FISAM
CONSULTING · FORMATION

LA VALIDATION/CONSERVATION DES SIGNATURES ÉLECTRONIQUES

Jean Marc Rietsch

JANVIER 2021

PLAN DU DOCUMENT

A propos de l'auteur

Jean-Marc Rietsch est ingénieur Civil des Mines et auditeur IHEDN, expert international en digitalisation, signature et archivage électronique, spécialiste de l'analyse des risques adaptée à la digitalisation et à la conservation sécurisée de données numériques.

Expert judiciaire près la Cour d'Appel de Paris.

Membre du Club EBIOS, la communauté des usagers et experts en gestion des risques et de IEESSE, Institut Européen d'Études en Sûreté-Sécurité pour les Entreprises.

Ses références se situent aussi bien dans le domaine financier avec l'AFD (agence française de développement), Arkea, Banques Populaires, BNP, Cetelem, Crédit Agricole, … que dans le domaine de la santé avec Ramsay Générale de Santé, ANAP (agence nationale d'aide à la performance dans le monde hospitalier), Stallergènes (laboratoire pharmaceutique), … ou encore dans d'autres domaines avec Arianegroup, Airbus, Orange, Docaposte, FDJ, groupe Boulanger, … sans oublier le domaine public avec l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), Chambre des Notaires de Paris, Imprimerie Nationale, … ainsi que des organismes gouvernementaux comme le Grand-Duché du Luxembourg, le Gouvernement de Monaco, …

Dépositaire de plusieurs brevets dont le plus récent publié en 2016 traite de la « Sécurité de données numériques »,

En matière de formation, il est à l'origine de deux BADGE (Bilan d'aptitude délivré par les Grandes Ecoles) en collaboration avec Mines ParisTech, sur le thème « Management de la dématérialisation et de l'archivage électronique » et « Management du patrimoine informationnel » ainsi que d'une formation certifiante sur 5 jours concernant la maîtrise d'un projet de digitalisation.

En complément à de nombreux articles, Jean-Marc Rietsch participe régulièrement à des livres blancs dont par exemple :

- Gouvernance de l'information et Big data ;
- Préservation des données/documents et transformation numérique ;
- Transformation numérique dans la santé : le « e-consentement ».

Il est également co-auteur de plusieurs ouvrages chez Dunod sur les thèmes de la dématérialisation et de l'archivage électronique.

La signature numérique s'impose dans le monde économique. Comme beaucoup d'innovations réussies, elle devient évidente pour ses utilisateurs, et lorsqu'un document papier à signer survient il apparait aussitôt comme une résurgence d'un passé sinon lointain, en tout cas chargé d'une certaine lourdeur.

Les bénéfices d'une signature numérique apparaissent nettement à l'ensemble des parties prenantes, avec en premier lieu le temps gagné, l'actif le plus précieux et le plus partagé, quelles que soient les responsabilités exercées. Le gain de temps n'est pas seulement celui réalisé lors de l'apposition d'une signature, mais lors de la circulation des documents, du suivi, de la gestion, de la conservation, bref, toutes ces activités invisibles que le numérique allège de façon considérable.
Une autre force de la signature est la fiabilité : l'intégrité du document et la qualité d'authentification des signataires, selon plusieurs modalités.

Tout ceci est sous tendu par l'opposabilité juridique, pierre angulaire de ce dispositif. Cette opposabilité est soigneusement encadrée par un règlement européen, des normes, textes et jurisprudences, bref, par tout un corpus assez complet mais également dense, à tiroirs, imposant parfois des principes abstraits difficiles à accorder avec la pratique des affaires.

La signature numérique ne fait pas exception aux autres pratiques ; sa mise en œuvre n'est pas une démarche binaire, mais représente une suite d'optimisations, de compréhension des exigences vs le contexte d'utilisation, d'appréciations du risque, objets d'itérations continues.

Ce travail au quotidien ne doit pas cacher une vision de long terme, pour assurer la pérennité des actes signés. Cette perspective est essentielle et ne doit pas être sacrifiée par les priorités du moment. C'est précisément l'objet de la validation. Ce terme ambigu laisse supposer une faille dans l'acte de signature, il n'en est rien. Au contraire, la validation est l'assurance d'une garantie dans le temps, en écho aux durées de conservation parfois très longues. Dernière sécurité, maillon essentiel de cette chaine de confiance à laquelle concourent l'ensemble des acteurs.

