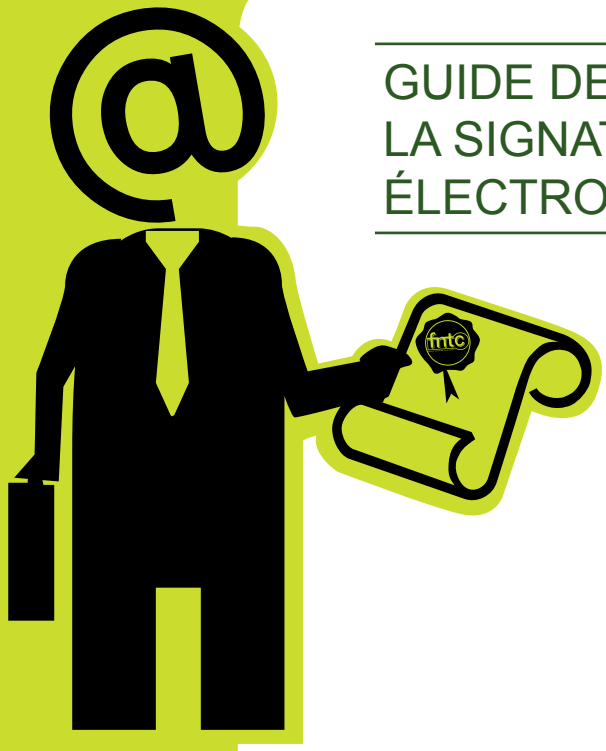
Fédération Nationale des Tiers de Confiance

GUIDE DE LA SIGNATURE ÉLECTRONIQUE



COLLECTION
LES GUIDES DE LA CONFIANCE
DE LA FNTC

Par le groupe de travail «signature électronique»
de la Fédération Nationale des Tiers de Confiance

Dans la collection les guides de la Confiance de la FNTC

>> Vade-mecum juridique de la dématérialisation des documents
(mars 2008)

>> Guide de la dématérialisation des marchés publics
(décembre 2006)

>> Guide de l'horodatage
(octobre 2004)

Prochaines parutions

>> Guide de la facture électronique

>> Guide de l'e-vote électronique

© Copyright octobre 2008

Le présent document est une oeuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de la FNTC (Fédération Nationale des Tiers de Confiance). La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par la FNTC ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'article L.122-5, d'une part, que *«les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective» et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, «toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite»* (article L.122-4 du Code de la Propriété Intellectuelle).
Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

Préface

La dématérialisation des documents et des échanges est désormais une réalité incontournable. Elle a aujourd'hui de multiples applications (télédéclarations, factures électroniques, appels d'offres, contrats en ligne, etc.) et apporte de nombreux bénéfices. Elle s'accompagne également de nouvelles exigences, notamment en matière de confiance et de valeur juridique : permettre au lecteur d'un document d'identifier la personne ou l'organisme qui l'a émis, garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a rédigé et le moment où le lecteur le consulte... Au même titre que les documents papier sont authentifiés par une signature manuscrite, les documents dématérialisés doivent offrir toutes les garanties en matière de preuve.

La signature électronique est la réponse essentielle à ces besoins.

En prolongement de son vade-mecum juridique de la dématérialisation des documents, la Fédération Nationale des Tiers de Confiance est heureuse de vous offrir **le guide de la signature électronique**. Il a pour but de faire un tour d'horizon de tout ce que vous avez toujours voulu savoir sur le sujet, et d'apporter des réponses concrètes à vos questions :
A quoi sert-elle ? Quels sont les enjeux et les perspectives ? Quels sont les bonnes pratiques en vigueur ? Comment la mettre en œuvre ? Quelles sont les exigences juridiques et techniques ? Quelles sont les initiatives des pouvoirs publics ?
Ce guide est le fruit des travaux des différents membres de la FNTC, acteurs du marché de la dématérialisation.

Les adhérents de la FNTC

Remerciements

Aux contributeurs

Dimitri Mouton et Stéphane Drai (CertEurope) ;
Sylvie Camus et Anne Gombert (France Telecom R & D) ;
Eric Caprioli et Pascal Agosti (Cabinet Caprioli & Associés) ;
Sabine Lipovetsky (Cabinet Kahn & Associés)

Et aux participants

Olivier Jury (Agysoft) ;
Jean-Jacques Milhem (Atos WorldLine) ;
Olivier Demilly (ChamberSign) ;
Nicolas Catel (Compagnie Nationale des Commissaires aux Comptes) ;
Jean-François Doucède (Conseil National des Greffiers des Tribunaux de Commerce-Infogreffe) ;
Stéphane Gasch (Conseil Supérieur de l'Ordre des Experts-Comptables) ;
Olivier Arous (Cryptolog) ;
Eric Laurent-Ricard (Ecosix) ;
Peter Sylvester (Edelweb) ;
Jean-Luc Fretard (Experian) ;
Gabriel Gil (GLI Services) ;
Hervé Schauer (Cabinet HSC) ;
Jean-Marie Pages (Inforsud) ;
Pascal Colin (Keynectis) ;
Frédéric Galland (Locarchives) ;
Loïc Sineau (Orsid) ;
Denis Bourdillon (Pitney Bowes Asterion) ;
Stéphanie Roussel (SR Développement) ;
Raymond de Bernis (TrustMission)

Sommaire

1/ Introduction

1.1 Introduction : le nécessaire essor de la signature électronique

Dès 1987, le prix Nobel d'économie Robert Merton Solow annonçait que l'outil informatique n'apporterait pas d'augmentation de la productivité si son adoption n'était pas accompagnée par une refonte des processus métier.
Impôts, relations à l'administration, e-commerce, marchés publics, relations clients / fournisseurs / partenaires, intranet, vie privée : vingt ans après, la quasi intégralité des échanges autrefois réalisés en papier sont passés à l'électronique : la dématérialisation est définitivement entrée dans les moeurs, et toutes les grandes structures se sont réorganisées de manière irréversible pour s'adapter à cette évolution.
Pourtant, dans la Gaule occupée de la dématérialisation, un petit village d'irréductibles a longtemps résisté à l'envahisseur : celui des flux sensibles, des documents engageant leur auteur, des échanges à valeur probatoire.
Le frein longtemps identifié à la dématérialisation de ces éléments (contrats, factures, offres commerciales…) était la sécurité : sécurité juridique, intégrité, garantie de provenance… La signature électronique, fonction aujourd'hui arrivée à maturité tant des points de vue législatif que technique et organisationnel, permet de débloquer la situation, et de dépasser le paradoxe de Solow pour atteindre les vrais bénéfices de la dématérialisation.
L'usage de la signature électronique peut se fonder sur des besoins différents, d'ordre juridique, fonctionnel, psychologique, sans que ces trois domaines soient exclusifs les uns des autres. Toutefois, la finalité réelle est toujours d'ordre économique.

1.2 A qui s'adresse ce guide

- Vous êtes un décideur et vous vous demandez ce que la signature électronique peut apporter à votre entreprise ?
- Vous êtes responsable marketing et vous aimeriez ouvrir des services en ligne sur internet ?
- Vous êtes responsable juridique et vous aimeriez alléger la masse de papier qui entoure la gestion de l'entreprise?
- Vous êtes DSI et vous vous demandez par quel bout prendre le déploiement de la signature électronique ?

Alors ce guide s'adresse à vous!

Constituée de professionnels reconnus des domaines de la sécurité et de la confiance, la FNTC s'est donné pour objectif, au travers de ce guide, de vous aider à aborder la signature électronique de manière pragmatique, en se fondant sur des réponses concrètes à des questions concrètes, et sur des exemples d'utilisation tirés de la vie réelle et qui correspondent à vos centres d'intérêt.

Ce guide, qui ne se veut pas technique, vous permettra de mesurer les apports possibles de la signature électronique, dans votre contexte quotidien, sans vous encombrer l'esprit de détails inutiles à ce stade de votre réflexion. Vous pourrez ensuite vous rapprocher des experts du métier avec une expression de besoin clarifiée qui vous permettra de mener votre projet dans les meilleures conditions.

Pour les inconditionnels de la technique, on trouvera en annexe une synthèse minimaliste (Annexe 3 - Eléments techniques), et l'on pourra se reporter aux nombreux ouvrages qui traitent du sujet, disponibles via Internet ou chez votre libraire habituel.

2/ F.A.Q.


Aspects juridiques


Aspects techniques


Aspects financiers et commerciaux


Aspects organisationnels


Confiance et sécurité

2.1 A quoi sert la signature électronique ? Qu'est-ce que ça apporte à mon entreprise, à mon organisation, à mon activité ?

C'est compliqué ?
Non ! La signature électronique est simple d'usage et déjà très répandue.

La signature électronique a d'ores et déjà fait son entrée dans l'entreprise,
dans l'administration et auprès des particuliers via les télédéclarations sociales et fiscales :
-TéléTVA ;
-TéléIR ;
-TéléC@rteGrise ;
-Télédéclarations sociales (DUCS, DDS-U…).
Ces démarches ont permis à toutes les entreprises utilisant une télé-déclaration de constater, d'une part la simplicité extrême de l'usage de la signature électronique, et d'autre part les gains de productivité induits dans les procédures administratives.

