*Club***PSCo**

Document pédagogique à l'attention des utilisateurs et porteurs d'applications de signature électronique

Version	Date	Description	Auteurs	Entité
1.0	27/06/2012	Document public, pour diffusion OID : 1.3.6.1.4.1.39270.2.1	E. Combet / J. Bordier	Club PSCo

Ce document est la propriété exclusive du *Club*PSCo,

Association loi de 1901, créée par acte authentique devant notaire en date du 18/1/2011.

Son usage est réservé à l'ensemble des personnes habilitées selon leur niveau de confidentialité.

Sa reproduction est régie par le Code de la propriété intellectuelle qui ne l'autorise qu'à l'usage privé du copiste

SOMMAIRE

I. OBJECTIF DE CE DOCUMENT 3
II. DIFFERENTES SIGNATURES ELECTRONIQUES, POUR DIFFERENTS USAGES 4
A. Principes et notions 4
B. Différents types de signature électronique, pour différents usages, en fonction des risques ... 5
1. Exemples concrets d'usages 5
2. Une approche fondée sur la gestion du risque métier 6
3. Les différentes signatures électroniques et les différents certificats 7
III. RECOMMANDATIONS A L'ATTENTION DES UTILISATEURS DE LA SIGNATURE ELECTRONIQUE 10
A. Comment s'équiper d'un certificat électronique 10
B. Comment signer électroniquement 13
C. Comment vérifier la qualité d'une information reçu signée électroniquement 14
D. Comment conserver les informations signées électroniquement 16
IV. RECOMMANDATIONS A L'ATTENTION DES PORTEURS DE PROJETS DE SIGNATURE ELECTRONIQUE 18
A. Introduction 18
B. Intégrer la signature électronique aux processus métier 19
C. Rappel : se mettre en capacité d'exploiter les informations signées dans le temps 22
V. ANNEXES 24
A. Cadre juridique 24
B. Exemples d'usages 26
C. Différentes formes et formats de signature électronique 29
1. Signature enveloppée, enveloppante et détachée 29
2. Différents formats de signature électronique 29
3. Facteurs de choix entre ces formes et formats 30
VI. TERMES FREQUEMMENT UTILISES 32
VII. BIBLIOGRAPHIE & standards 35

I. OBJECTIF DE CE DOCUMENT

En France, la loi du 13 mars 2000 et son décret d'application du 30 mars 2001, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, a reconnu l'existence de la signature électronique sécurisée selon des critères stricts.

L'ordonnance 2005-1516 du 8 décembre 2005 a défini le terme de « Prestataire de Services de Confiance » (PSCO), comme toute personne offrant des services tendant à la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique. Ce terme recouvre les Prestataires de Services de Certification Électronique (PSCE), et les prestataires intervenant dans les domaines de l'authentification, la signature, l'horodatage et la confidentialité des échanges.

L'association « Club PSCO » a pour objet de regrouper l'ensemble des Prestataires de Services de Confiance (les « PSCO ») afin notamment d'encourager l'utilisation des services de confiances et de favoriser l'interopérabilité de ses services entre les utilisateurs.

Les membres du « Club PSCO » ont identifié la nécessité de renforcer le référentiel documentaire existant sur la signature électronique, pour encourager de façon pédagogique son usage, et faire part des retours d'expériences de ses membres sur ces problématiques complexes.

L'objet de ce document est de décrire, à l'aide d'exemples concrets, les notions et les usages de la signature électronique, et de fournir une série de recommandations à l'attention à la fois des porteurs de projets de signature électronique, et des utilisateurs de la signature électronique.

II. DIFFERENTES SIGNATURES ELECTRONIQUES, POUR DIFFERENTS USAGES

A. Principes et notions

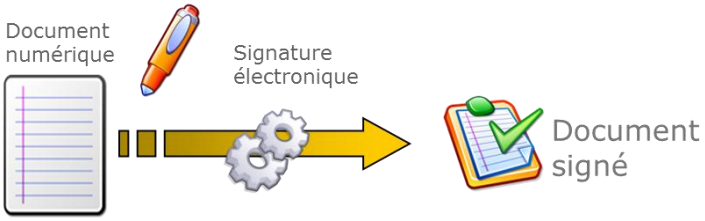
La signature électronique est la transposition dans le monde numérique de la signature manuscrite, et connue historiquement dans sa forme « papier ».

Elle a pour principales caractéristiques **d'identifier celui qui la produit** (le signataire) et de **garantir que la pièce numérique ainsi signée ne sera plus altérable** dans le temps, à l'issue de cette opération.

La signature électronique est aujourd'hui le seul procédé informatique permettant de donner la même valeur juridique à un écrit électronique qu'à un écrit traditionnellement papier.

Dans le monde numérique, comme dans les processus traditionnels non dématérialisés, tous les documents ne nécessitent pas d'être signés.

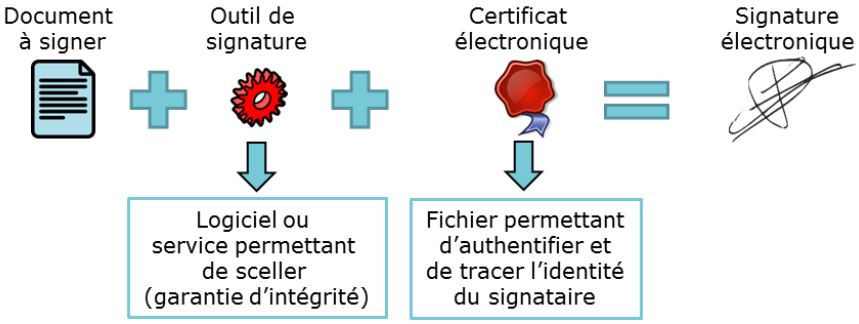
Néanmoins, dès lors que l'organisation, ou que l'individu, à l'origine de la production d'une pièce numérique (document / son / image) souhaite pouvoir prouver qu'il est bien l'auteur de cette pièce, et qu'elle est représentative de sa volonté, qu'elle est bien sa création, et qu'elle n'a pas été altérée depuis sa création, il n'a pas d'autres choix que de produire une signature électronique de cette pièce.



La signature électronique est donc le moyen permettant à une organisation, ou à un individu, qu'il est bien le producteur unique d'un fichier numérique devenu infalsifiable.

La signature électronique n'est pas simplement l'apposition d'une image numérisée de la signature manuscrite, sur un document numérique, elle consiste en l'usage de procédés cryptographiques, permettant de **faire le lien entre l'identité du signataire et le contenu du document** et de le rendre intègre, pour interdire sa falsification ultérieure.

Pour atteindre ce double objectif, la seule technique existante à ce jour consiste en l'utilisation de deux outils informatiques : **le certificat électronique**, délivré par une « Autorité de Certification », **et l'application de signature électronique**.



B. Différents types de signature électronique, pour différents usages, en fonction des risques

1. Exemples concrets d'usages

La signature électronique est aujourd'hui utilisée dans de nombreuses applications, et se démocratise progressivement quel que soient les secteurs d'activités concernés.

A titre d'exemple, on peut noter que la signature est mise en œuvre dans les processus métiers suivants :

- **Achats publics** : les entreprises souhaitant remettre une offre à un établissement public de façon électronique sont dans l'obligation de signer les pièces de leur offre de façon électronique. Cette pratique se démocratise progressivement, les établissements publics imposants de plus en plus à leurs fournisseurs de répondre via ce canal. Dans ce cas, **le signataire est une personne physique**, disposant d'un pouvoir du mandataire social pour remettre cette offre ;
- **Factures** : les entreprises souhaitant dématérialiser leurs factures, en format PDF, conformément à l'article 289-V du Code Général des Impôts, sont dans l'obligation de signer leur facture de façon électronique. En pratique, **la signature est réalisée sur un serveur**, sur lequel est installé le certificat électronique émis au nom de l'entreprise signataire. [1] ;
- **Contrats clients :** de nombreuses entreprises procèdent désormais à la dématérialisation des processus de souscription de leurs contrats clients, en mettant en œuvre des procédés, à distance ou en agence, permettant une souscription électronique et une validation électronique de ce contrat. En matière de signature électronique, les modalités de mise en œuvre sont variables en fonction du type de relations (en agence ou en ligne) et du niveau de risque associé au contrat. Par exemple, la souscription à certains contrats de téléphonie mobile est désormais possible en agence après signature électronique du client et de l'opérateur.
- **Etat Civil :** certaines administrations, et les notaires notamment, peuvent demander la vérification d'informations d'état civil à la mairie de naissance des citoyens concernés par leurs procédures, de façon électronique. En mairie, à réception de ces demandes de vérification, les **Officiers d'Etat Civil procèdent**

[1] Il est à noter que l'exigence du CGI relative à la signature électronique de factures, par une personne morale, est incohérente avec la notion de signature électronique, telle que définie dans le code civil, et visant généralement des personnes physiques. Cette disposition créé néanmoins un précédent intéressant sur lequel de nombreux usages, de signature de bulletins de paye, de contrats, s'appuient aujourd'hui.

