



CRITERII DE CALIFICARE PENTRU AUDITORI

în vederea realizării auditului necesar acreditării
furnizorului S.C. CERTSIGN S.A.

I. Preambul

Legislația în vigoare în domeniul semnăturii electronice prevede posibilitatea acreditării furnizorilor de servicii de certificare. Această acreditare se acordă de către Ministerul Comunicațiilor și Societății Informaționale la cererea furnizorilor, 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.

Pentru obținerea sau reînnoirea acreditării furnizorul de servicii de certificare trebuie să îndeplinească toate condițiile necesare emiterii de certificate calificate și să utilizeze dispozitive securizate de creare a semnăturii electronice, omologate de o agenție de omologare agreată de autoritate. În cadrul procesului premergător acordării sau reînnoirii calității de furnizor de servicii de certificare acreditat se vor face verificări atât în ceea ce privește declarațiile conținute în documentația depusă la Ministerul Comunicațiilor și Societății Informaționale, cât și asupra concordanței dintre sistemele, procedurile și practicile afirmate a fi folosite și cele existente în realitate.

Verificarea îndeplinirii condițiilor de acreditare se face de către un auditor desemnat de către MCSI, în urma parcurgerii procesului de calificare a auditorilor prevăzut de Ordinul Ministrului nr. 473/09.06.2009 privind procedura de acordare, suspendare și retragere a deciziei de acreditare a furnizorilor de servicii de certificare, cu modificările și completările ulterioare.

Prezentul document cuprinde condițiile minimale care trebuie îndeplinite de către auditori pentru a fi incluși pe lista candidaților calificați în vederea realizării auditului, precum și conținutul documentației de calificare.

După primirea documentației de calificare din partea candidaților, MCSI va verifica respectarea criteriilor prezentate, va întocmi și va comunica furnizorului care a solicitat acreditarea lista candidaților calificați. Furnizorul va selecta, dintre candidații calificați, auditorul care va fi desemnat de către MCSI pentru efectuarea auditului de acreditare.



II. Legislație aplicabilă și standarde relevante din domeniul securității informației și furnizării de servicii de certificare calificată pentru semnătura electronică

- Legea nr.455/2001 privind semnătura electronică;
- Hotărârea de Guvern nr. 1259/2001 privind aprobarea normelor tehnice și metodologice pentru aplicarea Legii nr.455/2001 privind semnătura electronică;
- Ordinul Ministrului nr.473/09.06.2009 privind procedura de acordare, suspendare și retragere a deciziei de acreditare a furnizorilor de servicii de certificare;
- Ordinul nr. 1000/26.10.2010 pentru modificarea și completarea Ordinului ministrului comunicațiilor și societății informaționale nr. 473 din 2009 privind procedura de acordare, suspendare și retragere a deciziei de acreditare a furnizorilor de servicii de certificare
- Directiva 1999/93/EC a Parlamentului European și a Consiliului privind cadrul comunitar referitor la semnătura electronică;
- ETSI TS 101 456 V1.4.3 (2007-05) "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates";
- ETSI TR 102 437 V1.1.1 (2006-10) "Electronic Signatures and Infrastructures (ESI); Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates)";
- ETSI TR 102 044 V1.1.1 (2002-12) "Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates";
- ETSI TR 102 040 V1.3.1 (2005-03) "Electronic Signatures and Infrastructures (ESI); International Harmonization of Policy Requirements for CAs issuing Certificates";
- ETSI TS 102 158 V1.1.1 (2003-10) "Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates";
- ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements
- ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management;
- ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management
- BS 7799-2 "Information security management – Part 2: Specification for information security management systems";



- ISO/IEC 15408-1:2005 Security techniques/Evaluation criteria for IT security/ Part 1: Introduction and general model;
- ISO/IEC 15408-2:2005 Security techniques/Evaluation criteria for IT security/ Part 2: Security functional requirements;
- ISO/IEC 15408-3:2005 Security techniques/Evaluation criteria for IT security/ Part 3: Security assurance requirements.

III. Cerințe pentru auditori IT

Auditul poate fi realizat atât de o persoană fizică, care îndeplinește condițiile necesare realizării acestei proceduri, cât și de o persoană juridică de drept privat.

În vederea realizării auditului necesar pentru acordarea calității de furnizor acreditat de servicii de certificare pentru semnătura electronică, selectarea persoanelor fizice/ persoanelor juridice calificate se va face după următoarele criterii obligatorii:

- a) metodologia de audit utilizată;
- b) bonitatea candidatului;
- c) existența unui sistem de management al calității implementat;
- d) experiența în domeniul auditului securității tehnologiei informației;
- e) îndeplinirea cerințelor pentru personalului implicat în activitatea de audit solicitată (aceste cerințe sunt prezentate la capitolul IV al acestui document);
- f) independența auditorului față de furnizorul de servicii de certificare care solicită acreditarea.

