Contractualisation en ligne

Réussir son projet de signature électronique

Livre blanc

Cryptolog International
6-8, rue Basfroi
75011 Paris
Tél.: +33 1 44 08 73 00
sales@cryptolog.com
www.cryptolog.com

CRYPTOLOG

Créateur de Confiance

TABLE DES MATIÈRES

Introduction

En préambule, prenons quelques instants pour répondre à cette question : quand prenons-nous la peine d'imprimer un document numérique aujourd'hui ? À bien y réfléchir, il n'existe plus guère que deux grandes situations de la vie courante : la relecture du document et... la signature de celui-ci. Les deux opérations sont d'ailleurs assez souvent concomitantes. Dans la grande majorité des autres usages (création, rédaction, conception, partage, stockage, etc.), le document « restera » électronique, accessible au travers d'un écran d'ordinateur, ce qui lui vaudra également d'être qualifié de « dématérialisé ».

Dans le premier cas, il s'agit d'une démarche de confort, car il est tout à fait possible de relire un document électronique sur son écran. La pratique est, avouons-le, encore malgré tout très répandue. Gageons que l'avènement des e-books et des tablettes tactiles, la banalisation des écrans plats à grande résolution ainsi que la pression exercée par la collectivité pour l'adoption d'une attitude éco-responsable devraient la rendre de plus en plus marginale. Sans oublier que les nouvelles générations communément appelées « générations Y » devraient encore davantage se passer du contact avec le papier.

Toutefois, dans le second cas, l'impression est malheureusement bien souvent inévitable. Car même si la signature électronique, en plus de dix ans d'existence, a gagné ses lettres de noblesse, elle reste aujourd'hui méconnue et surtout encore très peu déployée.

Et pourtant, aujourd'hui le marché est profondément en attente de solutions simples et fiables permettant notamment de signer à distance des documents contractuels. Nous recevons presque quotidiennement chez Cryptolog des demandes en ce sens. Cela va de la petite société de spectacle, qui fait appel chaque mois à quelques dizaines d'intermittents du spectacle, à la grande compagnie d'assurance, qui souhaite transformer rapidement les visiteurs de son site en clients, en leur faisant signer en ligne des polices d'assurance.

Que ce soit en BtoB ou en BtoC, les besoins et les attentes sont énormes. Ne serait-ce que dans le secteur du e-commerce, on peut aujourd'hui tout acheter et tout vendre sur Internet, payer en quelques clics, se faire livrer, suivre l'état d'avancement de sa commande... sauf malheureusement signer un contrat ! À l'heure actuelle, la signature électronique est indubitablement l'élément manquant du e-commerce et du m-commerce.

En BtoB, outre l'accélération des processus commerciaux, le déploiement de solutions de signature à distance est également motivé par la réduction des déplacements et des envois postaux, ainsi que la simplification apportée par la mise en œuvre de processus entièrement dématérialisés.

Malgré tout, dès qu'un document électronique s'apprête à prendre une dimension légale, en raison de l'absence de solution alternative, il est malheureusement encore trop souvent imprimé.

Tout l'enjeu de ce livre blanc est de contribuer à changer cette situation en expliquant comment appréhender un projet de signature électronique dans le contexte spécifique de la contractualisation en ligne. Et ce, avec un parti pris assumé de ne masquer aucune difficulté. Car elles existent et sont pour partie responsables de cette situation lacunaire. Les ommettre serait contraire à nos valeurs de transparence et d'intégrité.

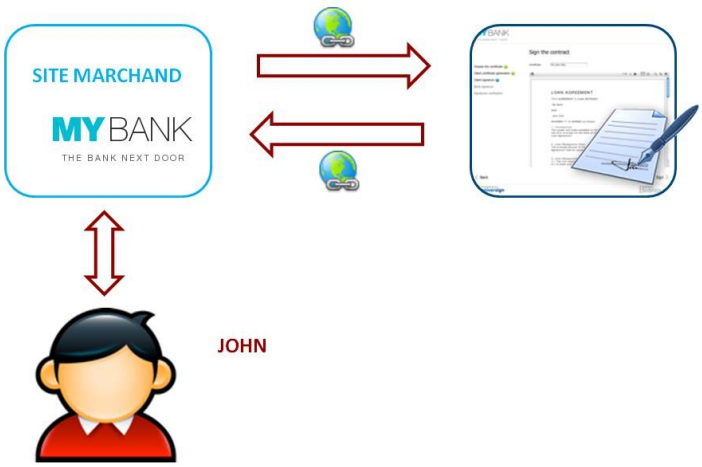
Il se peut même qu'à l'issue de cette lecture, vous tiriez la conclusion que la signature électronique n'est pour pas faite pour vous. Qu'importe, si votre besoin d'information a été assouvi et que la signature électronique ne vous est plus étrangère, alors nous serons déjà satisfaits.

Bonne lecture et bonne signature !

1. Le défi de la signature de contrats en ligne

1.1. Description des usages

Avant toute chose, qu'entend-on par signature de contrats en ligne ? Pour fixer les idées, le mieux est sans doute de prendre deux exemples purement fictifs : celui de John Doe et celui d'Alice Martin.



En visitant le site de la MyBank, John Doe s'apprête à emprunter 1000 dollars en souscrivant un crédit en ligne. Après avoir sélectionné le montant de son prêt, et avoir été informé sur les conditions de l'offre (taux d'intérêt, mensualité, durée du prêt, etc.) le site de la MyBank lui présente un document PDF reprenant l'ensemble des termes de son contrat. John déroule le document jusqu'à la dernière page à la suite de quoi un bouton *« Signer »* situé sous le document devient actif en changeant de couleur. John n'a plus qu'à cocher deux cases indiquant qu'il a bien lu et compris les termes du contrat et qu'il souhaite signer le contrat, avant de cliquer sur le bouton *« Signer »*. Un message de succès lui indique alors que l'opération a réussi. Il est redirigé ensuite vers une page où il peut télécharger son contrat également signé par la MyBank. Dans le même temps, celle-ci a pris le soin de lui envoyer un e-mail avec en pièce jointe le contrat signé. À l'ouverture du document dans Adobe Reader, John peut visualiser que le document est bien signé en ouvrant l'onglet consacré aux propriétés de la signature.