à la signature électronique de leurs réponses, pour attester de leur traitement et fiabiliser le processus métier.

D'autres exemples sont détaillés en annexe de ce document, et il ne s'agit pas d'une liste exhaustive, tant les possibilités d'usages sont diverses.

Ces exemples démontrent à la fois :

- Le caractère « **transverse** » de la signature électronique, applicable quel que soit le secteur d'activité ;
- La **multiplicité des possibilités de mise en œuvre**, que le signataire soit une personne physique, ou une personne morale (un serveur informatique en pratique) ;
- La **diversité des enjeux, des risques associés**, et des niveaux de sécurité sous-jacents en conséquence.

2. Une approche fondée sur la gestion du risque métier

Comme le démontrent les exemples concrets d'usages, la signature électronique peut être mise en œuvre dans des conditions diverses, pour des usages extrêmement variés, et selon des niveaux de fiabilité plus ou moins élevés, pour des enjeux plus ou moins critiques.

Les critères principaux permettant de déterminer les moyens à mettre en œuvre pour produire une signature électronique sont à lier au « **risque métier** », c'est à dire à l'identification des impacts en termes de responsabilités, en termes financiers, d'image, de préjudices potentiels au regard des usages visés.

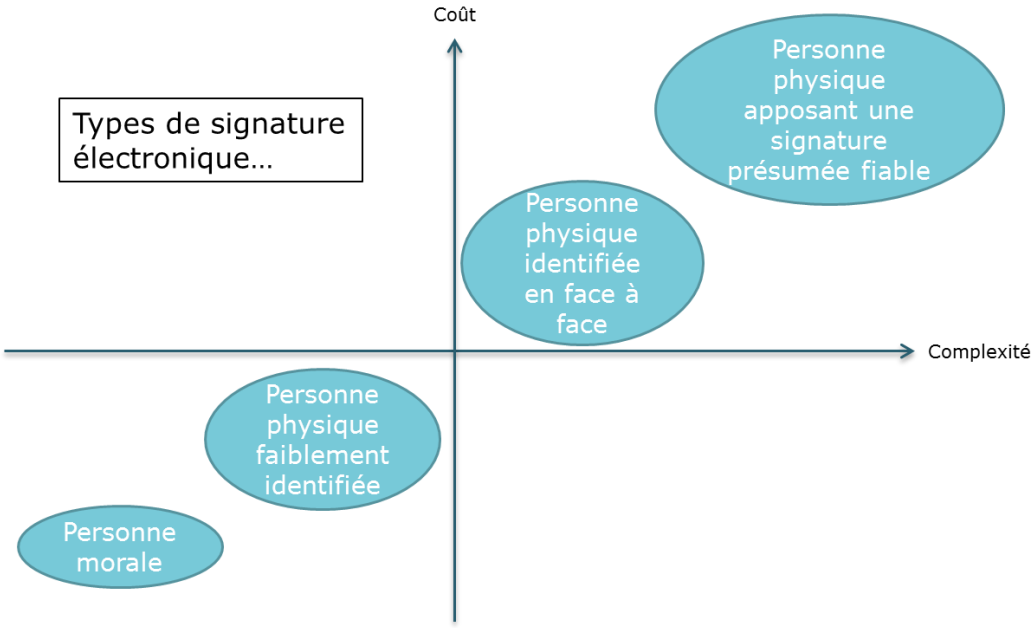
Le rationnel est en effet relativement simple :

Pourquoi signer ?	Pour qui signer ?	Quelle valeur a ma signature ?
Signer sert à prouver qui est à l'origine d'une information numérique, et cette signature ne s'impose **que si le risque de ne pas disposer de cette preuve** peut générer un préjudice	**Signer sert les besoins des « destinataires »** qui ont besoin de savoir nominativement qui est à l'origine de la signature électronique ou simplement quelle est l'organisation dont émane cette information numérique	Signer sert à **donner une valeur juridique** à mon information numérique dans l'hypothèse d'une contestation ultérieure.

Sur le fond, ce rationnel est très similaire à celui traditionnellement connu dans l'univers papier. La preuve de l'identité est en effet démontrée de façon plus ou moins « fiable » selon le type d'information manipulée, et selon le risque associé.

Document non signé	Tampon de l'organisation	Signature manuscrite	Signature d'actes authentiques

En fonction de ces différents niveaux de risques, le cadre juridique et les moyens proposés par les acteurs du marché se sont donc adaptés pour fournir une palette d'outils et de services couvrant la multitude des situations potentielles des utilisateurs de la signature électronique.



Le choix du « type de signature » est le principal critère déterminant ultérieurement les conditions de mise en œuvre, mais il impacte les coûts et complexités ultérieurs liés à la mise en œuvre.

En synthèse, et à l'image des recommandations issues du décret « Référentiel Général de Sécurité » (cf. V.A Cadre juridique), **ce choix doit être issu d'une analyse de risques liée aux usages visés,** une **analyse des contraintes juridiques et réglementaires**, qui pèsent sur le signataire, et sur les modalités opérationnelles réalistes de mise en œuvre, notamment celles relatives aux conditions de distributions des certificats électroniques (cf. 3 Les différentes signatures électroniques et les différents certificats).

3. Les différentes signatures électroniques et les différents certificats

En fonction des choix issus de l'analyse des risques, différents types de signature peuvent être produits, en fonction :

- De la « qualité sécuritaire » du certificat électronique et du type de signataire (personne morale ou personne physique) ;
- De l'architecture retenue pour la mise en œuvre.

Les certificats électroniques :

Le cadre juridique a fixé en synthèse plusieurs niveaux de qualité pour les certificats et les signatures électroniques.

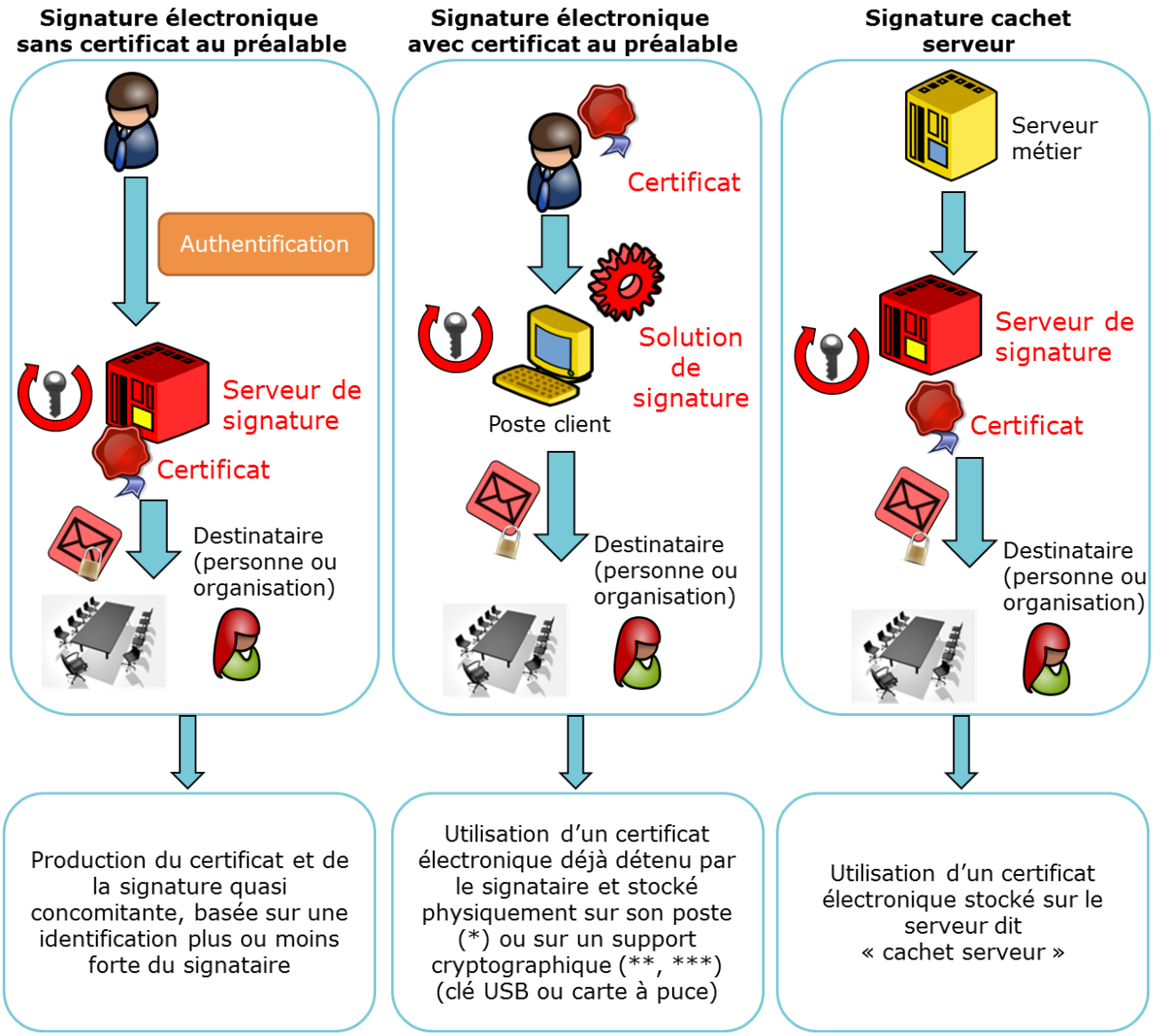
La notion suivante d'étoiles (*, **, ***) provient du décret « Référentiel Général de Sécurité » (cf. V.A Cadre juridique), qui, même s'il ne s'applique strictement qu'aux échanges entre les autorités administratives et leurs destinataires, constitue une échelle de « valeur » pour le marché français.