IV. Cerințe pentru personalul care va realiza auditul

- să fie absolvenți de studii superioare în domeniul tehnologiei informației (experiența vastă și studiile de specialitate suplimentare pot fi echivalente unui astfel de nivel de studii) și să aibă cunoștințe și abilități în domeniul managementului securității informației și a infrastructurii PKI (public key infrastructure);
- să aibă cel puțin patru ani de experiență practică în domeniul tehnologiei informației, din care cel puțin doi ani într-o funcție din cadrul departamentului de management al securității informației;
- să fi urmat un curs de instruire de cel puțin 5 zile având ca subiect auditul sistemelor informatice, auditul sistemelor de management și managementul proceselor de audit;



- să aibă calificări/atestări pe standardele menționate la Capitolul II sau pe standarde echivalente;
- să aibă experiență în domeniul auditului sistemelor informatice.

Auditorul desemnat să conducă echipa de audit (auditorul șef) trebuie să îndeplinească în plus următoarele condiții:

- să fi efectuat cel puțin trei audituri complete în domeniul tehnologiei informației, ca auditor calificat;
- să aibă cunoștințe și calități de conducere a procesului de audit;
- calități personale: capacitatea de a conduce un audit în concordanță cu procedura de audit, capacitate organizatorică.

Pentru realizarea auditului, echipa de audit poate fi asistată de experți, care să aibă și să demonstreze cunoștințe specifice în domeniul de audit: cerințe și reglementări legale referitoare la furnizorii de servicii de certificare, cunoștințe tehnice privind infrastructura de chei publice, evaluarea amenințărilor, vulnerabilităților și riscurilor din punct de vedere al securității informației pentru furnizorii de servicii de certificare.

V. Conținutul documentației de calificare

Documentația de calificare trebuie să asigure o descriere corectă și concisă a îndeplinirii de către persoana fizică/ persoana juridică a condițiilor de calificare. Pentru o abordare uniformă a documentației de calificare și obținere a unui grad maxim de comparabilitate, documentația de calificare va fi organizată astfel:

1. Pagina de titlu: numele persoanei fizice/ persoanei juridice, adresa, număr telefon, fax.
2. Data depunerii documentației de calificare, numele persoanei de contact.
3. Cuprins: identificarea clară a textului prin număr de secțiuni sau pagină.
4. Considerente operaționale: se va oferi o descriere a companiei, subliniind metodele de operare, structura operațională, serviciile oferite. Această descriere trebuie să demonstreze capacitatea candidatului de a îndeplini cerințele de calificare în scopul selecției pentru realizarea auditului în vederea acreditării furnizorului de servicii de certificare.
5. Metodologia de lucru (Cap. III lit. a): se va descrie modalitatea de abordare a procesului de audit în cazul auditului realizat în scopul verificării condițiilor de acreditare a furnizorului, conform legii nr.455/2001 privind semnătura electronică.



6. Prezentarea experienței în domeniu (Cap. III lit. d): se va prezenta un document în care se va descrie experiența în efectuarea auditului sistemelor informatice; se va prezenta o listă de referințe de la cel puțin trei clienți către care s-au oferit servicii de audit al sistemelor informatice, audit al sistemelor de management al securității informației. Lista va conține:
 - a. Numele clientului.
 - b. Data la care s-a efectuat auditul
 - c. Adresa clientului
 - d. Persoana de contact
 - e. Numărul de telefon/fax.
7. Prezentarea CV-urilor personalului care va realiza auditul (Cap. III lit. e): se va face o prezentare completă din punct de vedere a personalului (experiență, instruire) care va fi angrenat în activitatea de audit pentru care se face calificarea.
8. Descrierea sistemului de management al calității (Cap. III lit. c).
9. Planificarea activității de audit solicitate.
10. Declarația candidatului (Cap. III lit. f): declarația de independență a auditorului față de compania și sistemul care vor fi auditate.
11. Documente financiare (Cap. III lit. b): se vor prezenta documente oficiale din care să rezulte cifra de afaceri realizată în ultimii trei ani, cu specificarea sumelor provenite din activități similare celei supuse atenției în cerințele de calificare, acolo unde este cazul.
12. Semnătura candidatului: în cazul unei persoane juridice, documentația de calificare trebuie semnată de către persoana cu drept de semnătură, cu precizarea în clar a numelui și funcției deținute.
13. Documentația de calificare: fiecare pagină a va fi numerotată, semnată și ștampilată, iar copiile xerox vor avea mențiunea “conform cu originalul”.