



Fédération des
Tiers de Confiance

GUIDE DE LA SIGNATURE ÉLECTRONIQUE



COLLECTION
LES GUIDES DE LA CONFIANCE
DE LA FNTC

*Par le groupe de travail
« e-signature et identité numérique »
de la Fédération des Tiers de Confiance*

DANS LA COLLECTION LES GUIDES DE LA CONFIANCE DE LA FNTC :

- 
- Guide de la signature électronique (octobre 2013)
 - Vade-mecum juridique de la dématérialisation des documents 6^{ème} édition (octobre 2013)
 - Guide de la traçabilité (octobre 2013)
 - Guide Normes et Labels de la dématérialisation (octobre 2013)
 - Guide l'interopérabilité des coffres-forts électroniques (mars 2012)
 - Le bulletin de paie électronique (mars 2012)
 - Du livret ouvrier au bulletin de paie électronique (mars 2012)
 - Guide du Document Hybride et de la Certification 2D (nov. 2011)
 - Fascicule e-paie « le rôle du bulletin de paie dans la reconstitution de carrière » (mars 2011)
 - Guide du vote électronique, nouvelle édition (mars 2011)
 - Guide de l'archivage électronique et du coffre-fort électronique (nov. 2010)
 - Au-delà de la migration Etebac (sept. 2010)
 - Guide de la Facture électronique (janv. 2010)
 - Du mandat au mandat électronique (déc. 2009)

PROCHAINE
PARUTION

- Guide de la créance numérique



© Copyright octobre 2013

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 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 autorisées 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 destinées 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.

SOMMAIRE

6	0	Préface
7	1	Introduction à la signature électronique
	1.1	La signature électronique : une réalité
	1.2	Une technologie, de nombreux bénéfices
	1.2.1	La signature électronique au service de la dématérialisation
	1.2.2	Les économies directes : la partie émergée de l'iceberg
	1.2.3	Les gains de productivité
	1.2.4	L'augmentation des ventes
	1.2.5	L'enrichissement des relations avec les partenaires
	1.2.6	Les garanties juridiques
	1.2.7	L'accroissement de la sécurité
	1.2.8	Le dynamisme de l'image de marque
	1.3	L'identité numérique : la base de la signature électronique
	1.3.1	Introduction aux identités numériques
	1.3.2	Une définition des identités numériques
	1.3.3	Le certificat, support de l'identité numérique
	1.3.4	La chaîne de la confiance
	1.4	Les définitions de la signature électronique
	1.4.1	Définition pratique
	1.4.2	Définition juridique
	1.4.3	Définition technique
	1.4.4	La signature électronique : plusieurs usages
	1.4.5	Quelques contre-exemples
	1.5	Que peut-on signer électroniquement ?
27	2	Les bonnes pratiques
	2.1	Réaliser une signature électronique
	2.1.1	Les différents modes de réalisation de la signature électronique
	2.1.2	Les formats de signature électronique
	2.1.3	Les éléments techniques complémentaires
	2.1.4	Faciliter l'usage de la signature électronique
	2.2	Vérifier une signature électronique
	2.3	Conserver des documents signés électroniquement
	2.4	Mener un projet de signature électronique
	2.4.1	La technique au service du projet
	2.4.2	Prendre en compte le facteur humain
	2.4.3	Raisonner à long terme
	2.5	L'interopérabilité
	2.5.1	L'interopérabilité des formats de signature électronique
	2.5.2	L'interopérabilité des certificats
	2.6	Ouverture à l'international
	2.7	La convention de preuve
	2.8	Respecter les normes et réglementations
43	3	Les textes juridiques applicables
	3.1	Le socle juridique de la signature électronique
	3.1.1	La signature électronique en droit privé
	3.1.2	La signature électronique en droit public
	3.2	Les évolutions juridiques et jurisprudentielles de la signature électronique
	3.2.1	Applications pratiques de la signature électronique
	3.2.2	Le projet de règlement du 4 juin 2012 comme solution au problème d'interopérabilité en Europe



4

Cas pratiques

51

- Signature électronique et délégation des pouvoirs bancaires
- BNP Paribas Guadeloupe dématérialise la signature client
- La signature électronique des Factures
- La signature électronique des attestations
- Signer et transmettre en ligne les contrats et documents officiels des transactions en capital : le service Eclosing
- Les cartes de professionnels de la Santé (CPS)
- Vosgelis, Office de Logement Social, dématérialise l'ensemble du processus de la commande publique
- Les cartes de Chronotachygraphe Numérique
- AXA déploie la signature électronique d'assurance-vie sur tablette tactile
- Huissiers de Justice : l'acte authentique sur support électronique et la signification électronique
- Dématérialisation des mandats bancaires par l'expert-comptable en tant que tiers de confiance sur jedeclare.com
- Signexpert – l'identité numérique de l'Expert-Comptable
- Infogreffe : des démarches administratives et légales simplifiées grâce à la signature électronique
- Les déclarations préalables aux travaux : la sécurité informatique au service de la sécurité des chantiers

5

Glossaire

66

6

Remerciement aux participants

70

0 PRÉFACE

Chaque jour dans le monde, des milliards de personnes échangent des milliards de documents numériques, qu'ils soient professionnels ou privés ; mais combien d'entre eux engagent vraiment leurs auteurs ?

En fait : nettement moins, et c'est bien normal car le besoin de s'engager se justifie lorsque les documents ont une valeur, qu'elle soit financière, juridique ou sentimentale. En effet, signer c'est s'engager, c'est affirmer son identité dans un contexte choisi.

Bien au-delà de l'acte technique désormais largement répandu, la signature électronique est un acte fort qui scelle un accord, affirme une position ou encore garantit une conformité à la réglementation ; dans tous les cas, c'est une démarche qui revêt une importance pour la personne physique ou morale qui signe.

La signature électronique est de ce fait étroitement liée à l'identité numérique du (des) signataire(s). C'est ce lien fort entre le document et la personne physique ou morale qui donne la valeur à l'acte et permet d'établir une relation de confiance entre les parties qui échangent les documents signés.

Avec Internet et notre monde connecté, les usages de la signature électronique se répandent dans tous les secteurs d'activité, la signature devient un enjeu économique, elle permet de réduire les coûts de process internes ou externes, de gagner du temps pour conclure un accord, et contribue à améliorer la relation client/usager.

La FNTC est fière de vous offrir cette nouvelle édition du guide de la signature électronique. Elle fait le point sur l'évolution de la réglementation, donne quelques conseils pratiques de mise en œuvre et dresse un panorama des usages en s'appuyant sur des exemples concrets d'utilisation dans divers secteurs d'activité.

Comme pour chaque guide de la FNTC, ce document est le fruit d'un travail collectif réunissant des experts techniques, juridiques, des acteurs économiques et les professions réglementées, membres de la FNTC.

C'est la marque de fabrique de notre fédération, et plus encore... Notre signature !

Bonne lecture

Pascal Colin
Président exécutif
FNTC

INTRODUCTION À LA SIGNATURE ÉLECTRONIQUE

1.1 La signature électronique : une réalité

1.2 Une technologie, de nombreux bénéfices

- 1.2.1 La signature électronique au service de la dématérialisation
- 1.2.2 Les économies directes : la partie émergée de l'iceberg
- 1.2.3 Les gains de productivité
- 1.2.4 L'augmentation des ventes
- 1.2.5 L'enrichissement des relations avec les partenaires
- 1.2.6 Les garanties juridiques
- 1.2.7 L'accroissement de la sécurité
- 1.2.8 Le dynamisme de l'image de marque

1.3 L'identité numérique : la base de la signature électronique

- 1.3.1 Introduction aux identités numériques
- 1.3.2 Une définition des identités numériques
- 1.3.3 Le certificat, support de l'identité numérique
- 1.3.4 La chaîne de la confiance

1.4 Les définitions de la signature électronique

- 1.4.1 Définition pratique
- 1.4.2 Définition juridique
- 1.4.3 Définition technique
- 1.4.4 La signature électronique : plusieurs usages
- 1.4.5 Quelques contre-exemples

1.5 Que peut-on signer électroniquement ?

1 INTRODUCTION À LA SIGNATURE ÉLECTRONIQUE

1.1 La signature électronique : une réalité

Inventée techniquement en 1976 par Rivest, Shamir et Adleman, introduite dans le droit européen en 1999 puis dans le droit français avec la loi du 13 mars 2000, la signature électronique est aujourd’hui entrée dans le quotidien des particuliers comme des professionnels.

Si la signature électronique n'est pas « un but en soi », elle est un élément constitutif indispensable des transactions réalisées par Internet et de la validité juridique des documents nativement électroniques.

C'est en effet elle qui permet de garantir l'identité d'un signataire, l'intégrité et la provenance d'un document et, plus largement, l'établissement de la confiance dans les échanges numériques.

Ce guide a pour but d'illustrer la diversité des usages réels qui sont faits de cette technologie ainsi que les bénéfices qui en sont tirés tant par les fournisseurs de services qui la mettent en œuvre (contractualisation en ligne, dématérialisation de factures, attestations dématérialisées, processus RH, feuilles de soins télétransmises...) que par les utilisateurs de ces services.

Nous nous attacherons à vous convaincre de son universalité et de la simplicité de sa mise en œuvre : au travers des différents modes de réalisation possibles, vous découvrirez que la maturité actuelle du marché des fournisseurs de solutions permet à chaque projet de trouver une réponse adaptée à ses enjeux – parmi lesquels viennent en tête l'ergonomie et l'utilisabilité par tous.

Ce guide se veut un manuel de mise en œuvre pratique de la signature électronique dans tous les contextes que vous pourrez rencontrer : aspects fonctionnels, aspects juridiques, aspects techniques, aspects organisationnels y sont détaillés au travers de définitions et de bonnes pratiques de manière à vous offrir un support concret dans la réalisation de vos projets.

De nombreux exemples vous sont présentés, dans la dernière partie du guide, sous forme de fiches : vous y trouverez certainement celui qui correspond à vos préoccupations, à vos besoins, à vos ambitions.

Gains directs et indirects, accélération de la relation commerciale et ouverture de nouveaux marchés, amélioration de la relation avec les clients et les partenaires, souci du développement durable : comment proposer un guide de la signature électronique sans commencer par les nombreux apports de cette technologie dans le quotidien de l’entreprise ? Alors, bonne lecture, et à bientôt pour échanger au cours des nombreux événements organisés par la FNTC !



1.2 Une technologie, de nombreux bénéfices

Une innovation technologique n'émerge pas sans nécessité, et ne se perpétue pas sans bénéfices concrets pour ceux qui la mettent en œuvre. S'agissant de la signature électronique, cet adage général est d'une application particulièrement facile, tant ses apports sont nombreux.

1.2.1 La signature électronique au service de la dématérialisation

La dématérialisation est en train de révolutionner nos vies : de plus en plus de documents ne sont jamais imprimés sur papier, mais sont générés nativement sous forme électronique, échangés via les réseaux de télécommunication, et conservés sous cette forme pendant toute leur durée d'utilité.

Dans ce contexte, la signature électronique remplit deux rôles majeurs, qui tendent à établir les conditions de la confiance dans les échanges numériques et donc à rendre possible la dématérialisation :

- la signature électronique d'un document (un contrat par exemple) confère à celui-ci une **valeur juridique équivalente à celle d'un document papier signé** de manière manuscrite, en marquant l'engagement de la personne qui a apposé la signature ;
- des fonctions connexes à la signature électronique (cachet, horodatage...) servent à offrir des conditions de **sécurité technique** en garantissant sa provenance, son intégrité, ou encore la date de sa réalisation.

Ainsi, la signature électronique est avant tout une fonctionnalité majeure des services de dématérialisation, et les gains qui sont à en attendre sont tous ceux issus de cette disparition des flux papier au profit de flux entièrement électroniques.

Détaillons maintenant ces bénéfices induits par la signature électronique.

1.2.2 Les économies directes : la partie émergée de l'iceberg

La signature électronique permet à la dématérialisation d'offrir des économies substantielles d'impression, d'affranchissement et de stockage de document : mettre à disposition un document sans avoir à l'imprimer et à le poster, recueillir la signature d'un client sans lui fournir un contrat en papier, envoyer ou recevoir des factures directement sous forme électronique sont autant d'illustrations de ces économies directes.

Prenons rapidement trois exemples.

Au niveau régional, le projet e-Bourgogne fait économiser à la Région l'impression et l'acheminement de 10 millions de feuilles de papier par an depuis plus d'une dizaine d'années.¹

Au niveau national, grâce à la dématérialisation mise en œuvre par l'Assurance maladie, plus d'un milliard de feuilles de soin annuelles ne sont plus échangées en papier, tous les échanges étant entièrement électroniques entre le professionnel de santé et l'Assurance maladie, et jusqu'aux mutuelles.²

À l'international, l'exemple de CECA (Caisse d'Épargne espagnoles) est à ce titre éloquent : en mettant en œuvre la signature électronique couplée à l'usage de tablettes de signature, les Caisse d'Epargne espagnoles réalisent une économie annuelle de papier de 6 750 tonnes, soit l'équivalent du fret de 28 Airbus A380, l'équivalent de 10 km² de forêt, ou l'équivalent des émissions de CO₂ de 20 000 voitures ou de 38 700 foyers !³

Toutefois, il ne s'agit là que de la plus petite source de gains dans la mise en œuvre de la signature électronique, comme vont l'illustrer les paragraphes suivants.

1.2.3 Les gains de productivité

Les véritables gains issus de l'usage de la signature électronique viennent de la refonte en profondeur des processus métier liés à la génération, au traitement et à la conservation des documents.

Il s'agit d'abord d'**optimisation des processus** : illustrons-le par l'exemple d'un grand groupe d'assistance, qui a dématérialisé les contrats passés avec ses prestataires. Le processus antérieur nécessitait la rédaction du contrat, sa validation par l'acheteur, son envoi en double exemplaire au prestataire pour paraphe et signature, l'attente du retour et les relances associées, une vérification humaine pour s'assurer que le prestataire n'avait pas modifié le document, puis son paraphe et sa signature en double exemplaire par la Direction des achats, l'envoi d'un exemplaire au prestataire, et le scan du contrat pour inclusion dans le Système d'Information.

► La modification du processus a permis la génération automatique du contrat, la signature électronique en ligne par le prestataire et par la Direction des Achats sans nécessité de contrôle supplémentaire puisque le processus interdisait toute modification, et son archivage à vocation probatoire immédiat dans un coffre-fort électronique intégré au SI. Le coût des traitements liés à un contrat a ainsi été divisé par 4 !

Ce même exemple nous permet d'illustrer de nombreux autres apports de l'usage de la signature électronique :

- **l'accélération du processus de contractualisation** grâce à un **gain de temps dans les traitements**, une contractualisation moyenne étant ramenée de plusieurs semaines à quelques jours ;

1 Source : www.e-bourgogne.fr

2 Voir fiche d'exemple CPS

3 Source : contribution BTC – ESBG Bruxelles – Mai 2011



- une **disponibilité permanente des documents originaux**, puisqu'il n'est plus nécessaire de rechercher le contrat papier dans les archives ;
- un couplage avec des contrôles complémentaires (attestations du prestataire) permettant une **sécurisation juridique du contrat** ;
- une **tracabilité accrue des actions** des différentes parties prenantes au processus de contractualisation ;
- une **mesure de la qualité du processus** de contractualisation au travers de tableaux de bord...

Ainsi, l'usage de la signature électronique, outre les gains en termes de ressources humaines nécessaires pour des tâches à faible valeur ajoutée, permet la mise en œuvre d'une démarche qualité sur le processus métier global.

1.2.4 L'augmentation des ventes

Dans un contexte BtoC marchand, l'amélioration du taux de conversion est l'objectif n°1 d'une solution de contractualisation en ligne. Le taux de conversion d'un site Internet, appelé aussi parfois taux de transformation (conversion rate en anglais) correspond au pourcentage de visiteurs ayant été convertis selon un « objectif de conversion » : achat d'un produit, ouverture d'un compte, inscription à une newsletter, etc.

Dans le secteur de la banque ou de l'assurance en ligne, par exemple, ce processus en plusieurs étapes permet à l'internaute de définir en quelques clics les principales modalités de son contrat, puis de le valider. Bien souvent, la dernière étape consiste encore en une invitation à imprimer le contrat, à le signer et à l'envoyer par La Poste à une adresse dédiée. Or, cette étape est incontestablement génératrice de pertes de conversions. Dans quelques cas, le contrat ne sera pas signé, ni même envoyé, et restera sur une pile avant de tomber aux oubliettes...

La mise en œuvre d'un processus aboutissant à la signature électronique d'un contrat ou d'un bulletin d'adhésion permettra d'augmenter significativement le taux de conversion.

Mais au-delà de cette accélération du processus de vente, synonyme d'amélioration de la performance commerciale, la signature électronique en ligne permet également d'ouvrir le champ de la contractualisation à des marchés plus difficilement accessibles par les méthodes commerciales traditionnelles : la création d'un site web de commerce en ligne est souvent la meilleure méthode pour atteindre une cible de clientèle à l'étranger, et la signature électronique permet de s'affranchir des difficultés liées à la distance géographique ou culturelle : ce que permettra à partir de 2014 le projet de règlement européen en cours de finalisation au jour de publication de ce guide.

1.2.5 L'enrichissement des relations avec les partenaires

Les échanges dématérialisés ne concernent évidemment pas que le secteur commercial, mais aussi les échanges avec les partenaires de l'entreprise : on pourra ainsi signer électroniquement des engagements de confidentialité, des partenariats, des documents de travail échangés dans le cadre de la recherche et développement... Le déploiement de services d'échange incluant la signature électronique permet

d'établir un cadre de confiance réciproque et de fidéliser les relations avec l'ensemble de l'écosystème de l'entreprise.