	Certificats personnes physiques (signature personne physique)			**Certificat personne morale**
⊘ (0 étoile)	*	**	***	
certificat remis dans des conditions définies par son producteur (ex : sur la base d'informations connues du porteur)	certificat remis sans face à face, mais sur la base d'un dossier d'enregistrement contenant une pièce d'identité	certificat remis après un face à face (avant ou lors de la remise)	certificat remis avec face à face sur un matériel certifié conforme au décret 2001-272	certificat « cachet serveur », remis au représentant de l'organisation
signature simple	signature simple	signature électronique sécurisée	signature électronique présumée fiable	signature électronique personne morale

Les entités économiques sont également intéressées par le RGS, et ceci pour trois raisons essentielles :

- Le RGS constitue un ensemble de bonnes pratiques adoptées par un nombre croissant d'acteurs, garantissant pour elles une cohérence avec les pratiques futures, lorsque la standardisation naissante deviendra réellement opérationnelle ;
- Elles peuvent utiliser des certificats RGS lors de leurs interactions avec des téléservices publiques nécessitant une labellisation « RGS » de leurs certificats ;
- Les normes RGS sont issues des normes ETSI (102 042 correspondant aux niveaux * et ** et 101 456 correspondant au niveau ***), normes européennes facilitant les échanges à valeur probante dématérialisés au niveau européen ou plus, ce qui ne manque pas d'intérêt pour des groupes français à stature internationale.

Les architectures de mise en œuvre envisageables :



Le choix d'architecture est conditionné par le type de certificat remis, et par la qualité recherchée pour la signature électronique. La matrice ci-dessous présente le rationnel de mise en œuvre généralement constaté.

	Signature électronique sans certificat au préalable	**Signature électronique avec certificat au préalable**	**Signature « cachet serveur » avec certificat au préalable**
Certificat pers physique ⊘			
Certificat pers. physique *			
Certificat pers. physique **			
Certificat pers. physique ***			
Certificat pers. morale			

III. RECOMMANDATIONS A L'ATTENTION DES UTILISATEURS DE LA SIGNATURE ELECTRONIQUE

A. Comment s'équiper d'un certificat électronique

Les utilisateurs de la signature électronique peuvent s'équiper d'un certificat électronique en contactant l'un des organismes référencés ci-dessous, selon les cas de figure :

- Leur organisation, ou leur tutelle, si celle-ci produit des certificats utilisables pour signer électroniquement des documents (ex : le notaire auprès du Conseil Supérieur du Notariat) ;
- Une Autorité de Certification du marché, qui commercialise des certificats électroniques, et propose généralement une gamme de services incluant potentiellement des certificats « personnes physiques » et des « certificats serveurs » (personne morale).

L'Etat référence publiquement les Autorités de Certification du marché, selon deux « labels officiels » :

- **Le label « certificat PRIS »** : label historique permettant de créer un environnement de confiance interopérable avec la sphère publique pour les offres de certificats. Ce **label est amené à disparaître à compter de 2013**, remplacé par le label RGS, quand toutes les applications métier (téléservices publiques) auront migrés pour supporter les certificats labellisés « RGS ».

  La liste des Autorités de Certification PRIS est disponible sur le site : http://www.telecom.gouv.fr/rubriques-menu/entreprises-economie-numerique/certificats-references-pris-v1/categories-familles-certificats-references-pris-v-1-506.html

- **Le label « certificat RGS »** : label existant depuis la parution du décret RGS (cf. V.A Cadre juridique), il s'applique progressivement à tous les téléservices publiques, et constitue désormais l'échelle de « valeur » dont dispose le marché.

  La liste des Autorités de Certification RGS est disponible sur les sites :

  - De la Direction Générale de la Modernisation de l'Etat : http://references.modernisation.gouv.fr/autour-du-rgs
  - De l'auditeur qui effectue les contrôles de ces services : http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=54&Itemid=14&lang=fr

Certaines Autorités de Certification ont fait certifier leurs offres selon les labels européens ETSI 102 042 et ETSI 101 456 (http://www.lsti-certification.fr/index.php?option=com_content&view=article&id=54&Itemid=14&lang=fr)

Les Autorités de Certification disposent généralement d'une gamme de certificats, pouvant couvrir tout ou partie des possibilités offertes par les référentiels décrits ci-dessus (cf. II.B.3 - Les différentes signatures électroniques et les différents certificats).

Pour savoir comment choisir son certificat électronique, parmi les différents types proposés par les Autorités de Certification, il faut avant tout se soucier :

- de la **compatibilité avec les applications cibles**

  Exemple: certaines plates-formes de marché n'acceptent pour l'instant que des certificats PRIS.
- de **la valeur juridique de la signature**

  *Exemple : si la signature électronique doit être sécurisée (cf. V.A Cadre juridique), la seule option consiste à faire l'acquisition d'un certificat RGS ** ou ***.*
- des **exigences éventuelles des utilisateurs des informations signées**, qui peuvent librement choisir de ne « reconnaître » que certaines Autorités de Certification du marché.

  Exemple : le secteur bancaire a défini une « Politique d'Acceptation Commune » permettant de lister les gammes de certificats acceptés pour les usages bancaires de la signature électronique.

Sur le plan pratique, obtenir un certificat est plus ou moins contraignant selon le niveau de sécurité associé (un certificat du niveau * étant plus simple à obtenir qu'un certificat du niveau ***). La procédure implique au moins deux étapes : la demande du certificat et la remise du certificat.

Demande de certificat :

Un futur porteur de certificat doit, pour en faire l'acquisition, suivre la procédure que lui indique l'Autorité de Certification qu'il a retenue (ou qui lui a été imposée).

Cette procédure implique généralement, pour la demande de certificat :

- **Dès le niveau *** pour les certificats RGS, ou pour les certificats PRIS : la constitution d'un dossier de demande de certificat, incluant au moins :
  - **un formulaire de demande** signé par un représentant légal de l'organisation, ou par une personne déjà connue par l'Autorité de Certification et référent pour son organisation (le mandataire de certification) ;
  - une **copie d'une pièce d'identité** en cours de validité ;
  - une **copie signée des conditions générales d'utilisation du service** ;

- **A partir du niveau ****, la constitution d'un dossier de demande équivalent et la réalisation d'un face à face physique entre le futur porteur du certificat et le représentant de l'Autorité de Certification, ou le mandataire de son organisation.

Remise du certificat :

Après traitement et acceptation du dossier de demande par l'Autorité de Certification, celle-ci reprend contact avec le futur porteur pour lui indiquer dans quelles conditions opérationnelles il peut le récupérer.

Les techniques utilisées par les Autorités de Certification pour sécuriser le processus de remise du certificat sont diverses, selon les spécificités propres à chacune d'entre elles et les exigences imposées par le niveau de qualité sécuritaire du certificat (ex : un certificat, à partir du niveau ** est nécessairement remis sur un support cryptographique (clé USB ou carte à puce)).

En pratique, différentes techniques sont généralement mises en œuvre parmi lesquelles :

- **Un ou plusieurs mails sont transmis au futur porteur** du certificat pour lui indiquer que son certificat est disponible et prêt à être retiré (en cliquant sur un lien dans le mail et en saisissant un code de retrait communiqué par ailleurs, ou en se rendant dans un lieu spécifique, par exemple) ;
- **Un support cryptographique (clé ou carte)** est transmis au porteur (à partir du niveau **), suivi par exemple de l'envoi de son code PIN dans un courrier séparé ou remis à l'occasion d'un face à face.

Les pratiques des Autorités de Certification sont variées, en fonction de leurs choix commerciaux ou opérationnels respectifs, mais ces pratiques sont auditées vis-à-vis du même référentiel d'exigences, garantissant ainsi une qualité et une sécurité homogène pour les différents types de certificats électroniques d'un même niveau.

Cycle de vie du certificat :

A l'image d'une carte bancaire, un certificat remis peut :

- Expirer (un certificat a une durée de validité limitée) ;
- Etre révoqué (déclaré perdu ou volé) ;
- Etre renouvelé (avant expiration).

L'Autorité de Certification est le point de contact pour ces différentes opérations de gestion et assure des services de support (hot line, mails d'alerte…) pour faciliter la gestion de ces certificats par leurs porteurs et leurs organisations.