• Exemple 8 : l'impôt sur le revenu (C to A)

Quelles économies espérer en utilisant la signature électronique ?
La signature électronique permet la *dématérialisation* des processus et des documents.

La vie de l'entreprise ou de toute organisation nécessite que certains documents soient signés par les employés, l'employeur, les partenaires, les clients et les fournisseurs. Il s'agit par exemple du contrat de travail et de ses avenants, du règlement intérieur, de la charte informatique, mais aussi des contrats, accords de confidentialité, partenariats, factures, etc.
Afin de faire des économies sur le papier, le stockage, le temps d'accès aux documents, la recherche d'information, l'entreprise ou l'organisation peut dématérialiser ces éléments, c'est-à-dire ne les produire qu'au format électronique, sans édition papier.
Ce n'est pas la signature électronique qui apporte directement une économie, c'est la dématérialisation des documents et les nouveaux processus de gestion mis en oeuvre à cette occasion. Mais il faut pour cela conserver à ces documents leur valeur juridique, donc leur apposer une signature. C'est là le rôle de la signature électronique.
La dématérialisation ne peut donc pas se faire sans signature électronique.
D'autres processus peuvent également être dématérialisés, comme les demandes de congés et leur validation, la gestion des notes de frais, les comptes-rendus d'entretiens de carrière, les comptes-rendus de réunions, etc. Dans tous ces cas, la signature électronique permet de formaliser l'accord des parties et est un facilitateur à la dématérialisation. C'est en cela qu'elle donne confiance dans le processus mis en oeuvre, puisqu'un document signé électroniquement ne peut plus être modifié ou réfuté.

• Exemple 7 : la validation de demandes de formations (B to E).

Quel gain peut m'apporter la signature électronique dans mon activité ?
La signature électronique facilite la signature des documents commerciaux tels que les contrats.

Grâce à la signature électronique, un contrat peut être passé sans rencontre physique et sans aucun échange de papier, avec la même valeur juridique.
Cette possibilité offre un gain de temps considérable tant dans les relations entre professionnels que vis-à-vis du grand public : la contractualisation dématérialisée permet à une entreprise d'acquérir de nouveaux clients bien plus facilement.

- Exemple 4 : l'acquisition de clientèle et la contractualisation sur Internet (B to C).
- Exemple 5 : la signature de contrat en ligne avec un certificat temporaire (B to C).

Quel gain d'image m'apporte la signature électronique dans mes rapports avec mes clients et mes partenaires
Modernité, innovation et écologie !

La signature électronique et, avec elle, la dématérialisation des processus de travail et d'échange, offre une image de modernité et d'innovation, mais aussi d'écologie grâce au « zéro-papier ».
Un exemple prestigieux : le Ministère de l'Economie, depuis une dizaine d'années, mise sur ces procédés pour améliorer son image.

- Exemple 6 : la transmission de documents professionnels (B to B).

Il va falloir y passer ?
Naturellement !

Dans la sphère fiscale, l'obligation est déjà effective.
Mais si les usages de la signature électronique sont en pleine expansion, c'est moins du fait d'obligations règlementaires que pour les avantages qu'elle offre aux entreprises et organisations qui s'en servent.
Au fur et à mesure que les grands groupes internationaux font ce choix pour sécuriser leurs échanges avec leur écosystème de partenaires, la dématérialisation et la signature électronique vont s'imposer à tous comme un procédé aussi incontournable qu'Internet et donner un levier supplémentaire de productivité.

2.2 J'ai des projets qui impliquent des échanges via Internet. Que va m'apporter la signature électronique ?

J'échange déjà par mail avec mes partenaires et clients, à quoi bon ajouter une signature électronique ?

La signature électronique sécurise et formalise les échanges.

Quel risque y a-t-il à échanger par simple mail sans signature électronique ?

> Un mail peut sans difficulté être envoyé au nom d'un tiers.

La signature électronique associe de manière inaltérable l'identité de l'émetteur au mail envoyé.
Il est donc impossible d'envoyer un mail signé électroniquement à la place de quelqu'un.
Il est également impossible à la personne qui a envoyé un mail signé électroniquement de nier cet envoi.

> Un mail peut être modifié après avoir été envoyé.

La signature électronique permet de prouver l'intégrité d'un message : une fois le mail signé électroniquement, toute modification ultérieure sera immédiatement détectée à l'ouverture.

> Un mail simple ne constitue qu'un commencement de preuve.

La signature électronique, de même que la signature manuscrite sur un papier, porte l'engagement du signataire sur le contenu du message.

Ainsi, la signature électronique apporte aux échanges par mail une plus grande sécurité et permet des échanges formalisés en toute confiance.

La plupart des solutions de messagerie incluent les fonctions de signature électronique. La vérification de signature se fait automatiquement à la réception d'un mail signé. L'usage du mail signé est donc en pratique d'une grande simplicité.

• Exemple 6 : la transmission de documents professionnels (B to B).

Quels documents nécessitent une signature électronique ?

Tout ce que vous signez de manière manuscrite peut (doit) être signé de manière électronique.

Le Code civil, dans son article 1316-4, définit la notion de signature. Cette définition est commune à la signature manuscrite et à la signature électronique. Le code civil donne ensuite des détails sur la définition technique de la signature électronique, mais il est important de se rappeler qu'une signature électronique est équivalente à une signature manuscrite, et qu'elle doit donc être utilisée dans les mêmes cas.

Définition de la signature :
La définition de la signature a été introduite par la loi du 13 mars 2000, lors de la consécration de la signature électronique. L'article 1316-4 du Code Civil énonce que *« 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. »*
Il est à noter que cette définition concerne la signature au sens large, qu'elle soit manuscrite ou électronique.

Fonctions de la signature :
- Perfection de l'acte : à défaut de signature, l'acte juridique ne constitue qu'un commencement de preuve par écrit ;
- Identification du signataire ;
- Adhésion au contenu de l'acte.

Définition de la signature électronique :
L'article 1316-4 alinéa 2 du Code Civil précise que la signature, *« Lorsqu'elle est électronique, consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans les conditions fixées par décret en Conseil d'Etat. »*

Certains usages de la signature électronique sont imposés par la loi. Par exemple la signature électronique est obligatoire pour :

- la télédéclaration de revenu : le certificat est fourni par l'administration fiscale ;
- le service Téléc@rtegrise qui permet d'obtenir un certificat de situation administrative ;
- la présentation d'une offre pour les marchés publics (article 48 I Code des marchés publics, et arrêté ad hoc). La signature doit être conforme au référentiel intersectoriel de sécurité (http://www.entreprises.minefi.gouv.fr/certificats/);
- la télédéclaration URSSAF. Celle-ci peut être réalisée par courrier électronique ou bien en ligne sur un site sécurisé ;
- la télédéclaration de TVA (TéléTVA) : lors d'une transmission EDI, c'est le « partenaire EDI » déclaré auprès de l'administration qui signe l'envoi, alors qu'en mode EFI, c'est le déclarant lui même qui signe ;
- les factures électroniques, (article 289 V du Code général des impôts).

• Exemple 3 : la signature de facture (B to B ou B to C).
• Exemple 8 : l'impôt sur le revenu (C to A).

Mais la signature électronique peut aussi être employée pour les actes non régis par des textes de loi :

- contrats ;
- constats ;
- formulaires internes d'entreprises ou d'organisations ;
- documents de travail…

• Exemple 4 : l'acquisition de clientèle et la contractualisation sur Internet (B to C).
• Exemple 5 : la signature de contrat en ligne avec un certificat temporaire (B to C)
• Exemple 6 : la transmission de documents professionnels (B to B).
• Exemple 9 : la demande d'injonction de payer (B to A).

Puis-je déléguer ma signature électronique ?
Bien entendu !

La signature est un acte personnel, qui lie l'identité du signataire au document signé (voir la définition ci-dessus). Il n'est donc pas possible de prêter à un tiers ses propres moyens de signature électronique afin qu'il signe en notre nom.
En revanche, de la même manière que pour une signature manuscrite, la délégation est possible : un délégué peut alors avoir le droit de signer à la place du titulaire. La signature est bien réalisée au nom du délégué, avec ses propres moyens de signature.
La délégation passe par la rédaction d'une attestation, qui indique :
· le délégataire ;
· le délégué ;
· l'objet de la délégation ;
· la durée de la délégation.
Cette attestation peut être électronique.
Selon les cas, elle devra être fournie systématiquement avec chaque document signé, ou simplement rester disponible en cas de vérification.

Quels formats de documents peut-on signer ?
Tous les types de fichiers peuvent être signés. Mais attention…

La signature électronique peut porter sur tout type de document (.doc, .xls, .pdf, .jpg, .tiff, email, formulaire xml…). Aucune contrainte technique n'empêche de réaliser une signature électronique et ce, quel que soit le format.

