

# Décrets, arrêtés, circulaires

## TEXTES GÉNÉRAUX

### MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE L'INDUSTRIE

#### INDUSTRIE

#### Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation

NOR : *INDI0403348A*

Le ministre délégué à l'industrie,

Vu la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 modifiée prévoyant une procédure d'information dans le domaine des normes et réglementations techniques ;

Vu le décret n° 2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique,

Arrête :

#### CHAPITRE 1<sup>er</sup>

#### Accréditation des organismes qui procèdent à l'évaluation des prestataires de services de certification électronique en vue de reconnaître leur qualification

**Art. 1<sup>er</sup>.** – Le Comité français d'accréditation (COFRAC), association déclarée le 4 mai 1994, ou tout organisme d'accréditation signataire de l'accord multilatéral de reconnaissance mutuelle pris dans le cadre de la coopération européenne des organismes d'accréditation (EA), ci-après nommé centre d'accréditation, est chargé d'accréditer les organismes qui procèdent à l'évaluation des prestataires de services de certification électronique en vue de reconnaître leur qualification. Le référentiel d'accréditation comprend la norme NF EN 45012 ou une norme équivalente, ainsi que les règles d'application établies par le centre d'accréditation.

**Art. 2.** – La demande d'accréditation adressée par un organisme à un centre d'accréditation doit comprendre les éléments suivants :

1. Les statuts de l'organisme, son règlement intérieur et tout autre texte régissant son fonctionnement ;
2. Les noms et qualités des dirigeants de l'organisme et des membres de son conseil d'administration ou des organes en tenant lieu ;
3. Les noms et les qualifications des personnels de l'organisme prenant part à la procédure d'évaluation ;
4. La description des activités de l'organisme, de sa structure et de ses moyens techniques ;
5. Les comptes des deux exercices précédents ;
6. La description des procédures et des moyens qui seront mis en œuvre par l'organisme pour évaluer les prestataires de services de certification électronique en vue de reconnaître leur qualification, compte tenu des normes ou prescriptions techniques en vigueur.

L'organisme demandeur doit en outre signaler au centre d'accréditation les liens éventuels qu'il a avec des prestataires de services de certification électronique. En ce cas, il doit préciser les mesures qu'il compte mettre en œuvre pour éviter tout conflit d'intérêts.

L'organisme demandeur doit disposer, conformément à la clause 2.1.2.e de la norme NF EN 45012, d'une structure en son sein qui préserve son impartialité. Cette structure doit notamment comprendre un représentant de la direction centrale de la sécurité des systèmes d'information, un représentant de l'agence pour le développement de l'administration électronique et un représentant de la direction générale de l'industrie, des technologies de l'information et des postes.

**Art. 3.** – Le centre d'accréditation instruit la demande d'accréditation. Il peut solliciter tous renseignements complémentaires de l'organisme demandeur. Il peut demander à effectuer des vérifications dans les locaux de l'organisme demandeur.

A l'issue de l'instruction, le centre d'accréditation prend une décision motivée qu'il notifie à l'organisme demandeur et dont il adresse copie à la direction centrale de la sécurité des systèmes d'information. Lorsqu'il accorde l'accréditation, le centre d'accréditation peut soumettre l'organisme bénéficiaire à des obligations particulières.

**Art. 4.** – L'accréditation est valable pour une durée qui ne peut excéder cinq ans. Les organismes accrédités informent le centre d'accréditation de tout changement par rapport aux éléments communiqués dans le dossier de demande d'accréditation.

Pendant la durée de l'accréditation, le centre d'accréditation effectue une surveillance régulière, qui peut conduire selon les cas à une suspension ou à un retrait de l'accréditation, en vertu des règles en vigueur dans le cadre de la coopération européenne des organismes d'accréditation. La suspension ou le retrait de l'accréditation ne peut être prononcé qu'après que le représentant de l'organisme précédemment accrédité a été mis à même de présenter ses observations. La direction centrale de la sécurité des systèmes d'information est informée de toute suspension ou de tout retrait d'accréditation.

**Art. 5.** – Le centre d'accréditation met à la disposition du public, notamment sur un site internet, la liste des organismes accrédités. Cette liste est tenue à jour.

## CHAPITRE 2

### Reconnaissance de la qualification des prestataires de services de certification électronique

**Art. 6.** – Un prestataire de services de certification électronique qui demande à être reconnu comme qualifié choisit un organisme accrédité pour procéder à l'évaluation de ses activités.

Le prestataire est tenu de fournir à l'organisme choisi tous les éléments nécessaires au bon accomplissement de la procédure d'évaluation.

**Art. 7.** – L'évaluation est effectuée par l'organisme aux frais du prestataire de services de certification. Son objet est de vérifier que le prestataire se conforme aux spécifications techniques relatives aux prestataires de services de certification en vue de la reconnaissance de sa qualification. Ces spécifications techniques, déterminées en annexe, précisent les exigences fixées par l'article 6 du décret du 30 mars 2001 susvisé.

A l'issue de la procédure d'évaluation, l'organisme accrédité établit un rapport qui est notifié au prestataire afin que celui-ci puisse, le cas échéant, formuler des observations sur son contenu.