B. Comment signer électroniquement

Disposer d'un certificat électronique et d'un **outil de signature** est nécessaire à la production d'une signature électronique.

Dans certains environnements (messagerie, outils bureautiques), l'outil de signature est nativement intégré mais la plupart des applications métier n'intègrent pas d'outils de signature électronique.

Il est donc nécessaire d'avoir accès à ce type d'outils. Il y a plusieurs manières de le faire :

- En **s'équipant d'un logiciel ou service de signature électronique** permettant de signer électroniquement des fichiers préalablement produits, dans différentes formes potentiellement (cf. V.C Différentes formes et formats de signature électronique).

  Note : par souci d'interopérabilité et de stabilité sémantique, il est recommandé de ne signer électroniquement que des fichiers dans des formats textes, PDF, images. Les documents issus de logiciels bureautiques posent un certain nombre de difficultés à l'occasion, par exemple, d'exécution automatique de macro.
- En utilisant le module « **signature** » de l'application métier (logiciel comptable, solution de gestion, …), si l'éditeur de cette application a déjà intégré cette fonctionnalité.

Dans ce dernier cas, l'outil de signature électronique devrait être intégré de façon ergonomique, sous la forme de :

- Un **serveur de signature**, produisant automatiquement des signatures électroniques, à l'aide d'un certificat « cachet serveur » par exemple, sans nécessité d'installer un outil particulier sur le poste du client. Ce type de solution n'est néanmoins pas approprié lorsque le certificat électronique a été installé préalablement sur le poste du client à l'occasion de sa remise (cf. II.B.3 Les différentes signatures électroniques et les différents certificats).
- Un **composant de signature**, effectuant le même type d'opérations techniques, déployé automatiquement avec l'application métier sur le poste. Une fois paramétré, ce composant permet d'utiliser les certificats installés sur le poste, et de communiquer avec les éventuels supports cryptographiques (carte à puce ou clé USB) fournis par l'Autorité de Certification ;

Lors de la réalisation de l'opération de signature électronique, quelle que soit l'architecture utilisée, il est nécessaire que le signataire s'engage à respecter les conditions fixées par la « **Politique de Signature** », qui doit être rendue accessible (sous la forme d'un lien dans les écrans de l'outil de signature ou préalablement distribuée au signataire par exemple).

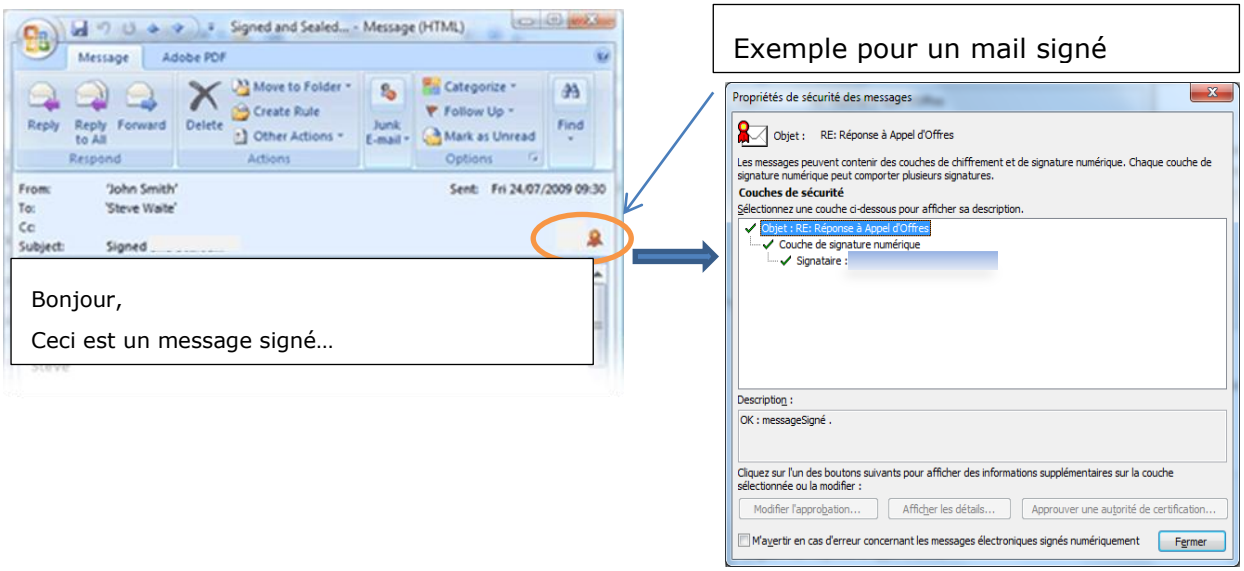
Ce document « Politique de Signature » expose notamment les conditions de production et de traitement des documents à signer, les modalités d'authentification et de création des identités à utiliser pour les signatures électroniques, les modalités de création, de conservation et de validation des signatures électroniques, les règles de protection physique et informatiques de l'environnement de création des documents et des signatures et fixe les **engagements, rôles et responsabilités des différents acteurs participant à ces opérations.**

Le *Club***PSCO** a par ailleurs rédigé un document d'aide à la rédaction de « Politiques de signature », disponible publiquement.

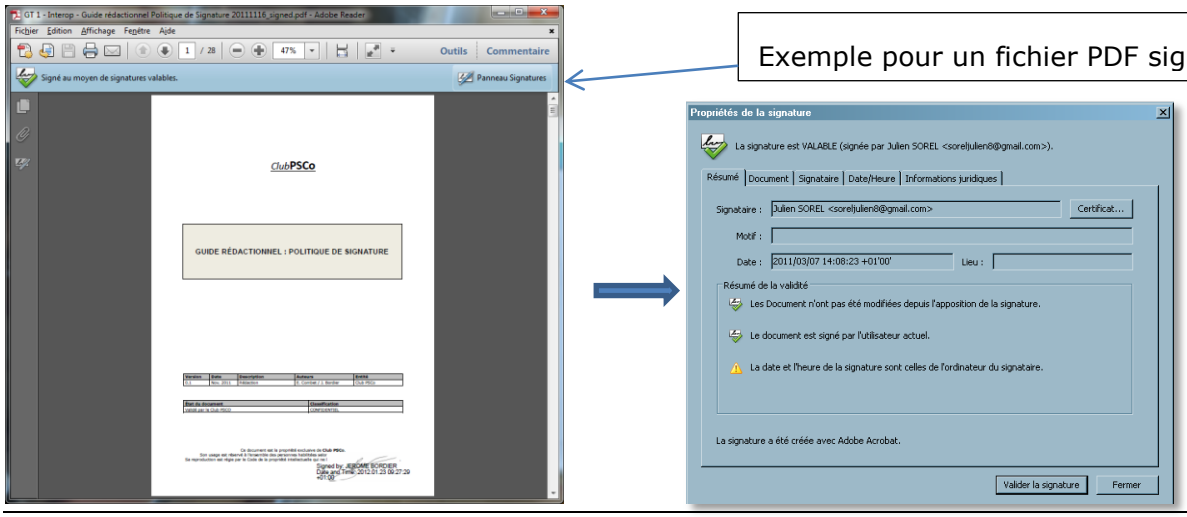
C. Comment vérifier la qualité d'une information reçu signée électroniquement

Une fois signée, **une information électronique doit faire apparaître explicitement qu'elle a été signée**.

Il est essentiel pour les destinataires d'informations signées de vérifier la signature pour s'assurer de la qualité des informations reçues et de l'identité de son signataire.



Exemple pour un mail signé



Exemple pour un fichier PDF signé

Pour vérifier une signature électronique, il suffit de :

- **Disposer du logiciel de lecture**, visualisation, associé au type d'information reçue (exemple : Adobe ® Reader, Microsoft ® Office, OpenOffice™, Thunderbird) ;
- **Utiliser les fonctions natives de vérification de signature** intégrées à ce logiciel, pour contrôler la qualité de la signature électronique.

Dans le cas de fonctions de signature intégrées à des applications métier, l'éditeur prévoit généralement la mise à disposition de fonctions de vérification, associées aux dispositions de conservation des informations signées (cf. D Comment conserver les informations signées électroniquement).

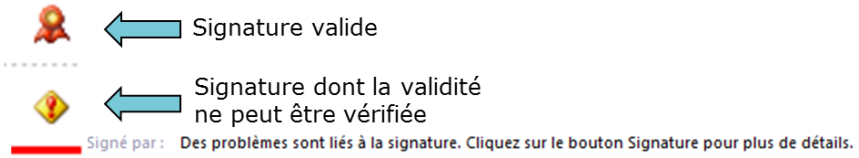
Pour qu'une signature électronique soit valide, il faut avant tout que :

- Le **certificat du signataire ait été valide** (non expiré, non révoqué) au moment de la signature électronique ;
- L'information **n'ait pas été modifiée** depuis l'opération de signature. En effet, l'une des vertus de la signature électronique est de protéger les informations électroniques signées contre toute altération, modification ultérieure, ce qui confère à ce type de signature une valeur ajoutée supplémentaire comparativement à la signature manuscrite traditionnelle.

