LEY DE FIRMA ELECTRÓNICA DE FRANCIA

Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique

Le Premier ministre,

Sur le rapport de la garde des sceaux, ministre de la justice,

Vu la directive 1999/93/CE du Parlement européen et du Conseil en date du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques ;

Vu le code civil, notamment ses articles 1316 à 1316-4 ;

Vu la loi no 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications, notamment son article 28 ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Décrète :

Art. 1er.

- Au sens du présent décret, on entend par :

1. « Signature électronique » : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil ;

2. « Signature électronique sécurisée » : une signature électronique qui satisfait, en outre, aux exigences suivantes

- être propre au signataire ;

- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;

- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ;

3. « Signataire » : toute personne physique, agissant pour son propre compte ou pour celui

de la personne physique ou morale qu'elle représente, qui met en oeuvre un dispositif de création de signature électronique ;

4. « Données de création de signature électronique » : les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique ;

5. « Dispositif de création de signature électronique » : un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique ;

6. « Dispositif sécurisé de création de signature électronique » : un dispositif de création de signature électronique qui satisfait aux exigences définies au I de l'article 3 ;

7. « Données de vérification de signature électronique » : les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique ;

8. « Dispositif de vérification de signature électronique » : un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique ;

9. « Certificat électronique » : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire ;

10. « Certificat électronique qualifié » : un certificat électronique répondant aux exigences définies à l'article 6 ;

11. « Prestataire de services de certification électronique » : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique ;

12. « Qualification des prestataires de services de certification électronique » : l'acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité.

Art. 2.

- La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en oeuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié.

Chapitre Ier. Des dispositifs sécurisés de création de signature électronique ➦

Art. 3. - Un dispositif de création de signature électronique ne peut être regardé comme sécurisé que s'il satisfait aux exigences définies au I et que s'il est certifié conforme à ces exigences dans les conditions prévues au II.

I. - Un dispositif sécurisé de création de signature électronique doit :

1. Garantir par des moyens techniques et des procédures appropriés que les données de création de signature électronique :

a) Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;

b) Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;

c) Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.

2. N'entraîner aucune altération du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

II. - Un dispositif sécurisé de création de signature électronique doit être certifié conforme aux exigences définies au I :

1o Soit par les services du Premier ministre chargés de la sécurité des systèmes d'information, après une évaluation réalisée, selon des règles définies par arrêté du Premier ministre, par des organismes agréés par ces services. La délivrance par ces services du certificat de conformité est rendue publique ;

2o Soit par un organisme désigné à cet effet par un Etat membre de la Communauté européenne.

Art. 4. - Le contrôle de la mise en oeuvre des procédures d'évaluation et de certification prévues au 1o du II de l'article 3 est assuré par un comité directeur de la certification, institué auprès du Premier ministre.

Un arrêté du Premier ministre précise les missions attribuées à ce comité, fixe sa composition, définit les procédures de certification et d'évaluation des dispositifs de création de signature électronique mentionnées à l'alinéa précédent ainsi que les procédures d'agrément des organismes d'évaluation. Il détermine, en outre, les obligations incombant à ces organismes et fixe les conditions dans lesquelles sont présentées et instruites les demandes de certification.

Chapitre II. Des dispositifs de vérification de signature électronique ➦

Art. 5. - Un dispositif de vérification de signature électronique peut faire, après évaluation, l'objet d'une certification, selon les procédures définies par l'arrêté mentionné à l'article 4, s'il répond aux exigences suivantes :

a) Les données de vérification de signature électronique utilisées doivent être celles qui ont été portées à la connaissance de la personne qui met en oeuvre le dispositif et qui est dénommée « vérificateur » ;

b) Les conditions de vérification de la signature électronique doivent permettre de garantir l'exactitude de celle-ci et le résultat de cette vérification doit sans subir d'altération être porté à la connaissance du vérificateur ;