1.2.6 Les garanties juridiques

Grâce à l'existence de règles européennes communes (Directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques, projet de règlement européen...) et à un cadre juridique français très fourni (loi du 13 mars 2000, décret du 30 mars 2001, RGS, Code général des Impôts, ...), et à l'existence sur le marché de nombreuses solutions techniques répondant aux obligations qui en découlent, la mise en œuvre de la signature électronique permet de s'assurer d'une parfaite sécurité juridique des documents échangés.

La conformité réglementaire est l'un des apports majeurs de l'usage de la signature électronique dans de nombreux domaines. On se reportera au chapitre juridique de ce guide pour de plus amples détails sur les textes applicables.

1.2.7 L'accroissement de la sécurité

Nous venons de voir l'apport de la signature électronique en termes de sécurité juridique. Mais la sécurité ne s'arrête pas là !

Un projet de signature électronique est l'occasion de revoir en profondeur l'estimation des risques et leur prévention. Si le secteur bancaire a ces dernières années mis à profit le durcissement des obligations qui lui incombent pour améliorer ses pratiques et renforcer sa sécurité, il en va de même de nombreux autres acteurs.

Ainsi, la signature électronique, contrairement à une signature manuscrite, est aisément vérifiable : plus de signature scannée et ré-imprimée, plus de fausse signature, plus de gri-gri illisible au bas d'une feuille ! **La signature électronique identifie de manière fiable le signataire.**

Par ailleurs, l'apposition d'une signature électronique rend toute modification ultérieure d'un document immédiatement détectable. **L'intégrité des actes juridiques étant ainsi garantie**, il n'est plus possible de remplacer subrepticement une feuille par une autre ou de gratter un chiffre pour le modifier.

Enfin, **la traçabilité** qui accompagne les échanges électroniques permet de réunir un faisceau d'indices venant encore conforter la reconnaissance probatoire d'un document signé électroniquement.

Vérifiabilité, intégrité, opposabilité, traçabilité des documents sont ainsi des apports fondamentaux de la signature électronique à la sécurité globale de l'entreprise.

4 Voir le chapitre juridique dans le présent guide



1.2.8 Le dynamisme de l'image de marque

Modernisme et éco-responsabilité sont indissociablement liés à l'usage de la dématérialisation. Nous avons vu que la signature électronique permet des économies de papier considérables : mis en avant, cet argument de développement durable devient le moteur d'une image renouvelée pour des entreprises traditionnellement très consommatrices de ressources fragiles.

Mais le gain d'image sera aussi lié à l'accélération des processus : l'usage des médias modernes (Internet, mais aussi smartphones ou tablettes) sera un levier important de compétitivité en permettant à un client de signer un contrat sans avoir à se déplacer ou à renvoyer un courrier.

La signature électronique étant encore en cours d'adoption, une société mettant en œuvre un tel projet fera aujourd'hui figure de précurseur. Vis-à-vis de son écosystème (clients, partenaires, fournisseurs, etc.), elle bénéficiera d'une image renforcée en termes de capacité d'innovation et d'utilisation des « dernières technologies ». Mieux, l'amélioration de l'expérience utilisateur apportée par la contractualisation électronique renforcera chez votre interlocuteur le sentiment d'avoir affaire à quelqu'un dont le souci est de lui simplifier la vie. Votre image de professionnalisme ne s'en trouvera que renforcée.

1.3 L'identité numérique : la base de la signature électronique

1.3.1 Introduction aux identités numériques

Dans la vie de tous les jours, nous disposons tous d'une identité d'Etat-civil, dont nous pouvons apporter la preuve à l'aide de nos papiers : carte nationale d'identité ou passeport, qui viennent parfois se compléter de justificatifs de domicile ou d'autres documents.

Par ailleurs, lorsque nous agissons dans le cadre professionnel, notre identité est liée à notre appartenance à l'entreprise qui nous emploie, au travers de titres aussi divers qu'une carte professionnelle, un badge d'accès, un extrait K bis, une délégation de pouvoir de signature, voire une simple carte de visite.

L'identité numérique que nous allons employer pour réaliser une signature électronique sera donc fonction du contexte dans lequel nous la réalisons.

Ainsi, pour la signature électronique, on sera amené à distinguer trois formes d'identité numérique.

L'identité d'une personne physique, signant pour son compte propre : elle se résume souvent à son prénom et à son nom, fréquemment associés à une adresse mail.

Cette identité numérique sera employée, par exemple, pour souscrire un contrat bancaire ou pour signer son courrier électronique.

L'identité numérique d'une personne physique agissant dans son cadre professionnel : dans ce cas, elle comporte en plus l'identification de l'entreprise à laquelle appartient le signataire, au travers par exemple de sa dénomination sociale et de son numéro SIRET.

Cette identité numérique sera employée, par exemple, pour signer une offre à un marché public ou un ordre de mission.

L'identité d'une personne morale, employée lorsque le signataire agit non en son nom propre, mais pour engager sa société : dans ce cas, ce sont les coordonnées de l'entreprise qui constituent les éléments principaux de l'identité numérique, le nom du représentant étant un élément complémentaire.

Cette identité numérique sera employée, par exemple, pour certifier la provenance d'un document ou pour signer une facture dématérialisée⁵.

Il existe d'autres formes d'identités numériques, par exemple un compte sur un réseau social, ou tout simplement une adresse mail. Toutefois, en l'absence d'un contrôle effectif de l'identité réelle de la personne qui se trouve derrière cette identité numérique, il est difficile de la considérer comme « un procédé fiable d'identification », et elle ne peut donc pas, dans le cas général, servir de base à la signature électronique.

1.3.2 Une définition des identités numériques

1.3.2.1 Les identités numériques, au pluriel

Avancer une définition de l'identité numérique serait hasardeux, comme l'indique la citation ci-dessous extraite de *Identité numérique, quelle stratégie pour l'État ?* (Secrétariat Général pour la Modernisation de l'Action Publique) :

« De l'identité formelle et établie par l'État, le monde numérique nous transpose donc vers un faisceau d'identités beaucoup plus multiforme, liées aux profils que l'individu crée pour se représenter sur ses réseaux sociaux, liées à ses activités, à sa banque, à son opérateur téléphonique, à son fournisseur d'accès, ... Dans cet ensemble d'identités, l'identité traditionnelle, régaliennne, a perdu sa situation de quasi-monopole, mais continue à jouer néanmoins un rôle essentiel : c'est l'identité reconnue pour l'exercice de la force publique, de la justice. »⁶

Il est donc plus juste, dans l'Internet moderne, de parler « des » identités numériques, au pluriel. Il existe en effet une différence fondamentale entre les identités déclaratives, auto-crées, que sont les divers avatars d'un internaute dans ses sphères d'activités sur la toile, et une identité fiable, éventuellement prouvée à partir de l'identité d'État-civil, qui peut servir à marquer l'engagement d'une personne sous la forme d'une signature électronique, qui est celle que nous considérons dans le présent guide.

5 Sous réserve de l'instruction fiscale à venir.

6 Source : SGMAP



1.3.2.2 Une tentative de définition

On pourrait dès lors définir l'identité numérique d'un signataire comme : « La capacité à identifier une personne physique ou morale sur Internet ».

Cette capacité à identifier une personne bénéficiera, selon le contexte dans lequel elle est établie et les moyens et processus mis en œuvre pour sa vérification (au travers de l'« enregistrement » ou « enrôlement »), d'un niveau de fiabilité plus ou moins élevé.

Il faudra bien entendu adapter le niveau de fiabilité requis pour l'identité numérique au contexte de l'application dans laquelle cette identité est requise pour la réalisation de la signature électronique.

1.3.2.3 La fiabilité de l'identité numérique

La confiance que l'on peut avoir dans une identité numérique sera fonction du processus d'enregistrement (ou d'enrôlement) mis en œuvre pour l'établir.

Aux débuts de l'histoire de la signature électronique, VeriSign, acteur technique de la certification, a défini trois niveaux d'enregistrement, appelés « classes » :

- **classe 1** : certification de l'identité d'un signataire sans autre contrôle que la validité de son adresse mail ;
- **classe 2** : certification de l'identité d'un signataire à distance, sur la base de copies de ses papiers d'identité ;
- **classe 3** : certification de l'identité d'un signataire suite à une rencontre en face à face, et sur présentation des papiers d'identité originaux⁷.

Un symbole « + » est ajouté à la classe pour mentionner le fait que le certificat d'identité délivré est hébergé sur un support cryptographique physique : carte à puce ou clef USB. (On se référera plus bas au paragraphe sur les certificats.)

En France, le Référentiel Général de Sécurité, publié par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), qui s'impose à toutes les administrations et se veut un référentiel de bonnes pratiques également pour le secteur privé, a défini des niveaux sous la forme d'étoiles correspondant à des niveaux de sécurité progressifs sur la qualité de certification de l'identité :

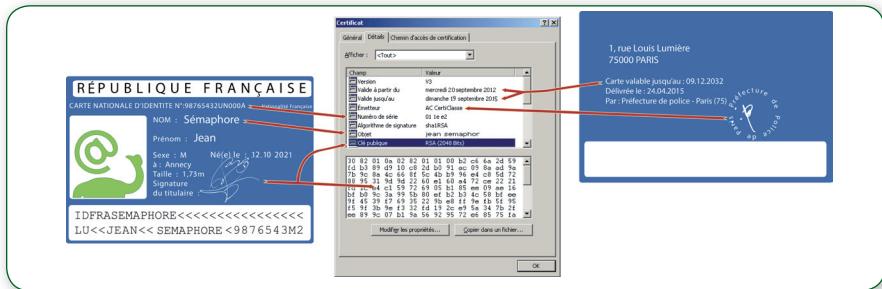
- **une étoile (*)** correspond à la classe 2 ;
- **deux étoiles (**)** correspond à la classe 3+ ;
- **trois étoiles (***)** correspond à l'émission d'un certificat qualifié de classe 3+ (voir chapitre juridique pour plus de détails).

⁷ Pour aller encore plus loin, la vérification de l'identité sur les bases d'État-civil devrait être rendue possible.

1.3.3 Le certificat, support de l'identité numérique

L'identité du signataire est portée par son **certificat**, qui est un support de l'identité numérique, infalsifiable, délivrée par une Autorité de Certification.

Ce certificat pourra comporter des éléments différents selon les usages qui en sont prévus et autorisés.



La délivrance d'un certificat est réalisée au travers des opérations suivantes, qui sont définies et contrôlées par l'Autorité de Certification qui s'engage sur l'identité ainsi certifiée :

1. L'enregistrement (ou enrôlement) du futur porteur :

Le demandeur du certificat prouve son identité en respectant le processus défini en fonction du niveau du certificat qu'il souhaite acquérir, ce niveau devant être conforme aux exigences du ou des services dans lesquels il sera amené à réaliser des signatures électroniques.

L'enregistrement est réalisé par l'Autorité d'Enregistrement.

2. La fabrication du certificat :

Une paire de clefs cryptographiques, appelées « clef privée » et « clef publique », est générée. L'identité du signataire et sa clef publique sont liées entre elles dans un fichier appelé le certificat, qui est scellé par l'Autorité de Certification de manière à garantir :

- sa provenance : c'est-à-dire l'Autorité de Certification émettrice ;
- son intégrité : il est impossible de modifier un certificat sans en rendre le scellement invalide ;
- son niveau de sécurité : le certificat mentionne la Politique de Certification définissant les règles appliquées lors de sa délivrance.

Le certificat est fabriqué par l'Opérateur de Certification.

3. La délivrance du certificat :

Le certificat et la clef privée correspondante (appelée également le « moyen de création de signature électronique ») sont remis à leur porteur selon le mode de délivrance défini dans la Politique de Certification. Ainsi, si le niveau de sécurité impose un support physique, une carte à puce ou une clef USB cryptographique sera remise au porteur ainsi qu'un code PIN, équivalent du code des cartes bancaires, qui permettra au seul porteur l'usage de sa clef privée pour réaliser des signatures électroniques.



Un certificat a une durée de vie limitée, et doit être renouvelé à l'issue de cette période.

Dans le cas où un certificat doit être annulé au cours de sa durée de vie (par exemple parce que son titulaire a quitté l'entreprise au titre de laquelle le certificat a été émis, s'il a perdu son support cryptographique ou si la confidentialité de sa clef privée est compromise), il est nécessaire de procéder à sa **révocation**. Le numéro de série est alors inscrit sur une « liste noire » appelée CRL (Certificate Revocation List) tenue par l'Autorité de Certification émettrice, et bien entendu scellée pour en garantir, là encore, la provenance et l'intégrité.

De nombreuses Autorités de Certification publiques et privées délivrent ainsi des certificats pour des usages différents. Afin de garantir leur interopérabilité et de faciliter le choix par les signataires, des « listes de confiance » sont publiées pour différents milieux professionnels. On peut citer par exemple :

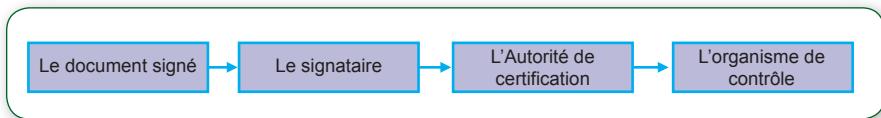
- au niveau français, la liste des certificats qualifiés RGS, tenue par l'ANSSI (<http://www.ssi.gouv.fr/>) ;
- la liste PRIS, qui a été remplacée officiellement par la liste RGS, mais est encore employée dans de nombreux services (<http://www.dgcis.gouv.fr/secteurs-professionnels/economie-numerique/securite-et-transaction>) ;
- la liste « ComPAC », pour la Politique d'Acceptation Commune du secteur bancaire français (<http://www.fntc.org/>) ;
- l'ASIP (Agence des Systèmes d'Information Partagés de Santé) : liste de révocation des CPS disponibles sur le site annuaire de l'ASIP santé <http://integrateurs-cps.asipsante.fr/pages/Listes-de-r%C3%A9vocation-CPS>
- la « Trusted List » européenne regroupant les listes des États membres, qui devrait être mise en ligne quelques temps après la mise en œuvre pratique de la proposition de Règlement européen en cours de finalisation (<http://references.modernisation.gouv.fr/trust-service-status-list-tsl> pour la partie française s'appuyant sur le RGS) ;
- au niveau européen, le projet PEPPOL pour la signature électronique des marchés publics (<http://www.peppol.eu/>) ;
- Chronotachygraphe : la liste de révocation n'est accessible qu'aux forces de contrôle et aux autorités de délivrance de l'espace européen sur le site <http://www.chronoservices.fr>.

Il existe des perspectives de normalisation au niveau européen pour l'acceptation des certificats dans les échanges dématérialisés, en cours de formalisation dans le projet de règlement européen non encore publié au jour de la rédaction de ce guide.

1.3.4 La chaîne de la confiance

L'établissement d'une identité numérique et son emploi pour la réalisation d'une signature électronique doivent permettre au destinataire du document signé d'avoir confiance dans la fiabilité du processus employé et donc dans la validité de l'acte qui lui est fourni par ce moyen.

La confiance s'établit au travers d'une chaîne qui part du document signé pour aboutir au contrôle de la fiabilité de l'Autorité de Certification, selon le schéma ci-dessous :



Ainsi, lorsque la signature électronique a été réalisée à l'aide d'un certificat émis par une Autorité de Certification inscrite sur la liste de l'ANSSI, la confiance dans la signature découle de la confiance dans l'Autorité de Certification, qui découle elle-même de la confiance dans les procédures d'audit annuel mises en œuvre pour le référencement RGS : l'identité du signataire ayant été certifiée après vérification des papiers d'identité du signataire, et l'audit garantissant que ce contrôle est bien systématiquement mis en œuvre, c'est au final l'État qui se porte garant de la fiabilité de l'identité numérique du signataire, établie à partir de son identité d'État-civil, et de la validité de la signature qui en découle.

Dans d'autres contextes, par exemple pour des échanges dans la sphère privée, la validité des signatures électroniques peut être établie d'une autre manière, grâce à une **convention de preuve**.

Il s'agit d'établir en amont les règles applicables pour la recevabilité juridique des documents et des signatures électroniques. Le document de convention de preuve, approuvé formellement par les parties prenantes à l'échange, pourra être pris en compte lors du règlement d'éventuels litiges.

L'établissement d'une convention de preuve est une bonne pratique permettant de fixer à l'avance les règles applicables en cas de litige ou de contestation, et de simplifier la résolution des litiges en cas d'action en justice, voire d'en diminuer l'occurrence. Toutefois, il faudra prendre garde lors de la rédaction de cette convention de preuve, celle-ci pouvant être largement impactée lorsque le client est un consommateur.

1.4 Les définitions de la signature électronique

La signature électronique est une réalité multiforme et il est impossible d'en donner une unique définition. Procédé technique à valeur juridique, garant de l'engagement d'une personne mais aussi vecteur de sécurité informatique, il est indispensable de passer par plusieurs angles de vue pour se l'approprier pleinement.

Nous allons ici définir la signature électronique d'un point de vue pragmatique, d'un point de vue juridique puis d'un point de vue technique, puis nous détaillerons les différentes formes qu'elle peut prendre et nous évoquerons quelques contre-exemples.