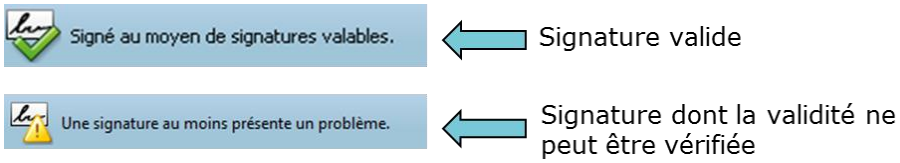
Les manipulations à effectuer pour vérifier une signature électronique sont généralement très limitées, le logiciel de visualisation (ou l'application métier) se chargeant de faire ces contrôles techniques et d'afficher visuellement au signataire et au destinataire l'état de la signature.

A titre d'exemple, ci-dessous deux représentations visuelles permettant d'identifier la signature et sa validité. Il est ensuite possible d'avoir des détails complémentaires sur la signature électronique et il est utile de se préoccuper des raisons d'une non validité éventuelle de la signature le cas échéant.

Pour un mail signé :



Pour un PDF signé :



D. Comment conserver les informations signées électroniquement

Etant donné que la signature électronique est produite pour attester de l'engagement pris par le signataire sur une information électronique, il va de soi que cette information, et la signature électronique associée, doivent être conservés, pendant la durée de contestation potentielle associée.

Ces deux éléments (information signée et signature) apparaissent sous la forme d'un fichier (signature enveloppante ou enveloppée) ou de deux fichiers (signature détachée). Quel que soit la forme de la signature électronique (cf. V.C.2 Différents formats de signature électronique), le ou les fichiers sont donc à conserver dans des conditions qui permettent dans le temps :

- Une **restitution « garantie »** en terme de capacité de visualisation des informations électroniques signées (d'où l'intérêt mentionné ci-dessus de ne retenir que des formats pérennes et interopérables en évitant de signer des documents bureautiques propriétaires et potentiellement illisibles quelques années après) ;
- Une **capacité de vérification ultérieure** de la signature en cas de contestation (dans les mêmes conditions que décrites au chapitre C Comment vérifier la qualité d'une information reçu signée électroniquement).

Il est donc nécessaire pour le signataire de s'assurer que des dispositions sont prises (par lui et, ou, par le promoteur de l'application métier de signature qu'il utilise) en matière de :

- **Sauvegarde et archivage informatique** des données signées, et des signatures électroniques (si la signature et l'information signée ne sont pas dans le même fichier). Les fichiers signés sont généralement conservés au sein de « **coffres forts électroniques** » ayant capacité à garantir une capacité de conservation dans le temps sans défaut, et à restituer plusieurs années, voire dizaines d'années plus tard, les données telles qu'elles ont été produites à l'époque ;
- **Horodatage des données signées**, pour assurer une capacité de vérification de la signature électronique dans le temps, si le besoin métier existe. En effet, l'horodatage d'une information signée permet de fixer un référentiel temps, intégré à la signature électronique sur le plan technique, et permettant ultérieurement de savoir précisément à quelle date (et heure) le signataire a utilisé son certificat électronique. Cette disposition permet ainsi de vérifier que ce certificat était effectivement valide (non expiré / non révoqué) à l'instant de la signature, potentiellement très longtemps après.

En matière de conservation, la signature électronique présente également une vertu intéressante, puisque chaque copie d'un fichier signé est elle-même une information originale, que rien ne différencie du fichier signé initialement. Chaque copie d'un fichier signé a donc la même valeur juridique que le fichier signé initialement (au contraire des photocopies ou copies numérisées d'un document papier portant une signature manuscrite).

IV. RECOMMANDATIONS A L'ATTENTION DES PORTEURS DE PROJETS DE SIGNATURE ELECTRONIQUE

A. Introduction

Les porteurs de projets de signature électronique sont généralement confrontés à une série de questions nouvelles, touchant à la fois des **dimensions techniques, organisationnelles, et juridiques**.

Considérant le fait que les choix d'architecture, de modèles de mise en œuvre, de niveau de qualité des certificats sont avant tout pilotés par des considérations relatives au risque, la principale recommandation initiale, lors du lancement du projet, consiste à **effectuer une analyse de ces risques**, **des contraintes réglementaires existantes**, pour **déterminer les besoins de sécurité**.

Les moyens à mettre en œuvre sont ainsi objectivement déterminables.

Les exemples cités en §II.B.1 sont d'ailleurs le reflet de ces analyses :

- En matière **d'achats publics**, comme en matière de **factures électroniques**, les moyens à mettre en œuvre (certificats, outils de signature) sont précisément décrits dans des textes réglementaires (même si les formats ne sont pas précisément définis, nuisant malheureusement à l'interopérabilité des solutions disponibles). Le porteur de projet de signature électronique devra donc s'attacher à retenir des moyens conformes à ces exigences juridiques ;
- En matière de **contrats clients**, plusieurs options sont envisageables, les contraintes réglementaires existantes n'étant pas particulièrement « dirigistes ». L'analyse de risques permet de déterminer le schéma optimal de mise en œuvre, combinant à la fois la simplicité d'usage, le meilleur retour sur investissement et un niveau de protection sécuritaire satisfaisant au regard des impacts éventuels liés à l'incapacité à prouver l'identité du client contractant ou à prouver l'intégrité du document souscrit. En pratique, les schémas de mise en œuvre varient entre :
    - **la signature électronique de contrats souscrits en ligne, sur base de certificat « cachet serveur »**, produite dès lors que le souscripteur communique certains paramètres permettant de l'identifier (potentiellement complétés par des échanges de SMS ou d'autres informations d'identification permettant de renforcer le niveau de sécurité) ;
    - **la signature électronique « personne physique »** (avec certificat préalablement remis ou pas). Le choix de remettre le certificat préalablement dépend dans ce cas de la capacité du promoteur de

l'application à faire suivre au souscripteur une procédure de remise du certificat (à des niveaux 0, * ou ** (cf. II.B.3) suivant le niveau de risque identifié).

- En matière de **dématérialisation des échanges en matière d'Etat Civil**, la « signature électronique sécurisée » (cf. VI) requise par les textes encadrants ces procédures nécessite la mise en œuvre de certificats électroniques sur support cryptographique (clé USB ou carte à puce) conforme au niveau **. Les choix relatifs aux certificats sont donc une nouvelle fois dictés par la réglementation applicable à la procédure dématérialisée.

Sur le plan des certificats et des outils de signature à utiliser**, il est recommandé d'utiliser des outils présentant des « labels de confiance »**, c'est-à-dire remis par des Prestataires de Services de Confiance (PSCo) ayant obtenu des diplômes comme la « qualification RGS », ou la « certification ETSI » de leurs opérations (cf. III.A).

Suivant les cas d'usages, les porteurs d'application de signature électronique doivent également déterminer d'autres modalités de mise en œuvre, notamment :

- Le **format de signature** (parmi les différents formats et standards existants tels que S/MIME, PKCS#7, CADES, PADES, XADES, PDF Signature) ;
- La **forme de la signature** (enveloppée / enveloppante / détachée) ;

L'annexe V.C de ce document permettra d'aider le porteur de projet dans ces choix de formes et de formats en présentant notamment les critères de choix associés. Le tableau des cas d'usages (cf. V.B) permettra également de présenter les pratiques actuelles du marché en fonction des secteurs d'activité et des typologies d'architecture informatique sous-jacentes.

Les porteurs de projet doivent également **se mettre en capacité de conserver**, restituer de façon lisible, vérifier dans le temps, les informations « originales électroniques » ainsi constitués pendant la durée de vie « utile » de ces informations. Le § C décrit les bonnes pratiques de mise en œuvre dans cet objectif.

B. Intégrer la signature électronique aux processus métier

La mise en œuvre de la signature électronique, le déploiement d'outils de signature électronique, doivent avant tout être conçus dans une logique centrée sur :

- **l'utilisateur signataire** (dans le cas de signature personne physique) ;
- **le (les) destinataire(s)** des informations signées.

Fondamentalement, la mise en œuvre de la signature électronique, en remplacement de la signature papier, n'a d'intérêt que si à la fois le signataire, et son (ses) destinataire(s)

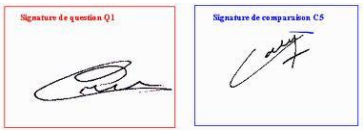
observent un gain qualitatif en matière de rapidité et d'efficacité. Si l'usage de la fonctionnalité de signature électronique apparaît comme plus fastidieux que l'usage de la signature papier, il est évident que le déploiement ne sera pas au rendez-vous.

En ce sens, on peut remarquer que la signature électronique présente un avantage important en évitant de faire parapher chaque page par le signataire, comme c'est la tradition dans le cas de la signature manuscrite.