De son côté, Alice Martin est à la tête d'une entreprise de bâtiment. Elle signe chaque mois plusieurs dizaines de contrats avec des prestataires de services qu'elle connaît bien. La gestion de tous ces documents est lourde. Elle passe son temps à « courir après les signatures... » Par ailleurs les contrats papier s'amassent dans son bureau et l'armoire aménagée l'an dernier pour archiver ses documents arrive déjà à saturation. Lasse de cette situation, elle décide de mettre en place une solution de signature électronique sur le site Web de sa société, au sein d'un extranet dédié. Pour chaque nouveau contrat, il lui suffit désormais de poster le document sur son interface Web et d'envoyer une invitation à le signer par e-mail à son partenaire. À la réception du message, celui-ci n'a plus qu'à cliquer sur un lien et à se connecter via son login/mot de passe au site Internet d'Alice pour signer électroniquement le contrat. Alice gagne un temps considérable et ses frais postaux ont drastiquement diminué. Elle a mis un terme au remplissage de son armoire en stockant les contrats numériques sur un espace disque sécurisé de la société.

Ces deux exemples permettent de se figurer à quoi peuvent ressembler les usages de la contractualisation en ligne. On pourrait les multiplier à l'infini. On remarquera simplement qu'ils partagent tous un certain nombre de points communs :

- la solution de contractualisation mise en œuvre permet à des personnes distantes de signer électroniquement un même document via un site Internet ;
- elle est source d'importants bénéfices : accélération des échanges, économie de timbres, réduction des déplacements, meilleure conversion clients, dématérialisation des documents, etc.

- pour des raisons souvent commerciales l'une des parties du contrat a un intérêt plus fort que l'autre à ce que celui-ci soit signé et sera en général celle qui portera le service de signature. Dans notre premier exemple, il s'agit de la MyBank, dans le second, il s'agit d'Alice et de sa société.

1.2. Bénéfices

Ils ont déjà en partie été évoqués plus haut mais essayons de les recenser précisément. Nous en voyons essentiellement cinq, même si ce nombre n'a rien d'exhaustif.

1.2.1 Optimisation du taux de conversion

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, la mise en œuvre d'un « tunnel de conversion » aboutissant à la signature électronique d'un contrat ou d'un bulletin d'adhésion permettra d'augmenter ce taux. Un tunnel de conversion est un processus en plusieurs étapes, permettant à l'internaute de définir en quelques clics les principales modalités de son contrat. À l'heure actuelle, la dernière étape consiste bien souvent 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 de bureau avant de tomber aux oubliettes...

1.2.2 Accélération des processus commerciaux

La signature électronique est à la signature manuscrite ce que l'email est au courrier postal. En termes de temps d'exécution, comparer une contractualisation papier à une contractualisation électronique revient à comparer un envoi postal avec un envoi par courrier électronique. En effet, la signature manuscrite d'un contrat de vente par deux (ou plusieurs) parties nécessite :

- soit une rencontre physique entre les signataires, ce qui dans certains cas pourra parfois s'avérer problématique, pour des contraintes d'agenda ou de distance entre les signataires ;
- soit un aller-retour de quelques jours du contrat par La Poste.

Dans les deux cas, le temps au bout duquel les deux parties sont chacune en possession d'un exemplaire signé n'a rien de comparable avec celui offert par une solution de signature électronique en ligne. La promesse d'une telle solution est en effet de permettre potentiellement à plusieurs individus répartis aux quatre coins du monde de signer le même document en quelques minutes. Selon les situations, cette accélération du processus de vente peut avoir un impact non négligeable sur la trésorerie de l'entreprise.

1.2.3 Réduction des frais postaux, des impressions et des déplacements

Là encore comparer signature manuscrite et signature électronique revient à comparer le courrier traditionnel avec l'e-mail. Nous viendrait-il aujourd'hui à l'esprit de se passer de ce dernier et de renoncer aux économies de temps, d'impression, de timbres que cette rupture technologique a suscité ? Raisonnablement non. Aujourd'hui, la signature électronique est la principale lacune du courrier électronique. Songez une fois encore aux documents que vous prenez la peine d'envoyer par la poste : hormis quelques cartes postales de vacances et quelques brochures commerciales impossibles à reproduire avec une imprimante bureautique, il y a fort à parier que la quasi-totalité d'entre eux sont le véhicule de votre signature. Or, ce mode de communication est d'un autre âge. À

l'évidence, avec le formidable essor des technologies numériques et le besoin incessant d'accélérer et de rationaliser les échanges, la signature électronique sera, demain, aussi naturelle que l'e-mail l'est devenu en une dizaine d'années. Les deux seront d'ailleurs fortement associés au sein de mécanismes de recommandés électroniques.

1.2.4 Simplification des opérations

Si les motivations d'un projet de signature électronique en ligne peuvent être d'ordre marketing/commercial ou d'ordre « ROIste », elles sont le plus souvent également d'ordre opérationnel. Outre une attitude « éco-responsable » au moins de façade, la suppression du papier offre une simplification non seulement du processus de contractualisation mais également du processus de conservation des contrats : les contrats signés électroniquement peuvent être conservés dans le SI de l'entreprise, sur un espace de stockage sécurisé, au même titre que toutes les autres informations.

1.2.5 Bénéfices d'image

La signature électronique étant encore peu répandue, 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 professionalisme ne s'en trouvera que renforcée.

1.3. Exigences de confiance

Si les gains d'un processus de contractualisation en ligne sont conséquents, celui-ci nécessite un certain nombre de prérequis de fiabilité. Il faut en effet que chaque signataire puisse :

- être sûr que son correspondant est bien celui qu'il prétend être, qu'il n'usurpe pas une identité ;
- marquer son engagement par un processus de signature fiable et non répudiable qui soit reconnu, le cas échéant, par un tribunal ;
- avoir la garantie que le document signé et notamment les termes du contrat ne puissent être modifiés par la suite sans que cela soit détecté ;
- disposer d'un exemplaire du contrat et de la preuve de l'engagement des deux parties.

2. La nécessité d'un mécanisme d'engagement numérique fiable

2.1. La falsification à l'heure du numérique

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. Cela vaut bien entendu pour la signature : si vous mettez votre nom et votre prénom au bas d'un document quel que soit son format et quel que soit le logiciel bureautique utilisé, personne ne considérera qu'il s'agit là d'une signature. Et ce pour la simple et bonne raison qu'il est impossible d'être sûr que ce soit vous qui ayez fait cette « modification ». Imaginons qu'à un instant donné, vous ayez tout de même voulu marquer votre engagement via ce procédé. Il vous sera possible à tout moment de faire volte-face en arguant que rien ne prouve que ce soit bien vous qui avez inscrit votre nom : *« je n'ai pas pu signer ce document puisqu'aujourd'hui je ne suis pas d'accord »*. Or, ce qu'on demande à une signature c'est de marquer un engagement ne pouvant être contesté par la suite (principe de non répudiation).