1.4.1 Définition pratique

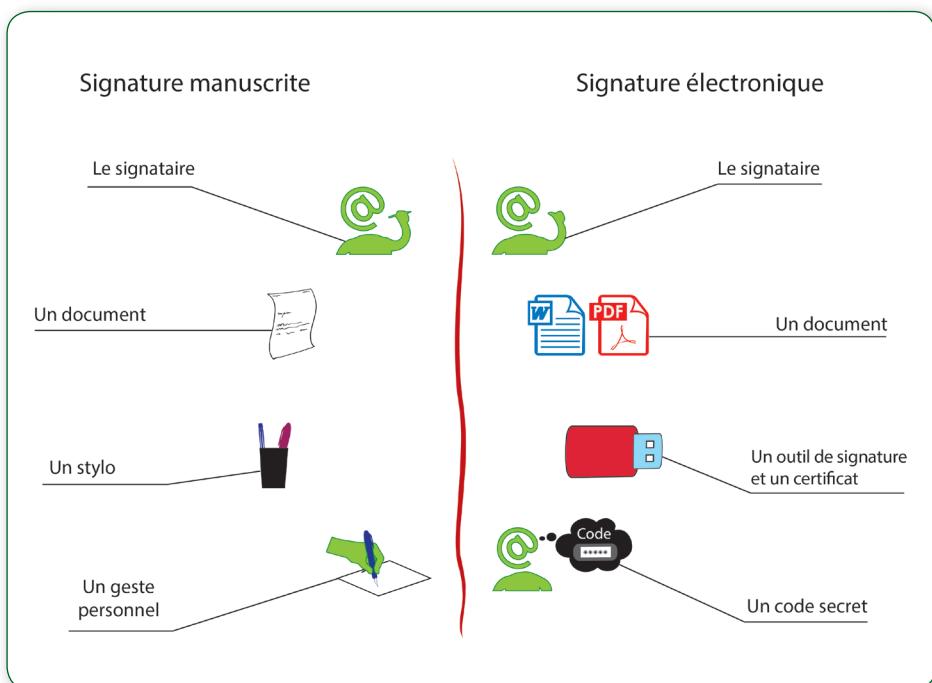
D'un point de vue intuitif, la signature électronique est l'équivalent d'une signature manuscrite, la différence portant sur la nature du document signé :

- une signature manuscrite porte sur un document papier ;
- une signature électronique porte sur un document électronique.

Les différences techniques qui en découlent seront détaillées dans la définition technique.

Le parallèle entre les deux formes de signatures peut être réalisé assez simplement :

- dans les deux cas, il y a un individu, le signataire, qui va marquer son engagement sur les termes du document à signer ;
- dans les deux cas, il y a un document, dont la nature change (un papier ou un fichier informatique) ;
- dans les deux cas, la signature sera réalisée à l'aide d'un instrument, qui sera un stylo dans le cas de la signature manuscrite, et un « outil de signature » et, dans le cas de la signature électronique, un logiciel appelé «outil de signature» et un certificat;
- dans les deux cas, il y a un secret détenu par le signataire : le geste qu'il est le seul à pouvoir réaliser, dans le cas de la signature manuscrite, et le code d'utilisation de son certificat dans le cas de la signature électronique.



1.4.2 Définition juridique

La loi du 13 mars 2000 a fait entrer la signature électronique dans le droit français en la définissant à l'article 1316-4 du code civil :

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.

Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. [...]

On se reportera au chapitre « Les textes juridiques applicables » pour plus de détail.

1.4.3 Définition technique

Comme nous l'avons vu ci-dessus, la réalisation d'une signature électronique nécessite :

- la garantie de l'intégrité du document ;
- un lien certain avec l'identité du signataire.

Ces propriétés sont obtenues par l'usage de la cryptographie. La réalisation technique d'une signature électronique consiste en un calcul mathématique réalisé à partir :

- du document à signer (ce qui garantira son intégrité) ;
- de la clef privée du signataire (ce qui garantira le lien avec son identité au travers du certificat).

Les deux concepts de cryptographie employés pour la signature électronique sont :

1. Le hachage, ou calcul d'empreinte :

La fonction standard recommandée pour cette opération s'appelle SHA256.

Une fonction de hachage est une fonction à sens unique qui permet, à partir d'un document, d'en obtenir un condensé de taille réduite qui dépend de l'ensemble des bits contenus dans le document d'origine.

À partir d'une empreinte, il est impossible de reconstituer un document qui lui correspondrait.

Les fonctions de hachage sont très dépendantes de l'entrée : ainsi, deux documents très proches auront des empreintes très différentes.

2. La cryptographie asymétrique :

La fonction standard la plus employée s'appelle RSA.

Nous avons vu dans le chapitre sur le certificat que le signataire dispose d'une « clef privée », qui est sous son contrôle exclusif, et d'une « clef publique », qui est incluse dans son certificat, qui sera joint à chacune de ses signatures.

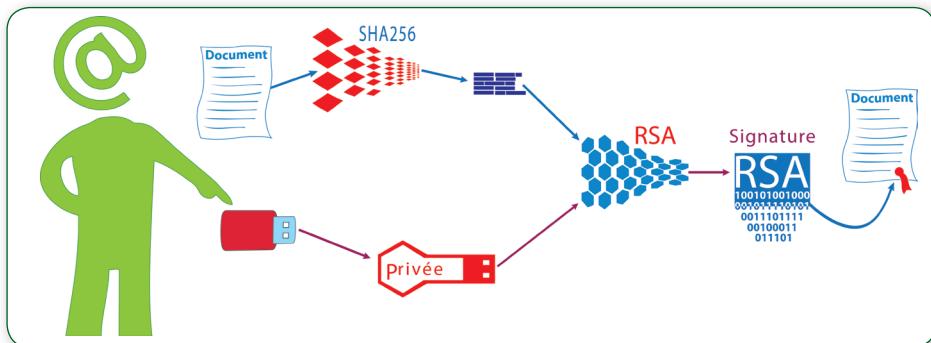
Ces deux clefs sont liées mathématiquement et permettent de faire les calculs inverses l'une de l'autre.

Il est bien entendu impossible de reconstituer la clef privée lorsqu'on ne dispose que de la clef publique.



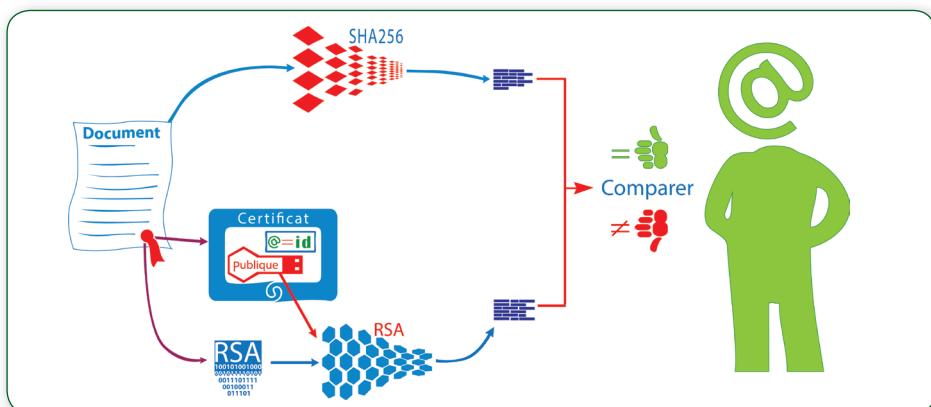
Lorsque l'on clique sur le bouton « signer », les opérations techniques suivantes sont réalisées, conformément à l'illustration ci-dessous :

- le document à signer est haché de manière à en obtenir un condensé (SHA256) ;
- le condensé du document et la clef privée du signataire sont employés pour effectuer un calcul mathématique (RSA) : le résultat de ce calcul est, du point de vue technique, la signature électronique ;
- la signature est jointe au document, ainsi que le certificat du signataire, qui permettra sa vérification.



La vérification technique d'une signature électronique passe par les opérations suivantes, illustrées dans la figure ci-dessous :

- le destinataire du document signé sépare le document lui-même de sa signature ;
- il extrait du certificat du signataire sa clef publique et s'en sert pour réaliser sur la signature le calcul RSA inverse : il obtient ainsi le condensé du document initialement signé ;
- il réalise à son tour le calcul du condensé du document reçu ;
- il compare les deux condensés ainsi obtenus : s'ils sont identiques, la signature portait bien sur le document reçu (lien avec le document), et a bien été réalisée par le porteur du certificat (lien avec l'identité du signataire).



Il ne s'agit ici que d'une définition technique des opérations réalisées. Nous verrons plus bas dans le chapitre sur la réalisation et la vérification de signature électronique que les aspects purement techniques sont insuffisants à garantir la validité d'une signature électronique.

1.4.4 La signature électronique : plusieurs usages

Nous avons décrit ci-dessus le mécanisme technique de la signature électronique. Il s'applique bien entendu aux signatures réalisées par les personnes physiques, mais peut également être employé de manière identique dans des contextes juridiques et fonctionnels différents, pour obtenir des « signatures électroniques » au sens technique, mais ayant une portée et un usage très différents : la signature de personne morale ou de serveur (aussi appelée « cachet »), et les différents usages de la signature à des fins purement techniques. On parlera alors de « scellement » et non de « signature ».

1.4.4.1 La signature de personne physique

La signature d'une personne physique est l'acte par lequel un individu s'engage sur les termes d'un document.

Il peut le faire en son nom propre, ou au nom de la société à laquelle il appartient. Cette distinction découle naturellement de la nature de l'acte signé, mais également du certificat employé pour réaliser la signature :

- s'il s'agit d'un certificat de personne privée, ce sera l'engagement d'un individu ;
- s'il s'agit d'un certificat professionnel associant le nom de l'employé à celui de sa société, ce sera l'engagement professionnel de la personne qui sera obtenu. Dans ce cas, il conviendra de vérifier que le signataire est bien habilité à engager sa société.

1.4.4.2 Le cachet électronique

Le cachet est une signature apposée au nom d'une personne morale.

Il sert à garantir la provenance et l'intégrité d'un document, et correspond à une « certification conforme ».

Il peut être réalisé automatiquement par un serveur, dans le cadre d'un processus automatisé de génération de documents, comme par exemple pour la dématérialisation des factures.

Il peut également être réalisé par un être humain qui dispose d'un certificat de personne morale, pour apposer ponctuellement un cachet sur un document. Dans ce cas, le nom du responsable peut apparaître dans le certificat, car il y a toujours un humain qui se porte garant des engagements d'une société.



1.4.4.3 Les scellements électroniques

Le procédé technique de signature électronique comporte des intérêts fonctionnels très importants :

- garantir la provenance d'un document ou d'une donnée ;
- garantir l'intégrité de cette donnée.

C'est pourquoi ce procédé est très largement employé à des fins purement techniques de scellement. Citons-en trois usages fondamentaux que nous avons déjà abordés dans ce guide :

- le scellement d'un certificat ;
- le scellement d'une liste de certificats révoqués ;
- le scellement d'un jeton d'horodatage.

Le scellement des certificats

Un certificat sert à lier l'identité d'une personne à sa clef publique. Cette certification d'identité est réalisée par une Autorité de Certification qui se porte garante de l'exactitude des données certifiées. Puisque ce certificat sera employé pour vérifier des signatures électroniques, il est fondamental qu'il soit inaltérable.

C'est pourquoi l'Autorité de Certification réalise un scellement sur chaque certificat qu'elle délivre.

Les bénéfices sont les suivants :

- le lien entre l'identité du signataire et sa clef publique est garanti ;
- l'identification de l'Autorité de Certification peut être vérifiée ;
- on peut donc vérifier, via sa Politique de Certification, les pratiques mises en œuvre pour le contrôle de l'identité du porteur.



Le scellement de la CRL

La Liste de Certificats Révoqués émise par une Autorité de Certification est la « liste noire » des certificats dont la validité n'est plus garantie suite à une « mise en opposition ».

Là encore, il s'agit d'un élément fondamental de la vérification des signatures électroniques.

À chaque ajout d'un certificat dans cette liste, l'Autorité de Certification en réalise donc un scellement, qui en garantit l'intégrité et la provenance.



Le scellement d'un jeton d'horodatage

Un jeton d'horodatage sert à placer dans le temps de manière certifiée l'existence d'un document ou d'une donnée.

Il est délivré par une Autorité d'Horodatage de la manière suivante :

- la donnée à horodater est hachée pour en obtenir un condensé ;
- ce condensé est associé à la date et l'heure courantes ;
- l'Autorité d'Horodatage appose un scellement sur l'ensemble de ces données.

Structure d'un jeton d'horodatage

Empreinte du document horodaté

Date et heure de l'horodatage

Lien vers la Politique d'Horodatage

Scellement
par l'AC

Les bénéfices sont les suivants :

- grâce au hachage, il n'est pas nécessaire de transmettre à l'Autorité d'Horodatage le document à horodater : il peut rester confidentiel et pourtant faire l'objet d'une datation garantie ;
- on peut vérifier à tout moment qu'un document horodaté est resté intégrer, grâce à l'inclusion de son condensé dans le jeton d'horodatage ;
- la date et l'heure incluses dans le jeton d'horodatage font foi de l'existence du document horodaté et peuvent ainsi servir à en prouver l'antériorité ;
- la Politique d'Horodatage définit le mode de réalisation des jetons d'horodatage et permet de garantir l'impossibilité d'antidater un jeton d'horodatage.

Nous verrons dans le chapitre consacré aux bonnes pratiques qu'il est important d'inclure un jeton d'horodatage dans les signatures électroniques pour les placer dans le temps.

1.4.5 Quelques contre-exemples

Chacun à son niveau en fait chaque jour le constat : les technologies numériques accélèrent les échanges d'informations, la création de documents et la production d'œuvres en général. Revers de la médaille, il est très facile de modifier le contenu d'un fichier numérique à son avantage sans laisser de trace et sans que l'on sache qui l'a modifié.

Supposons que la « signature » se limite à inscrire son prénom et son nom au bas d'un document, quel que soit son format et quel que soit le logiciel bureautique utilisé : comment être sûr que ce soit le « signataire » qui ait apposé ces mentions ? Il serait bien entendu possible à toute personne disposant du logiciel bureautique concerné d'ouvrir le document, de le modifier pour inscrire le nom d'une autre personne, et de modifier ainsi le « signataire » à l'insu de tous ! Un tel procédé ne peut donc pas servir à marquer l'engagement de l'auteur d'un document puisqu'il sera possible à tout moment de contester cet engagement. Le principe de « non répudiation » ne peut ainsi pas être garanti.



Il en va de même de l'inclusion dans un document bureautique du scan d'une signature manuscrite : rien n'empêche un éventuel fraudeur de copier cette image pour l'inclure dans un autre document, et ainsi de constituer à partir d'un document « signé » un autre document de son choix à la signature tout aussi valable... C'est-à-dire tout aussi peu valable !

Il est également possible de remplacer l'image de la signature manuscrite par celle de la signature de quelqu'un d'autre, et ainsi de changer le signataire d'un document.

L'inclusion dans un document du nom d'une personne ou de l'image de sa signature manuscrite ne peut donc pas être considérée comme une signature électronique.

Ce qui vaut pour l'identité du signataire vaut aussi pour le contenu du document en lui-même. Un mécanisme d'engagement numérique doit absolument conserver l'intégrité du document (absence d'altération), faute de quoi une modification du document postérieure à sa signature serait possible.

Enfin, cela vaut aussi pour la date de la signature : en l'absence de mécanisme fiable permettant d'apposer une date sur un contrat électronique, alors l'une des deux parties pourra toujours contester la date d'exécution de celui-ci de la sorte : « Oui j'ai bien signé ce contrat mais je viens de le faire et à l'époque des faits il n'avait pas cours. ».

NB : Contrairement aux idées reçues, les documents PDF sont tout aussi facilement modifiables que les documents Word ou Open Office. Le seul moyen de les rendre infalsifiables est... De leur apposer une signature électronique !

1.5 Que peut-on signer électroniquement ?

Le mécanisme technique de signature électronique ne dépend pas du format des données que l'on souhaite signer : il est ainsi possible de réaliser une signature sur un document bureautique, une image, une vidéo, des données brutes ou tout autre fichier informatique, quel qu'en soit la nature.

Toutefois, lorsque la signature électronique est employée pour recueillir l'engagement du signataire, il est préférable de la faire porter sur un document intelligible par un être humain !

Certains cas d'usage méritent d'être précisés :

- Signer électroniquement un zip n'équivaut pas à signer électroniquement chacun des documents contenus dans le zip : il convient de réaliser la signature de chacun des documents avant de constituer le zip qui contiendra les documents et leurs signatures.
- Le format S/MIME permet de signer électroniquement les courriers électroniques. De même que pour un zip, signer électroniquement un mail contenant une pièce jointe n'est pas équivalent à l'envoi par mail d'une pièce jointe signée.

LES BONNES PRATIQUES

2.1 Réaliser une signature électronique

- 2.1.1 Les différents modes de réalisation de la signature électronique
- 2.1.2 Les formats de signature électronique
- 2.1.3 Les éléments techniques complémentaires
- 2.1.4 Faciliter l'usage de la signature électronique

2.2 Vérifier une signature électronique

2.3 Conserver des documents signés électroniquement

2.4 Mener un projet de signature électronique

- 2.4.1 La technique au service du projet
- 2.4.2 Prendre en compte le facteur humain
- 2.4.3 Raisonner à long terme

2.5 L'interopérabilité

- 2.5.1 L'interopérabilité des formats de signature électronique
- 2.5.2 L'interopérabilité des certificats

2.6 Ouverture à l'international

2.7 La convention de preuve

2.8 Respecter les normes et règlementations

2 LES BONNES PRATIQUES

2.1 Réaliser une signature électronique

Nous avons vu dans le paragraphe consacré à la définition technique de la signature électronique comment cette signature était calculée.

