ARCHIVAGE DES PREUVES

DE SIGNATURE ÉLECTRONIQUE À LA VOLÉE

FÉDÉRATION DES TIERS DE CONFIANCE DU NUMÉRIQUE
www.fntc-numerique.com

Archivage des preuves de signature électronique à la volée

fntc

L'ASSURANCE D'USER EFFICACEMENT ET EN TOUTE SÉRÉNITÉ DU NUMÉRIQUE

Introduction

Depuis plusieurs années, face à la complexité de la mise en œuvre de la signature qualifiée [1] qui nécessite, bien souvent, de disposer d'un moyen physique pour réaliser l'opération de signature, l'usage de la signature, dite à la « volée », s'est développé afin de répondre à des besoins qui ne requièrent pas un très haut niveau de sureté juridique tel que prévu par le règlement eIDAS.
Cette signature à la volée présente l'avantage de ne pas nécessiter de moyens techniques spécifiques, un ordinateur personnel, une tablette ou bien souvent un simple *smartphone* suffisent. Les avantages de ce mode de signature sont nombreux : simplicité d'emploi, coût relativement faible…

Les cas d'usage sont très variés mais tous ont la même exigence, à savoir, démontrer en cas de contentieux :

- L'identité du ou des signataire(s) ;
- Le consentement par le signataire au contenu de l'acte signé (du moins devant les tribunaux français) ;
- Le respect des exigences réglementaires et des usages en fonction du signataire. Il est important que le professionnel (qui maitrise parfaitement le sujet) mette en œuvre un processus de contractualisation qui ne vienne modifier les droits et obligation du particulier qui, par définition, n'est pas au fait de ces sujets et procédures.

Cependant, il s'avère que la conservation dans le temps de ce type de document signé pose problème. En effet, du fait de caractère éphémère de certains composants de cette signature, il est difficile de revalider celle-ci dans le temps. L'une des solutions pour palier à cet inconvénient est de disposer, à côté du document signé, d'un fichier de preuves qui contient l'histoire de la signature de ce document. Le présent guide fournit une description de ce qu'un tel fichier doit inclure *a minima*.

Nous recommandons à toute société qui souhaite mettre en œuvre des signatures à la volée d'obtenir de leur prestataire de signature, en même temps que le document signé, un fichier de preuves associé.
Afin d'aider les décideurs, il a été joint en annexe :

- Une présentation du cadre juridique de la signature numérique à la volée ;
- La liste des normes applicables ;
- Et enfin, des exemples d'usages de la signature à la volée.

(1) Voir l'annexe I du présent document sur le règlement eIDAS pour la définition des niveaux de signature.

Rappels techniques sur la signature électronique

Une signature électronique peut être réalisée de deux façons différentes, suivant le lieu où sont réalisés les calculs cryptographiques :

1 En local :

c'est-à-dire sur le poste du signataire, soit via une carte à puce ou une clé USB, notamment dans le cas d'une signature qualifiée, soit via un fichier contenant les moyens de signatures (certificat et clés) et un logiciel ;

2 A distance :

dans ce cas, les moyens de signature sont générés, voire maintenus dans le temps, sur le serveur d'un prestataire de confiance.

3 Dans ce dernier cas :

• La durée de vie du certificat électronique peut-être très limitée dans le temps ou durable, de quelques heures à quelques mois ;

• La clé de signature peut-être à usage unique (éphémère) pour une seule transaction de signature de documents ou réutilisable :

- si elle est éphémère, elle doit être détruite à la fin de la transaction ;

- sinon elle est conservée par le prestataire de confiance ;