c) Le vérificateur doit pouvoir, si nécessaire, déterminer avec certitude le contenu des données signées ;

d) Les conditions et la durée de validité du certificat électronique utilisé lors de la vérification de la signature électronique doivent être vérifiées et le résultat de cette

vérification doit sans subir d'altération être porté à la connaissance du vérificateur ;

e) L'identité du signataire doit sans subir d'altération être portée à la connaissance du vérificateur ;

f) Lorsqu'il est fait usage d'un pseudonyme, son utilisation doit être clairement portée à la connaissance du vérificateur ;

g) Toute modification ayant une incidence sur les conditions de vérification de la signature électronique doit pouvoir être détectée.

Chapitre III. Des certificats électroniques qualifiés et des prestataires de services de certification électronique ➦

Art. 6. - Un certificat électronique ne peut être regardé comme qualifié que s'il comporte les éléments énumérés au I et que s'il est délivré par un prestataire de services de certification électronique satisfaisant aux exigences fixées au II.

I. - Un certificat électronique qualifié doit comporter :

a) Une mention indiquant que ce certificat est délivré à titre de certificat électronique qualifié ;

b) L'identité du prestataire de services de certification électronique ainsi que l'Etat dans lequel il est établi ;

c) Le nom du signataire ou un pseudonyme, celui-ci devant alors être identifié comme tel ;

d) Le cas échéant, l'indication de la qualité du signataire en fonction de l'usage auquel le certificat électronique est destiné ;

e) Les données de vérification de signature électronique qui correspondent aux données de création de signature électronique ;

f) L'indication du début et de la fin de la période de validité du certificat électronique ;

g) Le code d'identité du certificat électronique ;

h) La signature électronique sécurisée du prestataire de services de certification électronique qui délivre le certificat électronique ;

i) Le cas échéant, les conditions d'utilisation du certificat électronique, notamment le montant maximum des transactions pour lesquelles ce certificat peut être utilisé.

II. - Un prestataire de services de certification électronique doit satisfaire aux exigences suivantes :

a) Faire preuve de la fiabilité des services de certification électronique qu'il fournit ;

b) Assurer le fonctionnement, au profit des personnes auxquelles le certificat électronique

est délivré, d'un service d'annuaire recensant les certificats électroniques des personnes qui en font la demande ;

c) Assurer le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de révoquer sans délai et avec certitude ce certificat ;

d) Veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision ;

e) Employer du personnel ayant les connaissances, l'expérience et les qualifications nécessaires à la fourniture de services de certification électronique ;

f) Appliquer des procédures de sécurité appropriées ;

g) Utiliser des systèmes et des produits garantissant la sécurité technique et cryptographique des fonctions qu'ils assurent ;

h) Prendre toute disposition propre à prévenir la falsification des certificats électroniques ;

i) Dans le cas où il fournit au signataire des données de création de signature électronique, garantir la confidentialité de ces données lors de leur création et s'abstenir de conserver ou de reproduire ces données ;

j) Veiller, dans le cas où sont fournies à la fois des données de création et des données de vérification de la signature électronique, à ce que les données de création correspondent aux données de vérification ;

k) Conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique.

l) Utiliser des systèmes de conservation des certificats électroniques garantissant que :

- l'introduction et la modification des données sont réservées aux seules personnes autorisées à cet effet par le prestataire ;

- l'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;

- toute modification de nature à compromettre la sécurité du système peut être détectée ;

m) Vérifier, d'une part, l'identité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation d'un document officiel d'identité, d'autre part, la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité ;

n) S'assurer au moment de la délivrance du certificat électronique :

- que les informations qu'il contient sont exactes ;

- que le signataire qui y est identifié détient les données de création de signature électronique correspondant aux données de vérification de signature électronique

contenues dans le certificat ;

o) Avant la conclusion d'un contrat de prestation de services de certification électronique, informer par écrit la personne demandant la délivrance d'un certificat électronique :

- des modalités et des conditions d'utilisation du certificat ;

- du fait qu'il s'est soumis ou non au processus de qualification volontaire des prestataires de services de certification électronique mentionnée à l'article 7 ;

- des modalités de contestation et de règlement des litiges ;

p) Fournir aux personnes qui se fondent sur un certificat électronique les éléments de l'information prévue au o qui leur sont utiles.