**Art. 8.** – Les rapports d'évaluation sont communiqués par les organismes accrédités à la direction centrale de la sécurité des systèmes d'information.

**Art. 9.** – L'organisme accrédité reconnaît ou non la qualification du prestataire de services de certification électronique au vu du rapport d'évaluation et des éventuelles observations du prestataire et en informe la direction centrale de la sécurité des systèmes d'information.

Lorsqu'il reconnaît la qualification d'un prestataire, l'organisme accrédité délivre une attestation qui décrit les activités couvertes par la qualification ainsi que la durée pendant laquelle l'attestation est valable. Il en adresse une copie à la direction centrale de la sécurité des systèmes d'information. Pendant cette durée, qui ne peut excéder trois ans, le prestataire doit faire l'objet d'un audit de surveillance au moins annuel de la part de l'organisme accrédité, qui peut conduire à une suspension ou à un retrait de l'attestation de la part de l'organisme accrédité. Ce dernier en informe alors aussitôt la direction centrale de la sécurité des systèmes d'information.

Les prestataires dont la qualification est reconnue communiquent à toute personne qui en fait la demande une copie de l'attestation délivrée par l'organisme accrédité.

**Art. 10.** – Les prestataires qui fournissent des services techniques aux prestataires de services de certification électronique délivrant des certificats électroniques qualifiés peuvent solliciter auprès d'un organisme accrédité, dans les mêmes conditions, une attestation de conformité de ces services aux spécifications techniques, figurant en annexe, qui leur sont applicables.

**Art. 11.** – L'arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation est abrogé.

**Art. 12.** – Le directeur général de l'industrie, des technologies de l'information et des postes est chargé de l'exécution du présent arrêté, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 26 juillet 2004.

PATRICK DEVEDJIAN

## A N N E X E

SPÉCIFICATIONS TECHNIQUES RELATIVES AUX PRESTATAIRES DE SERVICES  
DE CERTIFICATION EN VUE DE LA RECONNAISSANCE DE LEUR QUALIFICATION

Les spécifications techniques relatives aux prestataires de services de certification en vue de reconnaître leur qualification, qui précisent les exigences fixées par l'article 6 du décret du 30 mars 2001 susvisé, sont celles définies dans le document AFNOR AC Z74-400 intitulé « Exigences concernant la politique mise en œuvre par les autorités de certification délivrant des certificats qualifiés », ou toute mise à jour de ce document.

Ces spécifications sont complétées par les spécifications techniques suivantes :

1. Spécifications techniques précisant l'article 6-II, alinéa *f*, du décret du 30 mars 2001 susvisé :

Le prestataire de services de certification doit notamment appliquer une procédure de sécurité garantissant la confidentialité des causes de révocation définitives des certificats électroniques qu'il a délivrés et s'assurer de l'accord du signataire avant de publier ces informations.

2. Spécifications techniques précisant l'article 6-II, alinéa *g*, du 30 mars 2001 susvisé :

Le module cryptographique utilisé par le prestataire de services de certification électronique pour les fonctions assurées dans les conditions prévues par le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, être certifié conforme par le Premier ministre aux exigences ci-après :

- assurer la confidentialité et l'intégrité des données de création de signature du prestataire de services de certification durant tout leur cycle de vie ;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- détecter les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée ;
- permettre de créer une signature électronique sécurisée, pour signer les certificats, qui ne révèle pas les données de création de signature du prestataire de services de certification et qui ne peut pas être falsifiée sans la connaissance des données de création de signature du prestataire de services de certification ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- si une fonction de sauvegarde et de restauration des données de création de signature du prestataire de services de certification électronique est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

Par ailleurs, si le prestataire de services de certification génère les données de création et de vérification de signature du signataire, destinées à un dispositif sécurisé de création de signature, le module cryptographique utilisé doit être certifié, pour cette fonction, dans les conditions prévues à l'article 3 du décret du 30 mars 2001 susvisé.

3. Spécifications techniques précisant l'article 6-II, alinéa *m*, du décret du 30 mars 2001 susvisé :

La vérification de l'identité de la personne à laquelle le certificat électronique qualifié est destiné est effectuée en sa présence sur présentation d'un document officiel d'identité comportant une photographie (notamment carte nationale d'identité, passeport, carte de séjour) par le prestataire de services de certification électronique ou par un mandataire qu'il désigne et qui s'engage auprès de lui par contrat. Ce contrat prévoit notamment que le mandataire est soumis aux mêmes obligations que le prestataire de certification électronique.

Lorsqu'un signataire se voit délivrer un certificat électronique destiné exclusivement à être utilisé dans le cadre de l'activité professionnelle qu'il exerce pour le compte d'une personne physique ou morale, cette personne physique ou morale peut demander à ce que les vérifications d'identité et de qualité du signataire soient déléguées à un mandataire qu'elle désigne. Elle s'engage alors par contrat avec le prestataire de services de certification électronique à ce que le mandataire procède aux vérifications d'identité dans les conditions visées au paragraphe précédent. Le prestataire de services de certification électronique s'assure de l'origine de cette demande et que les données recueillies par le mandataire sont communiquées dans des conditions sécurisées permettant notamment d'en garantir l'origine et l'intégrité.