

Textes de loi relatifs à la signature électronique en France

Depuis la loi du 13 mars 2000, la signature électronique a une valeur légale en France. Cette loi a été complétée par plusieurs décrets qui en précisent les conditions d'application, notamment les critères fixant les conditions de validité et la présomption de fiabilité d'une signature électronique.

Ce document résume le contenu de chacun de ces textes de loi.

1 En résumé

Depuis la loi du 13 mars 2000 l'écrit sous forme électronique est reconnu au même titre que l'écrit sous forme papier en France. Pour se faire, il faut notamment que l'auteur d'un écrit électronique puisse être identifié, d'où la nécessaire notion de *signature électronique*. Cette même loi reconnaît la valeur juridique des procédés de signature électronique, sous certaines conditions.

Cependant **la démonstration de fiabilité du procédé de signature électronique reste à la charge du signataire**, ce qui peut constituer un frein à l'utilisation massive des documents électroniques.

Le décret du 30 mars 2001 a défini la *signature électronique sécurisée* qui doit remplir certaines conditions. Une signature électronique sécurisée peut être *présumée fiable*, **ce qui inverse la charge de preuve de fiabilité de la signature**. Pour cela, elle doit être établie à l'aide d'un *dispositif de création sécurisée* et sa vérification doit reposer sur l'utilisation d'un *certificat électronique qualifié*.

Pour être reconnu *sécurisé* un dispositif de création de signature électronique doit satisfaire à certaines exigences définies dans le décret du 30 mars 2001 et doit être *certifié conforme* à ces exigences, après un processus d'évaluation décrit dans le décret du 18 avril 2002.

Pour être déclaré *qualifié* un certificat électronique doit comporter certains éléments obligatoires et être délivré par un prestataire de services de certification électronique respectant certaines exigences définies dans le décret du 30 mars 2001. Après un processus d'évaluation décrit dans l'arrêté du 31 mai 2002, un prestataire peut être reconnu comme *qualifié*, ce qui vaut présomption de conformité à ces exigences. **L'attestation de qualification a une durée maximale d'un an.**

Loi du 13 mars 2000	<ul style="list-style-type: none">- validité de l'écrit sous forme électronique- reconnaissance juridique de la signature électronique- démonstration de fiabilité à la charge du signataire
Décret du 30 mars 2001	<ul style="list-style-type: none">- définition de la signature électronique sécurisée présumée fiable :-> inversion de la charge de preuve mais nécessité de :- certification du dispositif de création de signature électronique- qualification du prestataire de services de certification électronique
Décret du 18 avril 2002	<ul style="list-style-type: none">- description du processus de certification des produits et systèmes relatifs aux technologies de l'information- conditions d'agrément des organismes chargés de l'évaluation
Arrêté du 31 mai 2002	<ul style="list-style-type: none">- description du processus qualification des prestataires de service de certification électronique- conditions d'agrément des organismes d'évaluation des prestataires de service de certification électronique

TAB. 1 – Textes de lois relatifs à la signature électronique en France

Type de signature	Conditions de validité ¹	Présomption de fiabilité
Signature électronique	Le procédé de signature assure l'identification du signataire et la garantie de l'intégrité de l'acte	non
Signature électronique sécurisée	Signature électronique : - propre au signataire ; - créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; - garantissant avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.	non
Signature électronique sécurisée présumée fiable	Signature électronique sécurisée - établie à l'aide d'un dispositif de création sécurisée ; - dont la vérification repose sur l'utilisation d'un certificat électronique qualifié.	oui

TAB. 2 – Les différents types de signatures électroniques en France

2 Loi no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

Elle modifie le code civil en introduisant les nouveautés suivantes :

- la preuve par écrit n'est pas spécifique à un support particulier ;
- **l'écrit sous forme électronique est admis au même titre que l'écrit sous forme papier**, sous deux conditions :
 1. la personne dont émane l'écrit peut être dûment identifiée. La loi introduit ainsi la notion de *signature électronique*,
 2. l'écrit est établi et conservé dans des conditions de nature à en garantir l'intégrité ;

La loi insère dans le code civil la définition suivante de la signature : "La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte."

Elle reconnaît la valeur juridique des procédés de signature électronique si ils assurent l'identification du signataire et la garantie de l'intégrité de l'acte. **Par défaut la démonstration de fiabilité du procédé de signature électronique est à la charge du signataire.** Cependant une signature électronique peut être *présumée fiable* (retournement de la charge de preuve) si le procédé de signature respecte certaines exigences définies par le décret du 30 mars 2001.

¹De plus l'écrit sous forme électronique sur lequel est apposée la signature doit respecter les deux conditions définies dans la loi du 30 mars 2000 lui permettant d'être admis au même titre que l'écrit sous forme papier :

1. la personne dont émane l'écrit peut être dûment identifiée ;
2. l'écrit est établi et conservé dans des conditions de nature à en garantir l'intégrité.

3 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

Il introduit la notion de *signature électronique sécurisée*, qui doit satisfaire les trois exigences suivantes :

1. être propre au signataire ;
2. être créée par des moyens que le signataire puisse garder sous son contrôle exclusif. L'EESSI (European Electronic Signature Standardization Initiative) est chargée de spécifier dans le formalisme des Critères Communs (sous la forme de profils de protection) les normes techniques relatives à cette exigence ;
3. garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.