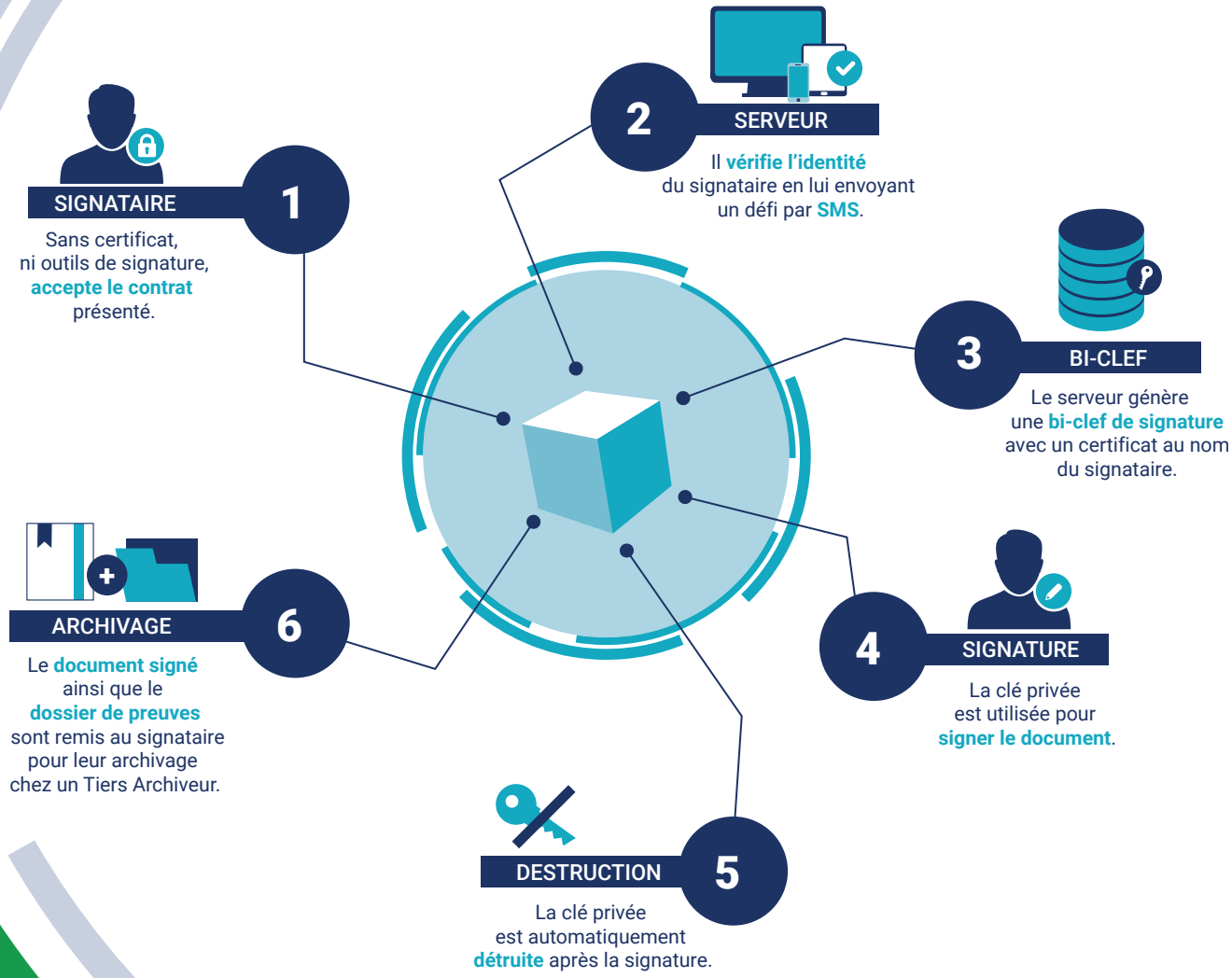
L'activation de la clé de signature (pour son utilisation) est basée sur une authentification du signataire distant :

- pour la signature simple, le facteur d'authentification doit être non rejouable, par exemple un « One Time Password » ;

- pour la signature avancée, il faut deux facteurs d'authentification de natures différentes.

Parcours de la signature à la volée

Le fichier de preuves n'est que la trace de cette histoire, trace qui permet dans le temps de démontrer l'existence d'un processus de signature et la validité du document associé.



Le fichier de preuves

Contenu du fichier de preuves

Le fichier de preuves doit contenir *a minima* les informations suivantes (*les informations en italique sont optionnelles mais recommandées*) :

Format du fichier de preuves

Il est recommandé que le fichier de preuve soit au format PDF/A (ISO 19005-2).

Il doit contenir le cachet serveur de l'opérateur de signature au format PAdES (ETSI TS 102 778) [5].

La documentation

Celle que doit fournir l'opérateur de signature à la volée doit préciser :

- Le contenu exact des fichiers de preuves fournis ;
- Le mode de transmission de ceux-ci ;
- Les moyens d'authentification de l'opérateur de signatures.