Que l'auteur de ce livre blanc soit remercié de sa contribution à cette mise en valeur.

Olivier Jaskulké
Directeur de programme
digitalisation
DRH/D2S

Validation et conservation des signatures électroniques dans le temps

Quels sont les éléments dont il faut disposer en cas de litige ?

Introduction

Après un démarrage frileux suite à la loi du 13 mars 2000, date à laquelle elle a été pleinement introduite dans notre droit, il est incontestable que la signature électronique se développe enfin de plus en plus tant en France qu'au sein de l'Union européenne, sans doute du fait que son équivalence juridique avec la signature manuscrite est désormais largement reconnue. Le règlement eIDAS est très clair sur le sujet en son article 25 « Effets juridiques des signatures électroniques » :

1. *L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée.*
2. *L'effet juridique d'une signature électronique qualifiée est <u>équivalent</u> à celui d'une signature manuscrite.*
3. *Une signature électronique qualifiée qui repose sur un certificat qualifié délivré dans un État membre est reconnue en tant que signature électronique qualifiée <u>dans tous les autres États membres.</u>*

En dehors des différents niveaux de signature existants tels que définis par le règlement européen eIDAS[1], même si elle est réalisée correctement, une signature électronique doit dans tous les cas s'accompagner d'un certain nombre de précautions afin d'être opposable le moment venu (d'autant plus si les documents ainsi signés sont appelés à produire des effets juridiques sur plusieurs années).

Ce livre blanc a ainsi pour objet de décrire les points d'attention liés à la signature électronique auxquels il est indispensable d'apporter des éléments de réponse concrets, au risque de se voir non seulement contester sa signature mais surtout de la voir invalidée, rendant caduques les conditions d'exécution du document auquel elle se rapporte.

Ce risque est d'autant plus important que l'on avance dans le temps et que les périodes d'archivage des documents signés s'allongent, dans la mesure où l'on ne disposera sans doute plus de tous les éléments nécessaires pour prouver la qualité de la signature au sens juridique du terme.

Bien heureusement des solutions existent que ce livre blanc a justement pour objectif de décrire.

[1] RÈGLEMENT (UE) N o 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 intérieur et abrogeant la directive 1999/93/CE

1. Rappels sur la signature électronique

1.1 Exigences légales

Au sens de notre Code civil son article 1367, précise :
« La signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte.
../..
Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.
La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. »

1.2 Différents procédés de signature électronique

Contrairement à une signature manuscrite, il existe plusieurs façons de réaliser une signature électronique, à savoir :

- L'image d'une signature manuscrite qui peut être vue comme l'équivalent du tampon encreur dans le monde physique ;
- La signature tablette, de plus en plus présente dans notre quotidien, y compris à la réception des colis ;
- La biométrie, principalement utilisée pour authentifier de façon forte une personne, son usage est strictement encadré à cause de son caractère de donnée personnelle ;
- Le recours à une bi-clé de chiffrement.

Cette dernière notion de bi-clé provient de l'emploi d'un algorithme de chiffrement asymétrique qui utilise deux clés différentes, l'une pour chiffrer et l'autre pour déchiffrer. Appliqué à la signature électronique, la clé privée est utilisée pour signer/chiffrer et la clé publique pour vérifier/déchiffrer la signature. La clé publique est enregistrée à l'intérieur d'un certificat électronique, voir infra.

Même si une grande partie du développement à venir peut s'appliquer à l'ensemble des procédés présentés, nous ne retiendrons ici que la signature électronique basée sur une bi-clé qui est de loin la plus répandue en particulier pour les échanges B2B ou B2C et dans le cas de documents contractuels et/ou de gestion.

1.3. Algorithmes utilisés

Le principe de fonctionnement de la signature électronique basée sur une bi-clé consiste dans un premier temps à calculer l'empreinte du document en utilisant un algorithme adapté, par exemple SHA, Whirlpool, RIPEMD ou encore Tripwire... Cette empreinte est unique pour chaque document, tout comme notre propre empreinte digitale, en tant qu'être humain.

Dans un deuxième temps le système chiffre/crypte cette empreinte à l'aide de la clé privée du signataire. Ce chiffrement est réalisé à l'aide d'un autre algorithme comme RSA, DSA ou encore ECC pour ne citer que les plus connus.