Mais cela vaut aussi pour le contenu du document en lui même. Imaginons que vous ayez une solution fiable de signature garantissant l'identité du signataire. Dans une situation contractuelle, comment s'assurer que, depuis sa signature, les termes du contrat sous forme numérique n'ont pas été modifiés 25 fois avec un bon logiciel de bureautique ? Un mécanisme d'engagement numérique doit absolument conserver l'intégrité du document (absence d'altération).

Enfin, cela vaut aussi pour la date de la signature : admettons que vous ayez résolu les deux points précédents, comment garantir que la date de signature est fiable et que le contrat court toujours ? Si vous n'avez pas 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 il y a très longtemps et aujourd'hui il n'a plus cours »*.

2.2. Une mauvaise idée : la signature manuscrite scannée

Pour signer un document numérique, la démarche qui d'emblée vient à l'esprit et semble la plus naturelle reste celle d'une signature manuscrite... mais numérisée ! Pour ce faire, on peut par exemple utiliser sa souris pour « tracer » une signature à l'écran, ou bien faire appel à des dispositifs de numérisation plus sophistiqués (tablette graphique, stylo numérique, scanner, etc.)

Or, il s'agit d'une très mauvaise idée ! Pour les raisons évoquées précédemment cette « signature » ne présente aucune garantie en termes d'identité du signataire et rend très facile l'usurpation d'identité. Une signature manuscrite scannée peut très facilement être reproduite à l'identique via un bon logiciel de retouche d'image. Mieux, une personne mal intentionnée peut très facilement se procurer votre signature manuscrite, la numériser et l'insérer dans un document, où il est écrit par exemple que vous lui devez des sommes d'argent exorbitantes... Enfin, ce procédé de signature n'apporte aucune garantie quant à l'intégrité du document et son absence de modification dans le temps.

À travers un arrêt de la Cour d'Appel de Besançon du 20 octobre 2000, confirmé par la Cour de Cassation le 30 mars 2003, la jurisprudence vient conforter cette position en soulignant le manque de fiabilité d'une signature manuscrite scannée et notamment l'incertitude pesant sur l'identification du signataire avec cette technique.

Numériser une signature revient donc à la copier. En justice, la signature numérisée correspond donc à une copie : sur le plan de la preuve, elle équivaut au mieux à un commencement de preuve par écrit.

2.3. La cryptographie à la rescousse

À l'évidence, sans outil spécifique, il est impossible de signer un document électronique aussi simplement que l'on signerait un document papier et de garantir son absence de modification dans le temps. Pour surmonter ces obstacles, il faut faire appel aux mathématiques et à la *cryptologie*. La cryptologie est, étymologiquement, la « science du secret ». Elle englobe la cryptographie — l'écriture secrète — et la cryptanalyse — l'analyse de cette dernière. La cryptologie était déjà utilisée dans l'antiquité mais elle a pris ses lettres de noblesse en tant que discipline scientifique académique dans les années 1970. La signature électronique ainsi que tous les mécanismes de gestion de la preuve électronique tels qu'ils sont définis actuellement dans les textes de loi et les standards européens reposent entièrement sur cette science.

L'objectif des paragraphes suivants est de présenter les grands principes de ces mécanismes de manière très vulgarisée en se gardant bien de rentrer dans les détails, quitte à les simplifier par souci de compréhension. Un lecteur familier des notions de signature électronique et d'horodatage pourra aisément poursuivre sa lecture à partir du chapitre 3.

2.3.1 Principe de la signature électronique

La signature électronique permet, à l'aide d'un procédé cryptographique, de garantir :

- l'identité du signataire ;
- l'intégrité du document signé ;
- la non-répudiation par le signataire du document signé.

Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle mais correspond à un nombre ou une suite de nombres. En effet, l'opération de signature cryptographique s'applique à un fichier et produit un nombre ou une suite de nombres appelée communément signature électronique ou cryptographique. Celle-ci sera non seulement liée à ce fichier mais également liée à la personne qui a fait l'acte de signer. Cette suite de nombre peut être externe au fichier ou bien incluse dans celui-ci comme c'est le cas pour les documents au format PDF, qui sont capables d'embarquer plusieurs signatures électroniques. Contrairement aux idées reçues sur la signature électronique, une opération de signature ne chiffre/crypte pas le document et ne le modifie pas. Toute modification sur le document ou sur la signature pourra cependant être décelée (principe d'intégrité). On pourra vérifier la validité de la signature ainsi que l'identité de la personne qui a signé lors d'une opération technique dite de « vérification de signature » .

Concrètement, pour une application de contractualisation en ligne, il sera fortement recommandé d'utiliser le format PDF très largement répandu, qui offre une bonne stabilité du document et permet d'embarquer des signatures électroniques. De plus, depuis la version 4 Adobe Reader permet de « décoder » et « visualiser » les signatures électroniques contenues dans un PDF dans un onglet dédié intitulé « panneau de signature ». Une fois de plus, il se peut qu'un PDF signé électroniquement ne contienne aucune représentation visible d'une signature manuscrite sur le document lui-même.

2.3.2 L'identification du signataire par certificat électronique

Pour réaliser une signature électronique, être en possession d'un document PDF et d'un logiciel de signature cryptographique ne suffit pas. Le signataire devra également se munir de ce que l'on appelle communément et de manière abusive « un certificat électronique ». Ce certificat électronique est

assimilable à une carte d'identité numérique permettant d'attester avec certitude de l'identité d'une personne. Il permet de signer des documents numériques en ayant la garantie que l'identité du signataire est reconnue sans aucune ambiguïté, ni contestation. Concrètement, il s'agit d'un fichier électronique contenant un certain nombre d'informations personnelles (nom, prénom, SIREN, etc.) ainsi qu'une clé privée permettant de réaliser des opérations de signature cryptographique. Il peut se matérialiser soit sous la forme d'un simple fichier logiciel dans un format spécifique (.pfx, .p12, etc), soit sous la forme d'un dispositif matériel (carte à puce, carte SIM, clé USB cryptographique, token). Appelés aussi SSCD (pour *Secure Signature Creation Device* en anglais), ces dispositifs matériels permettent de sécuriser la clé privée qui, comme son nom l'indique est propre au signataire et ne doit pas être volée, ni partagée. L'accès à cette clé est protégé par un mot de passe que le signataire devra connaître pour réaliser des signatures.