IDENTIFIANT*

- L'opérateur de signature [2] ;
- Celui qui a initié le processus de signature ;
- Chaque signataire avec notamment :

Identification [3]

Nom ;
Prénom ;
N° téléphone ;
Adresse e-mail ;
Adresse IP (Internet Protocol) ;

- **Liaison avec le ou les documents signés**
  - Empreinte (*Hash*) du document ;
  - Algorithme du calcul de l'empreinte (*hash*) ;
  - *Nom du document ;*
- **Traces de connexion au serveur** (date et heure, notamment) ;
- **Traces horodatées** de tous les évènements significatifs du processus de signature depuis le déclenchement par l'initiateur de collecte jusqu'à l'envoi des documents aux parties signataires comme :
  - *Traces d'envoi OTP ;*
  - *Traces d'envoi de SMS ;*
  - *Traces d'envoi d'e-mails ;*
- **L'horodatage des signatures** (conforme à la norme ISO 8601 [4])
- **La trace de la vérification** du jeton d'horodatage

* Identifiant unique du fichier de preuves (l'unicité s'entend pour un opérateur de signature donné) ;

(2) Le RIC peut être un moyen de définir un identifiant de l'opérateur (voir le « Guide pratique de mise en œuvre du Relevé d'Identité de Coffre-fort numérique »).

(3) Il convient en fonction du type de données à caractère personnel collectées dans le fichier de preuves de mettre en œuvre des moyens techniques, des processus et des contrôles conformes au RGPD (Règlement 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE).

(4) ISO 8601 Data elements and interchange formats — Information interchange — Representation of dates and times.

(5) Un moyen simple de contrôler une signature PAdES est d'ouvrir le document dans une version récente de Reader d'Adobe. Il suffit de cliquer sur le panneau « signature » pour voir le contenu de celle-ci et pour pouvoir la vérifier.

En Conclusion

La signature électronique « à la volée » est un outil simple pour permettre la contractualisation entre deux parties. Mais, dans ce cadre, se pose la question de l'archivage des documents numériques signés.

En mettant en œuvre le fichier de preuve de signature et en assurant l'intégrité dans le temps de l'ensemble document signé et son fichier de preuve de signature associé, il y a là un moyen simple et peu coûteux de conserver la validité d'un contrat numérique dans le temps.

Le présent guide souhaite démontrer que la constitution de ce fichier de preuves est simple à réaliser.

Remerciements

Pascal Agosti (Caprioli & Associés), Alain Borghesi (Cecurity.com), Denis Bourdillon (PRO Archives Systèmes), Séverine Denys (Docapost), Joseph Elias (Asterion), Amélie Frezier (Edicom), Gabriel Gil (GLI Services), Franck Leroy (Docapost), Jean-Louis Pascon (Open Bee), Bruno Ricci (Cecurity.com), Hervé Streiff (Locarchives).

Annexes I, II et III

fntc

L'ASSURANCE D'USER EFFICACEMENT ET EN TOUTE SÉRÉNITÉ DU NUMÉRIQUE

ANNEXE I

Cadre juridique

Le législateur européen avait adopté dès 1999, une directive encadrant le régime juridique applicable aux signatures électroniques (6). Cette directive visait à renforcer la confiance sur les réseaux numériques au sein de l'Union Européenne. Cependant, les différentes lois de transposition de cette directive dans les états membres ont créé des exigences diverses et variées. Après 15 ans d'application, le législateur européen a constaté que l'harmonisation souhaitée n'avait pas eu lieu et que les technologies utilisées avaient évolué depuis 1999. Suite à ce constat, le législateur européen a adopté le règlement n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché int érieur (7), abrogeant ainsi la directive de 1999.

Les considérants issus de ce règlement définissent trois objectifs principaux :

- *susciter la confiance,*
- *résoudre les problèmes du marché unique numérique,*
- *et renforcer la sécurité juridique.*

La directive 1999/93/CE a été abrogée et ce sont donc les nouvelles dispositions relatives à la signature électronique **qui sont applicables le 1er juillet 2016**. La transition s'effectuera jusqu'au 1er juillet 2020, date d'expiration potentielle du dernier certificat émis sous l'emprise de la précédente directive.

La signature électronique permet de garantir l'intégrité du document signé et l'identité du signataire.