Toutefois, limiter la réalisation d'une signature électronique au calcul mathématique qui la sous-tend serait une erreur, car il existe de multiples manières de permettre à l'utilisateur de signer électroniquement, et on ne peut, dans ce domaine, mettre en avant une solution unique qui satisferait l'ensemble des besoins.

Nous allons d'abord présenter les différents modes de réalisation de la signature électronique, puis nous parlerons des formats standard existants, avant d'évoquer les éléments complémentaires qu'il convient à inclure dans les signatures pour permettre leur vérifiabilité dans le temps, et enfin décrire les éléments organisationnels qui permettent son adoption par les utilisateurs.

2.1.1 Les différents modes de réalisation de la signature électronique

En fonction des contraintes liées au projet et aux signataires, il est possible d'envisager des manières de réaliser la signature électroniques très différentes.

Nous allons ici en décrire quatre, qui sont les plus répandues, mais qui ne sauraient être exhaustives. Le paragraphe consacré à la facilitation de l'usage de la signature électronique décrira d'autres options afin de compléter ce panorama.

2.1.1.1 La signature électronique « autonome »

Dans ce mode de réalisation, le signataire dispose sur son poste de travail d'un logiciel de signature électronique, ainsi que d'un certificat qu'il a acquis auprès d'une Autorité de Certification, par exemple sous la forme d'une carte à puce.

NB Le certificat nécessite une installation sur le poste de travail, mais cette installation est réalisée une seule fois, suite à quoi le signataire peut se servir de son certificat sans aucune contrainte technique.

Après avoir démarré le logiciel de signature, le signataire sélectionne le document à signer.

Le logiciel accède alors à la carte à puce et demande la saisie du code PIN.

Une fois le code PIN saisi, la signature électronique est réalisée dans la carte à puce, puis transmise au logiciel qui en fera la mise en forme selon le format attendu.



L'utilisateur est, dans ce cas, totalement autonome pour réaliser des signatures électroniques. C'est notamment le choix qui a été fait pour la signature électronique des experts-comptables, Signexpert.

2.1.1.2 La signature électronique via une applet

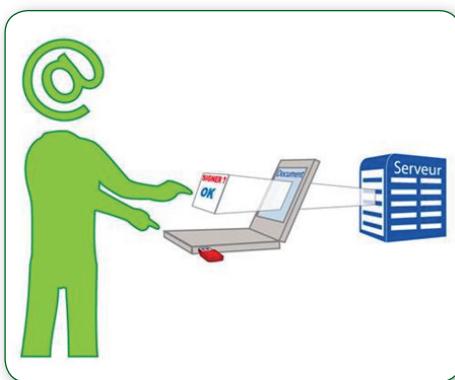
Dans ce mode de réalisation, le signataire dispose sur son poste de travail uniquement d'un certificat qu'il a acquis auprès d'une Autorité de Certification, par exemple sous la forme d'une carte à puce.

NB Le certificat nécessite une installation sur le poste de travail, mais cette installation est réalisée une seule fois, suite à quoi le signataire peut se servir de son certificat sans aucune contrainte technique.

Le service dans lequel la signature est nécessaire contient un programme téléchargeable appelé une « applet ». Lorsque l'utilisateur doit signer, cette applet est automatiquement chargée sur son poste et exécutée.

Le document à signer est présenté à l'utilisateur qui confirme sa volonté de signer. L'applet accède alors à la carte à puce et demande la saisie du code PIN.

Une fois le code PIN saisi, la signature électronique est réalisée dans la carte à puce, puis transmise à l'applet qui en fera la mise en forme selon le format attendu.



Dans ce cas, l'utilisateur dispose d'un certificat qu'il pourra employer dans divers services, sans avoir besoin sur son poste d'un logiciel de signature électronique, puisque ce logiciel (l'applet) lui est transmis à chaque besoin. La signature reste sous son contrôle exclusif puisque, sans saisie du code PIN, elle ne pourra pas être réalisée. Le format de la signature électronique est choisi par l'applet en fonction du service dans lequel elle s'exécute, de manière transparente pour le signataire.

C'est notamment le choix qui a été fait par la majorité des plates-formes de réponse aux marchés publics.

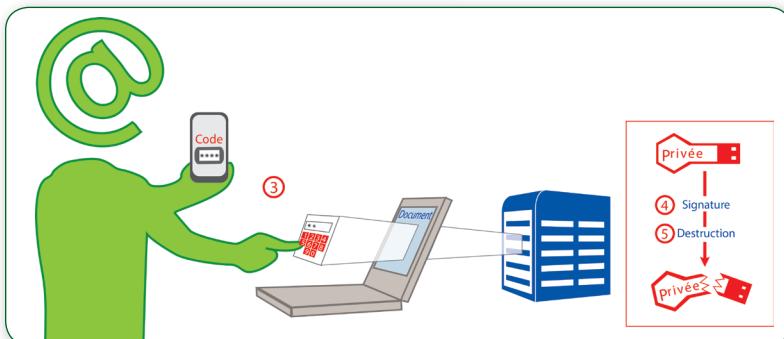
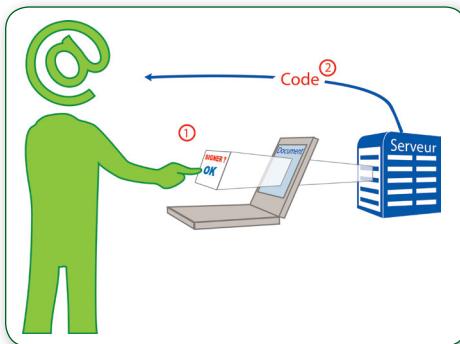
2.1.1.3 La signature électronique « à la volée »

Dans ce mode de réalisation, le signataire dispose uniquement d'un moyen d'authentification, qui lui permettra de prouver son identité vis-à-vis de la plate-forme. Il pourra s'agir par exemple d'un numéro de téléphone mobile sur lequel il recevra un code à usage unique, qu'il devra ressaisir.

Le service dans lequel la signature est nécessaire présente à l'utilisateur le document à signer. Lorsque l'utilisateur confirme sa volonté de signer, le procédé d'authentification du signataire se déclenche (par exemple par l'envoi d'un sms, comme indiqué ci-dessus).

Une fois le signataire authentifié, la plate-forme de service (ou un Tiers de Confiance auquel elle fait appel) génère un certificat au nom du signataire, réalise elle-même la signature électronique, puis détruit la clef privée correspondante de manière à garantir qu'elle ne soit utilisée qu'une fois.

Le document signé peut alors être envoyé au signataire ou mis à sa disposition.



Dans ce cas, aucune contrainte d'usage n'est imposée au signataire : ce procédé est d'une grande souplesse et d'une grande ergonomie pour l'utilisateur.

Le niveau de sécurité de la signature sera celui du procédé d'authentification employé : saisie d'un mot de passe ou d'un code à usage unique... (On se reportera pour ce point au chapitre « La fiabilité de l'identité numérique ».)

C'est notamment le choix qui a été fait par de nombreux services de contractualisation en ligne.



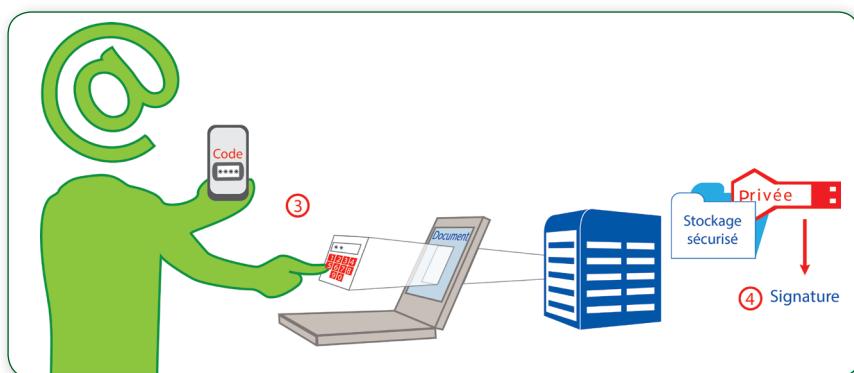
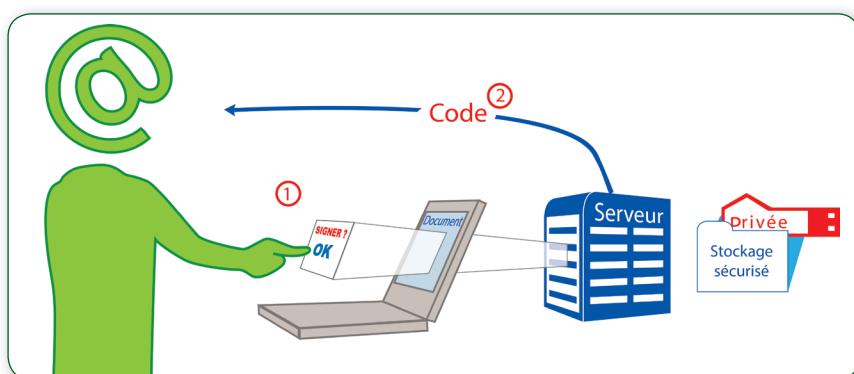
2.1.1.4 La signature électronique par « carte à puce virtuelle »

Dans ce mode de réalisation, comme pour la signature électronique à la volée, le signataire dispose uniquement d'un moyen d'authentification, qui lui permettra de déclencher l'utilisation de son certificat par la plate-forme.

Un certificat permanent au nom du signataire est généré en amont de l'utilisation du service, mais au lieu d'être remis au titulaire comme dans le cas de la signature électronique autonome, ou d'être temporaire comme dans le cas de la signature électronique à la volée, il est conservé sur le serveur au sein d'un module cryptographique physique (HSM pour Hardware Security Module) : ce module constitue une « carte à puce virtuelle ».

Le service dans lequel la signature est nécessaire présente à l'utilisateur le document à signer. Lorsque l'utilisateur confirme sa volonté de signer, le signataire transmet son code de déblocage qui permet à la carte à puce virtuelle de réaliser la signature électronique.

Le document signé peut alors être envoyé au signataire ou mis à sa disposition.



Dans ce cas, aucune contrainte d'usage n'est imposée au signataire : ce procédé est d'une grande souplesse et d'une grande ergonomie pour l'utilisateur.

Le niveau de sécurité de la signature dépendra du mode de délivrance du certificat dans la carte à puce virtuelle, et de la sécurisation de la transmission du code de déblocage.

C'est notamment le choix qui a été fait par de nombreux services de contractualisation en ligne où l'usager revient de manière récurrente.

2.1.2 Les formats de signature électronique

Il existe trois formats principaux pour les signatures électroniques, comportant chacune l'acronyme AdES pour « Advanced Electronic Signature » :

- **XAdES** : signature électronique XML.

Il s'agit d'un format de stockage des signatures électroniques qui peut être indépendant des données signées (la signature constitue alors un fichier XML à part du document signé, qui peut être à n'importe quel format), ou inclus dans le document signé si ce document est lui-même au format XML.

Le format XAdES permet la signature multiple du même document par plusieurs signataires.

Aucun élément graphique ne permet d'identifier la présence d'une signature.

- **CAdES** : aussi appelé PKCS#7 ou CMS.

Le format CAdES (CMS Advanced Electronic Signature) permet de stocker des signatures électroniques « détachées » (la signature est dans un fichier à part, à transmettre en même temps que le document signé) ou « opaques », c'est-à-dire que le document est inclus dans une « enveloppe » qui comporte aussi la signature.

Les deux options comportent des avantages et des inconvénients :

- dans le cas des signatures détachées, pour transmettre un document signé, il faut envoyer les deux fichiers simultanément, mais le document initial est lisible avec le logiciel qui lui est nativement associé sans aucune manipulation ;
- dans le cas des signatures opaques, il faut disposer d'un outil pour extraire de l'enveloppe le document lorsque l'on souhaite le lire : faute de cet outil, l'enveloppe n'est pas exploitable directement, par exemple par un logiciel bureautique.

Aucun élément graphique ne permet d'identifier la présence d'une signature.

- **PAdES** : signature électronique PDF.

Le format PAdES (PDF Advanced Electronic Signature) est le format des signatures électroniques incluses dans les documents PDF.

Il permet la signature multiple du même document par plusieurs signataires, sous la forme de sur-signatures : chaque signataire signe non seulement le document, mais aussi les signatures déjà apposées par les signataires précédents.

La signature peut optionnellement apparaître graphiquement dans le document lorsqu'on le visualise avec le logiciel Adobe Reader. En cliquant sur cet élément graphique entièrement personnalisable, une fenêtre de vérification technique de la signature s'affiche.



Chacun de ces formats se décline en six sous-formats offrant des niveaux de sécurité successifs :

- AdES-BES (Basic Electronic Signature) correspond aux exigences minimales requises pour la réalisation de signatures électroniques sécurisées ;
- AdES-T (Timestamp) permet d'inclure dans la signature un jeton d'horodatage ;
- AdES-C (Complete) permet d'inclure des références à la chaîne de certification et à la liste de révocation ;
- AdES-X (Extended) permet d'inclure un horodatage des références incluses dans AdES-C pour éviter leur modification ;
- AdES-X-L (Long-term) permet d'inclure les certificats et la liste de révocation au lieu de simples références à ces éléments ;
- AdES-A (Archiving) permet de renouveler périodiquement les horodatages afin de garantir une certitude d'intégrité au fil du temps.

2.1.3 Les éléments techniques complémentaires

Nous avons vu au paragraphe précédent que les formats standard de signature électronique offraient des options sur le contenu des signatures électroniques.

Il est de bonne pratique d'inclure les éléments suivants dans chaque signature électronique :

- la chaîne de confiance complète du certificat du signataire : grâce à elle, la vérification de la signature pourra remonter jusqu'à l'entité qui a certifié l'identité du signataire ;
- un jeton d'horodatage : grâce à lui, la date et l'heure de réalisation de la signature seront connues avec certitude, ce qui permet d'une part de placer dans le temps l'engagement du signataire, et d'autre part de contrôler que le certificat du signataire n'était pas révoqué au moment de la signature ;
- une preuve de validité du certificat au moment de la réalisation de la signature, sous la forme d'une liste de certificats révoqués, ou d'un jeton OCSP (Online Certificate Status Protocol) garantissant que le certificat n'est ni périmé, ni révoqué.

2.1.4 Faciliter l'usage de la signature électronique

L'introduction de la signature électronique dans les processus de l'entreprise ou dans la relation client est un changement fondamental des pratiques habituelles.

C'est pourquoi il importe d'en faciliter le plus possible l'appropriation par l'usage des outils adaptés.

Envisageons trois de ces outils, utilisés conjointement à des certificats numériques, destinés chacun à un usage précis.

2.1.4.1 L'usage d'un parapheur électronique

Un parapheur électronique est un logiciel collaboratif permettant à un ou plusieurs processus métier de soumettre des documents à la validation et à la signature des décideurs définis dans le cycle de vie du document.

Les avantages de l'usage d'un tel outil sont multiples :

- il permet de gérer automatiquement la soumission du document au signataire et le retour du document signé dans la chaîne métier ;
- il permet au signataire de disposer en un seul endroit de l'ensemble des documents qu'il a à signer ;
- il permet d'inclure des étapes de validation / corrections préalables à la signature ;
- il permet de gérer les délégations de signature en cas d'absence ;
- rendu accessible en situation de mobilité, il permet au signataire de réaliser les signatures même lorsqu'il est hors de l'entreprise.

Ainsi, le parapheur électronique reproduit et améliore le fonctionnement des parapheurs papier en offrant centralisation et souplesse dans le processus de signature.

2.1.4.2 Les tablettes de signature

L'acte de signature électronique est souvent perçu par les signataires, du fait de sa nature technique prépondérante, comme présentant une perte de solennité par rapport à la signature manuscrite, dans laquelle le geste est primordial.

Il est possible de compléter le processus de signature électronique par la saisie à l'aide d'un stylet sur une tablette graphique d'une image de la signature manuscrite. Cette image pourra être incluse dans le document, par exemple dans le champ de signature électronique d'un document PDF.

La signature manuscrite ainsi capturée ne se substitue évidemment pas à la signature électronique, et n'a pas valeur juridique de signature : il s'agit d'un complément permettant au signataire de mieux comprendre l'acte qu'il réalise et offrant au document une allure « habituelle » grâce à l'image qu'il inclut.

Certaines solutions vont plus loin : grâce à l'enregistrement via la tablette des données de pression, de vitesse et d'inclinaison du stylet, des données graphologiques peuvent être incluses dans la signature manuscrite capturée : ces données permettront a posteriori un contrôle renforçant potentiellement la certitude sur l'identité du signataire.

Ce dispositif est aujourd'hui fréquemment employé pour les signatures de contrats en agences par le grand public, couplé avec la signature électronique « à la volée ».



2.1.4.3 Les codes 2D

Certains documents générés et signés électroniquement nécessitent, dans leur cycle de vie, d'être imprimés pour être présentés dans un contexte où la transmission d'un document électronique n'est pas possible.

Il existe des solutions permettant d'inclure dans le document un codage des données essentielles du document et de la signature électronique correspondante : ainsi, à l'aide d'une « douchette », le destinataire peut relire automatiquement ces éléments et en vérifier la validité.

La signature électronique devient donc vérifiable... Sur un document papier ! Ces usages « hybrides » se développent principalement dans les domaines d'accessibilité difficile (par exemple pour le suivi des marchandises dans le fret maritime).

2.2 Vérifier une signature électronique

Une différence fondamentale entre la signature électronique et la signature manuscrite est la faculté à la vérifier avec certitude... Faculté qui devient même une obligation à chaque usage d'un document signé électroniquement !