Le certificat électronique est délivré par ce que l'on appelle une autorité de certification, dont le rôle est de vérifier l'identité et de faire le lien entre la clé privée et l'identité du signataire. Cette étape nécessite un certain nombre d'opérations de vérification d'identité, contraignantes pour le demandeur de certificat :

- à minima l'envoi de photocopies de pièces d'identité pour les procédures les plus souples
- un déplacement physique du demandeur auprès de l'autorité de certification et une vérification d'identité en face à face pour les politiques de certification les plus avancées. Lors de cette étape, le demandeur présente ses papiers d'identité contre remise du certificat. Dans ce cas, il s'agira souvent d'un dispositif matériel de création de signature (clé USB cryptographique par exemple).

Intuitivement, on comprend que plus la démarche sera lourde, plus le dispositif remis sera « matériel » et plus le certificat ainsi que les signatures qu'il produira seront de « bonne qualité ». En contrepartie, plus celui-ci sera coûteux, et moins nombreuses seront les personnes qui souhaiteront s'équiper.

Comme nous le verrons dans le prochain chapitre consacré au cadre légal, contrairement à la signature manuscrite, la signature électronique peut avoir différents « niveaux » de valeur juridique. Celui-ci varie en fonction de plusieurs critères au premier rang desquels figure le « niveau du certificat utilisé », ou en termes plus consacrés « son degré de qualification ».

2.3.3 Le principe de l'horodatage

On l'a vu, la signature électronique consiste à apposer un nom sur un document numérique. L'horodatage électronique, quant à lui, consiste à apposer à tout type de fichier (fichier texte, audio, vidéo, etc.) **une date fiable** sous la forme d'un **jeton d'horodatage**.

Un jeton d'horodatage garantit :

- l'existence d'un fichier à une date donnée
- que celui-ci n'a pas été modifié au bit près depuis cette date (principe d'intégrité)

Tout comme la signature électronique, l'horodatage garantit l'intégrité du document. Mais contrairement à la signature électronique, ce procédé ne contraint pas le signataire à l'utilisation d'un certificat électronique. Un simple appel en Web service auprès d'une autorité d'horodage suffira pour horodater un document. Dans une optique d'intégrité, il s'agit là d'un atout de mise en œuvre notable par rapport à la signature électronique. Concrètement, un jeton d'horodage se présente sous la forme d'une suite d'octets qui pourra être externe au document ayant été horodaté, au sein par exemple d'un fichier doté d'une extension spécifique (.ers, .tsp, etc.) Ou bien, comme pour la signature, il pourra être embarqué au sein du document d'origine : là encore une bonne pratique consiste à utiliser le format PDF qui peut contenir plusieurs jetons d'horodatage. Enfin, une opération d'horodatage ne chiffre pas le document et ne le modifie pas.

3. Cadre légal : que dit la loi ?

Après avoir rapidement brossé les différents mécanismes de preuve cryptographique permettant aujourd'hui de signer et de dater un document numérique, intéressons-nous au cadre juridique de la signature électronique. Celui-ci a largement évolué depuis une dizaine d'années et les textes législatifs régissant la preuve électronique en France et en Europe sont aujourd'hui bien identifiés, stables et « matures ». En revanche, ils sont nombreux et, avouons-le, relativement impénétrables pour le néophyte. Contentons-nous ici d'en mentionner les principaux et de les synthétiser.

3.1. Législation

Le texte fondateur, définissant un cadre communautaire pour les signatures électroniques en Europe, est la directive européenne du 13 décembre 1999.

La transposition française s'est effectuée en de nombreuses étapes dont les principales sont :

- 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 électronique ;
- le décret n°2001-272 du 30 mars 2001, pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, modifié par le décret n°2002-535 du 18 avril 2002 ;
- le décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;
- la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés ;
- 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 organismes qui procèdent à leur évaluation ;

La création de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) avec le décret n°2009-834 du 7 juillet 2009 et l'élaboration du Référentiel Général de Sécurité (RGS) suite à l'ordonnance n°2005-1516 du 8 décembre 2005 et au décret n°2010-112 du 2 février 2010 sont venues encore densifier cette législation.

Que retenir de ces différentes publications ?

Essentiellement, une chose : au travers de ces différents textes, la législation française et le cadre européen distinguent deux types de signatures avec deux niveaux de validité juridique différents :

- la signature électronique ou **« signature simple »**
- la signature électronique **« présumée fiable »**

3.2. La signature électronique dite « simple »

Dans ce premier cas, selon l'article 4 de la loi 2000-230 du 13 mars 2000, la signature électronique *« consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ».* À ce niveau, le procédé de signature électronique dit « simple » n'est pas présumé fiable

mais l'écrit signé ainsi sous forme électronique ne pourra être refusé en justice au titre de preuve dès lors que le procédé permet d'identifier le signataire et de garantir le lien avec l'acte signé. En cas de contestation, il est nécessaire de prouver la fiabilité du procédé de signature électronique utilisé. Ce type de signature est aujourd'hui exploité dans la très grande majorité des usages.

3.3. La signature présumée fiable

En quoi consiste-t-elle ? Par rapport à la signature simple, la signature électronique présumée fiable renverse la charge de la preuve : en cas de contestation, il appartiendra à celui qui met en cause la fiabilité de la signature d'en apporter la preuve. Elle pourra prétendre en justice à un niveau de reconnaissance équivalent à celui de la signature manuscrite.

La force probante de cette signature est incontestablement plus élevée que celle de la signature électronique simple. Mais elle requiert un certain nombre d'exigences particulièrement lourdes à mettre en œuvre dans le cadre d'un projet de signature électronique :

1. la signature électronique doit être sécurisée, autrement dit, il s'agit d'une signature cryptographique ;
2. elle doit être créée par un dispositif sécurisé de création de signature (SSCD), c'est-à-dire par un dispositif matériel certifié conforme à un certain nombre d'exigences ;
3. la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié. Les certificats délivrés par les autorités de certification électronique qualifiées sont présumés qualifiés. L'arrêté du 26 juillet 2004 encadre et définit la reconnaissance de la qualification des prestataires de services de certification électronique (ou autorité de certification).