Tout algorithme ayant ses propres faiblesses, il s'agit là d'un des points de vigilance à prendre en compte afin de protéger à long terme la signature contre l'obsolescence cryptographique liée à l'augmentation régulière de la puissance de calcul des ordinateurs et à la sagacité des chercheurs et bien sûr des hackers.

1.4 Notion de certificat électronique

Afin d'établir le lien entre la signature électronique et le signataire, on utilise un certificat électronique. Il s'agit d'un véritable passeport numérique, délivré par une autorité de certification (AC) à la manière d'une autorité qui délivre une pièce d'identité (voir § 1.5 Enrôlement ci-après). Le certificat électronique constitue de fait le lien entre une identité numérique et une personne physique. Un certificat électronique contient entre autres la clé publique et d'autres informations permettant de vérifier la signature a posteriori.

La structure d'un certificat électronique est normalisée par le standard X509V3, norme de cryptographie de l'union internationale des télécommunications (UIT) qui fait que l'on retrouve les mêmes informations quel que soit le certificat, et en particulier :

- Numéro de série unique ;
- Dates de validité du certificat ;
- Détenteur du certificat ;
- Signature du certificat par la clé privée de l'Autorité de certification.

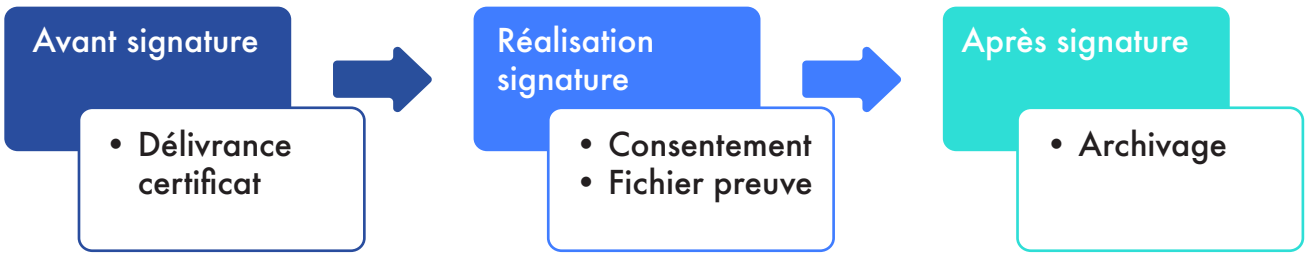
1.5 Enrôlement

La qualité du lien entre une identité numérique et une personne physique repose sur l'enrôlement c'est à dire la façon dont le prestataire de service de confiance (ou PSCO), en l'occurrence l'Autorité de certification, vérifie l'identité présumée du futur signataire avant de pouvoir lui délivrer une clé privée et un certificat électronique contenant la clé publique correspondante (une bi-clé).

Cette vérification consiste dans un premier temps à obtenir différents éléments d'identification de la part du futur signataire comme des pièces d'identité. Dans un deuxième temps des contrôles sont opérés nécessitant au besoin la présence physique du signataire afin de contrôler la cohérence des informations présentes sur les documents présentés et le signataire. Ce face à face est de plus en plus réalisé à distance en s'appuyant sur des outils techniques basés sur de la vidéo, dont la fiabilité doit être absolument garantie et vérifiable.

1.6 Le cycle de vie de la signature électronique

Le cycle de vie de la signature comprend trois grandes étapes décrites ci-après tout aussi importantes l'une que l'autre en matière de preuve.



1. Avant signature obtention d'un certificat électronique

Afin de pouvoir signer il est nécessaire pour le signataire de disposer d'une bi-clé (clé privée et clé publique correspondante dans le certificat de signature). C'est à ce stade qu'intervient la notion d'enrôlement vue précédemment qui consiste à vérifier l'identité du signataire en s'appuyant sur les différentes étapes suivantes :

- Fourniture de document(s) d'identité,
- Contrôle du caractère authentique des documents,
- Contrôle de cohérence entre les documents et le signataire en tant que personne.

Chaque étape peut être réalisée avec plus ou moins de précision avec ou sans la présence physique ou à distance du signataire, ce qui aura une influence sur le type de bi-clé/certificat délivré. De façon simplifiée il existe ainsi trois grandes familles de certificat basées sur la qualité du lien avec la personne signataire, de faible à élevé en passant par le substantiel pour reprendre la terminologie du règlement eIDAS.