Art. 7. - Les prestataires de services de certification électronique qui satisfont aux exigences fixées à l'article 6 peuvent demander à être reconnus comme qualifiés.

Cette qualification, qui vaut présomption de conformité auxdites exigences, est délivrée par les organismes ayant reçu à cet effet une accréditation délivrée par une instance désignée par arrêté du ministre chargé de l'industrie. Elle est précédée d'une évaluation réalisée par ces mêmes organismes selon des règles définies par arrêté du Premier ministre.

L'arrêté du ministre chargé de l'industrie prévu à l'alinéa précédent détermine la procédure d'accréditation des organismes et la procédure d'évaluation et de qualification des prestataires de services de certification électronique.

Art. 8. - Un certificat électronique délivré par un prestataire de services de certification électronique établi dans un Etat n'appartenant pas à la Communauté européenne a la même valeur juridique que celui délivré par un prestataire établi dans la Communauté, dès lors :

a) Que le prestataire satisfait aux exigences fixées au II de l'article 6 et a été accrédité, au sens de la directive du 13 décembre 1999 susvisée, dans un Etat membre ;

b) Ou que le certificat électronique délivré par le prestataire a été garanti par un prestataire établi dans la Communauté et satisfaisant aux exigences fixées au II de l'article 6 ;

c) Ou qu'un accord auquel la Communauté est partie l'a prévu.

Art. 9. - I. - Au titre de la déclaration de fourniture de prestations de cryptologie effectuée conformément aux dispositions de l'article 28 de la loi du 29 décembre 1990 susvisée, le prestataire de services de certification électronique doit, quand il entend délivrer des certificats électroniques qualifiés, l'indiquer.

II. - Le contrôle des prestataires visés au I est effectué par des organismes publics désignés par arrêté du Premier ministre et agissant sous l'autorité des services du Premier ministre chargés de la sécurité des systèmes d'information.

Ce contrôle porte sur le respect des exigences définies à l'article 6. Il peut être effectué d'office ou à l'occasion de toute réclamation mettant en cause l'activité d'un prestataire de services de certification électronique.

Lorsque le contrôle révèle qu'un prestataire n'a pas satisfait à ces exigences, les services du Premier ministre chargés de la sécurité des systèmes d'information assurent la publicité des résultats de ce contrôle et, dans le cas où le prestataire a été reconnu comme qualifié dans les conditions fixées à l'article 7, en informent l'organisme de qualification.

Les mesures prévues à l'alinéa précédent doivent faire l'objet, préalablement à leur adoption, d'une procédure contradictoire permettant au prestataire de présenter ses observations.

Chapitre IV. Dispositions diverses

Art. 10. - Le présent décret est applicable en Nouvelle-Calédonie, en Polynésie française, aux îles Wallis et Futuna et à Mayotte.

Art. 11. - Le ministre de l'économie, des finances et de l'industrie, la garde des sceaux, ministre de la justice, le ministre de l'intérieur, le secrétaire d'Etat à l'outre-mer et le secrétaire d'Etat à l'industrie sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 30 mars 2001.

Lionel Jospin

Par le Premier ministre :

La garde des sceaux, ministre de la justice,

Marylise Lebranchu

Le ministre de l'économie,

des finances et de l'industrie,

Laurent Fabius

Le ministre de l'intérieur,

Daniel Vaillant

Le secrétaire d'Etat à l'outre-mer,

Christian Paul

Le secrétaire d'Etat à l'industrie,

Christian Pierret