Cependant, dans certains domaines, des contraintes sont imposées sur le format des données. Les formats XML (par exemple pour les échanges fiscaux) et PDF (par exemple pour l'archivage) sont ainsi souvent mis en avant.

Il convient de noter que certains documents peuvent avoir un contenu dynamique : c'est le cas des macros contenues notamment dans les documents bureautiques. La présence de ces macros n'empêche pas de signer le document. Toutefois, une macro peut afficher un texte différent à chaque ouverture du document, sans que cela invalide la signature électronique.
Ainsi, un champ dynamique contenant la date peut se mettre à jour automatiquement, un montant de contrat pourrait être modifié selon une règle prédéfinie…
Quelle valeur aurait alors le document signé ?
Il est donc préférable d'apposer la signature électronique sur des documents statiques, non susceptibles de changer, ou de vérifier avant de signer électroniquement l'absence de champs dynamiques dans les documents.

• Voir chapitre : Les bonnes pratiques.

Puis-je imprimer un document signé électroniquement ?
Oui mais attention à la valeur de cette impression.

Il est toujours possible d'imprimer un document qui a été signé électroniquement.
De la même manière, il est possible de scanner un document papier signé de manière manuscrite.
Mais dans les deux cas, c'est l'original qui a une valeur juridique : cet original est le document électronique dans le premier cas, et le document papier dans le second cas.

Afin d'imprimer la signature elle-même, il convient de la rendre intelligible à un être humain, car une signature électronique n'est qu'un code informatique abscons. C'est le rôle des logiciels de vérification de signature, qui permettront d'imprimer un compte-rendu de vérification attestant de la validité de la signature électronique.

2.3 Quelle est la valeur de la signature électronique ?

Quelle est la différence entre une signature électronique et une signature manuscrite ?
Aucune différence, sauf la nature du document et le mode de réalisation.

La signature électronique a la même valeur que la signature manuscrite dès lors qu'elle permet l'identification de celui qui l'appose ainsi que la manifestation du consentement des parties aux obligations qui découlent de cet acte (article 1316-4 du Code civil).

Il est important de noter qu'en cas de litige, c'est le juge qui appréciera souverainement le caractère probant de la signature et par là sa valeur juridique, et ce que la signature soit manuscrite ou électronique (articles 285 et suivants du Code de procédure civile).

J'ai scanné ma signature manuelle et je l'ai insérée dans le document, quelle valeur a-t-elle ?

L'image d'une signature manuscrite ne constitue pas une signature électronique !

La signature scannée apposée sur un document électronique n'a pour les juristes que la valeur d'un commencement de preuve au sens du Code civil. Cela signifie que si la partie adverse dénie la valeur juridique du document contenant la signature scannée produit en justice, elle peut y parvenir au motif que le procédé de signature n'est pas fiable au sens du Code civil.

Quelle est la différence entre une signature électronique et une signature électronique sécurisée ?

Toutes les signatures électroniques ont la même valeur juridique !

Rappelons que, d'un point de vue strictement juridique, peu importe que les signatures électroniques soient « simples », « sécurisées », ou qu'elles utilisent des « certificats qualifiés » : elles ont toutes la même valeur juridique.
On met souvent en avant la « présomption de fiabilité », attachée aux signatures électroniques sécurisées réalisées selon le dispositif spécifié à l'article 1316-4, al. 2 du Code civil et à l'article 2 du décret du 30 mars 2001.
Il faut toutefois rappeler à ce sujet deux éléments :
> L'apport juridique de la signature « emportant présomption de fiabilité » est faible dans le cadre de relations B to B ou B to C.
> Les exigences relatives à la signature sécurisée sont contraignantes à mettre en oeuvre, et ne concerneront dans la pratique qu'une population très réduite, principalement les professions réglementées pour la perfection des actes authentiques.

Mes partenaires sont à l'étranger. Nos signatures électroniques ont-elles la même valeur ?

La signature électronique est définie au niveau européen et dans tous les pays industrialisés.

Les signatures électroniques réalisées dans différents pays ont une valeur transfrontalière dès le moment où les dispositifs de signature électronique utilisés sont reconnus comme étant équivalents entre eux (par voie contractuelle ou par reconnaissance étatique). Le cadre juridique dans les Etats membres de l'Union européenne découle de la transposition d'une directive communautaire (directive 1999/93/CE).
Il faut analyser au cas par cas les cadres législatifs locaux pour déterminer les modalités d'établissement d'une équivalence des signatures électroniques.

• Exemple 2 : la signature électronique dans un contexte international (B to A)

2.4 Je souhaite déployer la signature électronique dans mon entreprise, mon organisation, ou au sein d'un projet. Comment faire ?

On entend toujours parler de certificats… Mais qu'est-ce que c'est ?
Le certificat est une « carte d'identité électronique » qui permet de réaliser des signatures électroniques.

La signature électronique nécessite l'utilisation d'un certificat. C'est grâce à lui que se fera le lien entre le document signé et l'identité du signataire, un peu comme, dans le cas d'une signature manuscrite, on pourra comparer la signature d'une personne avec celle qui figure sur sa carte d'identité ou au dos de sa carte bancaire.

• Annexe 2 - Le cycle de vie du certificat.

De quoi a-t-on besoin pour signer ?
Pour signer, il faut un certificat (la carte d'identité) et un logiciel de signature (le stylo).

Le signataire doit disposer :

- de son certificat électronique : selon le contexte, ce certificat peut être acheté auprès d'une Autorité de Certification du marché, ou bien délivré en interne par l'entreprise ou l'organisation à laquelle appartient le signataire ;
- d'un outil de signature électronique : la fonctionnalité de signature électronique est en général directement intégrée dans l'application qui la nécessite (exemples : messagerie, plate-forme de marchés publics, télédéclaration des impôts et de la TVA…). Dans le cas contraire, on emploiera un outil de signature du marché, dédié à ce seul usage.

Je n'ai pas de certificat, puis-je signer quand même ?
Le certificat est indispensable pour signer.
Mais il peut être produit au moment de la signature.

A ce jour, la législation ne permet pas de réaliser de signature électronique sans utilisation d'un certificat faisant foi de l'identité du signataire.
Certaines applications proposent la génération du certificat au moment où son usage est nécessaire, avec une durée de validité très courte (de l'ordre de quelques minutes). Dans ce cas, les démarches préalables d'obtention d'un certificat et d'installation sur le poste de travail ne sont pas nécessaires.
Toutefois, les offreurs de tels services doivent disposer d'informations minimum relatives au signataire.

• Exemple 5 : la signature de contrat en ligne avec un certificat temporaire (B to C)

Qu'entend-on par « vérification de signature » ?
Vérifier une signature, c'est s'assurer de sa valeur !

La signature électronique ne fournit pas, comme la signature manuscrite, un élément graphique immédiatement identifiable et qui suffise à reconnaître le signataire.
La vérification de la signature électronique nécessite l'utilisation d'un outil, qui analyse le code de la signature et affiche de manière lisible les éléments pertinents :

- validité de la signature ;
- identité du signataire ;
- date de la signature…

Cet outil de vérification est en général inclus dans l'application dans laquelle le document signé est échangé. Les informations de vérification sont alors présentées à l'utilisateur sans action de sa part.
Dans le cas contraire, on utilisera un outil de vérification de signature du marché, dédié à ce seul usage.

NB 1 : La personne qui vérifie une signature n'a pas besoin de disposer d'un certificat à son nom.

NB 2 : Si la vérification de signature manuscrite nécessite de connaître à l'avance l'élément graphique et de le reconnaître, la signature électronique s'abstrait de tout contexte préalable. Il est ainsi bien plus difficile de forger une fausse signature électronique, ou d'en fausser la vérification, que de falsifier une signature manuscrite.

3/ Les usages

Les cas d'usage de la signature électronique présentés ci-dessous, souhaitent illustrer la diversité des situations dans lesquelles ce procédé s'applique, en empruntant des exemples à tous les domaines : B to B (échanges entre entreprises), B to A (échanges entre entreprises et administration), B to C (échanges entre entreprises et clients), C to A (échanges entre citoyens et administration), B to E (échanges entre l'entreprise et ses employés), ou A to A (échanges entre administrations).

3.1 La signature électronique garante de la valeur juridique des échanges

3.1.1 Les règles applicables et la convention de preuve

Certains secteurs d'activité bénéficient de règles spécifiques fixées par des textes juridiques et déterminant le cadre dans lequel la signature électronique doit être réalisée. Parmi ces secteurs, on peut citer : les professions réglementées (officiers publics et ministériels), les marchés publics, la facture électronique, etc...
Ces usages ne sont qu'une exception à la règle générale.
Hors de ces cas particuliers, les règles déterminant les moyens de preuve ou encore la charge de la preuve peuvent faire l'objet de conventions, c'est-à-dire que les parties peuvent déroger par contrat aux dispositions du Code civil en matière de preuve. Ces conventions vont permettre aux parties de régler à l'avance la question de la force probante des contrats qu'elles concluent en ligne. Dans les contrats de consommation, il est possible d'insérer des clauses aménageant le système de preuve sous réserve, pour le professionnel, de respecter la législation en matière de clauses abusives.
En l'absence de telles conventions, c'est au juge que reviendra le soin de régler les conflits de preuve, spécialement entre deux preuves sur des supports différents (papier et numérique), conformément à l'article 1316-2 du Code civil. Ainsi, il déterminera quelle est la preuve qui lui semble le plus vraisemblable.
En matière de signature électronique, la convention de preuve décrira les procédures techniques à suivre afin d'établir, conserver et produire une signature reconnue comme valable entre les parties.
Dans le cadre d'une application ou d'un contexte métier précis, une politique de signature pourra définir qui est autorisé à signer, selon quels droits et autorisations, comment la signature sera réalisée et comment elle sera réalisée. Un tel document sert principalement à rappeler, dans le cadre de la conduite du changement, les règles souvent implicites liées au droit de signer déjà en vigueur dans la société.