Les degrés de fiabilité de la signature électronique

Du point de vue technique, **le Règlement prévoit les mêmes niveaux de sécurité de la signature électronique qu'en droit français**. L'article 3 énonce trois niveaux :

Simple

- « *des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer* » (art 3 al 10).

Avancée

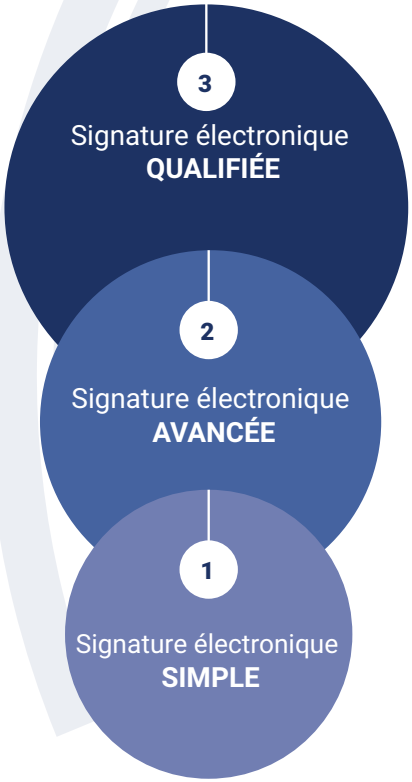
- « *une signature électronique qui satisfait aux exigences de l'article 26. Elle doit être liée au signataire, permettre d'identifier ce dernier, elle doit avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif et être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable (intégrité)* ». (art 3 al 11) ;

(6) Directive 1999/93/CE du 13 décembre 1999 (Directive 1999/93/CE du 13 décembre 1999, JOCE n° L. 13, 19 janvier 2000, p.12 s ; E. Caprioli, 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).

(7) JOUE L. 257 du 28 août 2014, p. 73 et s. Pour plus de détails, voir E. Caprioli, Signature électronique et dématérialisation, éd. LexisNexis, 2014 ; concernant la Proposition de Règlement, E. Caprioli, P. Agosti, La régulation du marché européen de la confiance numérique : enjeux et perspectives de la proposition de règlement européen sur l'identification électronique et les services de confiance, Comm. Com. Electr., n° 2, février 2013, p. 10-19 ; Th. Piette-Coudol, Une législation européenne pour la signature électronique (À propos du règlement européen sur l'identification électronique et les services de confiance), Droit de l'immatériel, n° 84, juillet 2012, p. 14 s.

Qualifiée

- « *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* ». (art 3 al 12).



De plus, le considérant 52 du Règlement intègre la signature électronique centralisée (« *remote electronic signature* »), c'est-à-dire activée à distance comme les signatures électroniques « à la volée ». Le même considérant précise « *afin que ces signatures reçoivent la même reconnaissance juridique que les signatures électroniques créées avec un environnement entièrement géré par l'utilisateur, les prestataires offrant des services de signatures électronique à distance devraient appliquer des procédures de sécurité spécifiques en matière de gestion et d'administration et utiliser des systèmes et des produits fiables, notamment des canaux de communication électronique sécurisés, afin de garantir que l'environnement de création de signatures électroniques est fiable et qu'il est utilisé sous le contrôle exclusif du signataire* ».

Concernant les effets juridiques des signatures électroniques

L'article 25 de la directive reprend les clauses de l'article 5 de la directive de 1999, relatives à la **non-discrimination** et à **l'assimilation**. Ce même article prévoit que l'effet juridique d'une signature qualifiée est **équivalent à celui d'une signature manuscrite**, ce qui n'est pas expressément prévu dans le code civil français.

Le règlement ne prévoit pas que la signature électronique garantisse expressément le consentement du signataire au contenu juridique de l'acte signé contrairement à l'article 1367 du code civil.

De plus, concernant la **signature électronique non qualifiée**, celle-ci ne peut se voir refuser d'effet juridique au seul motif qu'elle se présente sous une forme électronique ou qu'elle ne satisfait pas à toutes les exigences de la signature électronique qualifiée (considérant n°49).