Ces deux dernières conditions ont deux conséquences particulièrement contraignantes :

- le signataire devra impérativement utiliser **une clé privée hébergée sur un support physique sécurisé**, qui plus est ayant subi un processus de certification. On pourra trouver notamment la liste des dispositifs certifiés sur le site de l'ANSSI.
- il devra se procurer **un certificat qualifié**. Or, la délivrance d'un certificat qualifié impose une vérification d'identité en face à face par l'autorité de certification.

En corollaire, l'acquisition d'un certificat qualifié sur support physique permettant une signature présumée fiable est **coûteuse**. Aujourd'hui, sur le marché, quelques centaines d'euros à minima seront nécessaires pour obtenir un tel dispositif...

3.4. La question du certificat

On voit donc maintenant combien la question du certificat est cruciale non seulement dans la mise en œuvre d'un projet de signature, mais également dans le développement du marché de la signature électronique. Beaucoup d'acteurs de ce marché se bornent simplement à dire qu'*«une signature électronique possède la même valeur juridique qu'une signature manuscrite »*. Ce raccourci ne vaut que lorsque la signature électronique est présumée fiable et a été produite avec un certificat matériel qualifié. Or, il s'agit aujourd'hui d'un usage très marginal pour les raisons évoquées plus haut, de coût du certificat et de complexité d'obtention de celui-ci. Ceci explique que la signature électronique ne se soit pas plus démocratisée depuis dix ans. Lorsqu'il s'agit d'équiper ses collaborateurs d'une flotte de certificats qualifiés, beaucoup de chefs de projets rechignent à se lancer dans l'aventure. Plutôt que de se rabattre sur la mise en œuvre d'un procédé de signature moins évolué, ils préfèrent jeter l'éponge.

Signalons que cette problématique n'aura, espérons le, plus cours dans quelques années puisque des chantiers nationaux sont en cours pour délivrer un identifiant numérique qualifié sur un support physique sécurisé : citons la carte nationale d'identité électronique qui hébergera en option un certificat ou encore le projet IdéNum, qui devrait permettre notamment de délivrer des certificats qualifiés sur les mobiles. Malheureusement ces projets vont prendre du temps avant de déboucher sur une réalité concrète.

Devant l'impérieuse nécessité qu'ont les entreprises à accélérer sans cesse leurs échanges, une signature électronique que nous qualifierons de « signature électronique business » se développe progressivement au sein du cadre juridique actuel de la signature simple. Comme nous l'avons vu, celui-ci ne définit rien de précis et laisse donc une grande liberté de déploiement en particulier en termes de certificat. En fonction du contexte, il s'agira donc de choisir quel « niveau de certificat » on souhaite déployer, associé à quelle « prise de risque ».

Lorsque les risques de contentieux juridiques sont faibles, on pourra par exemple se contenter d'un certificat à usage unique pour lequel la vérification d'identité est quasi inexistante. Dans ce type de scénario, le certificat est logiciel et créé à la volée au moment de la signature en utilisant les données personnelles que le signataire a saisies dans un formulaire. La signature n'a que très peu de force probante mais en contrepartie le coût des certificats est quasi nul.

À l'inverse, lorsque la situation le permet, on pourra décider d'équiper les signataires de certificats matériels qualifiés obtenus après vérification des identités en face-à-face par une autorité de certification.

Entre ces deux situations extrêmes, on pourra opter par exemple pour un certificat logiciel dont la délivrance nécessite simplement l'envoi de photocopies de pièces d'identité...

4. Les critères de choix d'une stratégie de signature électronique

Compte-tenu des contraintes du cadre légal et du principe même de la signature électronique reposant sur l'utilisation d'un certificat, avant de se lancer dans un projet, il convient d'identifier les critères de décision d'une stratégie de contractualisation en ligne. Quels sont les critères importants permettant d'évaluer s'il est pertinent ou non de mettre en œuvre un tel projet à l'heure actuelle ?

4.1. Le volume de signatures

Le volume des signatures que vous allez être amené à gérer est certainement le premier critère à prendre en compte. En deçà de quelques centaines de signatures par an, il se peut que le jeu n'en vaille pas la chandelle et que le stylo reste encore votre meilleur ami pour collecter des signatures...

4.2. La fréquence de signatures

Les signataires vont-ils être amenés à signer une seule fois un document ou bien de manière récurrente ? Dans le deuxième cas, il est sans doute intéressant de les équiper d'un certificat permanent.

4.3. La connaissance des signataires

Ce critère est décisif pour apprécier quelle stratégie adopter en termes de délivrance de certificats. De deux choses l'une :

- soit les personnes qui seront amenées à signer sont connues et en nombre limité. Dans ce cas, la délivrance de certificats permanents s'avère très pertinente.
- soit vous ne les connaissez pas et leur nombre est incertain : dans ce cas il peut s'agir typiquement d'internautes qui visitent votre site Internet et vous n'avez pas d'autre choix que de délivrer des certificats temporaires créés à la volée pour le besoin de signature.

4.4. La propension à contester la signature

On l'oublierait presque mais il s'agit d'un critère important lors de la mise en œuvre d'un projet de contractualisation en ligne. En BtoC, l'expérience montre que la contestation autour d'un engagement contractuel porte beaucoup moins sur la fiabilité du mécanisme de signature que sur les termes du contrat. Ceci est particulièrement vrai dans le domaine de l'assurance : en souscrivant à un contrat, l'assuré cherche en effet à être couvert vis-à-vis d'un risque et est donc peu enclin à nier une signature, ce qui signifierait, de fait, qu'il n'est pas assuré. Prenons l'exemple de l'assurance habitation : lors de la déclaration d'un vol, ou d'une dégradation sur son lieu d'habitation, un assuré cherchera par exemple à contester le montant de la valeur mobilière pour laquelle il est assuré, mais en aucun cas la signature de son contrat. Il ne dira pas *« je n'ai rien signé »* puisqu'il cherche à obtenir un remboursement ! Mais plutôt *« Ce n'ai pas ce que j'ai signé à l'origine. Vous avez modifié le contrat : la valeur mobilière était à 35 000 euros et pas à 10 000 comme c'est écrit aujourd'hui dans le contrat que vous m'avez envoyé ! ».* Or, comme nous le verrons plus loin, sur ce point l'horodatage, en garantissant l'intégrité du document dans le temps, offre une parade redoutable et permet de balayer ces objections.