3.1.2 Les deux rôles juridiques de la signature

Un document électronique peut être requis à titre de preuve dès le moment ou conformément à l'article 1316-1 du Code civil, la personne dont l'écrit sous forme électronique émane est dûment identifiée et qu'il est établi et conservé dans des conditions de nature à en garantir l'intégrité.
L'utilisation de la signature électronique permet de s'assurer que les deux fonctions mentionnées à l'article 1316-1 du Code civil sont bien réunies.

Les articles 1108-1 et 1108-2 du Code civil traitent de la validité des actes juridiques conclus sous forme électronique. Il pourra s'agir, par exemple, de l'écrit formalisant un cautionnement commercial, un contrat de bail, un contrat de crédit à la consommation ou de crédit immobilier, un contrat de travail à durée déterminée, les statuts de société, etc. A défaut d'écrit, ces actes seraient juridiquement nuls.
Désormais, un écrit sous forme électronique constatant un de ces actes sera valable dès le moment où les conditions entourant son établissement et sa conservation sont assurées, à savoir les mêmes que celles prévues pour les fonctions probatoires de l'écrit.
C'est dire l'importance de la signature électronique qui doit être considérée comme l'élément central du dispositif juridique en matière d'actes électroniques.

3.1.3 Exemple 1 : la signature des marchés publics (B to A)

Lorsqu'une entreprise répond par la voie électronique à une procédure de marchés publics, elle a l'obligation de signer certains éléments de son envoi, en particulier l'acte d'engagement.
C'est cet acte d'engagement, co-signé par la personne publique lors de l'attribution du marché, qui deviendra le contrat. Le mécanisme est donc semblable à l'état de l'art des procédures papier.
Pour signer électroniquement, l'entreprise doit être munie d'un certificat référencé pour cet usage par le Ministère de l'Economie, des Finances et de l'Emploi.
Elle doit suivre la procédure de signature décrite sur la plate-forme de marchés publics.
Le signataire doit être une personne habilitée à engager l'entreprise, ou disposer d'une délégation lui donnant ce pouvoir.
Des milliers d'entreprises procèdent déjà de cette manière, sans aucune difficulté, le processus étant défini par le Code des marchés publics, mis en oeuvre par les plates-formes de dématérialisation, grâce aux certificats de signature référencés par le Ministère de l'Economie, des Finances et de l'Emploi.

La FNTC a publié en 2006 un Guide de la confiance consacré à la dématérialisation des marchés publics

3.1.4 Exemple 2 : la signature électronique dans un contexte international (B to A)

Un groupe aéronautique européen a répondu à un appel d'offres de l'administration américaine qui exigeait que les réponses soient exclusivement transmises par voie électronique. De même, tous les échanges tels que accords de confidentialité, documents administratifs entre cette administration et les industriels sont électroniques.
Pour être en mesure d'être conforme à ces exigences, le groupe européen s'est s'équipé de certificats électroniques reconnus par les administrations européennes et américaines de façon à ce que les documents électroniques signés aient une valeur légale reconnue dans chacun des pays, via un mécanisme appelé la certification croisée (ou cross-certification).
Grâce à ce procédé mis en oeuvre par des tiers de confiance reconnus par les administrations respectives, ce groupe européen a remporté l'appel d'offres en question.

3.2 La signature électronique au service des processus métier

3.2.1 Les apports fonctionnels de la signature électronique

La signature électronique garantit l'origine d'un document et son intégrité.
Ces aspects fonctionnels permettent de se protéger dans les transactions quotidiennes sur internet ou sur un intranet.

3.2.2 Exemple 3 : la signature de facture (B to B ou B to C)

Lorsqu'elle est dématérialisée fiscalement, la facture peut être signée soit par une personne physique, soit par une personne morale. Dans ce second cas, l'outil de signature se trouve sur le serveur du facturier et la signature est apposée au nom de l'entreprise ou de l'organisation émettant la facture.
Si la signature électronique des factures a une portée juridique, dans la mesure où elle est imposée par les textes (cf Annexe 1 - Liste des textes légaux et normatifs), elle répond également à un autre besoin, plus fonctionnel : celui de garantir l'intangibilité du document. En effet, une facture, une fois signée électroniquement, ne peut plus être modifiée.
Enfin, elle garantit sa provenance, remplaçant ainsi le simple papier à en-tête utilisé dans le processus papier de facturation. En effet, la signature électronique garantit le lien du document avec l'identité du signataire.

3.2.3 Exemple 4 : l'acquisition de clientèle et la contractualisation sur Internet (B to C)

Un groupe, spécialiste du crédit à la consommation, a entièrement dématérialisé son processus d'acquisition de clientèle : grâce à un enregistrement en ligne disponible 24h/24, le particulier peut remplir un formulaire, envoyer des copies de ses documents d'identité et obtenir après validation par un agent un certificat lui permettant d'apposer sa signature électronique sur son contrat d'adhésion.

Les gains de productivité d'un tel processus sont évidents : le client n'a pas besoin de se déplacer ni d'envoyer ses documents, tout se fait en ligne, sans attente, et la valeur juridique du contrat demeure identique à celle d'un contrat papier.

3.2.4 Exemple 5 : la signature de contrat en ligne avec un certificat temporaire (B to C)

Les banques offrent à leurs clients sur Internet une offre grandissante de produits et services bancaires. Pour souscrire à certains de ces services, par exemple, pour un crédit à la consommation, la signature d'un contrat est légalement obligatoire. Une quinzaine d'établissements financiers proposent aujourd'hui à leurs clients particuliers de signer ces contrats en ligne.
Ce service est assuré 24h sur 24 par un opérateur agréé qui délivre des certificats temporaires selon les informations fournies par les banques. Ceci permet au client internaute de procéder à la signature de son contrat de crédit alors qu'il n'était pas en possession préalable d'un certificat ; cette procédure ne nécessite donc aucun équipement pour le client. Cette application ouvre l'usage de la signature de contrat en ligne à tous les clients internautes des banques ou organismes de crédit à la consommation.

3.3 La signature électronique pour la confiance dans les échanges

3.3.1 La sécurité au service de la confiance

Grâce à la signature électronique, l'émetteur d'un document a une garantie de sécurité sur la propriété et l'intégrité de ses données. Cet acte, au-delà de sa portée juridique, qui est toujours présente, permet de donner du poids, de formaliser, de se rassurer.
Tout ce que l'on fait par mail en se demandant si cela vaut quelque chose, tout ce que l'on ne fait pas par mail de peur que ça ne vaille rien, tous les envois que l'on n'ose pas faire sur Internet de peur de se faire spolier, tous ces actes sont facilités par la signature électronique qui permet la traçabilité des actions et l'intangibilité des documents. Ces échanges deviennent possibles, non par l'apparition d'un nouveau procédé technique, mais par la disparition d'un frein psychologique.
Les exemples sont nombreux en B to B : courriers recommandés, preuves et accusés de réception signés, factures, propositions commerciales, bons à tirer, flux vidéo… L'entreprise signe ces actes pour les formaliser et ainsi les rendre dématérialisables.
De même, au sein de l'entreprise, la signature des demandes de congés ou des demandes d'achat permet une responsabilisation des individus et fluidifie les processus internes.

3.3.2 Exemple 6 : la transmission de documents professionnels (B to B)

Une jeune entreprise de conseil en marketing a développé le concept de « ConsoRéalité » : elle filme les consommateurs chez eux ou dans les magasins, analyse leurs comportements et transmet ces études à ses clients, grands noms du secteur agro-alimentaire.
Pour une telle structure, l'usage de la signature électronique doit être avant tout simple, tant pour l'émetteur des données que pour le destinataire.
La signature ne fait pas partie à proprement parler du processus métier.
En revanche, elle permet à une jeune entreprise innovante de se sécuriser par rapport à sa clientèle en garantissant l'intégrité du travail fourni et en protégeant l'originalité de la méthode de travail. Elle offre également l'occasion de donner de l'entreprise une image « de pointe », de dynamisme au sein des nouvelles technologies.
Enfin, non intrusive, elle permet au client de conserver la liberté de copie, d'impression, d'exploitation des études commanditées.