Une bonne pratique consiste à repenser le processus de signature sans se limiter à une simple transposition de l'existant papier, pour l'optimiser et faciliter l'adoption par les utilisateurs.

Plusieurs fonctionnalités peuvent être mises en œuvre en électronique dans cet objectif, comparativement au processus de signature papier :

- **co-signature et contre signature** : la signature électronique permet de simplifier, d'accélérer, les processus de signature pour lesquels plusieurs signataires sont requis. Comparativement à la signature manuscrite, l'électronique permet de différencier :



la co-signature : permettant de savoir que deux personnes (au moins) ont signé sans savoir précisément l'ordre chronologique de réalisation de ces signatures ;

la contre signature : permettant d'identifier techniquement l'ordre chronologique des signataires ;

- **signature électronique en masse (ou signature groupée)** : permettant de signer plusieurs documents en une seule fois. Néanmoins dans ce cas, chaque document apparaît ensuite comme individuellement signé S'il s'agit de signatures pour une personne physique, la bonne pratique consiste à lui proposer de visualiser les informations qu'il va signer.

Les applications intégrant la signature les plus abouties, celles qui se déploient le plus facilement, sont avant tout celles dans lesquelles la fonctionnalité de signature électronique est :

- considérée comme une **fonctionnalité supplémentaire** d'un processus métier électronique déjà outillé (et pas comme un logiciel supplémentaire à utiliser, sans lien avec le SI ou avec l'application métier sous-jacente) ;

- **ergonomiquement totalement intégrée** aux applications existantes pour ne pas perturber visuellement les signataires, ne pas rompre la chaîne logique applicative à laquelle ils sont habitués.

Sur le plan de l'ergonomie utilisateur, il est à noter qu'une bonne pratique consiste à afficher une image de la signature manuscrite au signataire sur l'écran, au moment où il appose sa signature électronique. Même si cet effet visuel ne présente aucune valeur juridique, l'expérience démontre qu'il a un impact psychologique non nul sur le signataire.

Le fait que la signature électronique ne peut, par nature, être imprimée, constitue également un frein « culturel » au déploiement. Aussi, il est recommandé de faire apparaître sur le document signé électroniquement, une note visuelle (code barre 2D) permettant à la fois d'observer, une fois imprimée, que ce document a été signé électroniquement, et d'obtenir des informations sur les modalités envisageables pour vérifier cet original électronique.

Vis-à-vis des destinataires, la bonne pratique consiste idéalement à :

- **Intégrer le plus automatiquement possible les informations signées reçus dans leurs propres outils** (SIs), leurs propres processus de gestion. Cela leur permettra ainsi de bénéficier d'une meilleure capacité de gestion (tri / recherche / classement) qu'avec le processus papier préexistant ;
- **Eviter au maximum d'imposer aux destinataires de s'équiper d'outils supplémentaires** (même gratuits) pour lire les informations signées et en vérifier la signature. En ce sens, la capacité des logiciels de lecture (tel qu'Adobe ® Reader pour le PDF, Microsoft ® Office ou OpenOffice™ pour les documents bureautiques, Outlook ou Thunderbird pour les mails) à visualiser et à vérifier les signatures est un bénéfice notable, facilitant la démocratisation de la signature électronique.

Quelques soient les architectures techniques, les applications dans lesquelles la signature électronique doit être intégrée, les différents éditeurs et opérateurs du marché disposent d'une palette d'outils, de services, facilitant la mise en œuvre, et l'intégration aux processus métier.

Ces outils, se présentent sous diverses formes, en fonction des cas d'usages métier :

Composant de signature	Service de signature	Serveur de signature	Logiciel de signature client
Composants à intégrer dans les applications métier (applet Java par exemple)	Appels (généralement Web services) à un service de signature en mode SaaS	Serveur à installer permettant de produire des signatures électroniques (cf. II.B.3)	Logiciel indépendant permettant la signature électronique d'informations (sans intégration particulière au SI)

Aussi, il est avant tout recommandé aux porteurs de projets de décrire la façon « idéale » dont pourrait se passer l'opération de signature, vue du signataire, les outils disponibles étant aujourd'hui en capacité de s'adapter à de très nombreux cas d'usages, de très diverses configurations techniques sous-jacentes.

Comme indiqué préalablement, il est également important, pour faciliter le déploiement, de mettre à disposition des signataires et des destinataires, un document décrivant les conditions dans lesquelles la signature électronique est produite, et ultérieurement vérifiable.

Ce document **« Politique de Signature »** est donc à rédiger par les porteurs de projet, préalablement à la mise en service du système intégrant les fonctionnalités de signature électronique.

C. Rappel : se mettre en capacité d'exploiter les informations signées dans le temps

Au-delà de l'opération de signature elle-même, les porteurs de projet doivent se soucier de « **gérer le cycle de vie de la signature électronique** », c'est-à-dire « se mettre en capacité et mettre en capacité les destinataires des informations signées de visualiser et de vérifier la signature électronique ».

Cette évidence sur le plan fonctionnel, induit des besoins qui ne sont pas toujours anticipés par les porteurs de projet :

Besoins de conservation : les besoins de conservation, d'archivage électronique, relatifs aux informations signées électroniquement portent à la fois sur les informations elles-mêmes (document, fichier structuré), et aussi sur des informations associées (listes de révocation, chaines de certification). Ces informations permettront ultérieurement de déterminer la validité de la signature et son contexte de création. Si les porteurs de projets ne sont pas en charge de gérer la conservation de l'ensemble de ces données, mais ils doivent néanmoins

s'assurer que tous les intéressés pourront récupérer ces informations en cas de besoins de vérification ultérieure de la qualité de la signature.

On compte parmi les données à conserver :

- **Les informations signées**, et les fichiers de signature associés, en cas de signature en forme « détachée » (cf. V.C) ;
- Les **informations techniques permettant d'attester de la validité du ou des certificats de signature utilisés**, intégrant les fichiers de chaînes de certification, listes de révocation associés ;
- Les documents présentant, à l'époque de la signature, les conditions de sa production et de sa conservation, notamment la **« Politique de signature »** de l'époque de la signature ;

Besoins d'horodatage : comme indiqué précédemment (III.D), les informations signées doivent être horodatées, ne serait-ce que pour se mettre en capacité de savoir à quelle liste de certificats révoqués faire référence en cas de besoin de vérification ultérieure. Cet horodatage peut prendre différente forme (allant d'une simple mention dans le contenu du document jusqu'à la mise en œuvre de dispositifs cryptographiques d'horodatage qualifié RGS ou certifié ETSI). Ce besoin est donc également à prendre en compte et il s'agit pour le porteur de projet de s'appuyer sur une solution d'horodatage adaptée au besoin métier, aux risques sous-jacent et cohérente avec les choix effectués pour le certificat et le type de signature retenu.

Besoins d'outils de vérification : les informations signées devront pouvoir être restituées, lisibles dans le temps, et leur signature électronique associée vérifiée. Aussi, les porteurs de projets doivent se préoccuper de disposer d'outils de signature permettant de vérifier les signatures produites à la date du jour mais également capables de vérifier dans le temps les signatures électroniques produites préalablement pour être toujours en capacité de vérifier les signatures de toutes les informations signées et conservées dans le temps. Cette perspective induit des besoins de capacité à tester les non régressions des nouvelles versions des logiciels et services des fournisseurs dans le temps, et les procédures humaines de tests associées.

V. ANNEXES

A. Cadre juridique

En synthèse, les différents textes encadrant juridiquement la signature électronique dans le code civil sont les suivants :

- **1999 (Europe) : Directive Européenne 1999/93/CE** : fixe les bases de l'équivalence entre l'écrit papier et l'écrit électronique.
- **2000 (France) : Loi n°2000-230 du 13 mars - Article 1316-4 du Code civil :**
  - Transpose la directive européenne ;
  - Définit le principe de présomption de fiabilité de la signature électronique
  - Introduit la notion de renversement de la charge de la preuve (charge à celui qui conteste une signature électronique)
- **2001 (France) : Décret n° 2001-272 du 30 mars** : défini les conditions d'application de la loi, et
  - Introduit les termes :
    - Dispositif sécurisé électronique de création de signature
    - Dispositif de vérification de signature électronique
    - Certificat électronique qualifié
    - Prestataires de services de certification électronique (P.S.C.E.)
  - Définit les conditions de mise en œuvre de la signature électronique sécurisée et les conditions d'obtention de la présomption de fiabilité de la signature électronique
- **2002 (France) : Arrêté du 31 mai 2002 précisant le décret n°2001-272**
  - Charge le COFRAC d'accréditer les organismes d'évaluation pour l'obtention du statut de P.S.C.E. (L.S.T.I. est la seule société accréditée à ce jour dans ce schéma)
  - Conditionne la reconnaissance de la qualification des P.S.C.E. à un audit effectué par l'un des organismes accréditée par le COFRAC, et à ses frais.
- **2004 (France) : Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (L.C.E.N.)**
  - Précise le régime de responsabilité des PSCE délivrant des certificats électroniques qualifiés ;
- **2004 (France) : Arrêté du 26 juillet : complète l'arrêté du 31/05/2002, relatif à l'accréditation des organismes qui procèdent à l'évaluation des P.S.C.E.**
  - Spécifie le référentiel d'accréditation des PSCE - norme NF EN 45012
  - Complète cette norme avec une série d'exigences techniques supplémentaires

De nombreux textes sectoriels référencent ce corpus juridique, pour « confirmer » les possibilités de dématérialisation et d'usage de la signature électronique dans des activités spécifiques.