Il est important de préciser que si l'on travaille avec des certificats permanents, cette étape de vérification de l'identité du signataire n'est à réaliser qu'une seule fois et reste valable pendant toute la durée de validité du certificat. A l'inverse l'usage de certificats éphémères impose de réaliser cette vérification (automatiquement le plus souvent) avant chaque signature.

2. Réalisation de la signature (consentement du signataire)

La création proprement dite d'une signature électronique se déroule en respectant les étapes suivantes :

- Identification du document ou des documents à signer,
- *Indication du ou des signataires (peut être réalisée en amont),*
- Pour chaque signataire :
  - o Authentification du signataire au moment de signer. Il s'agit de confirmer la réalité de l'identité alléguée (signataire) et non plus de vérifier l'identité comme pour l'enrôlement,
  - o Enregistrement du consentement du signataire (en général en cochant une case)
  - o Réalisation technique de la signature électronique à partir de la clé privée du signataire et la mise en œuvre de l'algorithme retenu.
- Réalisation et scellement du fichier des éléments techniques de preuve.

3. Après signature

Lorsque la signature a été réalisée d'autres opérations sont encore à prendre en compte, à savoir :

- *Validation de la signature (voir chapitre 3 « Solutions pratiques »),*
- Archivage du document signé dans des conditions permettant de garantir son intégrité à long terme (jusqu'à échéance de la durée de conservation légale et/ou expiration du délai de prescription relatifs au type de document signé voire ad vitam aeternam pour des documents patrimoniaux) ainsi qu'un niveau de confidentialité adapté,
- Archivage du fichier des éléments techniques de preuve associé au document signé dans les mêmes conditions que ce dernier.

1.7 Validité de la signature électronique

Pour être retenue comme preuve la signature électronique doit permettre de démontrer :

1/ L'identité du signataire,
2/ Le consentement du ou des signataires au contenu du document (aux engagements qui y figurent s'il s'agit d'un contrat),
3/ Le lien entre le document signé et le(s) signataire(s),
4/ L'intégrité du document.

En cas de besoin il sera donc nécessaire d'apporter la preuve que toutes ses exigences ont bien été satisfaites. Pour ce faire il peut être judicieux de faire appel à un service de validation de signature, objet du chapitre suivant.

2. La validation de signature électronique

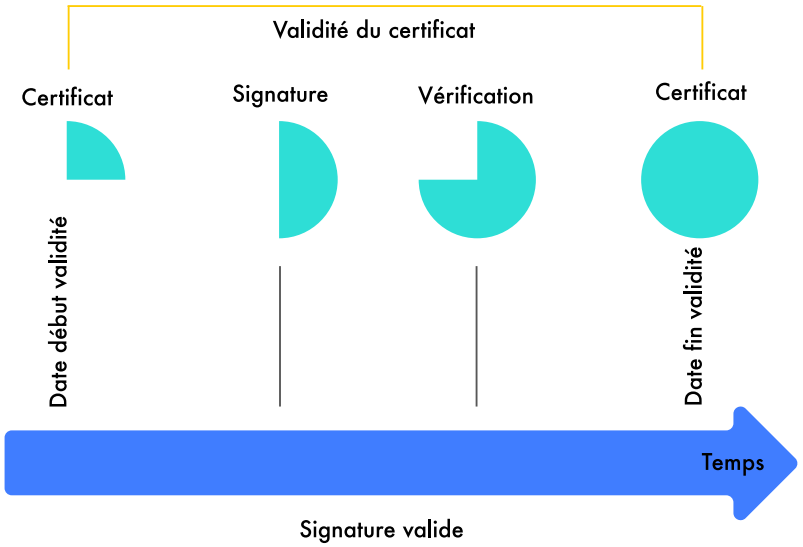
2.1 Les facteurs de risque liés à la signature électronique

La notion de temps est extrêmement importante dans le cadre de la signature électronique comme nous allons le voir dans ce qui suit.