3.3.3 Exemple 7 : la validation de demandes de formations (B to E)

Un grand groupe de télécom a mis en place, sur son intranet, un processus tout électronique de demande de formations : l'employé remplit en ligne un formulaire décrivant la formation souhaitée. Son supérieur hiérarchique valide la demande et consent ainsi à l'engagement financier correspondant en réalisant une signature électronique du formulaire.
Cet usage de la signature électronique vient compléter la gamme des fonctionnalités liées au déploiement des outils de sécurité au sein du groupe.

3.4 La signature électronique pour améliorer la productivité

3.4.1 Une brique de la dématérialisation

La notion de signature est ancienne et n'est pas considérée comme un élément créateur de valeur ou de processus. Par extension, la finalité de la signature électronique demeure de transposer la notion de signature dans le monde électronique afin de rendre possible le processus global de dématérialisation.
A titre d'exemple, la Commission européenne, à travers la dématérialisation des marchés publics européens, vise deux objectifs : l'augmentation de la concurrence, qui améliorera l'efficacité économique de l'acte d'achat et entraînera des économies de fonds publics – et la lutte contre la corruption, grâce à la transparence et à la traçabilité offertes par les processus électroniques.

3.4.2 Exemple 8 : l'impôt sur le revenu (C to A)

En 2007, 7,6 millions de déclarations de revenu transmises par voie électronique ont permis aux services de l'Etat une économie de traitement importante.
La signature électronique, dans ce cas, est utilisée à des fins économiques autant que juridiques, et apporte un service apprécié par le déclarant.
Cet exemple illustre que la signature électronique améliore la productivité de l'Etat tout en augmentant la qualité du service aux citoyens : au-delà de la déclaration des revenus, le certificat délivré permet d'accéder à son compte fiscal et de bénéficier d'informations en temps réel sur le portail du gouvernement (http://www.impots.gouv.fr).

3.4.3 Exemple 9 : les déclarations au Registre du Commerce et la requête en injonction de payer (B to A)

Les greffes de tribunaux de commerce grâce à leur portail www.infogreffe.fr permettent aux chefs d'entreprise de procéder en quelques clics à leurs immatriculations et déclarations modificatives au Registre du Commerce et des Sociétés.
Ces déclarations et pièces annexées transitent sur la plate-forme Infogreffe puis sont archivées sur le coffre-fort électronique du Greffe compétent pour contrôler la déclaration. Cette procédure dématérialisée sécurisée permet au chef d'entreprise d'obtenir son extrait de Registre du Commerce (K-bis) dans des délais très réduits après contrôle de conformité des collaborateurs du Greffier.
Dans la même logique de «e-services aux entreprises» les greffes des tribunaux de commerce permettent aux entreprises d'accélérer le recouvrement de leurs créances commerciales grâce à un service entièrement dématérialisé de requête en injonction de payer.
La requête et les pièces justificatives sont transmises et signées électroniquement par le créancier sur le portail d'Infogreffe. La procédure est enclenchée sans délai et permet un rendu de décision très rapide.
D'autres services sont en cours de livraison comme le dépôt des comptes électroniques, le placement électronique des assignations, les demandes de renvoi en ligne, le bureau virtuel du juge.
Ces exemples et projets illustrent que les téléprocédures développées par les Greffes des Tribunaux de Commerce associées à l'usage d'une signature électronique sécurisée améliorent la mission de service public rendue aux entreprises et aux justiciables.

4/ Les bonnes pratiques

4.1 Introduction

Tout projet informatique et, au-delà, tout projet d'entreprise ou d'organisation, est unique.
Toutefois, un certain nombre de règles permettent, si on les suit, d'éviter la majorité des écueils susceptibles de se présenter. Nous les rappelons ici.

4.2 La technique au service du projet

4.2.1 La signature électronique : un domaine techniquement mûr

La signature électronique est trop souvent vue comme un domaine purement technique et d'une grande complexité. Ce préjugé provient de l'histoire de ce domaine : les outils techniques ont été mûrs bien avant les aspects juridiques, ce qui a laissé la communication sur le sujet entre les mains des techniciens.
Pour autant, cette avance de maturité technique est une très bonne chose, puisque grâce à elle, la technique ne constitue justement plus le frein aux projets de signature électronique. Les projets qui incluent l'usage de la signature électronique doivent donc être menés du point de vue métier et organisationnel, de même que tout autre projet de l'entreprise ou de l'organisation.

4.2.2 S'entourer de professionnels compétents

La signature électronique est à la croisée de plusieurs domaines : technique, juridique, organisationnel, ergonomique. Les compétences nécessaires à la réussite d'un projet de signature électronique sont rarement toutes présentes dans l'entreprise ou dans l'organisation, et encore plus rarement auprès d'une même population.
Il est donc fondamental, pour réussir son projet, d'obtenir du conseil et de l'assistance aussi bien que des prestations techniques, auprès de professionnels compétents ayant de l'expérience dans le domaine.

4.2.3 Adapter le niveau de sécurité aux besoins

La signature électronique appartient au domaine de la sécurité informatique. Pour autant, ce n'est pas en « blindant » les aspects sécuritaires que l'on assurera au mieux les chances de succès du projet. Il convient d'adapter le niveau de sécurité à l'objectif poursuivi, notamment en termes juridiques.
Il existe différents niveaux de sécurité liés à la signature et aux certificats, dont on trouvera la définition en annexe (cf La qualité des certificats). L'essentiel est de définir clairement ses objectifs en termes métier, de procéder à une analyse de risque technique et juridique, et de conserver bon sens et esprit critique lors du choix de la solution à déployer.

4.3 Prendre en compte le facteur humain

4.3.1 Mettre l'utilisateur au centre des usages

Qu'il s'agisse d'un client, d'un employé, d'un partenaire, c'est toujours un être humain qui sera l'utilisateur final du système de signature électronique mis en place.
Etant donné l'enjeu multiple du projet (juridique, économique, etc.), il est fondamental d'obtenir l'adhésion de l'utilisateur au système déployé.

4.3.2 Penser les services du point de vue ergonomique

Un produit complexe à utiliser est un produit mal conçu.
La signature manuscrite est extrêmement simple à réaliser : l'utilisateur prend un stylo et écrit son nom au bas de la feuille.
La signature électronique doit atteindre le même niveau de simplicité.
L'ergonomie doit être un des éléments principaux du choix d'une solution.

4.3.3 Formation des utilisateurs

Même si les logiciels ou services web se veulent « intuitifs », il est indispensable de fournir aux utilisateurs une formation adaptée à leurs besoins : cours et travaux pratiques, e-learning ou autoformation, manuel illustré, aide en ligne…
La formation doit être adaptée à la cible : on n'apportera pas le même niveau d'expertise à un commercial devant signer quotidiennement ses réponses aux appels d'offres et à un prospect devant, une seule fois, signer en ligne son contrat d'adhésion.
Mais ces deux populations, pour des raisons différentes, ne peuvent être laissées seules face à un nouveau dispositif aussi important que la signature électronique.

4.3.4 Conduite du changement

Lorsque la signature électronique vient modifier les habitudes de travail dans l'entreprise ou dans l'organisation, il faut anticiper ces modifications et les accompagner : si les contrats reçus sont désormais électroniques et non plus papier, faut-il un écran plus grand ? Comment réalise-t-on l'archivage pour garantir la conservation à long terme des documents électroniques ? Comment l'agent vérifie-t-il la signature ? Comment le client obtient-il une copie de son contrat ? Tous les services devant traiter le document signé sont-ils prêts à le faire (services techniques, juridiques, commerciaux, ressources humaines, etc.) ?
Il suffit qu'un maillon de la chaîne de traitement n'adhère pas au nouveau processus pour que l'ensemble du projet soit remis en cause. Il importe donc d'expliquer à tous et à chacun le pourquoi de la modification du processus, les changements que cela implique et les moyens mis à leur disposition pour remplir leur mission.

4.3.5 Sensibilisation des utilisateurs

La signature électronique appartient au domaine de la sécurité informatique. De ce fait, les utilisateurs seront amenés à manipuler des objets ou des fichiers sensibles et qu'il faut protéger : clefs USB, cartes à puce, codes PIN ou mots de passe, etc. Chaque utilisateur doit être sensibilisé à l'importance de ces éléments et à l'attention qu'il doit porter à leur préservation, tant pour l'entreprise ou l'organisation que pour lui-même, puisqu'une signature électronique engage la personne qui la réalise.

4.4 Raisonner à long terme

4.4.1 Des projets structurants

Les projets de signature électronique sont en général structurants pour l'entreprise ou l'organisation, car ils entraînent des modifications en profondeur des pratiques professionnelles.

Il convient donc de mener ces projets avec une vision stratégique, et non de manière isolée. La direction de projet devra ainsi prendre en compte :

- les implications juridiques ;
- la dimension humaine (modification des conditions de travail, des relations avec la clientèle, etc.) ;
- l'aspect économique (quels investissements, quel retour attendu ?) ;
- les implications à long terme (généralisation, évolution progressive du Système d'Information et des procédures de l'entreprise ou de l'organisation, conservation des données, etc.)