Jurisprudences existantes

Les tribunaux se sont déjà saisis de la question de la valeur juridique de la signature électronique à la volée dans le domaine bancaire et assurantiel. Ainsi, les avenants à des contrats de crédit à la consommation (crédit revolving) dans le cadre de Cours d'appel (Cour d'appel de Nancy, 14 février 2013 [8] ; Cour d'appel de Douai, 2 mai 2013) ont été signés à l'aide de ce type de signature et conservés dans des fichiers de preuve (qui contiennent l'ensemble des éléments de preuve concernant la réalité d'une opération donnée – Cf. § 4).

Le Juge considère qu'une signature électronique simple (y compris établie à la volée) est suffisante dès le moment où les exigences juridiques prévues dans le Code civil (identification du signataire, manifestation du consentement, intégrité) sont respectées. Ce constat met bien en exergue le fait que ce que le Juge attend, est de pouvoir démontrer **la fiabilité d'un procédé de contractualisation**.

Liens avec le RGPD

Les questions relatives à la protection des données à caractère personnel (pour tous les services de confiance y compris les signatures électroniques à la volée) sont traitées à l'article 5 du Règlement eIDAS qui indique :

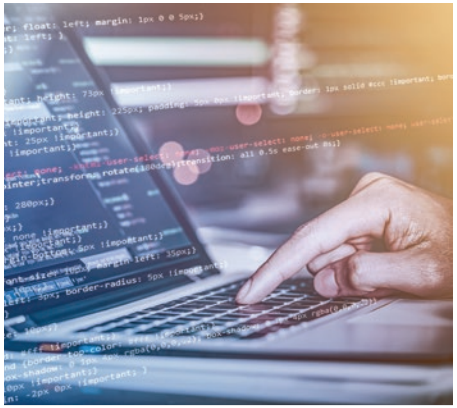
« *1. Le traitement de données à caractère personnel est effectué conformément aux dispositions de la directive 95/46/CE.*

2. Sans préjudice des effets de droit donnés aux pseudonymes en vertu du droit national, l'utilisation de pseudonymes dans une transaction électronique n'est pas interdite ».

En mai 2018, les Prestataires de Services de Confiance devront prévoir une démarche de privacy by design pour tous les traitements relatifs aux porteurs de certificats.

Que retenir du cadre juridique

Si mon problème n'est pas de devenir un spécialiste du droit de la preuve mais de mettre en œuvre une signature à distance.



Les textes juridiques existent et il n'y a pas lieu d'attendre quoi que ce soit pour se mettre à déployer des signatures électroniques à la volée. Ces dernières ont une valeur juridique qui peut être équivalente à celles d'autres signatures électroniques dès le moment où le signataire/Prestataire peut rapporter la preuve de leur fiabilité (en produisant par exemple les Politiques de Certification ou de Gestion de Preuve).

(8) V. E. Caprioli, Première décision sur la preuve et la signature électronique d'un contrat de crédit à la consommation, JCP éd. G n°18, 2013, 497, p.866 à 869 et Comm. Com. Electr. 2013, Juin, Etude 11, p. 13 à 17. D'autres décisions reprenant la même argumentation et où la signature électronique n'a pas été déniée, existent : CA Douai, 8e ch., 1re sect., 2 mai 2013, v. Comm. Com. Electr. n° 2, Février 2014, com. 22, note E. Caprioli.

ANNEXE II

Les normes

Pour la vérification des identités qui aboutissent à la création d'un certificat à clé publique, les normes sont les suivantes :	
EN 319 411 Partie 1	Pour les certificats standards : *http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.02.00_20/en_31941101v010200a.pdf*
EN 319 411 Partie 2	Le complément pour les certificats qualifiés : *http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.02.00_20/en_31941102v020200a.pdf*
Pour le contrôle exclusif de la clé de signature :	
EN 419 241 Partie 1	- Niveau SCAL1 - pour un niveau de confiance faible. - Niveau SCAL2 - pour un niveau de confiance élevé. *NB : le règlement eIDAS demande un niveau de confiance élevé pour la signature avancée.*
Pour la certification des équipements de création de signature :	
EN 419 241 Partie 2	• pour le module d'activation de la signature à distance.
EN 419 221 Partie 5	• pour le module cryptographique.
Pour la qualification des prestataires de confiance utilisant un composant de création :	
ETSI TS 119 431 Partie 1*	• en cours de rédaction) • La commission européenne publie des « *Trust List* » :
EN 419 221 Partie 5	• pour le module cryptographique.
Pour les prestataires :	
https://webgate.ec.europa.eu/tl-browser/#/	
Pour les équipements de création de signature :	
https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds	

Que retenir des normes

Si mon problème n'est pas de devenir un TSP mais de mettre en œuvre une signature à distance conforme à mes besoins ?