Dans le domaine spécifique des Autorités Administratives, le législateur a également produit les textes ci-dessous, qui, s'ils ne s'appliquent pas nécessairement à la sphère privée, servent aujourd'hui de référentiel de bonnes pratiques :

- **2005 (France) : Ordonnance n°2005-1516 du 8 décembre 2005, relative aux échanges [...] entre les autorités administratives**
  - Définit les principes de R.G.S. (Référentiel Général de Sécurité) et R.G.I. (Référentiel Général d'Interopérabilité)
  - Promulgue positivement les effets de la signature électronique dans TOUS les échanges administratifs (dans le respect du RGS et du RGI)
- **2010 (France) : Décret n° 2010-112 du 2 février 2010, dit « décret R.G.S. » (Référentiel Général de Sécurité)**
  - Définit les règles et exigences de sécurité, qui s'appliquent aux autorités administratives, et aux systèmes d'information qui communiquent avec elle, selon plusieurs niveaux de « force sécuritaire » : une, deux ou trois étoiles (*, **, ***)
  - Définit un ensemble de règles de sécurité pour la gestion de la sécurité de l'information
  - Référence un ensemble de documents annexes définissant la marche à suivre pour émettre des certificats suivant :
    - Leur type : Particulier, Entreprise, Administration, Serveur
    - Le service de sécurité cible : Authentification, Signature, Confidentialité, Horodatage
    - Le niveau de « qualité sécuritaire » : *, **, ***

B. Exemples d'usages

Les exemples d'usages de la signature électronique sont nombreux, et les moyens mis en œuvre sont assez divers.

A titre d'illustration, les membres du *Club***PSCo** ont identifiés une liste (non exhaustive) d'exemples d'applications typiques dans lesquelles la signature électronique est aujourd'hui préconisée :

Application (ex : WebBanking, téléservice, facture…)	**Signataire** (ex : personne physique, serveur…)	**Destinataire** (ex : personne physique,SI Tiers…)	**SI signataire** (ex : application métier interne, portail internet, messagerie)	**SI cible** (ex : application métier interne, portail internet, messagerie, Acrobat Reader...)	**Volume** (ex : 100 000 signatures par an)	**Format utilisé** (ex : S/MIME, PKCS#7, CADES, PADES, XADES, PDF Signature)	**Délai de conservation** (ex : 5 ans, 10 ans, …)	**Forme** (ex : enveloppée / enveloppante / détachée)
Télé@ctes	Notaire / Collaborateur	Conservation des Hypothèques	Application métier	Application métier	30 000 signatures par jour	XAdES-T	30 ans	envelopée
Acte authentique	Notaire	Personne Physique	Application métier	Application métier	1 000 signatures par an	XAdES-T / A	75 ans	envelopée
Frais de déplacement	Gendarme	Administration	Application métier	Application métier	850 000 signatures par an		5 ans	
Vérification de l'Etat Civil	Officier d'Etat Civil en mairie	Administrations, notaires	Logiciel métier de la collectivité ou application web	Application métier	25 millions	PDF/A inclus dans un XAdES-T	75 ans	détachée

Signature de contrats en ligne	Organisme de crédit et consommateur	Organisme de crédit et consommateur	Portail internet	Portail métier de l'organisme de crédit et service d'archivage électronique	plus de 1 million par an	PAdES / XAdES	10 ans minimum	
Scellement de fiches de paie	Fabricant pour le compte de l'employeur	Employé	Application interne du fabricant de l'employeur	SI de l'employeur	plusieurs milliers par mois	Variable	5 ans	
Achats publics	Entreprise	Administration	Portail internet	SI de l'administration	plusieurs milliers par mois	PKCS#7	10 ans et plus	détachée ou enveloppée
Factures (selon CGI 289-V)	Entreprise prestataire	Entreprise cliente	Logiciel de facturation & opérateur de dématérialisation	SI client	plusieurs milliers par mois	PDF Signature	10 ans	
Contrats clients	Prestataire & client	Prestataire & client	Application métier	Application métier	plusieurs milliers par an	PAdES	Entre 5 et 30 ans selon la nature du contrat	enveloppée
Fichiers d'ordres bancaires	Trésorier d'entreprise	Banque	Application métier	SI Banque	Plusieurs centaines par an	eBics Format spécifique bancaire	2 ans	
Financement des TPE	Expert-Comptable	Banque	Document bureautique ou sur le portail de la banque	SI Banque	Plusieurs milliers par an	PDF pour les documents bureautiques et format de la banque si signature sur	5 ans	Enveloppée pour le PDF, variable si signature sur le portail de la banque

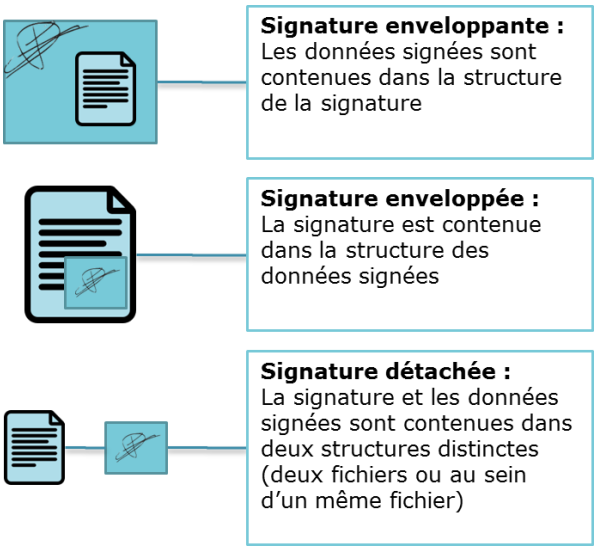
						portail		
Lettre recommandée	Emetteur (entreprise ou particulier)	Destinataire (entreprise ou particulier)	Document bureautique envoyé via l'interface émetteur du portail de l'opérateur	Interface destinataire du portail de l'opérateur	Plusieurs millions par an	XAdES ou autre format en fonction de l'opérateur	10 ans	Détachée ou enveloppée selon les opérateurs

C. Différentes formes et formats de signature électronique

1. Signature enveloppée, enveloppante et détachée

Il existe différentes formes de signature électronique, chacune d'entre elles étant potentiellement utile en fonction des cas d'usages métiers, de l'architecture sous-jacente.

En synthèse :



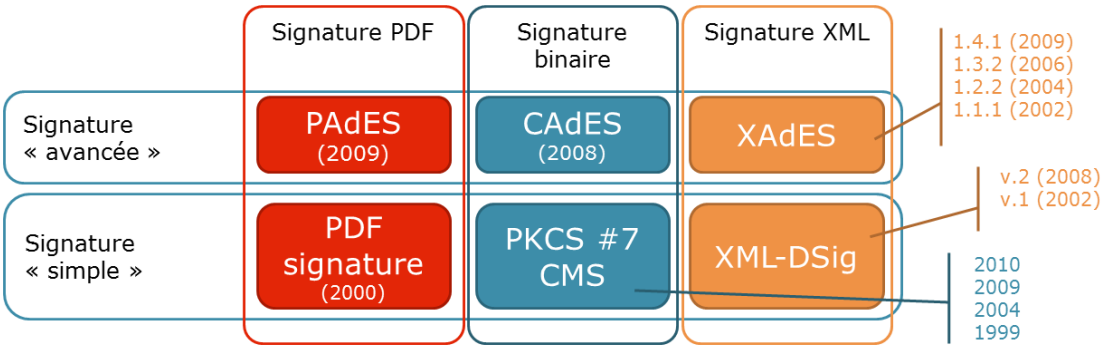
2. Différents formats de signature électronique

Pour des raisons historiques, et pour des raisons techniques liés aux différents types de fichiers qu'il est envisageable de signer (informations structurées, non structurées, contenus multimédia, codes source…), plusieurs formats de signature coexistent aujourd'hui sur le marché.

Ils sont regroupés entre 3 grandes familles :

- **Binaires**
  - PKCS #7
  - CMS, S/MIME
  - CAdES
- **XML**
  - XML-Dsig
  - XAdES
- **PDF (enveloppée)**
  - Signature PDF (PKCS #7)
  - PAdES

Les signatures désormais considérées comme « de facto » le standard du marché sont les signatures de types « avancées » (AdES: *Advanced Electronic Signature)* standardisées au niveau européen par l'ETSI.



Les standards de type PKCS#7, bien que très répandus car simples en termes de mise en œuvre, ne sont pas recommandés, car ils présentent ensuite des difficultés en termes d'interopérabilité et conduisent à des problèmes réguliers de vérification.