4.4.2 Organiser et planifier le déploiement

La signature électronique se fait grâce à un certificat et à un outil de signature. Chacun de ces éléments a ses propres règles de gestion.
Le déploiement de l'outil de signature se fait comme pour tout outil informatique, soit via la mise à disposition d'un service (sur l'intranet ou sur internet), soit via le déploiement du logiciel sur chaque poste de travail. Cela nécessite bien entendu un plan de déploiement et une formation des utilisateurs.

Les certificats s'apparentent plus au déploiement de badges professionnels : ils sont personnels, souvent matérialisés par un objet physique (carte à puce, clef USB). Leur déploiement dans l'entreprise ou l'organisation, ou auprès de son écosystème (partenaires, fournisseurs, clients) représente un projet à part entière.
Un parc déployé de certificats est en effet un ensemble vivant qu'il faut gérer de manière dynamique : que fait-on en cas de perte de la carte, d'oubli du code porteur, de vol, de départ d'un employé, d'arrivée d'un nouvel employé, d'appel à des prestataires en régie auxquels il faut donner accès au service, d'expiration d'un certificat nécessitant son renouvellement…
Le cycle de vie des certificats doit donc être entièrement défini, et la structure adaptée à sa gestion doit être mise en place et dotée de la formation, de la sensibilisation et des moyens adéquats.
Une annexe présente le cycle de vie du certificat.
cf Annexe 2 - Le cycle de vie du certificat.

4.4.3 Une ouverture sur l'avenir

Déployer un parc de certificats de signature dans l'entreprise ou l'organisation est le premier pas qui permet l'ouverture de nombreux services utilisant le certificat : contrôle d'accès à des applications web, authentification forte, chiffrement de données, accès distant au Système d'Information, etc.
Un projet de signature électronique doit prendre en compte cet aspect d'investissement structurant.

5/ Conclusion

A travers ses apports fonctionnels, juridiques et organisationnels, la signature électronique est une brique incontournable des projets de dématérialisation.
C'est grâce à elle que se réalisera la modernisation des processus de travail des entreprises comme des administrations.

Techniquement et organisationnellement mûre, cette technologie vous tend les bras au travers de professionnels compétents et reconnus, regroupés au sein de la Fédération Nationale des Tiers de Confiance.

6/ Annexe 1 - Liste des textes légaux et normatifs

Textes français

- Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information ;
- Décret n° 2001-272 du 30 mars 2001 pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ;
- 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 ;
- Arrêté du 28 février 2003 portant nomination au comité directeur de la certification en sécurité des technologies de l'information ;
- Loi du 21 juin 2004 pour la confiance dans l'économie numérique prévoyant le régime de responsabilité applicable aux PSCE ;
- Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des PSCE et à l'accréditation des organismes qui procèdent à leur évaluation ;
- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;
- Ordonnance du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique prise en application de l'article 26 de la loi pour la confiance dans l'économie numérique ;
- Bulletin officiel des impôts, numéro spécial 3 C.A. N°136 du 7 août 2003 relatif à la facture électronique.

Textes communautaires

- Directive européenne du 13 décembre 1999 sur un cadre communautaire pour la signature électronique ;
- Directive européenne du 8 juin 2000 « commerce électronique » ;
- Décision de la Commission du 14 juillet 2003 (2003/511/CE) relative à la publication des numéros de référence de normes généralement admises pour les produits de signatures électroniques conformément à la directive 1999/93/CE du Parlement européen et du Conseil.

Normes

- AFNOR Z74-400 « exigences concernant la politique mise en oeuvre par les autorités de certification délivrant des certificats qualifiés. » et la spécification technique ETSI dont elle est la traduction : ETSI 101 456 - « Policy requirements for Certificate Authorities issuing qualified certificates ».

7/ Annexe 2 - Le cycle de vie du certificat

Le certificat

La signature électronique lie l'identité du signataire avec le document signé.
L'élément qui permet de faire ce lien est le certificat.
Le certificat est une carte d'identité électronique, grâce à laquelle le destinataire du document signé pourra vérifier la signature et savoir par qui elle a été réalisée.

Afin de pouvoir faire foi de l'identité d'une personne, le certificat doit être délivré par un professionnel compétent : l'Autorité de Certification.

Le certificat contient diverses informations, parmi lesquelles on peut citer :

- l'identité du porteur ;
- des dates de début et de fin de validité ;
- l'Autorité de Certification émettrice ;
- la clef publique du porteur
  (élément technique servant à faire les vérifications de signature).

L'Autorité de Certification, l'Autorité d'Enregistrement, l'Opérateur de Certification, la Politique de Certification

De la même façon qu'une préfecture délivre des cartes d'identité – après avoir vérifié cette identité grâce à des pièces justificatives –, une autorité de certification, ou AC, délivre des certificats après une phase d'enregistrement.

L'autorité de certification (AC) est l'entité morale qui signera et délivrera les certificats en son nom, à la façon de la préfecture de police pour une carte d'identité.
Exemples d'autorités de certification :

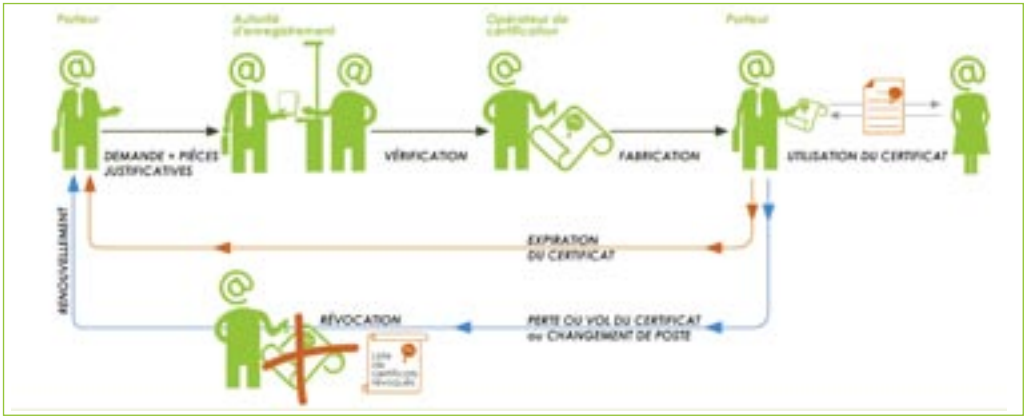
- une grande entreprise pour délivrer des certificats à ses employés ;
- un opérateur de services pour ses clients ;
- une banque pour ses clients particuliers ou professionnels ;
- une administration.

Le porteur ne demande pas directement son certificat à l'AC, de même qu'un individu ne va pas frapper à la porte du préfet pour exiger sa carte d'identité. Il va plutôt s'adresser à un guichetier qui rassemblera les justificatifs, les vérifiera, et les transmettra afin de déclencher l'émission de la carte.
C'est le rôle joué par l'**autorité d'enregistrement (AE)**, qui vérifie tous les éléments requis pour la création du certificat.
Exemples d'autorités d'enregistrement :

- une agence commerciale d'une banque ou d'un opérateur ;
- le correspondant RH d'un employé d'une entreprise ;
- un simple site web, à condition que l'AE dispose de moyens complémentaires pour vérifier l'identité du sujet : adresse e-mail, authentifiant et mots de passe transmis par une voie tierce telle que le courrier postal…

Une fois l'enregistrement effectué, une requête de certification est émise à l'attention de l'AC. Néanmoins, l'AC étant une entité morale, la requête est reçue et traitée par un **opérateur de certification (OC)** qui agit au nom de l'AC en appliquant les règles qu'elle a définies au sein de sa **politique de certification (PC)**. L'OC se charge d'analyser la requête, de la vérifier, de la traiter et de délivrer le cas échéant un certificat. Au-delà de la délivrance de certificats, il gère également leur cycle de vie, comme leur publication, leur renouvellement après expiration ou leur révocation.

Le cycle de vie du certificat



La qualité des certificats

Il existe plusieurs référentiels permettant de juger de la qualité d'un certificat.
Historiquement, on s'est longtemps référé à la notion de classe.
Puis, pour les besoins des téléprocédures en ligne, le Ministère des Finances a mis en place un référencement officiel.
Pour tous les échanges avec l'administration, c'est maintenant la Politique de Référencement Intersectoriel de Sécurité (PRIS) qui fait foi.

7.1.1 La notion de classe de certificat

Un standard définit trois classes de certificats, selon le degré de vérification d'identité.
• **Classe 1 :** l'autorité d'enregistrement vérifie juste l'adresse mail du porteur ;
• **Classe 2 :** le porteur indique son identité à l'autorité d'enregistrement par l'envoi d'une copie de pièces justificatives ;
• **Classe 3 :** le porteur prouve son identité à l'autorité d'enregistrement par la présentation des pièces justificatives originales lors d'un contrôle en face en face.