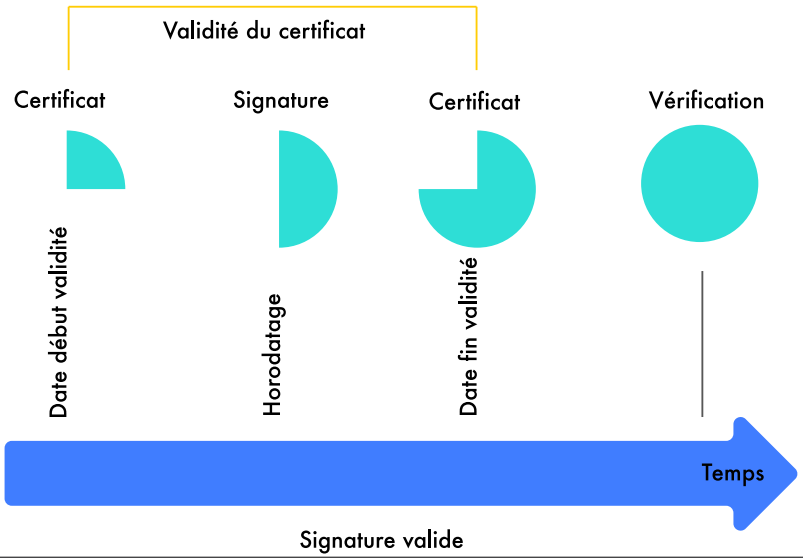
1. Durée de validité des certificats électroniques

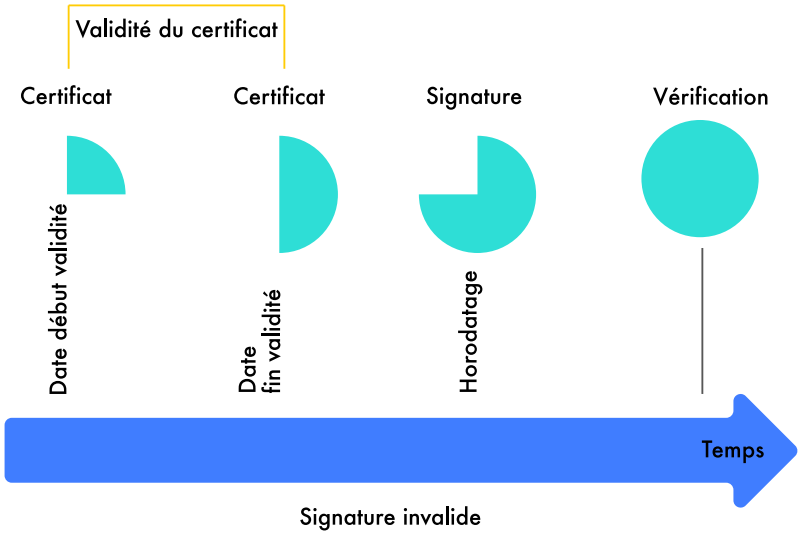
Les certificats électroniques possèdent des durées de vie limitée (en général 2 ou 3 ans) et il est donc nécessaire de vérifier que la signature a été réalisée à un moment où le certificat était encore valide.

Si la vérification est réalisée à un moment où le certificat est encore valide il n'y a pas de problème particulier puisque nous sommes toujours dans la zone de validité du certificat.



Si la vérification a lieu après la fin de validité du certificat il sera nécessaire de rechercher l'heure de la signature grâce à un horodatage réalisé au moment de la signature afin de contrôler que le certificat était valide au moment de la signature.





Mais que se passe-t-il si le certificat utilisé pour le jeton d'horodatage a lui-même atteint sa limite de validité. Il s'agit d'un problème auquel il faut effectivement penser et surtout résoudre pour ne pas se trouver dans l'incapacité de pouvoir démontrer la validité d'une signature.

2. Révocation des certificats électroniques

Sachant qu'un certificat électronique peut être révoqué à tout moment (comme on fait opposition sur une carte bancaire), il est donc indispensable de vérifier qu'il n'était pas révoqué au moment où la signature a été apposée. Pour ce faire il est nécessaire d'interroger l'Autorité de Certification qui a émis ce certificat électronique. Cette interrogation est réalisée dans la grande majorité des cas à l'aide d'une requête de type OCSP (Online Certificate Status Protocol).

3. Niveau de confiance des Autorités de Certification

Les Autorités de Certification (émetteurs des certificats électroniques) entrant dans la constitution d'une signature électronique peuvent bien évidemment, comme toute entreprise, cesser leur activité et ce qu'elle qu'en soit la raison. En conséquence il sera très difficile d'y faire appel lorsque l'on désirera valider une signature électronique réalisée à partir d'un certificat émis par une Autorité de Certification ayant cessé son activité.