Le préjugé selon lequel la signature électronique a toujours la même valeur qu'une signature manuscrite joue également ici en notre faveur : la plupart du temps, le consommateur ayant souscrit à une offre sur Internet un peu rapidement s'adressera au service client en disant *« j'ai changé d'avis je ne veux plus souscrire à votre offre »* plutôt que *« votre signature électronique n'a pas de valeur, je n'ai rien signé »*. Il bénéficiera d'ailleurs souvent d'un délai de rétractation plus ou moins long selon les secteurs.

De manière générale, selon les environnements il faudra s'attacher à évaluer le plus objectivement possible la probabilité de contestation autour du procédé de signature. Avec comme objectif de placer le curseur au meilleur endroit en termes de délivrance de certificat...

4.5. Les enjeux en cas de contestation d'une signature

Dernier critère et non des moindres, celui des enjeux financiers. Devez-vous gérer des contrats à quelques dizaines ou à plusieurs millions d'euros ? Selon la réponse à cette question, la stratégie à adopter sera bien différente. Dans le second cas, vous ne pourrez pas vous permettre de prendre des risques et mieux vaut se doter d'un procédé de signature fiable ! On l'aura compris : un projet de signature électronique comporte, comme tout projet, une certaine part de risque, qui nécessite d'être analysé et estimé.

Dans les deux prochains chapitres, nous allons nous placer dans deux situations couramment rencontrées mais bien différentes. Nous évaluerons dans chacune des situations, à l'aune de ces critères, quelle stratégie adopter pour mettre en œuvre un projet de signature de contrats en ligne.

5. Opter pour le déploiement de certificats en cercle restreint

5.1. Contexte

Dans ce chapitre, nous avons choisi de nous placer dans une situation assez courante en environnement BtoB où :

- les signataires sont en nombre limité ;
- ils sont clairement identifiés ;
- ils signent régulièrement des contrats.

Typiquement, pour reprendre nos exemples d'introduction, cette situation est celle d'Alice Martin : elle correspond à une relation classique client-fournisseur, dans laquelle une société contractualise de manière récurrente avec un certain nombre de prestataires connus et référencés.

5.2. Certificat matériel ou logiciel

À l'évidence, il s'agit là d'un contexte relativement confortable qui offre la possibilité d'équiper chaque signataire d'un certificat permanent qu'il soit logiciel ou matériel. Si le contexte est suffisamment critique et si le budget le permet, on pourra même opter pour des certificats matériels qualifiés. Mais la plupart du temps, on se contentera de certificats non qualifiés qui permettent une signature électronique simple.

Lorsque l'on abaisse ainsi le niveau de sécurité au niveau de la certification, il est alors très judicieux de recourir à des mécanismes contractuels complémentaires comme notamment celui de la convention de preuve, afin de parer à toute contestation possible autour du procédé de signature .

5.3. Une bonne pratique : la convention de preuve

La convention de preuve est un contrat conclu entre entreprises ou entre entreprises et particuliers qui a pour objet de définir les modes de preuve admissibles entre les parties, la charge de la preuve et les modalités de règlement des conflits de preuve. Elle permet de garantir la force probante des documents produits par une solution de signature électronique et d'organiser un renversement de la charge de la preuve.

Lors de la mise en œuvre d'un système de contractualisation électronique, les parties peuvent ainsi s'accorder conventionnellement pour reconnaître la valeur probante des contrats conclus au moyen de celui-ci et pour prévenir toute contestation autour de sa fiabilité.

Selon les termes de l'article 1316-2 du Code civil, à défaut de convention de preuve valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens, le titre le plus vraisemblable. Mais lorsqu'une convention de preuve a été valablement conclue entre les parties, le juge doit l'appliquer. Cela peut permettre d'organiser par avance la façon dont lesdits conflits pourront être résolus et donc d'en prévoir l'issue.

Malgré tout, les juges disposent d'un libre pouvoir d'appréciation. Par ailleurs, une convention de preuve ne doit bien sûr pas porter atteinte à des règles d'ordre public ainsi qu'aux dispositions légales et réglementaires sur les clauses abusives.

5.4. L'insertion de la signature manuscrite numérisée

Dans un contexte de dématérialisation d'une relation contractuelle existante, il sera vivement conseillé d'offrir aux utilisateurs habitués à signer manuellement, la possibilité de visualiser dans les documents signés leurs signatures manuscrites numérisées. En effet, la connaissance des signataires permet d'envisager avant la mise en œuvre de la solution, de réaliser la numérisation de la signature de chaque futur signataire. Cette image sera par la suite insérée dans le document numérique en lieu et place d'une signature manuscrite, à chaque fois que celui-ci fera une signature électronique.

Cette « astuce d'implémentation » permettra de conserver les habitudes et de coller à l'existant en rendant visible la signature électronique de chaque signataire : elle sera un atout précieux pour convaincre les utilisateurs attachés à leur signature et potentiellement hostiles à la mise en œuvre de de la contractualisation électronique.

6. Une stratégie pragmatique dans un contexte marchand en ligne

6.1. Contexte

Dans ce chapitre, nous avons choisi de nous placer dans une situation bien différente de celle du chapitre précédent dans laquelle :

- les signataires ne sont pas connus à l'avance
- ils sont en nombre indéterminé
- ils ne vont signer qu'une seule fois un document (la fréquence de signature est faible)

Ces paramètres sont ceux d'un contexte marchand dans lequel un opérateur Internet cherchera via son site à convertir ses visiteurs en clients, en leur faisant signer directement en ligne des contrats commerciaux. Il pourra s'agir d'une banque, d'une assurance, d'un opérateur télécom, d'un loueur de matériel ou de tout acteur présent sur la toile ayant un fort intérêt à mettre en œuvre un tunnel de conversion aboutissant à une signature électronique contractuelle.