3. Facteurs de choix entre ces formes et formats

Le choix de la forme et du format de signature est un sujet assez technique, qui dépend de plusieurs facteurs, et notamment :

- **L'environnement métier** dans lequel est produit la signature électronique (signature personne physique ou personne morale ; signature faite par un logiciel client de signature ou intégrée au sein d'une application métier par exemple) ;
- Le **type de données à signer**, selon qu'elles sont structurées (exemple : fichier XML) ou non structurées (exemple : fichier PDF) ;
- Le **type et l'équipement du destinataire** qui exploitera le document signé, selon que le document doive ultérieurement être lisible dans le cadre d'une application métier ou non. En effet, l'un des paramètres à prendre en compte est la capacité de vérification qu'a le destinataire, et donc l'équipement dont il dispose à priori.

Pour un même type de format de document métier, plusieurs types de formes de signature électronique sont possibles, sans impact ni relation avec la valeur juridique du document signé.

A titre d'exemple, on peut par exemple noter certains critères de choix entre ces différents formats (sans pour autant faire de ces exemples des critères de choix absolus) :

- La forme de signature d'un document PDF la plus adaptée est sans doute la forme enveloppée, si l'on souhaite que le destinataire reçoive un seul fichier lisible à partir de son lecteur traditionnel et intégrant la signature. Cela lui évite ainsi de devoir s'équiper de logiciels de vérification de ces signatures électroniques ;

- La signature électronique de fichiers structurés (type XML) de gros volume est la forme « détachée » pour des raisons de performance (temps de production de la signature). Cette forme présente néanmoins le désavantage de devoir manipuler et conserver de façon liée deux fichiers au lieu d'un seul pour des signatures enveloppantes ou enveloppées ;
- La signature électronique de fichiers structurés (type XML) est généralement exploitée par des applications métier, et la forme la plus simplement exploitable est généralement la forme XAdES (enveloppée ou enveloppante) ;

VI. TERMES FREQUEMMENT UTILISES

De nombreux termes sont utilisés sur le marché, pour définir les différents types de signature électronique, certains étant parfois mal interprétés, ou ne s'appuyant pas sur un référentiel réglementaire « officiel ».

L'objet de cette section est donc de présenter les termes « officiels » applicables, à la différence d'autres pouvant être interprétables de façons diverses :

« Signature électronique avancée » : termes officiels, définis dans l'article 5.1 de la Directive européenne 1999/93/CE, consacrant **l'équivalence de la signature électronique avec la signature manuscrite**, dès lors que cette signature est produite à l'aide d'un certificat qualifié et créé par un dispositif sécurisé de création de signature électronique.

« Signature électronique à valeur probante » : toute signature électronique peut être présentée devant la justice. L'article 1316-1, de la loi 2000-230 du 13 mars 2000, indique d'ailleurs *« 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 »*. L'article 1316-3 de la même loi précise que *« L'écrit sur support électronique a la même force probante que l'écrit sur support papier »*. La validité de cette signature sera ensuite dépendante des conditions dans lesquelles elle a été produite, de la qualité (niveau de sécurité) du certificat et de l'application de signature utilisée lors de cette opération, ce qui sera à démontrer lors de l'éventuel contentieux portant sur la validité de cette signature.

« Signature électronique présumée fiable » : même si toutes les signatures électroniques sont recevables en justice (cf. ci-dessus), certaines sont considérées à priori comme « présumées fiables » sur le plan juridique. Cette notion est définie dans l'article 1316-4 du code civil, et dans les décrets et arrêtés d'applications associées. En pratique, cette présomption de fiabilité ne peut être atteinte que par l'usage d'un certificat qualifié (de niveau conforme au référentiel ETSI 101 456 ou RGS ***).

« Signature électronique sécurisée » : cette notion est juridiquement définie dans le décret 2011-272. Elle définit un niveau de qualité pour la signature électronique, sous réserve qu'il puisse être démontrée qu'elle est à la fois :

- propre au signataire ;
- créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- lié de façon garantie avec l'acte auquel elle s'attache, tel que toute modification ultérieure de l'acte soit détectable.

Il s'agit d'un niveau de qualité « intermédiaire » entre une signature électronique « simple » (ne présentant aucune garantie à priori) et un niveau de qualité « présumé fiable » (décrit ci-dessus). L'usage de la signature électronique sécurisée n'est toutefois généralement constaté que dans des téléservices administratifs et dans les usages des professions réglementées.

« Cachet serveur » : cette terminologie est définie dans le « Référentiel Général de Sécurité ». Une signature électronique « cachet serveur » en créée, en pratique, par un certificat « cachet serveur » émis au nom de la personne morale propriétaire de ce certificat (3 niveaux de sécurité *, **, *** existent pour ce type de certificats).

« Politique de Signature » : document exposant notamment les conditions de production et de traitement des documents à signer, les modalités d'authentification et de création des identités à utiliser pour les signatures électroniques, les modalités de création, de conservation et de validation des signatures électroniques, les règles de protection physique et informatiques de l'environnement de création des documents et des signatures et fixe les engagements, rôles et responsabilités des différents acteurs participant à ces opérations.

« Signature numérique » : ces termes sont généralement associés à la représentation graphique faite de la signature manuscrite. Ils sont officiellement définis dans le cadre de la dématérialisation dans le domaine pénal par exemple. Ainsi, le décret n° 2010-671 du 18 juin 2010 précise article R. 249-11. *« La signature numérique consiste en une signature manuscrite conservée sous forme numérique après avoir été apposée sur un écran tactile, au moyen d'un appareil sécurisé garantissant l'intégrité de l'acte dès que la signature a été enregistrée ».* Ce type de signature ne présente néanmoins pas le même niveau de valeur juridique qu'une signature électronique étant entendu que « *un même document pourra faire l'objet d'une signature électronique d'un professionnel et d'une signature numérique du justiciable* » (cf. circulaire associée du 19 juillet 2010).

« Signature électronique qualifiée » : ces termes ne sont pas directement définis légalement. Il s'agit généralement d'un « abus de langage », signifiant sur le fond « signature électronique présumée fiable », c'est-à-dire produite sur la base d'un certificat électronique qualifié.

« Cachet électronique » : ces termes ne sont pas légalement définis. Il s'agit généralement d'offres de services fournis sous ce label par des prestataires spécialistes du marché.

« Cachet électronique postal » : Le cachet électronique postal est principalement une autorité de vérification de signature et d'horodatage électronique qui vérifie et trace, comme une preuve, l'intégrité du contenu de l'information électronique

« Signature électronique niveau 3 » : ces termes, couramment utilisés sur le marché, ne sont pas représentatifs d'un niveau de qualité « officielle » de la signature électronique (tout comme les termes « certificat électronique de niveau 3 »).

VII. BIBLIOGRAPHIE & STANDARDS

Bibliographie :

Auteur / Source	Référence	Date de publication
ANSSI	Memento sur la signature électronique v0.94	25/08/2004
ANSSI	Module de formation sur la signature numérique	
Commission européenne	Directive européenne 1999/93/CE	13/12/1999
Legifrance	Loi n°2000-230 : Loi sur la signature électronique	13/03/2000
Legifrance	Décret n° 2001-272 : Décret d'application	30/03/2001
Legifrance	Arrêté du 26 juillet 2004 : reconnaissance de la qualification des PSCE	26/07/2004
Legifrance	Ordonnance n°2005-1516 du 8 décembre 2005	08/12/2005
Legifrance	Décret n° 2010-112 dit décret RGS	02/02/2010
FNTC	Guide de la signature électronique	10/2008

Standards :

Normes européennes ETSI

Certificats électroniques :

ETSI TS 102 042 : Policy requirements for certification Authorities issuing public key certificates

ETSI TS 101 456 : Policy requirements for certification authorities issuing qualified certificates

ETSI TS 102 280 : X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons

ETSI TS 102 023 : Policy requirements for time-stamping authorities

Signatures électroniques :

ETSI TS 101 733 : CMS Advanced Electronic Signatures (CAdES)

ETSI TS 101 903 : XML Advanced Electronic Signatures (XAdES)

ETSI TS 102 778 : PDF Advanced Electronic Signature Profiles (PAdES)

Horodatage :

ETSI TS 101 861 : Time stamping profile

Normes européennes CEN : décrivant les exigences relatives aux matériels et logiciels nécessaires à la production de signatures électroniques

Normes françaises :

Référentiel Général de sécurité, définissant les politiques relatives aux différents niveaux de certificats électroniques, et les exigences en matière de signature électronique et d'horodatage notamment

Profils de protection de l'ANSSI : cahier des charges décrivant les exigences relatives aux des outils et services de sécurité certifiés ou qualifiés par l'ANSSI

Normes internationales :

X509v3 : Format des certificats électroniques, tels que définis par Union internationale des télécommunications.

RFC 5280 : Certificats électroniques

RFC 3161 : Horodatage électronique

RFC 2375 : XML-Signature Syntax and Processing