La vérification d'une signature électronique nécessite trois étapes :

1. La vérification technique de la signature, que nous avons vue dans le paragraphe consacré à la définition technique de la signature.

Elle consiste à vérifier les aspects cryptographiques de la signature.

Si elle est la plus complexe techniquement, elle est la plus simple en pratique, car elle est entièrement prise en charge par les outils.

2. La vérification de la chaîne de confiance.

Elle consiste à vérifier la validité du certificat du signataire, sa non révocation, le certificat de l'Autorité de Certification émettrice, et le fait que cette Autorité de Certification soit référencée dans une liste officielle, ou soit acceptée dans la Politique de Signature Electronique du service incluant la vérification.

Cette étape est également en grande partie automatisée.

Ces deux étapes sont largement simplifiées en électronique par rapport à la signature manuscrite.

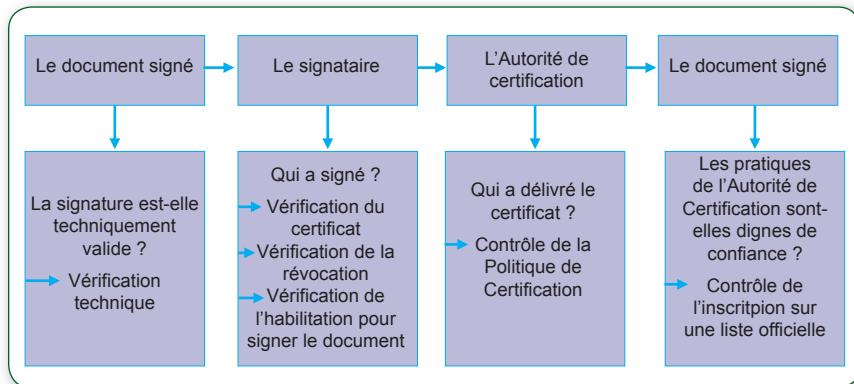
3. La vérification de l'habilitation du signataire.

Cette ultime étape consiste à s'assurer que le signataire, dont l'identité a été garantie par les étapes précédentes, avait bien le droit de signer l'acte dont la signature est en cours de vérification.

Cette vérification peut se faire au travers de plusieurs méthodes : une liste de signataires habilités prédéfinie, la vérification du Kbis de l'entreprise d'appartenance du signataire, l'existence d'une délégation de pouvoir lui concédant l'habilitation (dont la validité doit aussi être vérifiée !)...

C'est dans la pratique la vérification la plus complexe à faire car elle est soumise à l'interprétation humaine. Mais cette vérification n'est pas spécifique à la signature électronique, elle doit aussi être réalisée pour une signature manuscrite.

Le processus de vérification de signature électronique peut se résumer par le schéma ci-dessous :



2.3 Conserver des documents signés électroniquement

Lorsque des documents signés électroniquement comportent une valeur de preuve, il convient de respecter les conditions prescrites par l'article 1316-1 du Code civil, qui dispose que « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. ».

Une bonne pratique permettant de garantir les conditions de conservation des documents signés électroniquement est l'archivage à vocation probatoire des pièces.

Lors de la mise en œuvre d'un projet de signature électronique, on pourra donc prévoir cet archivage, en respectant les principes suivants :

- toujours stocker la signature électronique avec l'acte auquel elle s'attache ;
- si l'on procède à des modifications de formats pour les besoins de l'archivage, conserver également le format original signé, car lui seul constitue un original ;
- élaborer un plan d'archivage et d'indexation garantissant la capacité à retrouver le document a posteriori, éventuellement plusieurs années après sa production et dans un contexte tout à fait différent du moment de sa production.

Voir le Guide de l'archivage électronique et du coffre-fort électronique, collection Les guides de la confiance, FNTC.



2.4 Mener un projet de signature électronique

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.

2.4.1 La technique au service du projet

2.4.1.1 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 pas un 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.

2.4.1.2 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 peut donc être utile, pour réussir son projet, en fonction de sa complexité, 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.

2.4.1.3 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, que nous avons évoqués dans le présent guide. 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.

2.4.2 Prendre en compte le facteur humain

2.4.2.1 *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. Étant donné l'enjeu multiple du projet (juridique, économique, etc.), il est fondamental d'obtenir l'adhésion de l'utilisateur au système déployé.

2.4.2.2 *L'ergonomie des services*

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.

2.4.2.3 *La 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.

2.4.2.4 *La 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.

2.4.2.5 *La 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.



2.4.3 Raisonner à long terme

2.4.3.1 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.)

2.4.3.2 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 ; l'oubli d'une carte au domicile d'un employé l'empêchera-t-il de travailler toute la journée...

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.

2.4.3.3 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.

2.5 L'interopérabilité

L'interopérabilité des usages est sans conteste la clef du succès à venir dans le domaine de la signature électronique.

Afin de permettre l'utilisation du même certificat pour des usages différents, il faut prendre en compte deux dimensions : interopérabilité des formats de signature, et interopérabilité des certificats eux-mêmes.

2.5.1 L'interopérabilité des formats de signature électronique

Nous avons vu qu'il existe plusieurs formats de signature électronique.

Il faut les respecter, car ils offrent une garantie de la capacité du destinataire du document signé à vérifier la signature.

Avant de choisir un format, on vérifiera, dans le domaine dans lequel on déploie la signature et auprès des partenaires directs ou indirects (l'administration par exemple), quel format est majoritairement employé, et pourra le plus facilement être reçu par tous les destinataires potentiels.

2.5.2 L'interopérabilité des certificats

De plus en plus d'applications ou de professions employant la signature électronique, le nombre de certificats déployés est désormais conséquent.

C'est pourquoi il est important, pour faciliter l'usage, de ne pas systématiquement coupler le déploiement d'un projet de signature électronique avec le déploiement de certificats ad hoc qui ne seraient utilisables que dans un service particulier, et qui seraient les seuls utilisables dans ce service.

Il convient donc d'ouvrir au maximum le service de signature électronique au plus grand nombre possible de certificats existants, pourvu que le niveau de sécurité qu'ils offrent soit compatible avec les impératifs du service. A cette fin, la Politique de signature électronique du service doit comporter :

- une dimension fonctionnelle et juridique, qui explicite quels certificats sont acceptés ;
- une dimension technique, permettant à l'administrateur du service d'ajouter ou de retirer aisément une famille de certificats à la liste des Autorités de Certification acceptées.

2.6 Ouverture à l'international

Les définitions de la signature électronique et les contextes d'acceptation juridique sont variés au sein de l'Union européenne, et plus encore au niveau mondial. C'est pourquoi tout projet de signature électronique ouvert à l'international nécessite une étude juridique préalable.



L'Europe avance vers une interopérabilité de cette technologie au travers de plusieurs projets.

Ainsi, une liste européenne des Autorités de Certification certifiées par chaque pays est publiée sous le nom de « trusted list ». Encore lacunaire, cette initiative est néanmoins une promesse d'une plus grande facilité d'emploi transfrontalier dans les années à venir.

Par ailleurs, un projet de règlement européen, encore en cours d'amendement au jour de rédaction de ce guide, s'est fixé pour ambition de définir des règles communes sur l'ensemble des services de sécurité, y compris l'émission de certificats et la signature électronique.

On peut encore citer le projet Peppol d'harmonisation des signatures électroniques dans le domaine des marchés publics.

Parmi les exemples concrets présentés plus bas, on trouvera un exemple de réussite au niveau international : le chronotachygraphe.

2.7 La convention de preuve

La convention de preuve est un accord passé entre des parties privées dans le but de déterminer à l'avance ce qui fera foi en cas de contentieux.

L'établissement d'une convention de preuve valide est une bonne pratique à promouvoir dans les projets qui nécessitent l'usage de la signature électronique.

Cette convention de preuve comportera notamment une Politique de signature électronique déterminant les signataires, le mode de certification de leur identité, le format des signatures électroniques, leur mode de réalisation, leur mode de vérification et leur sémantique.

2.8 Respecter les normes et règlementations

Comment ne pas conclure ce chapitre sur les bonnes pratiques sans revenir sur l'importance du respect des standards et de la législation !

Ces éléments étant abordés dans les paragraphes consacrés aux différents formats de signature électronique et au chapitre juridique, nous ne ferons que rappeler ici que les normes sont indissociables de l'interopérabilité, et que le respect de la loi est impératif.

LES TEXTES JURIDIQUES APPLICABLES

3.1 Le socle juridique de la signature électronique

- 3.1.1 La signature électronique en droit privé
- 3.1.2 La signature électronique en droit public

3.2 Les évolutions juridiques et jurisprudentielles de la signature électronique

- 3.2.1 Applications pratiques de la signature électronique
- 3.2.2 Le projet de règlement du 4 juin 2012 comme solution au problème d'interopérabilité en Europe

3 LES TEXTES JURIDIQUES APPLICABLES

Prenant sa source d'inspiration dans la loi type de la CNUDCI sur le commerce électronique en 1996⁸, la directive 1999/93/CE⁹ du 13 décembre 1999 du Parlement européen et du Conseil, constitue à ce jour une **référence juridique essentielle du cadre juridique applicable à la signature électronique**. Elle y est définie à l'article 2 comme « *une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification* ».

3.1 Le socle juridique de la signature électronique

3.1.1 La signature électronique en droit privé

Transposant en droit français la directive 1999/93/CE, la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique¹⁰ a inséré dans les articles 1316 et suivants du Code civil les notions de preuve, d'écrit et de signature électroniques. Cette dernière se définit à l'article 1316-4 alinéa 2 du Code civil comme : « *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 des conditions fixées par décret en Conseil d'Etat.* ».

Un procédé fiable de signature électronique doit donc **identifier le signataire, garantir le lien (logique) entre l'acte et la personne dont il émane et assurer l'intégrité de l'écrit signé**. Il est également important comme le rappelle l'article 1316-4 al. 1 du Code civil que **la signature manifeste le consentement de l'auteur au contenu de l'acte. Ces fonctionnalités juridiques sont essentielles**.

A l'heure actuelle, seules les signatures électroniques basées sur la cryptologie à clé publique (à savoir les signatures numériques) répondent a priori à ces exigences légales et notamment à la garantie du lien entre la signature et le message (ou le fichier) par le biais de la clé privée de signature correspondant à la clé publique contenu dans le certificat électronique. Par conséquent, seule la signature numérique pourra être considérée comme une signature électronique sécurisée.

8 V. E. Caprioli et R. Sorieul, *Commerce international électronique : vers l'émergence de règles juridiques transnationales*, J.D.I. (Clunet), n°2, 1997, p. 323-393.

9 Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, JOCE n° L. 13, 19 janvier 2000, p.12 s. V. notamment *La directive européenne n°1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques*, Gaz. Pal. du 29 octobre au 31 octobre 2000, p. 5 et s. ; égal, FNTC (sous la direction d'Eric Caprioli), *Vade-mecum juridique de la dématérialisation*, 6ème éd. 2013.

10 V. notamment E. Caprioli, *La loi française sur la preuve et la signature électroniques dans la perspective européenne*, J.C.P. éd. G, 2000, I, 224 et *Ecrit et preuve électroniques dans la loi n°2000-230 du 13 mars 2000*, J.C.P. 2000, éd. E, cah. dr. entr. n°2, Suppl. au n°30, p.1- 11.



Celle-ci se définit suivant l'article 1.2 du décret n° 2001-272 du 30 mars 2001¹¹ pris pour application de l'article 1316-4 du Code civil comme : « 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 ».

Cette signature électronique sécurisée est présumée fiable, contrairement aux autres types de signature dont la fiabilité devra être démontrée, si elle est « *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* »¹². Au vu de cette définition doivent donc être pris en compte, outre la signature électronique sécurisée, le dispositif sécurisé de création de signature électronique et le certificat électronique qualifié pour bénéficier de la présomption de fiabilité. Or, comme en dispose l'article 6 du décret du 30 mars 2001, un certificat qualifié doit être émis par un Prestataire de Services de Certification Électronique répondant à des exigences de fiabilité, et contenir au moins un ensemble d'éléments :

- 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.».*

Le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information¹³ ainsi que l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des

¹¹ J.O. du 31 mars 2001, p. 5070. V. E. A. Caprioli, *Commentaires du décret n°2001-272 du 30 mars 2001 relatif à la signature électronique*, *Revue de Droit Bancaire et Financier*, n°3, mai-juin 2001, n°105, p. 155 ; L. Jacques, *Le décret n°2001-272 du 30 mars 2001 relatif à la signature électronique*, *JCP*, éd. G, 2001, *Aperçu rapide*, p. 1601 ; F. Coupez, C. Gailliègue, *Vers une signature électronique juridiquement maîtrisée. A propos de l'arrêté du 31 mai 2002*, *Com. Comm. Elect.*, novembre 2002, p. 8 et s.

¹² Art. 2 du décret du 30 mars 2001.

¹³ J.O. du 19 avril 2002, p. 6944. V. A. Penneau, *La certification des produits et systèmes permettant la réalisation des actes et signatures électroniques (à propos du décret 2002-535 du 18 avril 2002)*, *D. 2002*, n° 26, p. 2065 ; et D & P, février 2003, p. 116, obs. E. Caprioli.

organismes qui procèdent à leur évaluation¹⁴ mettent en place le corpus de règles nécessaires pour mettre en place une signature électronique sécurisée présumée fiable en se rapportant notamment à des normes techniques précisées au niveau communautaire¹⁵.

On peut consulter la liste des prestataires qualifiés sur le site de LSTI : <http://www.lsti-certification.fr>.

On notera que tous les types de signatures électroniques sont recevables devant les tribunaux et qu'il n'est pas nécessaire de disposer d'une signature électronique sécurisée présumée fiable pour que sa valeur juridique et sa force probante soient reconnues. En effet, toute méthode ou procédé technologique qui permet de réaliser les fonctions juridiques d'identification de l'auteur, d'approbation du contenu de l'acte et de fiabilité pourra être reconnue comme remplissant les exigences légales d'une signature, que ce soit du fait de son caractère sécurisé (et reposant sur un dispositif sécurisé de création et un certificat qualifié) (en amont) ou de la démonstration devant les tribunaux de cette fiabilité pour une signature électronique simple (en aval).

3.1.2 La signature électronique en droit public

En droit privé comme en droit public, la directive 1999/93/CE a vocation à s'appliquer. L'article 3 § 7 de la directive précise en outre que « *les Etats membres peuvent soumettre des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires [...]* ».

C'est ainsi qu'en droit français, l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives¹⁶ et entre les autorités administratives est venue préciser le cadre juridique relatif aux échanges électroniques dans la sphère publique. Elle pose notamment des règles en matière de signature électronique pratiquement identiques à celles issues du droit privé.

L'article 8 de ladite ordonnance précise en effet que « *Les actes des autorités administratives peuvent faire l'objet d'une signature électronique. Celle-ci n'est valablement apposée que par l'usage d'un procédé, conforme aux règles du référentiel général de sécurité mentionné au I de l'article 9, qui permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte* ». Mais l'ordonnance crée un référentiel différent : le **Référentiel**

14 J.O. du 7 août 2004, p. 14104

15 Décision de la Commission n° 2003/511 du 14 juillet 2003 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, J.O.C.E. L. 175 du 15 juillet 2003, p. 45 et s.

16 J.O du 9 décembre 2005, p. 18896 et s ; E. A. Caprioli, *Des échanges électroniques entre les usagers et les autorités administratives d'une part, et entre ces dernières d'autre part*, JCP éd. A et CT, 2006, n°1079, p. 432 et s.



Général de Sécurité¹⁷. Il détermine les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique entre les usagers et les autorités administratives et entre les autorités administratives (notamment les fonctions d'authentification, de signature électronique, de confidentialité et d'horodatage). Des niveaux de sécurité sont proposés aux autorités administratives afin qu'elles déterminent pour leurs téléservices le niveau adapté en fonction de la sensibilité des opérations.

À ce propos, un arrêté du 15 juin 2012¹⁸ a quelque peu modifié le régime en vigueur relatif à l'emploi de la signature électronique dans le cadre des marchés publics. Cet acte réglementaire illustre parfaitement la problématique qui vient d'être exposée. En effet, les signataires par voie électronique, dans le cadre d'un marché public, sont autorisés à « *utiliser le certificat et la signature de leur choix* ». Les signataires ne seront plus contraints d'utiliser le système de signature électronique imposé par la plateforme de dématérialisation de l'acheteur public. La principale condition résultant de cette liberté en est que le certificat utilisé devra répondre aux règles du Référentiel Général de Sécurité (RGS), ou, du moins, à des conditions de sécurité équivalentes.

Afin de clore cette partie, il serait intéressant d'aborder le cas de la proposition de règlement du 4 juin 2012 supposée remplacer la directive 1999/93/CE. Ce texte de la Commission européenne permettrait d'uniformiser les transactions électroniques en Europe pour les administrations, les entreprises et les particuliers. Il serait question entre autres questions d'harmoniser les dispositions relatives aux signatures électroniques dans les différents pays membres. « *Il sera possible à une société établie dans un État membre de répondre par voie électronique à un appel d'offres public lancé par une administration d'un autre État membre sans craindre que sa signature électronique ne soit bloquée à cause d'exigences nationales spécifiques ou de problèmes d'interopérabilité* »¹⁹ .

¹⁷ Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, J.O. du 4 février 2010, p. 2072 ; Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques, J.O. du 18 mai 2010, p.9152.

¹⁸ Arrêté du 15 juin 2012 relatif à la signature électronique dans les marchés publics, J.O. du 3 juillet 2012.