6.2. L'utilisation d'un certificat à usage unique

Il y a évidemment très peu de chance pour que les visiteurs du site Internet en question soient en possession d'un certificat permanent. Il n'y a donc pas d'autre choix que de les équiper. Et pourtant, il est totalement exclu ici de procéder à une véritable vérification d'identité par une quelconque autorité de certification : en l'occurrence cette opération serait bien plus lourde et freinante que la simple impression du contrat, sa signature et son envoi par La Poste. Dans ce cas de figure, le site marchand n'a pas d'autre solution que « d'agir en tant qu'autorité de certification » et de délivrer ce que l'on appelle un certificat logiciel dit « temporaire » ou « à usage unique ». De même structure qu'un certificat permanent, celui-ci est généré à partir des informations déclaratives que l'utilisateur renseigne dans un formulaire Internet. Il est créé à l'occasion de la signature et ne sera utilisé qu'une seule fois lors de celle-ci. Si l'internaute ne renseigne que son nom et son prénom, la valeur probante d'un document électronique signé de la sorte sera à l'évidence assez faible. Malgré tout, **il ne pourra être refusé en justice au titre de preuve** dans le cadre de la signature simple qui, rappelons-le, est définie comme un procédé permettant d'identifier le signataire et de garantir le lien avec l'acte signé.

Dès lors, pour le site marchand il conviendra donc de fiabiliser l'identification de chaque personne connectée s'apprêtant à signer un contrat, en constituant un faisceau de preuves, permettant le cas échéant de servir un argumentaire juridique en faveur de la fiabilité du procédé utilisé. Pour collecter ces éléments de preuves, une technique consiste à mettre en œuvre ce que nous appelons « un chemin de preuve ».

6.3. La constitution d'un chemin de preuve

Ce chemin de preuve est un processus formaté et systématique ayant principalement trois objectifs :

- réaliser une identification la plus fiable possible du futur client ;
- collecter un maximum d'éléments de preuve pouvant être utilisés en cas d'une hypothétique contestation ultérieure de l'engagement contractuel ;

- durcir le mécanisme de contractualisation en ligne afin de dissuader la souscription de visiteurs peu intéressés par le service proposé et qui auront par la suite une forte inclination à dénoncer l'existence d'une relation contractuelle.

Ce processus sera intelligemment imbriqué au sein du tunnel de conversion mis en œuvre.

6.3.1 La collecte d'un maximum de données d'identification

Pour le site marchand, il s'agira d'une part d'aller un peu plus loin dans la collecte d'informations personnelles que les traditionnels formulaires Internet d'inscription à un service en ligne. Cette étape consistera à proposer un formulaire de renseignements enrichi par un certain nombre de champs comme la date de naissance, le lieu de naissance, la situation professionnelle, le numéro de mobile de la personne mais également son numéro de carte d'identité, sa date de délivrance, le nom de l'autorité ayant délivré la carte d'identité, etc. La présence d'un tel formulaire au sein du processus de contractualisation servira la génération du certificat de signature. Elle sera également dissuasive pour les internautes n'ayant qu'une faible motivation à souscrire au service proposé et contribuera à assurer une « bonne qualité de conversion ».

D'autre part, le site marchand aura tout intérêt à enregistrer les données de connexion : les cookies auquels il est fortement recommandé de faire appel mais surtout l'adresse IP qui sera une information supplémentaire déterminante d'identification de l'internaute.

6.3.2 La vérification d'identité par e-mail ou SMS

Cette opération consiste à délivrer par e-mail ou SMS un code à usage unique, dont la connaissance sera indispensable pour l'acte de signature : au moment de signer, il sera demandé à l'internaute de saisir ce code dans une fenêtre. Cette opération permettra de valider que celui-ci est bien le détenteur de l'adresse e-mail ou du numéro de mobile qu'il a renseigné. Dans le cas d'un envoi de SMS, cette vérification sera un élément de preuve important pour attester de l'identité de la personne dans un contexte sensible.

6.3.3 La vérification de l'engagement contractuel

Il n'y a là rien de bien plus sophistiqué que les traditionnelles cases à cocher que l'on rencontre souvent lors de l'inscription à un service en ligne :

-*« Je certifie avoir pris connaissance des conditions générales et particulières de vente disponibles sur le site...»*

-*« Je déclare avoir lu l'intégralité du contrat... »*

-*« En cliquant sur le bouton signer ci-dessous, je reconnais avoir compris la portée de mon engagement contractuel vis-à-vis de... »*

-etc.

Cette vérification pourra être accompagnée d'une obligation de l'internaute de visualiser chaque page du contrat qu'il s'apprête à signer.

6.3.4 Le paiement en ligne

L'adhésion à un contrat en ligne débouchera bien souvent sur un acte de paiement en ligne via une carte de crédit. Or, cet acte participera, comme tous ceux cités précédemment, à l'identification du signataire ; après avoir payé, ce dernier pourra difficilement faire volte-face et contester son engagement numérique.

6.4. Faire bon usage des conditions générales de vente et de souscription

Afin de mettre toutes les chances de son côté, un site souhaitant mettre en œuvre la souscription en ligne devra impérativement tirer parti de ses conditions générales de vente. A défaut, s'il n'en possède pas, il pourra rédiger des conditions générales de souscription ou d'adhésion. De la même manière qu'une convention de preuve, ces documents permettent d'organiser un renversement de la charge de la preuve : en y incluant une clause ad hoc, tout site Internet, marchand ou non, pourra donner une valeur juridique pleine et entière à l'ensemble de ses moyens de preuve électronique. Celle-ci pourra avoir la forme suivante :

-« Il est entendu entre les Parties que les moyens de preuve électronique administrés par le site XXX feront seuls foi entre elles. Les registres informatisés de XXX seront considérés par les parties comme preuves des communications, commandes, adhésions, paiements et transactions intervenus entre les parties. »

En particulier, la dernière phrase de ce paragraphe sera de nature à donner une valeur probante forte à l'ensemble des éléments d'identification collectés lors du chemin de preuve précédemment évoqué : il serait donc dommage de s'en passer...