Les normes sont des guides de bonnes pratiques, pour une utilisation volontaire. Lorsque le service (ou une partie) est rendu par un prestataire, il convient que ce dernier fournisse un service qui soit conforme aux bonnes pratiques.

Il faut notamment faire attention à ce que les certifications mises en avant par le prestataire, correspondent effectivement au service vendu. Par exemple un prestataire peut être qualifié européen pour le service d'horodatage et vendre un service de signature en laissant croire que le service est qualifié (voire certifié…) au niveau européen.

ANNEXE III

Cas d'usage

Contrat de travail

Ce type de contrat se réalise en deux phases :

Phase 1

Le candidat rencontre son futur employeur et lui fournit dans le cadre de son dossier de candidature différentes pièces dont des justificatifs d'identité et de domicile.

Phase 2

Lors que le candidat est retenu, son futur employeur :

- Lui fait parvenir son contrat de travail, qui peut comporter plusieurs documents complémentaires, au format PDF ;
- Lui fait parvenir par SMS le code de signature du certificat « *à la volée* », qui a été généré à son intention à partir des informations récupérées lors de l'entretien de sélection qui s'est déroulé en « *face à face* ». L'employeur joue le rôle d'une autorité d'enregistrement ;

En fonction de la nécessité pour le salarié de signer d'autres documents dans l'avenir (notes de frais…) le certificat peut être à usage unique comme à usage multiple ;

- Lui fait signer à distance les divers documents par la saisie de ce code confidentiel.

À la fin du processus l'employeur

- **Doit archiver pour son propre compte :**
  - le contrat de travail et tous les documents qui ont été signés ;
  - toutes les pièces ayant permis d'identifier parfaitement le salarié et de lui délivrer un certificat à la volée, éventuellement à usage unique ;
- **Doit remettre au salarié son contrat de travail signé, par exemple dans un coffre-fort numérique personnel.**

Contrat de travail (dit d'usage) : exemple « stadier »

Lors d'un match de foot, par exemple, le club va envoyer le contrat de travail à tous les stadiers enregistrés dans la liste (exemple 1 000) et seuls les premiers à répondre (500 par exemple) pourront signer leur contrat.

Ce type de contrat se réalise en trois phases :

Phase 1

- le candidat rencontre son futur employeur et lui fournit dans le cadre de son dossier de candidature différentes pièces dont des justificatifs d'identité et de domicile. Pour les candidats retenus l'employeur archive toutes les pièces ayant permis d'identifier parfaitement le salarié et de lui délivrer un certificat à la volée, à usage unique uniquement. L'employeur joue le rôle d'une autorité d'enregistrement.

Phase 2

Lorsqu'un match de foot est programmé l'ensemble de tous les candidats vont recevoir, généralement une semaine avant :

- Leur contrat de travail (dit d'usage) au format PDF ;
- Par SMS le code de signature du certificat « *à la volée mais à usage unique* », qui a été généré à son intention à partir des informations récupérées lors de l'entretien de sélection qui s'est déroulé en « *face à face* ».

Phase 3

- Tant que le nombre prévu de stadiers n'est pas atteint, les candidats pourront signer à distance les divers documents par la saisie de ce code confidentiel ;
- Dès que le nombre est atteint tous les certificats non utilisés seront révoqués afin qu'ils ne puissent plus être utilisés.

Dans ce cas précis la signature électronique nécessite un test en temps réel de la validité du certificat (jeton OCSP).

À la fin du processus l'employeur :

- Doit archiver pour son propre compte : le contrat de travail et tous les documents qui ont été signés ;
- Doit remettre au salarié son contrat de travail signé, par exemple dans son coffre-fort numérique personnel.

Contrat de complémentaire santé souscrit sur un portail internet

Cas d'un nouveau client

Dans ce cas où le souscripteur du contrat est inconnu de la compagnie d'assurances celui-ci va devoir :

- Choisir le contrat qui lui convient ;
- Renseigner un certain nombre d'informations personnelles sur son identité et de celles des personnes qu'il souhaite assurer avec lui ;
- Indiquer les références bancaires du compte qui recevra les divers remboursements ;
- Payer la première échéance.