¹⁹ Proposition de Règlement préc. § 3.2.a, p.4.

3.2 Les évolutions juridiques et jurisprudentielles de la signature électronique

3.2.1 Applications pratiques de la signature électronique

Au fil des jurisprudences, la recevabilité en preuve de signatures fondées sur des moyens technologiques a pu être affinée, notamment autour des notions d'identification et de fiabilité²⁰. Par exemple, une décision de la Cour d'appel de Fort-de-France du 14 décembre 2012²¹ a pu estimer que le scan d'une signature manuscrite n'avait pas la même force probante qu'une signature manuscrite. Les juges ont estimé que, d'une part, en l'absence de production d'un certificat, la signature en question ne saurait être considérée comme une signature électronique. D'autre part, la signature scannée « *est insuffisante pour s'assurer de l'authenticité de son engagement juridique comme ne permettant pas une parfaite identification du signataire* ». Cette décision doit être approuvée. Il est, en effet, tout à fait possible à quiconque qui disposerait du fichier informatique comportant le scan de la signature manuscrite, de reproduire celle-ci indéfiniment. Il n'y a dès lors aucune garantie que la signature émane réellement de son auteur. Donc les conditions de fiabilité, d'identification... ne sont pas respectées.

Dans cette même lignée, la Cour de cassation a déjà pu estimer qu'une lettre de licenciement sur laquelle figurait une signature manuscrite numérisée était irrégulière et ne disposait par conséquent d'aucune valeur probatoire²².

Un exemple de prise en compte de la (vraie) signature électronique par un arrêt de la Cour d'appel de Nancy²³ qui est venu se prononcer non pas sur la fiabilité de la signature, mais sur la validité de la preuve du contrat de crédit à la consommation ayant fait l'objet d'une signature électronique. La Cour est ici venue infirmer le jugement du tribunal d'Epinal du 12 décembre 2011 qui avait considéré comme forclos le délai d'une action en paiement d'un établissement de crédit. Brièvement en l'espèce, la société Carrefour Banque avait consenti un troisième avenant à un crédit renouvelable, établi pour la première fois sous forme électronique (les précédents étant sous forme papier). Après plusieurs échéances restées impayées, la société de crédit assigna l'emprunteur en justice pour demander le remboursement des sommes et produisait pour justifier du dernier avenant le document « *fichier de preuve de la transaction* ». Le tribunal d'instance d'Epinal avait écarté cet élément en affirmant que « *le document « fichier de preuve de la transaction » est insuffisant pour s'assurer non*

²⁰ *En ce sens, à propos d'une signature scannée (non admise) pour la signature d'une déclaration d'appel, CA Besançon, 20 oct. 2000, JCP éd. G, 2001, II, 10606, p. 1890 et s., note E. A. Caprioli et P. Agosti ; confirmé par la Cour de cassation le 30 avril 2003, Bull. civ. 2003, n°118, p. 101 et s. (disponible sur le site : www.legifrance.gouv.fr)*

²¹ CA Fort-de-France, ch. civ. 14 déc. 2012, n° 12/00311 : JurisData n° 2012-033784 ; E. A. Caprioli, *Une signature scannée ne vaut pas signature électronique, Communication Commerce électronique n° 5, Mai 2013, comm. 60.*

²² Cass. soc. 17 mai 2006, no 04-46.706.

²³ CA Nancy, ch. 2, 14 févr. 2013, n° 12/01383 : JurisData n° 2013-004062 ; E. A Caprioli, *Première décision sur la preuve et la signature électronique d'un contrat de crédit à la consommation, JCP éd. G, 2013, 497, p.866 à 869 et Comm. Com. Electr. 2013, Juin, Etude 11, p. 13 à 17.*



seulement de l'engagement de Monsieur X puisqu'aucun élément de la prétendue signature électronique ne permet de faire le lien entre l'offre de prêt non signée et le document produit, en l'état simple fichier imprimé sans garantie d'authenticité, ni justification de la sécurisation employée. ». A la vérité, c'est la preuve du contrat qui avait été mal présentée aux juges²⁴. Sur la base de cette constatation, le Tribunal d'instance jugeait l'action de la société de crédit forclosé. La Cour d'appel de Nancy dans son arrêt du 14 février 2013, se fondant sur les dispositions de l'article 1316-4 du code civil et du décret n°2001-272 du 30 mars 2001, dispositions relatives à la signature électronique, a relevé que la société de crédit « produit aux débats le fichier de preuve de la transaction émis par l'autorité de certification [...]. La mention du numéro de l'avenant sur le fichier de preuve permet de vérifier que c'est bien cet avenant qui a été signé électroniquement par monsieur X. Par conséquent, la preuve de la signature par monsieur X de l'avenant du 4 septembre 2008 est rapportée, contrairement à ce qu'a jugé le tribunal. ».

Notons qu'à aucun moment, le client absent pendant le litige et non représenté n'a contesté la fiabilité de la signature électronique, ni dénié sa signature. Carrefour banque a donc bénéficié d'une présomption de fiabilité étonnamment concédée (puisque sans contradicteur).

3.2.2 Le projet de règlement du 4 juin 2012 comme solution au problème d'interopérabilité en Europe

Il faut le reconnaître, la directive 1999/93/CE a largement contribué à une certaine harmonisation des pratiques relatives à la signature électronique sur le marché intérieur. Mais des disparités persistent rendant « les transactions électroniques transnationales impossibles »²⁵. La Commission européenne reconnaît d'ailleurs l'obsolescence de ce texte. « Des divergences dans la mise en œuvre au niveau national dues à des différences d'interprétation de la directive par les États membres, le recours de fait à une dérogation pour les applications du secteur public, des normes dépassées et des obligations mal définies en matière de contrôle donnant lieu à des problèmes d'interopérabilité transnationale, à une situation fragmentée dans l'UE et à des distorsions dans le marché intérieur »²⁶. Cette directive ne permettait clairement pas une utilisation transnationale sûre et fiable de la signature électronique.

Dans un souci de remédier à cette défaillance, la Proposition de règlement du Parlement européen et du Conseil sur l'identification électronique et les services de

24 V. E. Caprioli sur la décision du tribunal d'instance d'Epinal, Comm. Com. Electr. 2013, Avril, com. 47.

25 Signature électronique : projet de règlement de la Commission européenne, JCP E et A, n° 24, 14 Juin 2012, act. 380.

26 Document de travail des services de la Commission, résumé de l'analyse d'impact accompagnant la proposition de règlement du parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (§ 2 et s de la Proposition de Règlement).

confiance pour les transactions électroniques au sein du marché intérieur²⁷ du 4 juin 2012 prévoit une harmonisation plus poussée, renforçant l'interopérabilité entre Etats en établissant « *des règles et pratiques communes* ». Seule la voie du règlement était pertinente pour parvenir à une interopérabilité concrète. Le choix d'abroger la directive par un règlement est d'autant plus pertinent que celui-ci aura vocation à s'appliquer directement dans les législations internes des Etats membres. Le règlement ne nécessite pas de lois de transposition pour prendre effet dans les ordres juridiques des Etats. Dans un autre registre, au travers de cette proposition de règlement, les niveaux de fiabilité semblent avoir été revus.

En plus de la signature électronique et la signature électronique avancée, le texte du 4 juin 2012 fait expressément état de la signature électronique qualifiée. Il serait question, au regard de l'article 3.8, « *d'une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié et qui repose sur un certificat qualifié de signature électronique* ». Cette formulation ressemble étrangement à celle de l'article 2 du décret du 30 mars 2001. Les conditions de fiabilité telles que décrites dans les articles 21 et suivant du règlement font de la signature électronique qualifiée le *fondement juridique et technique pour l'interopérabilité dans le marché européen de la confiance*. Les normes relatives à la fiabilité seront identiques dans les Etats, leur permettant ainsi d'avoir un même socle juridique. L'interopérabilité ne sera ainsi plus entravée par des différences entre les législations nationales, au moins sur le plan de la signature électronique qualifiée. Enfin, le texte aborde également la signature électronique qualifiée sous l'angle de la preuve. Les « *services de validation et de conservation* » des signatures électroniques qualifiées ont été pris en compte aux articles 26 et 27. Cela constitue une avancée remarquable comparativement à la directive 1999/93/CE qui ne prenait en compte que la phase d'établissement de la signature électronique. De plus, outre la coordination et la publication des identités électroniques régaliennes, le projet traite de l'horodatage, de l'authentification de sites web, des sceaux électroniques, des documents électroniques et de la responsabilité des prestataires de services de confiance.

²⁷ PE et Cons. UE, prop. de règl. COM(2012) 238 : <http://ec.europa.eu>. - V. notamment Th. Piette Coudol, *Une législation européenne pour la signature électronique* : RLDI juill. 2012, n° 2838. ; É. A. Caprioli et P. Agosti, *La régulation du marché européen de la confiance* : Comm. Com. Electr. 2013, étude 3.

CAS PRATIQUES

Signature électronique et délégation des pouvoirs bancaires

BNP Paribas Guadeloupe dématérialise la signature client

La signature électronique des Factures

La signature électronique des attestations

Signer et transmettre en ligne les contrats et documents officiels des transactions en capital : le service Eclosing

Les cartes de professionnel de la Santé (CPS)

Vosgelis, Office de Logement Social, dématérialise l'ensemble du processus de la commande publique

Les cartes de Chronotachygraphe Numérique

AXA déploie la signature électronique d'assurance-vie sur tablette tactile

Huissiers de Justice : l'acte authentique sur support électronique et la signification électronique

Dématérialisation des mandats bancaires par l'expert-comptable en tant que tiers de confiance sur jedeclare.com

Signexpert – l'identité numérique de l'Expert-Comptable

Infogreffé – des démarches administratives et légales simplifiées grâce à la signature électronique

Dict.fr – les déclarations préalables aux travaux : la sécurité informatique au service de la sécurité des chantiers



Signature électronique et délégation des pouvoirs bancaires

Dirigeants d'entreprises, trésoriers et comptables observent une dématérialisation croissante des échanges avec les banques. La signature électronique y apporte de véritables gains.

POURQUOI ?

Parmi les responsabilités des dirigeants, deux activités sont essentielles pour assurer une bonne maîtrise des risques à savoir :

- 1/Gérer les pouvoirs bancaires et
- 2/ S'assurer que les ordres de paiement (virements de salaires, règlement des factures fournisseurs, paiement des taxes et impôts...) sont signés (et si nécessaire contresignés) par les personnes dûment autorisées. Ces tâches peuvent s'avérer délicates et très coûteuses notamment lorsqu'elles s'adossent à des processus traditionnels sous forme papier ou lorsque l'environnement est complexe et changeant (fusion, acquisitions, changement de dirigeants....).

QUI ?

Le dirigeant, le directeur financier et/ou les responsables trésorerie ont besoin de suivre tout changement dans la chaîne de délégation de pouvoirs bancaires afin de s'assurer que ces changements sont bien pris en compte au niveau de la chaîne des paiements. Il est non seulement essentiel que l'information soit fiable mais également qu'elle soit transmise et traitée rapidement.

COMMENT ?

L'utilisation de la signature électronique permet une dématérialisation complète de cette procédure et permet d'assurer la traçabilité et la conservation des données susceptibles d'être exigées comme justificatifs et comme preuves.

Une clé USB contenant un certificat (clé privée) est remise en main propre au signataire habilité (Trésorier, Dirigeant de filiale ou d'établissement,...). Ce dernier, après avoir vérifié la conformité des ordres avec sa délégation de pouvoir et contrôlé la justification des paiements, peut alors signer électroniquement les fichiers de paiement via une application qui les transmet à la banque.

« La signature électronique entre dans la sphère des pouvoirs bancaires de manière progressive dans une logique de maîtrise des risques opérationnels. »

LES GAINS

Au niveau des processus, la signature électronique permet la dématérialisation complète et évite les ordres fax ou courrier disjoints des fichiers de paiement. Elle permet ainsi des échanges fiables, plus rapides et une meilleure prise en charge par la banque.

Pour les signataires, la signature électronique permet plus de souplesse : ainsi un dirigeant peut signer les ordres (virements de salaires par exemple) où qu'il se trouve.

Au plan des risques, elle permet d'éviter des pertes financières potentiellement conséquentes lorsque, par exemple, un virement important est effectué vers le compte d'un fraudeur, ou, lorsque, au contraire, un ordre de virement n'est pas effectué parce qu'un nouveau signataire autorisé n'est pas encore connu de la banque.

BNP Paribas Guadeloupe dématérialise la signature client



Précursor dans le secteur bancaire, la filiale du groupe améliore depuis 2012 son Entrée en Relation Client en faisant appel à des technologies novatrices pour réduire les coûts de traitement et accélérer la gestion des dossiers. La signature du client est dématérialisée avec l'utilisation d'une tablette de signature capturant la signature manuscrite électronique, dans un process hautement sécurisé, validant les pré-requis légaux français.

POURQUOI ?

- Réduction des coûts de traitement papier et uniformisation efficiente de l'archivage des documents
- Amélioration de la sécurité des documents
- Accessibilité en temps réel aux documents signés et accélération des traitements des dossiers clients

COMMENT ?

- Sous contrôle du vendeur, une application web crée le contrat.
- Le client appose sa signature manuscrite à l'aide d'une tablette de signature.
- Une signature électronique à la volée vient parfaire l'acte, qui est alors archivé chez deux Tiers de Confiance.
- Les données graphologiques de la signature manuscrite sont conservées et peuvent être vérifiées en cas de contestation.

QUI ?

- Contractualisation en face à face en agence bancaire
- Force de vente bancaire focalisée sur le conseil client
- Clientèle privée et entreprises

LES GAINS

- Facilité des recherches et du travail des équipes bancaires
- Sécurisation de l'accès aux données et de la conservation des documents
- Forte réduction des coûts
- Automatisation des traitements métier
- Prise en main par les forces de vente intuitive.
- Forte acceptation client, l'outil de capture de signature s'inscrivant dans un acte habituel
- Image novatrice pour la banque.

« Chaque transaction s'affiche sur l'écran de la tablette de signature. Pour confirmer les transactions, le client est invité à apposer sa signature directement sur l'écran. Une fois la signature apposée, le document ne peut plus être modifié. Si nécessaire, une copie papier peut être fournie au client », commente Éric Guillaume, Responsable de secteur de centre informatique au sein de la BNP Paribas Guadeloupe. « Ce gain de temps est très appréciable par les forces de vente, cela leur offre une plus grande disponibilité afin d'échanger avec leur client qu'à effectuer des tâches administratives »



La signature électronique des Factures

L'entreprise SPORTPULSION avait un besoin évident à partir d'un seul fichier d'édition d'envoyer ses factures à l'ensemble de ses clients.

POURQUOI ?

La facture reste un document qui doit suivre obligatoirement des règles précises en papier ou en électronique.

Les 10 000 factures annuelles étaient toujours émises par courrier par manque d'informations et par crainte d'investissement important.

COMMENT ?

Une solution globale a été retenue car elle répondait aux trois besoins simplement et rapidement.

Pour l'ensemble des émissions de factures, un certificat de personne morale du marché a été retenu : la signature électronique est donc un cachet.

La solution récupère le fichier unique pour découper, horodater, signer, archiver et traiter chaque facture pour SPORTPULSION.

Puis en fonction du destinataire, la méthode demandée par le client destinataire est appliquée : PDF signé, courrier poste classique ou transfert FTP.

QUI ?

Après consultation auprès de la comptabilité et du service informatique, la méthode actuelle constituait à éditer un seul fichier d'impression.

Suite à une enquête client, le besoin se divisait en trois types de destinataires :

- PDF avec signature électronique,
- Courrier classique et transfert FTP vers leur plus gros client,
- Intersport.

LES GAINS

Les gains directs sont les délais de réception des factures par les destinataires qui sont maintenant immédiats et les coûts de transmission par facture qui sont passés de 2,10 € HT à 0,85 € HT dans le cadre d'un envoi poste et à 0,27 € HT pour un envoi dématérialisé fiscalement avec horodatage, signature, archivage et GED 10 ans.

L'investissement de base de la solution étant de 750 € HT, le ROI a été réalisé en un seul mois !

« La solution intègre en automatique, une signature électronique qualifiée, délivrée par une autorité de confiance permettant de garantir notre identité et l'intégrité de nos factures dématérialisées » Laurence Lambert, responsable administratif et financier, SPORTPULSION.

Les entreprises doivent donner périodiquement des attestations à leurs donneurs d'ordre : d'un casse-tête irrésoluble du temps des échanges papier, c'est devenu très simple grâce à la signature électronique.

POURQUOI ?

La lutte contre la fraude, qu'elle soit sociale ou fiscale, fait peser sur les donneurs d'ordre de multiples contraintes réglementaires qui engagent leur solidarité financière, leur image et la responsabilité pénale de leurs dirigeants. Dans ce contexte, les coûts administratifs de collecte, de contrôle et de saisie des informations et, au sens large, la gestion de l'information concernant les fournisseurs peuvent être colossaux. Le service e-attestations a pour fonction la collecte dématérialisée des justificatifs exigés par le Code du travail.

COMMENT ?

Le service se voulant un facilitateur de la collecte des documents, et s'adressant à des fournisseurs de toutes natures (groupes internationaux, PME, artisans...), le choix a été fait d'intégrer le module de signature électronique au cœur du service, dans la page de dépôt de chaque pièce, sous la forme de signature électronique à la volée.

Une convention de preuve acceptée formellement par les utilisateurs du service renforce la valeur juridique des signatures ainsi réalisées sur la base de l'identité numérique du signataire gérée dans la plate-forme.