Plus la classe est élevée, plus le niveau de garantie offert par le certificat est élevé, et plus la procédure de délivrance est contraignante.
Toutefois, cette notion ne prend en compte que les contrôles effectués lors de l'enregistrement du porteur (rôle de l'Autorité d'Enregistrement), et non les conditions dans lesquelles le service d'émission de certificats est exploité (rôle de l'Opérateur de Certification). Elle est donc largement insuffisante pour qualifier la qualité des certificats.

7.1.2 Le référencement PRIS

La Politique de Référencement Intersectorielle de Sécurité (PRIS), définit une qualification des certificats en fonction du niveau de sécurité attendu par les services qui les emploient.
Afin de promouvoir l'usage de la signature électronique en France, le Ministère de l'Economie, des Finances et de l'Emploi a mis en place ce référencement, qui permet aux Autorités de Certification de mettre en avant la qualité des certificats qu'elles émettent.
Les certificats ainsi référencés sont utilisables dans de nombreux services nécessitant la signature électronique, et notamment pour les téléprocédures de la sphère publique, les marchés publics, etc.
Bien qu'initialement conçue pour les usages de la sphère publique, ce référencement est largement reconnu également dans la sphère privée.

Deux normes se sont succédés : PRIS V1 et PRIS V2. On trouve la liste des familles de certificats référencés PRIS sur : www.adele.gouv.fr/synergies/certificats

Politique de Référencement Intersectorielle de Sécurité (PRISv2)
PC type – Signature

Dans le cadre d'une application d'échanges dématérialisés avec l'Administration, le responsable de l'application décide quel niveau de sécurité de la présente PC Type est requis. Ce niveau de sécurité découle des résultats de l'analyse de risque qu'il doit mener sur son application, notamment le niveau de risque identifié et les objectifs de sécurité correspondants.

Niveau (***)
Les certificats de signature objets de la présente PC Type sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité afin de pouvoir signer indûment des données sont très forts (intérêt pour les usurpateurs, effets de la signature, etc.).

Niveau (**)
Les certificats de signature objets de la présente PC Type sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité afin de pouvoir signer indûment des données sont forts (intérêt pour les usurpateurs, effets de la signature, etc.).

Niveau (*)
Les certificats de signature objets de la présente PC Type sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité afin de pouvoir signer indûment des données existent mais sont moyens (intérêt pour les usurpateurs, effets de la signature, etc.).

7.1.3 Les certificats qualifiés

Plusieurs normes françaises et internationales permettent de garantir la qualité de l'Opérateur de Certification et de l'Autorité de Certification.

Les Opérateurs de Certification audités et reconnus conformes à la norme AFNOR Z 74-400 / ETSI TS 101456 sont dits Opérateurs de Certification Qualifiés.
Les Autorités de Certification auditées et reconnues conformes à l'arrêté du 26 juillet 2004 sont aptes à émettre des Certificats Qualifiés.

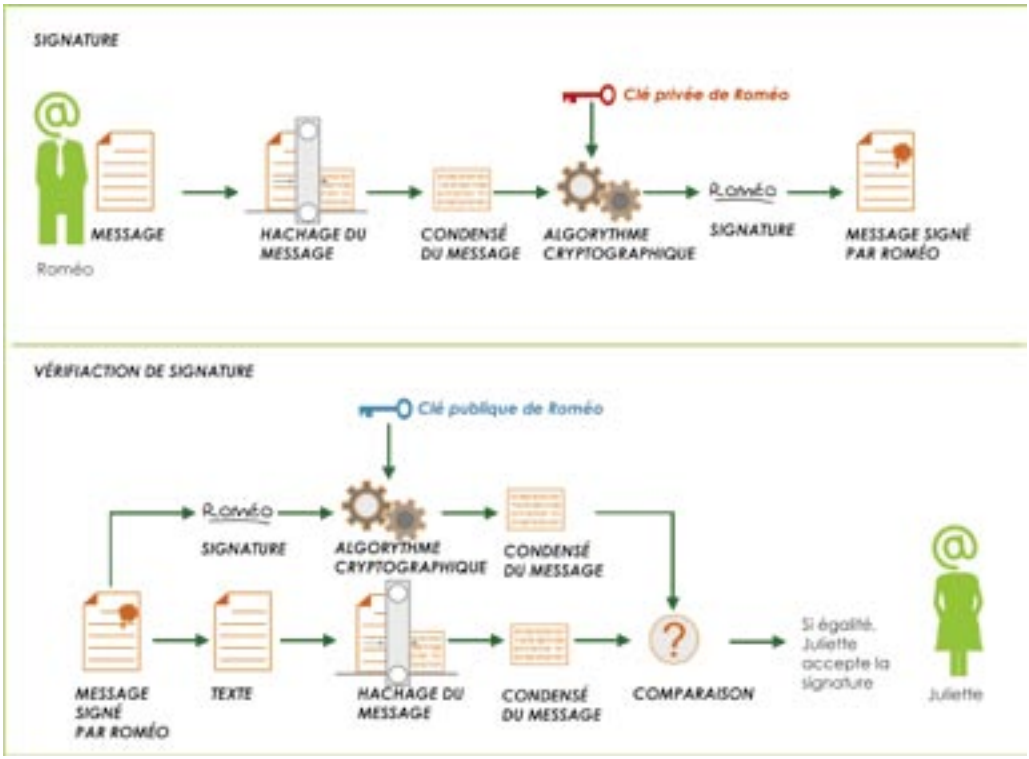
La Qualification garantit un niveau très élevé de sécurité et de qualité de service. La liste des acteurs qualifiés est disponible sur :
http://www.lsti.fr

Les certificats qualifiés, nécessaires à la réalisation de signatures électroniques sécurisées emportant présomption de fiabilité (cf § 2.3) répondent aux exigences de l'arrêté du 26 juillet 2004. Lorsqu'une telle signature est réalisée, en cas de contentieux, l'article 1316-4 du Code civil prévoit que la charge de la preuve relative à la validité de la signature incombe au plaignant.

8/ Annexe 3 - Eléments techniques

8.1 La cryptographie à clef publique

Il existe de nombreux ouvrages qui traitent de la cryptographie à clef publique. Le lecteur intéressé s'y reportera.
Les schémas ci-dessous illustrent le fonctionnement de la signature électronique et de sa vérification.



Compléments à la signature électronique

8.1.1 Contrôle de validité du certificat

Lorsque l'on vérifie la signature d'un document, on doit vérifier la validité du certificat du signataire. A cette fin, l'Autorité de Certification met à disposition de tous la Liste des Certificats Révoqués (LCR) (cf Le cycle de vie du certificat).
L'outil qui réalise la vérification de la signature téléchargera automatiquement cette LCR et vérifiera que le certificat du signataire n'y figure pas.
Le service de contrôle de révocation peut également être rendu au moyen d'un service en ligne, appelé OCSP (Online Certificate Status Protocol).
Un jeton de vérification OCSP ou une CRL peut être inclus dans la signature au moment où elle est réalisée. De cette manière, il ne sera pas nécessaire d'interroger le service de contrôle des certificats au moment de la vérification.

8.1.2 Horodatage de la signature

Lorsque l'on vérifie la signature d'un document, on doit vérifier la validité du certificat du signataire. Le certificat du signataire peut être expiré au moment où l'on réalise la vérification de signature (par exemple un an après). Mais ce qui compte est que le certificat du signataire n'ait pas été expiré au moment où la signature a été réalisée.
Afin de le garantir, la signature peut comporter un horodatage : il s'agit d'un élément technique garantissant le jour et l'heure auxquels la signature a été réalisée.

Cet horodatage peut prendre différentes formes :

- une date incluse manuellement dans le document signé ;
- une date incluse automatiquement dans la signature elle-même ;
- un jeton d'horodatage certifié délivré par une Autorité d'Horodatage ;
- une preuve de validité externe fournie par une Autorité de Gestion de Preuve, qui fait foi de la vérification de la signature lors de sa réalisation ou de sa réception.

Guide de l'horodatage

8.1.3 Archivage du document signé

Un document signé électroniquement a une valeur juridique : il est souvent important de le conserver de manière pérenne pour les besoins ultérieurs de l'entreprise ou de l'organisation. C'est le rôle de l'archivage électronique.

8.1.4 Autres usages du certificat

Lorsque l'on déploie des certificats, ils peuvent avoir d'autres usages que la signature électronique. La multiplicité des usages du certificat, support indispensable de la signature électronique, permet un retour sur investissement rapide lors de son déploiement dans l'entreprise ou l'organisation.

Authentification / contrôle d'accès : le certificat peut remplacer le classique couple identifiant / mot de passe pour contrôler l'accès des utilisateurs à un site, à un service, ou même au poste de travail. L'usage du certificat pour le contrôle d'accès augmente considérablement le niveau de sécurité.

Chiffrement (cryptage) de données : le certificat permet de réaliser des échanges de données confidentielles, mais aussi la sécurisation du disque dur de l'ordinateur par un cryptage systématique des données.

9/ Annexe 4 – Glossaire

Archivage (électronique)
Ensemble des actions, outils et méthodes mis en oeuvre pour réunir, identifier, sélectionner, classer et conserver des contenus électroniques, sur un support sécurisé, dans le but de les exploiter et de les rendre accessibles dans le temps, que ce soit à titre de preuve (en cas d'obligations légales notamment ou de litiges) ou à titre informatif.