6.5. Conserver l'impact psychologique de la signature manuscrite

Quitte à le répéter, nous sommes convaincus que dans tout processus de signature électronique, il convient souvent de conserver un acte de "signature manuelle" qui permettra au signataire de réaliser psychologiquement qu'il est en train de signer quelque chose et qu'il est en train de s'engager. Dans un processus de contractualisation en ligne, on pourra par exemple demander à l'Internaute de tracer sa signature dans une fenêtre. Cette signature n'a, rappelons le, aucune valeur juridique, et sera inévitablement accompagnée d'une véritable signature électronique mais elle s'ajoutera à l'ensemble des éléments d'identification collectés lors du chemin de preuve. Surtout, cette étape réduira considérablement les velléités de contestation de notre nouveau client autour de la validité de la signature, puisque « dans son esprit » il aura signé. Il s'agit ici d'écarter les protestations du type : « *je ne me suis pas rendu compte que j'avais signé quelque chose ».*

6.6. La garantie d'intégrité apportée par l'horodatage électronique

Comme nous l'avons déjà évoqué la contestation autour d'un engagement contractuel porte beaucoup moins sur la fiabilité du mécanisme de signature (*« je n'ai rien signé »)* - que sur les termes du contrat (*« Ce n'est pas ce que j'ai signé. Vous avez modifié le contrat »).* Or, ces objections ne seront jamais prises au sérieux par un juge à partir du moment où le document a correctement été horodaté, même si par ailleurs la signature est discutable. Car l'horodatage d'un contrat électronique garantit d'une part l'existence de ce contrat à une date donnée mais également que celui-ci n'a pas été modifié au bit près depuis cette date (principe d'intégrité). Contrairement à la signature électronique, ce procédé n'astreint pas le signataire à l'utilisation d'un certificat électronique. Un simple appel en Web service auprès d'une autorité d'horodatage suffira pour horodater un document. Encore faut-il choisir une autorité d'horodatage suffisamment fiable et digne de confiance.

Dans l'attente d'autorités d'horodatage permettant de délivrer en France des jetons d'horodatage présumés fiables en justice, il faudra porter son choix sur les autorités d'horodatage qualifiées RGS dont l'usage est imposé aux administrations par le « décret RGS » dans le cadre des échanges inter-administrations ou avec leurs usagers.

Être qualifié RGS signifie que les conditions d'hébergement, le taux de disponibilité, les règles de sécurité, les processus techniques et organisationnels ont été scrupuleusement et régulièrement audités par un organisme de certification indépendant officiel. À l'heure où nous écrivons ces lignes, il n'existe pas aujourd'hui de niveau de qualification plus abouti en France. En faisant appel à une autorité d'horodatage de ce type, vous mettrez ainsi toutes les chances de votre côté pour rassurer un interlocuteur sur l'exactitude des dates et des documents fournis dans une situation de contentieux juridique.

6.7. Former son service clientèle à ce canal de souscription

On l'a vu, la signature électronique au moyen d'un certificat temporaire n'est pas exempte de faille et impose la mise en œuvre d'un certain nombre de mécanismes complémentaires d'identification du signataire. Dans ce contexte, il conviendra d'adopter une politique de SAV plutôt conciliante dans laquelle les conseillers clientèles chercheront à tout prix à éviter le contentieux en cas de contestation sur la signature ou l'engagement contractuel. Notamment, ils ne devront pas hésiter à adopter une démarche proactive d'annulation des contrats lorsque les objections vis-à-vis du processus de signature se feront trop fortes. Cela passe bien évidemment par la formation des opérateurs à ce nouveau canal de souscription.

Conclusion

Ainsi comme nous avons pu le constater dans les deux chapitres précedents, la stratégie à adopter pour la mise en œuvre d'un projet de signature électronique pourra être très différente en fonction du contexte. Il conviendra d'abord de passer celui-ci au tamis des différents critères évoqués au chapitre 4 :

- le volume et la fréquence de signature sont-ils élevés ?
- peut-on dresser une liste des futurs signataires ?
- la probabilité de contestation sur l'engagement contractuel est elle forte ?
- les enjeux sont-ils importants ?

La réponse à ces questions permettra d'évaluer rapidement s'il est pertinent de mettre en œuvre un tel projet à l'heure actuelle et quelle est la démarche à adopter en termes de délivrance de certificat. En fonction du contexte, il faudra s'attacher à définir le « niveau de certificat » que l'on souhaite déployer, associé à quel degré d'identification des signataires.

Enfin, quel que soit le scénario retenu, il est fortement recommandé :

- d'organiser un renversement de la charge de la preuve via des documents contractuels complémentaires : convention de preuve, conditions générales de vente, ou de souscription ;
- de conserver un acte de "signature manuelle" et de matérialiser la signature électronique par une signature manuscrite numérisée. Ces artifices, qui pour les raisons décrites au chapitre 2 n'ont aucune valeur juridique, permettront néanmoins aux signataires de conserver leurs habitudes, et de réaliser psychologiquement qu'ils sont en train de s'engager ;
- de faire appel à un horodatage qualifié RGS afin de sceller électroniquement le document contractuel numérique et de détecter toute modification ultérieure à la signature. En garantissant l'intégrité du document dans le temps, l'horodatage permet de balayer toutes les objections consistant à remettre en question le contenu du document.

À propos de Cryptolog

Cryptolog est un éditeur logiciel à la pointe de l'innovation en matière de signature électronique, d'horodatage et de gestion de la preuve. L'offre Cryptolog se compose d'une suite complète de solutions logicielles sur étagères, de services hébergés clés en main et d'un conseil d'expert sur la signature électronique.

Dans une volonté d'industrialisation des réponses aux projets de signature électronique, Cryptolog développe et commercialise depuis 2010 la plate-forme SaaS www.universign.eu d'horodatage et de signature électronique. En particulier, cette offre extrêmement modulaire permet d'ajouter à n'importe quel site Web une fonctionnalité de signature électronique. Aussi rapide à intégrer qu'un service de paiement en ligne, celle-ci présente les caractéristiques suivantes :

- signature de documents au format PDF ;
- affichage ou non du contrat avant signature ;
- compatibilité avec tous les certificats du marché ;
- génération à la volée de certificats à usage unique ;
- envoi d'un code à usage unique par Email ou SMS en cas de génération de certificats ;
- insertion d'une image matérialisant la signature (signature manuscrite numérisée ou logo) ;
- insertion de texte lors de la signature (nom, prénom, date de signature) ;
- horodatage qualifié RGS de chaque signature ;
- intégration en quelques heures ;
- paiement à la consommation (tarification au volume de signature) ;

Cette solution offre un large choix d'options de mise en œuvre et pourra s'adapter à tous types de scénarios de signature électronique en ligne et en particulier ceux décrits dans ce livre blanc.

CRYPTOLOG

Créateur de Confiance

Cryptolog International

6-8, rue Basfroi
75011 Paris
Tél.: +33 1 44 08 73 00
sales@cryptolog.com

www.cryptolog.com