Faisant suite à cette saisie la compagnie va :

- Lui présenter un contrat, qui comporte plusieurs documents réglementaires, au format PDF ;
- Lui fait parvenir par SMS le code de signature du certificat « à la volée » qui a été généré pour son usage ;
- Lui faire signer les divers documents par la saisie de ce code confidentiel.

Quelle est la valeur juridique d'un tel contrat puisqu'il n'est pas possible :

- D'identifier avec certitude le signataire et donc d'authentifier sa signature ;
- De s'assurer de la réalité des informations fournies par le signataire.

Le contrat est pourtant juridiquement valable suite à la signature électronique par la compagnie d'assurances, car en tant que professionnel l'assureur devait prendre toutes les mesures pour garantir ses droits et devoirs ainsi que ceux de son client particulier.

Toutefois, dans le cas des complémentaires santés

Il y a un processus de connexion avec la CPAM (NOEMIE) qui permet à l'assureur de récupérer toutes les informations relatives au souscripteur et à ses ayants droits ; L'assureur peut donc comparer ces informations avec celles déclarées par le souscripteur ;

- L'assureur peut aussi procéder à la vérification des coordonnées bancaires grâce au premier paiement (par carte bancaire) et à l'IBAN qui a été fourni.

Tant que ces informations n'ont pas été communiquées et intégrées dans le système d'information (SI) de l'assureur, celui-ci ne peut pas techniquement rembourser d'éventuels frais de santé. L'assureur profite donc de ce délai (15 jours environ) pour vérifier une éventuelle fausse déclaration (intentionnelle ou non) afin de résilier le contrat signé et ce avant tout remboursement.

Signature électronique d'un Acte d'Engagement

Contrat entre un organisme public et une société privée

La réglementation impose que l'Acte d'Engagement (nom du contrat avec les organismes publics) soit signé aussi bien par l'organisme public que par son prestataire.

Dans la pratique l'Acte d'Engagement est imprimé et doit donc être signé de manière physique par les deux personnes physiques mandatées pour.

Compte tenu du fait que très peu de sociétés disposent d'un certificat électronique la solution consiste à faire une convention de preuves entre les parties :

Phase 1

L'organisme public émet son appel d'offres et indique dans le document dénommé RC (Règlement de la consultation) que si la société désire répondre elle accepte de signer l'AE de manière électronique avec un certificat qui sera émis en son nom, à partir des informations portées sur le document DC1, si sa candidature est retenue.

Phase 2

La société candidate qui postule à cet Appel d'Offres envoie à cet organisme public tous les documents demandés.

Phase 3

Lorsque la société candidate est retenue, l'organisme public :

- Lui fait parvenir L'AE (Acte d'engagement), qui peut comporter plusieurs documents complémentaires, au format PDF ;
- Lui fait parvenir par SMS le code de signature du certificat « *à la volée* », qui a été généré à son intention à partir des informations récupérées sur les pièces justificatives envoyées dans le dossier de candidature. L'organisme public joue le rôle d'une autorité d'enregistrement ;
- Lui fait signer à distance les divers documents par la saisie de ce code confidentiel.

À la fin du processus l'organisme public doit :

- Archiver, pour une durée de 10 ans, l'ensemble des pièces fournies par la société candidate (obligation réglementaire) ; Toutes les preuves sont donc bien archivées ;
- Doit remettre à la société retenue son AE signé.

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

Elle regroupe aujourd'hui les principaux professionnels de la dématérialisation répartis en 4 collèges en fonction de leur activité professionnelle, tous concernés directement ou indirectement par la sécurisation des échanges électroniques et la conservation des informations. Elle réunit 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). Elle a pour but d'établir la confiance, de promouvoir la sécurité et la qualité des services dans le monde de l'économie numérique, d'offrir une garantie aux utilisateurs et de défendre les droits et intérêts liés à la profession des Tiers de Confiance.

www.fntc-numerique.com

fntc

L'ASSURANCE D'USER EFFICACEMENT ET EN TOUTE SÉRÉNITÉ DU NUMÉRIQUE