La signature électronique sécurisée est recevable comme preuve en justice mais la démonstration de fiabilité du procédé de signature est à la charge du signataire. Cependant la charge de preuve est inversée si la signature électronique est *présumée fiable*. Pour cela elle doit respecter les exigences suivantes :

1. elle est établie à l'aide d'un *dispositif de création sécurisée* ;
2. la vérification de cette signature repose sur l'utilisation d'un *certificat électronique qualifié*.

3.1 Dispositif de création de signature électronique sécurisé

Pour être qualifié de *sécurisé*, un dispositif de création de signature électronique doit :

1. respecter les exigences définies dans l'article 3 du décret, notamment que "les données de création de signature électronique peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers" ;
2. **être certifié conforme à ces exigences par un organisme agréé** (objet du décret du 18 avril 2002).

3.2 Certificat électronique qualifié

Pour être considéré comme *qualifié*, un certificat électronique doit comporter des éléments définis dans l'article 6 et **être délivré par un prestataire de services de certification électronique respectant certaines exigences**, définies dans le même article, notamment :

- 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 ;
- utiliser des systèmes de conservation des certificats électroniques garantissant notamment que l'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;
- pour la délivrance du certificat, exiger la présentation d'un document officiel d'identité et conserver les caractéristiques et références des documents présentés ;
- avant la délivrance d'un certificat, informer la personne par écrit des modalités de contestation et de litige.

Les prestataires de services de certification électronique qui satisfont à toutes ces exigences peuvent demander à être reconnus comme *qualifiés*, **ce qui vaut présomption de conformité aux exigences** (objet du décret du 31 mai 2002).

4 Décret no 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

Ce décret définit le cadre juridique français de l'évaluation et de la certification de produits ou systèmes relatifs aux technologies de l'information, ce qui inclut les dispositifs de création de signature électronique. Les administrations y sont invitées à recourir à des produits ou systèmes certifiés.

La certification d'un produit ou système nécessite une phase préalable d'évaluation, menée à la demande d'un commanditaire et effectuée par un CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information) selon une définition initiale du produit ou système à tester ainsi que des objectifs de sécurité. Les CESTI sont agréés par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Informations) pour un domaine d'activité (par exemple : informatique et réseaux, composants électroniques et logiciels embarqués).

À la fin de l'évaluation, le CESTI remet au commanditaire et à la DCSSI un rapport technique d'évaluation confidentiel. Finalement **la DCSSI conclut ou non à la délivrance d'un certificat** et élabore un rapport de certification qui précise les caractéristiques de sécurité proposées. Le certificat est délivré par le Premier Ministre, **il atteste que le produit ou système répond aux objectifs de sécurité spécifiés et que l'évaluation a été conduite conformément aux normes en vigueur**. Concernant les dispositifs de création de signature électronique, le processus d'évaluation s'appuie sur des formalismes issus des Critères Communs (profil de protection notamment).

5 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

En vue d'obtenir une qualification telle que définie dans le décret du 30 mars 2001, un prestataire de services de certification électronique doit demander une évaluation auprès d'un organisme accrédité. Ce dernier mène l'évaluation pour vérifier la conformité des services avec les exigences décrites dans le décret du 30 mars 2001 "ainsi que les normes, prescriptions techniques et règles de bonne pratique applicables en matière de certification électronique". Ensuite il établit pour le prestataire un rapport d'évaluation, dont la DCSSI peut prendre connaissance si elle le désire.

L'organisme accrédité décide ou non de la qualification du prestataire et délivre une attestation décrivant les services couverts par la qualification ainsi que sa durée, **qui ne peut excéder un an**.

Pour obtenir une accréditation à l'évaluation des prestataires de services de certification électronique, un organisme doit adresser à un centre d'accréditation (en France la COFRAC - Comité Français d'Accréditation) une demande comportant un certain nombre de renseignements obligatoires. À l'issue de l'instruction le centre d'accréditation décide ou non de l'accréditation de l'organisme, en en informant la DCSSI. L'accréditation est accordée pour une durée de deux ans renouvelable.

6 Liens utiles

- Loi du 30 mars 2000

<http://www.juriscom.net/txt/loisfr/l20001303.htm>

- Décret du 30 mars 2001

<http://www.juriscom.net/txt/loisfr/d20010330.htm>

- Décret du 18 avril 2002

<http://www.ssi.gouv.fr/fr/reglementation/decret2002-535.html>

- Arrêté du 31 mai 2002

<http://www.ssi.gouv.fr/fr/reglementation/arr31052002.html>

- site de la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Informations)

<http://www.ssi.gouv.fr/fr/dcssi/>

- faq de la DCSSI sur le décret du 30 mars 2001

http://www.ssi.gouv.fr/fr/faq/faq_sigelec.html

- faq de la DCSSI sur l'évaluation et la certification

http://www.ssi.gouv.fr/fr/faq/faq_ec.html

- liste des CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information)

<http://www.scssi.gouv.fr/fr/confiance/cesti.html>

- site de l'EESSI (European Electronic Signature Standardization Initiative)

<http://www.ict.etsi.org/EESSI/eessi-homepage.htm>