Autorité de Certification (AC)
Egalement appelée Autorité Certifiante (ou Certificate Authority en anglais). Entité responsable de l'émission, de la délivrance et de la gestion des certificats électroniques. L'autorité de Certification est responsable des certificats émis en son nom.

Autorité d'Enregistrement (AE)
Entité responsable de l'identification et de l'authentification des demandeurs de certificats électroniques au profit d'une Autorité de Certification.

Autorité d'Horodatage (AH)
Entité responsable de la délivrance des jetons d'horodatage, aussi appelés contremarques de temps, sur des données qui lui sont présentées. Elle garantit ainsi la date qui est apposée sur tous les documents et signatures issus de l'Autorité de Certification et de l'Autorité d'Enregistrement.

Certificat Électronique
Équivalent d'un passeport dans le monde physique, le certificat électronique joue le rôle de pièce d'identité électronique. L'identité de son propriétaire est garantie par l'Autorité de Certification qui lui a délivré ce certificat.
Le certificat est un document sous forme électronique attestant du lien entre les données de vérification de signature (clés cryptographiques publiques) et l'identité du signataire.

Certificat (Électronique) qualifié
Certificat électronique répondant aux exigences de l'article 6 du Décret du 30 mars 2001.

Chiffrement
Opération par laquelle une donnée intelligible est rendue inintelligible afin d'en protéger la confidentialité.

Clé publique / clé privée / bi-clé
La clé publique est un élément mathématique qui peut être rendu public et dont l'usage est de vérifier les signatures électroniques réalisées par la clé privée associée. Une clé publique peut aussi être utilisée pour chiffrer des données qui sont déchiffrées par la clé privée associée. La clé publique et la clé privée forment ensemble la bi-clé.

CRL ou LCR (Liste des Certificats Révoqués)
Liste des numéros de série des certificats qui ont fait l'objet d'une révocation. Cette liste est tenue à jour et publiée régulièrement par l'Autorité de Certification et rendue disponible à tous les utilisateurs de certificats.

Cryptographie
La cryptographie regroupe l'ensemble des techniques qui permettent la gestion de secrets. Il existe deux types de cryptographie : la cryptographie symétrique dite à « clé secrète » et la cryptographie asymétrique dite à « clé publique ».
Le principe de la cryptographie à clé secrète consiste à utiliser un seul secret ou une même clé pour chiffrer et déchiffrer les informations. Pour la cryptographie à clé publique, il y a 2 clés différentes : une clé dite « publique » et une clé dite « privée » qui n'est connue que de son utilisateur.

Dématérialisation
Mécanisme consistant à transformer l'échange traditionnel des documents, sous forme papier, en un échange électronique, via Internet, tout en conservant la même validité qu'un échange sous forme papier.

Dispositif Sécurisé de Création de Signature (DSCS)
Matériel ou logiciel destiné à mettre en application les données de création de signature électronique (clé cryptographique privée, propre au signataire) et certifié par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) pour cette utilisation.

Force probante
Efficacité d'un moyen de preuve.

Horodatage
Service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet évènement s'est réalisé.

Infrastructure à Clés Publiques (ICP)
Également appelée IGC (Infrastructure de Gestion de Clés) ou PKI (Public Key Infrastructure) en anglais. Ensemble des moyens techniques, humains, documentaires et contractuels mis à la disposition d'utilisateurs pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé pour les échanges électroniques.

Intranet
Réseau utilisé à l'intérieur d'une entreprise ou de toute autre entité organisationnelle utilisant les techniques de communication d'internet (IP, serveur HTTP).

LCEN
Loi pour la Confiance dans l'Économie Numérique.
Loi française sur le droit de l'Internet, transposant la directive européenne 2000/31/CE.

OCSP
Online Certificate Status Protocol
Protocole internet de vérification d'un certificat électronique décrit dans la RFC 2560. Les communications OCSP étant de la forme «requête/réponse», les serveurs OCSP sont appelés *répondeurs OCSP.*

Opérateur de Certification (OC)
Assure la fourniture et la gestion des certificats électroniques. Son rôle consiste à mettre en oeuvre une plate-forme technique sécurisée dans le respect des exigences énoncées dans la Politique de Certification.

Politique de Certification (PC)
Également appelée Certificate Practice Statement (CPS) en anglais. Définit les procédures selon lesquelles les certificats sont générés et gérés. Elle permet de définir le lien de confiance entre l'utilisateur final et le porteur du certificat.

Présomption de fiabilité
Les exigences liées à la mise en place d'une signature électronique permettant de bénéficier de la présomption de fiabilité du procédé de signature électronique sont les suivantes :
• la signature électronique met en oeuvre une Signature Électronique Sécurisée (SES) ;
• cette SES est établie grâce à un Dispositif Sécurisé de Création de Signature Électronique (DSCS) ;
• la vérification de la Signature Électronique repose sur l'utilisation d'un certificat électronique qualifié.

PRIS
Politique de Référencement Intersectorielle de Sécurité.
Il s'agit du référentiel documentaire qui définit des exigences pour différentes fonctions de sécurité. Il concerne les produits de sécurité et les prestataires de services de confiance utilisés dans le cadre des échanges dématérialisés entre usagers et autorités administratives ainsi qu'entre autorités administratives. Les spécifications techniques retenues dans la PRIS sont regroupées sous la forme de niveaux de sécurité d'exigences croissantes de * à ***.

Services de Certification (électronique)
Services délivrés par un prestataire de services de certification (électronique).
Exemples : délivrance de certificats électroniques, service d'annuaire de certification, fourniture de CRL, fourniture de jeton d'horodatage, archivage...

Signature Électronique
Donnée sous forme électronique, qui :
- est jointe ou liée logiquement à d'autres données électroniques (l'acte signé) ;
- identifie le signataire ;
- garantit le lien du signataire avec l'acte signé.
La signature électronique est réalisée à l'aide de certificats en utilisant les méthodes de cryptographie asymétrique.

Signature Électronique Sécurisée (SES)
Il s'agit d'une signature électronique qui satisfait aux trois 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.

Tiers de Confiance
Organisme habilité à mettre en œuvre des signatures électroniques reposant sur des architectures d'Infrastructure à Clés Publiques

La Fédération Nationale des Tiers de Confiance

La Fédération Nationale des Tiers de Confiance (FNTC) est aujourd'hui reconnue comme un acteur essentiel de la sécurisation des échanges électroniques et de la conservation des informations, maillons essentiels à la maîtrise de l'ensemble de la vie du document électronique.

Elle compte aujourd'hui près de 70 membres regroupant des professionnels répartis en 4 collèges en fonction de leur activité professionnelle, tous concernés directement ou indirectement par la sécurisation des échanges électroniques et la conservation des information. Elle regroupe les opérateurs et prestataires de services de confiance (acteurs de l'archivage électronique, de la certification, de l'horodatage et des échanges dématérialisés ; les éditeurs et intégrateurs de solutions de confiance ; les experts et les représentants des utilisateurs ainsi que les institutionnels et les professions réglementées.

La FNTC pour but d'établir la confiance, de promouvoir la sécurité et la qualité des services dans le monde de l'économie numérique, de garantir les utilisateurs et de défendre les droits et intérêts liés à la profession des Tiers de Confiance.

Ils sont membres de la FNTC

Accelya ; achatpublic.com ; Adap ; Agysoft ; Apeca ; Aproged ; Archiv'Alpha ; Aspheria ; Atos WordLine ; Bruno Couderc Conseil ; Caprioli & Associés ; CDC CEE ; Cecurity.com ; Celtipharm ; CertEurope ; ChamberSign ; Chambre Nationale des Huissiers de Justice ; Click & Trust ; Compagnie Nationale des Commissaires aux Comptes ; CodaSystem ; Conseil National des Greffiers de tribunaux de Commerce ; Conseil Supérieur de l'Ordre des Experts-Comptables ; Cryptolog ; DARVA ; DHL Global Mail ; Digimedia ; Docubase Systems ; Ecosix ; Edelweb ; Ernst & Young ; Esker ; Esopica ; Experian ; Fedisa ; Forum Atena ; France Telecom R & D ; G.L.I. Services ; Greffe du TC de Bobigny ; Hervé Schauer Consultants ; Imaterialis ; Info Service Europe ; Inforsud Editique ; interb@t ; Ip-label ; jedeclare.com ; Kahn & Associés ; Keynectis ; Lex Persona ; Locarchives ; Maileva ; Mailwatcher ; Micrographie Services ; Microlist ; MIPIH ; Neuflize OBC ; Omnikles ; Orsid ; Pitney Bowes Asterion ; Quintess ; SafeNet ; Scala ; S.I.S. ; Société Générale d'Archives ; Sogelink/DICT.fr ; SR Développement ; Stocomest ; Syrtals ; TrustMission ; Vaughan Avocats ; Voxaly

Conception graphique et illustrations : www.idsg.fr

www.fntc.org