Les documents signés sont automatiquement déposés pour archivage dans un coffre-fort électronique, qui garantit leur disponibilité et leur intégrité.

Grâce à l'usage du format de signature électronique PAdES, inclus visuellement dans les documents PDF, la vérification de la signature peut être faite par le donneur d'ordre ou les instances de contrôle d'un simple coup d'œil.

QUI ?

Le service, fourni en mode SaaS, permet la transmission de justificatifs signés électroniquement entre les fournisseurs et leurs donneurs d'ordre.

La signature électronique y est employée pour garantir la provenance et l'intégrité des documents, et pour marquer l'engagement des fournisseurs sur l'exactitude des informations transmises.

LES GAINS

La signature électronique permet d'obtenir des originaux électroniques, dont la provenance et l'intégrité sont garanties. Elle est une source importante d'économies en temps passé sur la constitution des dossiers de conformité, tant pour les fournisseurs que pour les donneurs d'ordre.

Bien plus, elle rend possible le respect des obligations légales, jusqu'ici trop souvent négligé du fait de la complexité d'obtention des pièces et de la charge de travail induite. Elle réduit donc le risque juridique correspondant.

« Je gagne du temps du temps et je suis plus sereine »
Delphine Verron, directrice générale de Labo Electro France, utilisatrice de la solution.

Signer et transmettre en ligne les contrats et documents officiels des transactions en capital : le service Eclosing

La société Eclosing a été fondée pour dématérialiser les processus contractuels des cabinets d'avocats d'affaires, notamment dans le cadre de closings de transactions financières. Ce savoir-faire lui a permis de développer une plateforme technologique de signature électronique dédiée à la signature et l'échange de documents pour les professions réglementées.

POURQUOI ?

Pouvoir piloter en ligne les transactions financières des entreprises (augmentations de capital, gestion de trésorerie, cessions de titres...) conformément aux meilleures pratiques du capital investissement.

Pouvoir constituer un espace d'échanges sécurisé (data room) et organiser la signature de tout document (contrats, courriers officiels) par toutes les parties impliquées.

Quel intérêt peut avoir une plate-forme de dématérialisation des opérations de financement ? Apporter un support qui facilite et accélère les transactions en capital et diminue les frais habituels pour ce type d'opérations.

COMMENT ?

Grâce aux services intégrés, fournis en mode SaaS, de data room électronique et de signature numérique de tous les contrats liés aux transactions financières (accords de confidentialité, contrats d'investissement, engagements d'apports, pactes d'actionnaires...).

Grâce à son partenariat avec des autorités de certification, la plateforme de closing permet la signature électronique à valeur probante de tout document : contrat, lettre de mission, bulletin de souscription, procès-verbaux, etc.

QUI ?

Dans le cadre de transactions en capital, les cédants, les cessionnaires et leurs conseils respectifs (avocats, experts-comptables...) sont soumis à des législations et meilleures pratiques strictes en termes d'échéancier et de documentation à signer.

Ces différents intervenants échangent donc de nombreux documents confidentiels (data room) et participent à la signature d'actes selon une séquence bien définie (engagement de confidentialité, lettre d'intention, contrats, procès-verbaux...).

LES GAINS

- Facilitation des transactions grâce à la dématérialisation des opérations de due diligence, de négociation et de closing.
- Gestion facilitée et accélération des transactions internationales grâce à des outils multilingues.
- Diffusion des meilleures pratiques du capital investissement.
- Réduction des coûts de transaction et de réalisation.
- Sécurisation des documents et des process.

« Grâce à ses solutions de data room et de signature électronique, Eclosing nous permet de proposer des services complémentaires à nos clients. Nos équipes peuvent désormais organiser la transmission sécurisée de documents volumineux et la signature en ligne de tout acte depuis un simple ordinateur connecté à internet. »
(Philippe & Partners, cabinet d'avocats d'affaires international).



Les cartes de professionnel de la Santé (CPS)

La carte CPS ou carte de professionnel de santé est une carte d'identité professionnelle électronique. Elle constitue le maillon final d'une chaîne de confiance qui permet à son titulaire d'attester de son identité et de ses qualifications professionnelles.

POURQUOI ?

La CPS est la clé d'entrée de la e-santé d'aujourd'hui et de demain. Elle permet aux professionnels de santé de :

- **s'identifier et éviter ainsi une usurpation de leur identité** (via le processus d'authentification) ;
- **apposer leur signature électronique** sur des documents ;
- **créer, alimenter et consulter le Dossier Médical Personnel** de leurs patients ;
- réaliser des actes médicaux à distance (télémédecine) ;
- **utiliser la messagerie sécurisée** des professionnels de santé.

Grâce à la **technologie sans contact**, elle peut être utilisée pour d'autres applications comme l'accès à des locaux.

COMMENT ?

Elle est attribuée automatiquement et gratuitement par l'Agence des Systèmes d'Information partagés de Santé (ASIP) après certification de l'identité par les autorités compétentes (Ordres et services de l'Etat) et enregistrement dans le répertoire partagé des professionnels de santé (RPPS). Cette Agence a notamment comme mission de définir les référentiels de sécurité et d'interopérabilité permettant l'échange et le partage des données personnelles de santé.

Ainsi, les professionnels disposent d'une seule carte, qui leur permet de signer électroniquement les feuilles de soins électroniques, mais également la dématérialisation des lettres aux confrères, ou encore les informations médicales de leur patient dans les Dossiers Médicaux Partagés (DMP)...

Désormais inscrite dans la pratique quotidienne des professionnels de santé, elle permet de supprimer chaque année plus d'un milliard de feuilles de soins papier, au plus grand bénéfice des assurés sociaux. Projet en avance sur ton temps, elle constitue, dans le cadre du projet de réglementation européenne, le modèle qui sera mis en œuvre dans l'ensemble des Etats de l'Union.

QUI ?

Selon la profession exercée et le niveau de responsabilité du porteur :

- la CPS pour les professions de santé réglementées ;
- pour les professionnels non réglementés et salariés d'une structure de soins :
- la CDE pour les responsables de structures de soins ;
- la CPE pour les personnels des établissements de soins ;
- pour les professionnels non réglementés et salariés de structures autorisées ;
- la CDA pour les responsables de structures ;
- la CPA pour les personnels de structure.

LES GAINS

La carte de professionnel de santé constitue un instrument essentiel du dispositif de sécurité des systèmes d'information de santé en sécurisant les échanges, et permet de garantir, via la signature de professionnel, le contenu et l'origine de l'information notamment pour permettre le partage des données médicales personnelles pour améliorer la qualité du système de santé, mais également la suppression du milliard de feuilles de soins.

Par ailleurs, sa conception permet de tenir compte des évolutions technologiques et des usages sans impact pour le professionnel de santé.

Vosgelis, Office de Logement Social, dématérialise l'ensemble du processus de la commande publique

Précurseur dans le secteur immobilier, Vosgelis a mis en œuvre une solution de dématérialisation de l'ensemble des échanges entre l'office et ses fournisseurs, au moyen d'une signature électronique, à partir de tout terminal informatique ou mobile, dans un processus sécurisé, respectant le cadre réglementaire aussi bien pour les collectivités publiques que les sociétés privées.

POURQUOI ?

- Simplifier et fiabiliser le processus de gestion de commandes, validation du service fait ainsi que la facturation, aussi bien pour les fournisseurs que pour l'organisme.
- Réaliser des économies financières.

COMMENT ?

- Mise en place d'une autorité de certification permettant de délivrer des certificats électroniques à tous les acteurs qu'ils soient physiques ou processus serveurs (fournisseurs, techniciens Vosgelis, service des achats, service financier, SI achats, SI comptable, etc.).
- Mise en place d'un parapheur permettant de faire signer à la volée, aussi bien sur un PC que sur une solution mobile ou Smartphone, les documents à tout moment. Ainsi le plombier valide la réalisation directement sur le chantier grâce à son Smartphone. Il n'a plus besoin d'aller au bureau.
- Possibilité de signature électronique à l'aide d'un certificat sur support physique (par exemple RGS (**)).
- Mise en place d'un siège social électronique permettant de délivrer tous les courriers simples ou recommandées avec AR dans le respect de la réglementation.
- Mise en place de l'auto-facturation.

QUI ?

- Les techniciens des agences qui émettent les commandes et vérifient le service fait.
- Les fournisseurs qui doivent réaliser les commandes dans les délais et fournir des attestations de réalisation des prestations.
- Les services comptables Vosgelis ou fournisseurs.

LES GAINS

- Diminution du temps de prise en compte des commandes par les fournisseurs (travaux urgents)
- Diminution du délai de règlement car le fournisseur valide sa prestation directement sur son site sans avoir à repasser au bureau
- Respect des procédures réglementaires car tous les documents qui doivent être signés, le sont.
- Simplification comptable pour l'office car grâce à l'auto-facturation l'organisme a la certitude que la facture correspond à la commande, d'où suppression des contrôles, et pour le fournisseur car il n'a plus à générer sa facture
- Mise à disposition du fournisseur d'un coffre-fort électronique lui permettant d'archiver tous les documents signés relatifs à la commande (appel d'offre, commande, attestations factures, ...)

La dématérialisation des échanges dans le processus de la commande et de facturation est la suite logique au processus de dématérialisation des marchés publics

Les cartes de Chronotachygraphe Numérique



La carte de Chronotachygraphe numérique, délivrée aux chauffeurs routiers et leurs employeurs permet l'enregistrement infalsifiable des temps de conduite.

POURQUOI ?

Dans une volonté de lutte contre la fraude, et d'harmonisation des politiques sociales dans le secteur du transport, le Règlement (CE) n° 2135/98 fixe les règles applicables au contrôle des temps de conduite et de repos sur la base d'un système de carte à puce et du boîtier électronique installé dans les véhicules (VU), ainsi que les modalités de contrôle et de garantie de l'interopérabilité.

Les temps de conduite enregistrés dans la puce et dans le VU sont consultables par l'entreprise pour établir la paye, et par l'ensemble des corps de contrôle dans l'espace européen.

COMMENT ?

Les cartes sont délivrées, après vérification de validité du permis de conduire du demandeur et interrogation de non existence d'une carte valide dans un autre Etat, par une Autorité compétente au sein de chaque Etat agréé par une autorité européenne.

La signature électronique est fondamentale, tout d'abord lors du calibrage du boîtier : à la fin de ces opérations, le technicien de l'atelier va signer électroniquement l'ensemble des informations.

Lors de la conduite du véhicule, le conducteur introduit sa carte dans le boîtier, cette dernière va permettre ainsi de signer, automatiquement les temps de conduite et de repos enregistrés.

Cette carte est devenue un outil parfaitement intégré dans la pratique des conducteurs routiers de marchandises et de voyageurs. Cette profession très réglementée bénéficie d'un modèle de carte complètement interopérable en Europe. Sa prochaine révision en 2017 devrait intégrer des moyens d'authentification et de signature standard afin d'autoriser encore plus de processus dématérialisés liés au Transport routier. A ce jour, plus de 11 millions de conducteurs européens sont dotés de cette carte ; en ce qui concerne la France, 700 000 conducteurs en disposent, ainsi que 50 000 entreprises.

QUI ?

Conducteur : chauffeurs, de PL de plus de 3,5T et de voyageurs (plus de 9 personnes).

Entreprise : sociétés de Transports afin de récupérer les données d'activités.

Atelier agréé : seuls les ateliers agréés ont la possibilité d'installer et d'assurer le calibrage du boîtier au véhicule associé.

Contrôleur : polices, douanes et contrôleurs des transports terrestres.

LES GAINS

La signature électronique a permis la sécurisation des données opposables. Le bénéfice de ce dispositif est multiple : amélioration de la sécurité routière (contrôle routier plus rapide et non discutable, respect du temps de conduite et de repos), égalité concurrentielle (harmonisation européenne).

L'ensemble du dispositif mis en œuvre a permis de créer la confiance de l'ensemble des acteurs, mais également les conditions d'appropriation des professionnels de l'espace européen.



© bloomua - Fotolia.com

AXA déploie la signature électronique d'assurance-vie sur tablette tactile

Le n°1 mondial de l'Assurance a équipé l'ensemble de son réseau commercial salarié itinérant de tablettes tactiles dotées d'une solution de signature électronique « dans le cloud » basée sur des cartes à puce virtuelles. Ainsi, chaque commercial en situation de vente à domicile peut récolter les informations de son client, présenter les produits, élaborer le contrat et recueillir la signature électronique du nouvel assuré entièrement sur sa tablette.

POURQUOI ?

Ce projet dénommé i-Nov a pour l'objectif de fournir aux commerciaux qui travaillent en majorité au domicile des clients un nouvel outil de travail composé :

- d'une tablette connecté en Edge/3G ou WIFI
- d'un CRM en cloud computing
- d'une application soutenant la démarche de vente dématérialisée
- d'outils de simulations produits
- d'une médiathèque de brochures produits et de vidéos

La signature électronique a pour objectif de permettre la conclusion du dossier directement sur la tablette.

COMMENT ?

- Le client visualise sur la tablette du commercial les documents qu'il doit signer.
- Le client trace sa signature manuscrite du bout du doigt sur la tablette comme il a l'habitude de faire avec un stylo.
- La conformité des informations saisies avec celles de la pièce d'identité du client, transmise via la tablette, est vérifiée.
- Un certificat au nom du client est généré dans la carte à puce virtuelle située dans le cloud.
- La signature électronique est réalisée grâce à ce certificat.

« La signature électronique est la dernière pièce à l'édifice de notre solution de vente à domicile sur tablette. Elle nous a permis d'atteindre une sécurité juridique maximale dans ce contexte et nous offre une continuité à tous les niveaux : fluidité du processus commercial, rapatriement automatique des contrats signés dans le SI, archivage numérique des documents, suppression totale de la composante papier, etc. A tous points de vue, c'est un succès. »

Franck Mouchel, DSI d'AXA France

QUI ?

- Les 3000 commerciaux salariés d'AXA France qui commercialisent majoritairement des produits Épargne, Retraite, Prévoyance ainsi que des produits bancaires.
- Les signataires à leur domicile qui sont essentiellement des particuliers et des professionnels.

LES GAINS

- Un gain de temps sur la démarche de vente avec 20 minutes en moyenne de gagnées en rendez-vous clientèle.
- Une automatisation du processus d'acquisition client avec rapatriement des contrats dans le SI immédiatement après signature.
- Une baisse des frais généraux (plaquettes, courrier, impressions, numérisation etc...)
- Un symbole de modernité favorable à l'image de marque de l'assureur.
- Un niveau de sécurité juridique rarement atteint dans un contexte de contractualisation électronique BtoC.



Huissiers de Justice : l'acte authentique sur support électronique et la signification électronique

Le 3 décembre 2008, la première minute d'un acte authentique d'huissier de justice sur support électronique - signé avec un certificat qualifié - a été déposée sur le Minutier Central de la profession, conformément aux dispositions du décret du 10 août 2005.

POURQUOI ?

La mise en place de **l'acte authentique sur support électronique** répond à une demande formulée par les huissiers de justice et les notaires, en décembre 1999, lors des travaux relatifs à l'élaboration de la loi du 13 mars 2000.

Les modes d'établissement et de conservation des actes authentiques sur support électronique des huissiers de justice – officiers Publics et Ministériels – ont été précisés par un décret du 10 août 2005.

COMMENT ?

Après visualisation à l'écran de l'acte au format PDF/A, l'Huissier de Justice muni d'un certificat qualifié sur clé USB, y appose sa signature électronique.

L'original de l'acte sur support électronique est conservé dans un **Minutier Central**, dans des conditions permettant d'assurer son intégrité et sa pérennité.

La **signification « électronique »** s'effectue via une plate-forme dédiée, dénommée SECURACT.

Elle permet à l'huissier de justice de délivrer des actes de procédure par voie dématérialisée en garantissant la sécurité, la confidentialité et l'intégrité de la transaction.

QUI ?

3.200 huissiers de justice Français, répartis dans **1.800** études, qui signifient 10 millions d'actes par an.

LES GAINS

Sécurité juridique établie par un Officier Public et Ministériel, dont l'apposition de la signature électronique confère l'authenticité à l'acte juridique sur support électronique.

Garantie de l'intégrité dans l'espace et dans le temps.

Réduction du support papier entraînant une diminution de la volumétrie des archives

Raccourcissement des temps d'accès à l'information, par la facilitation de la consultation des actes et l'accélération de leur mise à disposition.

Économies d'énergie, d'occupation d'espace, réactivité et efficacité accrues.

Octobre 1999 : premiers tests de signature électronique dans la profession

Décembre 2008 : premier dépôt d'un acte authentique sur support électronique dans le Minutier Central

Novembre 2012 : première signification électronique d'un acte authentique

Dématérialisation des mandats bancaires par l'expert-comptable en tant que tiers de confiance sur jedeclare.com

Jusqu'à présent, pour dématérialiser la récupération des relevés bancaires, il fallait commencer par un mandat papier ! Maintenant, avec sa signature électronique Signexpert, l'expert-comptable, en tant que Tiers de Confiance, peut mettre en œuvre une « vraie dématérialisation » du mandat tout électronique à destination des banques.

POURQUOI ?

Jedeclare.com, première plate-forme d'échanges numériques au service des experts comptables, intègre Signexpert, permettant au titulaire du compte la dématérialisation de divers documents, dont le mandat pour la collecte des relevés bancaires.

Ce mandat, signé par le client et l'expert-comptable donne autorisation à l'expert-comptable de collecter, pour le compte de son client, les relevés bancaires.

Jusqu'à présent, pour la majorité des banques, ce mandat était en papier, signé par le titulaire du compte et son expert-comptable, puis remis à la banque pour vérification.

