevăzute în anexa nr. 3 la Ordinul ministrului comunicațiilor și societății informaționale nr. 473/2009, cu modificările și completările ulterioare.	0 zile	25
27.	În cazul respingerii cererii de acreditare, autoritatea va comunica furnizorului motivele respingerii.	0 zile	25
28.	Decizia de acreditare va fi comunicată furnizorului pe suport hârtie și în format electronic, semnată digital de către MCSI.	0 zile	25
29.	MCSI va înscrie în Registrul furnizorilor de servicii de certificare mențiunea privind acreditarea FSC.	0 zile	25