Désormais, avec Signexpert, l'expert-comptable peut dématérialiser totalement le processus : il scanne le mandat papier signé par le client et le signe, certifiant ainsi la signature du client avec sa signature électronique.

Le portail jedeclare.com, se charge du transfert sécurisé vers toutes les banques et de son archivage.

COMMENT ?

Détails du processus :

- le mandat est envoyé sur le portail jedeclare.com au format PDF ;
- sur le portail jedeclare.com, le document est signé en ligne par l'expert-comptable ;
- après signature électronique, le mandat est adressé à la banque, dans l'espace sécurisé du client, puis archivé, l'original papier du mandat étant conservé au sein du cabinet.

QUI ?

Ce dispositif est déployé avec plusieurs banques.

Seul l'expert-comptable est habilité à signer le document numérisé.

Il s'assure et se porte garant de la signature effective du mandat papier par son client.

A noter que le mandat papier, signé par le client et l'expert-comptable, reste l'original, conservé au sein du cabinet. C'est cet original papier qui sera présenté en cas de contestation sur le fond.

Une dématérialisation totale, dès le début du processus, peut être envisagée, sous réserve que l'entrepreneur lui-même soit titulaire d'une signature électronique acceptée par le réseau bancaire. En effet, Signexpert est référencée PAC et EBICS.

LES GAINS

- Traçabilité.
- Gestion des incidents par le back office de Jedeclare.com à partir des archives.
- Vitesse de mise à disposition.
- Fiabilité des signatures.
- Partage de l'information entre les trois parties...

« La signature électronique m'a permis d'accélérer les processus au sein de mon cabinet. Je collecte les mandats de mes clients et en un clic, ils sont envoyés sur jedeclare.com et simultanément adressés à la banque, la bonne agence, voire le bon service, sans contrainte de mon côté. »

Cabinet Sogarex

La dématérialisation des échanges entre les entreprises implique la nécessité de sécuriser les flux et documents numériques entre chacun des acteurs. Au premier rang des acteurs de ces échanges se trouve l'expert-comptable. Au-delà de son rôle opérationnel de producteur de document, il est aussi conseil et représente l'entreprise dans de nombreuses circonstances. La sécurisation de son identité numérique est vitale !

POURQUOI ?

L'expert-comptable est un professionnel intervenant en qualité de conseil auprès des entreprises, associations et structures publiques. Inscrit à l'ordre des experts-comptables, il est soumis à des règles strictes de contrôle qualité et d'assurance.

Pour protéger l'entreprise cliente d'une contrefaçon éventuelle, il est important de lui permettre de distinguer les vrais experts comptables des faux agissant illégalement, de garantir l'intégrité des documents produits par le professionnel et faire bénéficier à tous les tiers destinataires directement ou indirectement d'un document certifié par l'expert-comptable avec la preuve de son origine, de son intégrité, voire de sa date de création.

COMMENT ?

Pour son identité électronique, l'Ordre a fait le choix d'un certificat de signature RGS***, un certificat authentification RGS** et d'un outil de signature électronique multi-format et multi-documents, de telle sorte que le professionnel soit immédiatement opérationnel. Les éditeurs professionnels ont intégré des modules de signature dans leurs suites logicielles, permettant une utilisation naturelle et automatique de la signature électronique. Enfin, les certificats Signexpert sont en cours d'intégration sur les plates-formes de services à destination des experts-comptables.

« Pour la profession des experts-comptables, Signexpert est une révolution. Pour la première fois, nous sommes reconnus et identifiés directement en tant que professionnels sur de nombreux portails, par nos clients et partenaires. Progressivement notre identité numérique nous permettra de lutter contre l'exercice illégal, protégeant ainsi les entreprises. »

QUI ?

La signature électronique Signexpert est diffusée exclusivement aux experts-comptables inscrits à l'Ordre. Signexpert a été conçue pour avoir une reconnaissance universelle et représenter la profession des experts-comptables en toute circonstance.

Son intégration se déploie sur l'ensemble de l'écosystème de l'expert-comptable et de l'entreprise. Son usage est très large puisqu'elle permet, à la fois de sécuriser la production du cabinet, de s'authentifier sur les sites web professionnels, comme Net-entreprises, jedeclare.com, Infogreff... , de signer en ligne lorsque c'est nécessaire, comme sur SYLAé, les banques, de certifier un document par un Tiers de Confiance, etc.

LES GAINS

Signexpert est la seule signature électronique qui atteste du statut d'expert-comptable.

Ce statut particulier de Signexpert permet :

- une dématérialisation totale y compris concernant les engagements et valeur probante des documents ;
- l'imputabilité des actes ;
- l'archivage numérique ;
- une facilité professionnelle des missions avec la notion de copie numérique...



SOURCE OFFICIELLE

Des démarches administratives et légales simplifiées grâce à la signature électronique

Dans le prolongement de la mission de service public des greffiers, Infogreffé a pour priorité de faciliter l'accès à ses services et permet de dématérialiser les principales démarches auprès des greffes des Tribunaux de commerce, l'information échangée et délivrée ayant une valeur légale.

POURQUOI ?

Depuis sa création en 1986, le G.I.E. Infogreffé met à disposition du public les données centralisées auprès de chacun des 134 greffes des Tribunaux de commerce.

Infogreffé diffuse, avec l'aide de chaque greffe du Tribunal de commerce de France, le registre des entreprises françaises.

Une justice de qualité impliquant la mise en place de moyens d'échange et de communication adaptés au monde moderne, les greffiers, acteurs de la dématérialisation des échanges de documents, se sont engagés dans un vaste projet de développement numérique et de simplification des formalités.

COMMENT ?

Les greffiers ont développé de nouveaux outils performants pour répondre aux besoins accrus d'échanges d'informations rapides attendus par les entreprises, les justiciables, et les professionnels du chiffre et du droit.

Infogreffé fait donc appel à un Prestataire de Service de Certification Electronique (PSCE) afin de délivrer des certificats numériques aux entreprises.

Ces certificats permettent de déposer les comptes annuels de leurs clients, mais aussi de signer les demandes en injonction de payer. Ces formalités sont réalisables, directement sur infogreffé.fr

En parallèle, les greffiers eux-mêmes signent électroniquement leurs actes authentiques (registres chrono, extraits KBIS...) qui sont par la suite archivés électroniquement.

QUI ?

Infogreffé assure la diffusion de l'information juridique et économique des entreprises pour le compte de l'ensemble des greffes des Tribunaux de commerce français.

Au-delà de son rôle de diffusion de l'information économique, Infogreffé permet de réaliser, de manière dématérialisée, les formalités légales, telles que l'immatriculation, les modifications ou la radiation au RCS, ainsi que certaines procédures.

Ainsi sont concernés :

1. L'ensemble des greffiers des Tribunaux de commerce qui souhaitaient proposer la dématérialisation des formalités au Registre du Commerce.
2. L'ensemble des entreprises du territoire français immatriculées au Registre du Commerce et des Sociétés (plus de 3,2 millions)

LES GAINS

- Procédure entièrement dématérialisée : pas de déplacements au greffe
- Délais de traitement réduits
- Procédure simplifiée : les formulaires sont pré remplis et les saisies sont guidées
- Volume de papiers traités fortement réduit : facilité de traitement et d'archivage
- Modernisation de l'image des Tribunaux de commerce, précurseurs et moteurs sur le marché de la dématérialisation

Les déclarations préalables aux travaux : la sécurité informatique au service de la sécurité des chantiers



Depuis 11 ans, DICT.fr est l'acteur majeur de la dématérialisation des formalités administratives préalables aux travaux, réunissant 35 000 utilisateurs autour de la prévention des endommagements de réseaux enterrés : entreprises de travaux, exploitants de réseaux, collectivités locales...

Promoteur des bonnes pratiques de la confiance électronique, DICT.fr a entièrement sécurisé son service pour garantir la sécurité technique et juridique de ses utilisateurs tout en conservant une égale simplicité d'usage.

POURQUOI ?

Le service DICT.fr est avant tout un service de nature juridique : les maîtres d'ouvrages et maîtres d'œuvre de travaux ont l'obligation légale d'informer à l'avance l'ensemble des exploitants de réseaux aériens, terrestres et subaquatiques ayant des ouvrages sur chaque commune concernée, afin de recueillir en retour de leur part des informations sur l'absence ou la présence d'ouvrages sur l'emprise des travaux prévus.

Les délais attachés à ces échanges sont définis et impératifs, ainsi que le formalisme des documents, qui impose une signature.

COMMENT ?

Afin de simplifier au maximum l'usage de la signature électronique et d'éviter d'être intrusif par rapport aux Systèmes d'Information nombreux et variés des utilisateurs, le choix a été fait de mettre en œuvre la signature électronique à la volée.

Ce mode de signature s'accompagne d'une traçabilité permettant la constitution de preuves offrant une garantie cryptographique d'intégrité, et archivées dans un coffre-fort d'archivage électronique.

Enfin, une convention de preuve acceptée formellement par tous les utilisateurs renforce la valeur juridique des documents électroniques échangés via le service.

QUI ?

- Les maîtres d'ouvrages et maîtres d'œuvre de travaux signent électroniquement les déclarations de travaux et les déclarations d'intention de commencer des travaux.
- Les exploitants de réseaux signent électroniquement les récépissés accusant réception de ces déclarations. 35 000 utilisateurs sont concernés par la signature électronique sur DICT.fr.

LES GAINS

Pour l'entreprise, mettre en œuvre la signature électronique constitue un investissement dans l'outil de production :

- mise en conformité juridique ;
 - modernisation ;
 - prise d'avance sur les concurrents.
- Les autres bénéfices de ce projet sont :
- la fidélisation des clients ;
 - les économies engendrées par la possibilité d'envoi tout-électronique au lieu des courriers et fax envoyés préalablement ;
 - la création d'une véritable « culture sécurité » au sein de l'entreprise.

« Avec la signature électronique, faire les déclarations est aussi simple qu'avant mais plus sûr juridiquement. Il est rassurant de disposer de récépissés signés et

5 GLOSSAIRE

Authenticité

Caractéristique d'un document dont on peut prouver qu'il est bien ce qu'il prétend être, qu'il a été effectivement produit ou reçu par la personne qui prétend l'avoir produit ou reçu, et qu'il a été produit ou reçu au moment où il prétend l'avoir été.

Archivage (électronique)

Ensemble des actions, outils et méthodes mis en œuvre 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)

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 signés électroniquement.

Cachet serveur ou cachet électronique

Procédé permettant la signature de données dématérialisées (documents, e-mail, accusés de réception...) par un serveur informatique au nom d'une personne morale.

Certificat Électronique

Un certificat électronique joue le rôle de pièce d'identité électronique et atteste du lien entre les données de vérification de signature et l'identité du signataire. L'identité du propriétaire du certificat est garantie par une Autorité de Certification.

Certificat Électronique qualifié

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

Clef publique / clef privée / bi-clef

La clef publique est un élément mathématique qui peut être rendu public et dont l'usage est de vérifier les signatures électroniques réalisées par la clef privée associée. La clef publique est scellée avec l'identité du signataire dans le certificat électronique associé. La clef publique et la clef privée forment ensemble la bi-clef.



Convention de preuve

La convention de preuve correspond à la possibilité pour les parties d'un contrat, de définir les règles qu'elles vont s'opposer, y compris les preuves électroniques.

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, scellée 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 « clef secrète » et la cryptographie asymétrique dite à « clef publique ».

Le principe de la cryptographie à clef secrète consiste à utiliser un seul secret ou une même clef pour chiffrer et déchiffrer les informations. Pour la cryptographie à clef publique, il y a 2 clefs différentes : une clef dite « publique » et une clef dite « privée » qui n'est connue que de son porteur légitime.

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 (clef cryptographique privée, propre au signataire) et certifié par l'ANSSI (Agence Nationale 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 une donnée (document, trace d'un événement) et une heure afin d'établir de manière fiable le moment auquel cette donnée a été établie.

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.

Intégrité

Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime.

Mot de passe

Élément de déverrouillage servant dans la vérification de l'identité annoncée d'une personne par un système d'information.

Voir aussi One Time Password (OTP).

Non-répudiation

La non-répudiation vise à garantir qu'un contrat, un accord ou une transaction ne peut être nié.

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.

One Time Password (OTP)

Mot de passe valide pour une utilisation unique lors de l'accès à un système d'information via internet notamment. Ce procédé permet d'améliorer la sécurité par rapport au mot de passe traditionnel (dit « statique »).

Voir Mot de Passe

Opérateur de Certification (OC)

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

PAC

La PAC ou Politique d'Acceptation Commune, signée en 2009 par l'ensemble des banques, sous l'égide du CFONB (Comité Français d'Organisation de Normalisation Bancaires), définit un cadre de référence des certificats électroniques acceptés par les applications bancaires

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.



Première partie

Preuve

Élément matériel (document contractuel sous forme papier ou électronique, attestation, fichier, etc.) qui démontre, établit, prouve la vérité ou la réalité d'une situation de fait ou de droit.

RGS

Référentiel général de Sécurité.

Il s'agit du référentiel documentaire établi par l'ANSSI 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 le RGS sont regroupées sous la forme de niveaux de sécurité d'exigences croissantes de * à ***.

Scellement

Opération cryptographique s'appuyant sur le mécanisme technique de la signature électronique dans le but de garantir la provenance et l'intégrité d'une donnée.

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

Objet du présent guide. Voir le chapitre sur les définitions de la signature électronique.

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

Appelé aussi Prestataire de Services de Confiance (PSCO).

(L'arrêté du 26 juillet 2004 entérine cette notion et les règles afférentes dans le droit français.)

Organisme dont les pratiques de sécurité permettent l'établissement d'un contexte de confiance pour les échanges entre des parties vis-à-vis desquelles il est neutre.

Dans le cadre de ce guide, un Tiers de Confiance habilité sera un Prestataire de Services de Certification Électronique (PSCE).

6

REMERCIEMENT AUX PARTICIPANTS

Pascal Agosti – Caprioli et associés
Nathalie Schlang – CertEurope
Renaud Badina – CertEurope
Alain Bobant – CNHJ
Bertrand Braux – Cryptolog
Stéphane Gasch – CS-OEC
Jean Saphores – CS-OEC
Sylvie Picon – CS-OEC
Dimitri Mouton – Demaeter
Pierre Patuel – Dpii Telecom
Bernard Delecroix – FNTC
Emmanuel de Ternay – GDOC Lasercom
Gabriel Gil – GLI Services
Thierry Piette-Coudol – Avocat
Gilles Taïb – Imprimerie Nationale
Pascal Colin – Keynectis-OpenTrust
Georges Muñoz – Keynectis-OpenTrust
Stéphanie Roussel – Syrtals
Thomas Kaeb – Wacom



A PROPOS DE LA FÉDÉRATION NATIONALE DES TIERS DE CONFIANCE

La Fédération Nationale des Tiers de Confiance (FNTC) est un acteur majeur 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.

Créée en 2001, la FNTC regroupe les professionnels de la dématérialisation, à savoir : 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 a pour but d'établir la confiance dans l'espace numérique, de promouvoir la sécurité et la qualité des services et de veiller au respect d'une charte d'éthique de la profession.

LES ADHÉRENTS FNTC*:

Accelya ; ACN ; ACOSS ; Actradis.fr ; Adminium ; AFCDP ; Alexandre Diehl ; AllPerf ; Almerys ; Alphacode ; APECA ; Argus DMS ; Ariadnext ; Asterion ; Bernard Starck ; Bruno Couderc Conseil ; Bull ; Cabinet Caprioli & Associés ; Security.com ; Cedricom ; Celtipharma ; CertEurope ; ChamberSign ; Chambre des Huissiers de Justice du Québec ; Chambre Nationale des Huissiers de Justice ; Chambre Nationale des Huissiers de Justice et Agents d'Exécution du Cameroun ; Cleona ; Compagnie Nationale des Commissaires aux Comptes ; Conex ; Conseil National des Greffiers de tribunaux de commerce ; Conseil Supérieur de l'Ordre des Experts-Comptables ; Corus ; Cryptolog ; DARVA ; Darwin Consulting & Finance ; Data One ; Data Syscom ; Demaeter ; Digimedia Interactivité ; Docapost BPO ; Docapost DPS ; Document Channel ; DPII Telecom ; Ecosix ; Edificas ; Edokial ; EESTEL ; eFolia ; Elcimai Financial Software ; Election Europe ; ESI ; Esker ; Esopica ; Forum Atena ; G.L.I. Ingénierie et Services ; Gdoc Lasercom ; Hervé Schauer Consultants ; Imprimerie Nationale ; IN Continu et Services ; Interb@t ; Isilis ; Issendis ; jedeclare.com ; Kahn & Associés ; Keynectis-OpenTrust ; Legalbox ; LeMore Avocats ; Locarchives ; Maileva ; Marc Chédru Conseil ; MIPIH ; Notarius ; Novapost ; Novarchive ; Odyssey Services ; Office des Postes et Télécommunications Polynésie Française ; OFSAD ; OPUS Conseils ; Perfect Memory ; PPI ; Primobox ; Provigis ; Sagemcom ; Scala ; SealWeb ; Sogelink/DICT.fr ; Stocomest ; Syrtals ; TESSI Ged ; UIHJ ; Univers Monétique ; ViaStorage ; Voxaly Electionneur ; Wacom ; Worldline ; Xeonys.

* Liste arrêtée au 1^{er} octobre 2013

Fédération Nationale des Tiers de Confiance
19, rue Cognacq-Jay
75007 – Paris
Tel. 01 47 50 00 50
info@fntc.org - www.fntc.org