Le règlement européen eIDAS, déjà largement cité, a heureusement prévu cette situation et impose à tout prestataire de services de confiance de type « qualifié » de disposer d'un plan actualisé d'arrêt d'activité afin d'assurer la continuité du service proposé. Cependant cela ne s'applique pour l'instant qu'aux prestataires qualifiés d'où notre mise en garde pour les autres cas (signature simple ou avancée).

3. Obsolescence cryptographique

Les algorithmes utilisés dans le cadre de la signature électronique peuvent, à moyen terme, être craqués et il est donc important de les surveiller et de prendre les mesures adaptées pour éviter de se voir confronter par exemple à de vraies fausses signatures ! D'où l'importance d'avoir recours à des prestataires de confiance dont les services permettent justement de se protéger contre un tel risque grâce aux services de validation et de conservation de signature présentés ci-avant.

2.2 Principe général de validation

La validation d'une signature électronique est réalisée pour répondre en grande partie à l'ensemble des risques décrits précédemment en réalisant l'ensemble des vérifications correspondantes. Elle revêt plusieurs aspects à la fois techniques et de niveau de confiance. L'on a malheureusement trop souvent tendance à se limiter aux seuls points techniques. Nous décrivons ci-après les grands principes de cette validation.

1. Informations de base

Pour réaliser l'ensemble des contrôles nécessaires, on s'appuie principalement sur les informations présentes dans le certificat électronique embarqué avec le document signé. On aura ainsi accès aux données suivantes :

- Les algorithmes utilisés pour le calcul d'empreinte et le chiffrement
- L'OID (numéro unique) de la Politique de Certification et le nom de l'Autorité de Certification dont elle dépend
- Les dates de validité du certificat
- La signature de l'Autorité de Certification
- La clé publique correspondant à la clé privée ayant servi à signer le document
- Le(s) usage(s) prévu(s) pour le certificat parmi : Authentification ou Signature ou Confidentialité

2. Vérifications techniques

Plusieurs éléments sont systématiquement contrôlés décrits rapidement ci-dessous.

A. Intégrité (non-altération) du document

Il s'agit souvent du premier contrôle réalisé qui se déroule de la façon suivante :

- On calcule l'empreinte du document,
- On déchiffre la signature grâce à la clé publique ce qui nous fournit l'empreinte du document d'origine, calculée au moment de la signature,
- Enfin on réalise une comparaison des deux empreintes qui doivent être identiques.

B. Validité du certificat

Vient ensuite la vérification de la validité du certificat qui se déroule en deux étapes :

- La première étape consiste à vérifier que la date de la signature (vérifiable grâce à l'horodatage) se situe bien dans la période de validité du certificat,
- La deuxième étape consiste à vérifier que le certificat n'était pas révoqué au moment de la signature. En général on utilise à cette fin une requête OCSP (Online Certificate Status Protocol) auprès de l'Autorité de Certification ayant délivré ce certificat.

3. *Vérifications du niveau de confiance*

Ces contrôles sont destinés à mesurer le degré de confiance que l'on peut accorder à l'Autorité de certification, émettrice de la clé privée ayant servi à signer le document. Pour ce faire il est possible de s'appuyer sur des listes de confiance et en premier lieu la European Union Trusted List (EUTL)[2]. Adobe gère également sa propre liste à travers son programme interne AATL pour Adobe Approved Trust List.

L'exercice est à répéter pour toutes les AC qui entrent en jeu dans la majorité des signatures électroniques, y compris pour l'horodatage et la signature du jeton correspondant. En effet le certificat émis par l'AC est lui-même signé par cette AC à l'aide d'une clé privée émise par une autre AC et ainsi de suite jusqu'à l'AC dite « racine », c'est ce que l'on appelle la chaîne de certification.

2.3. Aspect légal de la validation de signature électronique

La validation des signatures électroniques qualifiées bénéficie d'ores et déjà d'une reconnaissance légale avec le règlement européen eIDAS en ses articles 32 *Exigences applicables à la validation des signatures électroniques qualifiées et* 33 *Service de validation qualifié des signatures électroniques qualifiées.*

Ces articles possèdent leur équivalent pour les cachets électroniques qualifié avec l'article 40.

[2] Les listes de confiance sont définies par le règlement européen eIDAS en son article 22

3. Les solutions pratiques pour la validation des signatures

D'après ce qui précède, la validation d'une signature électronique est une étape très importante et nous allons maintenant aborder la façon pratique de la réaliser ou mieux de la faire réaliser.

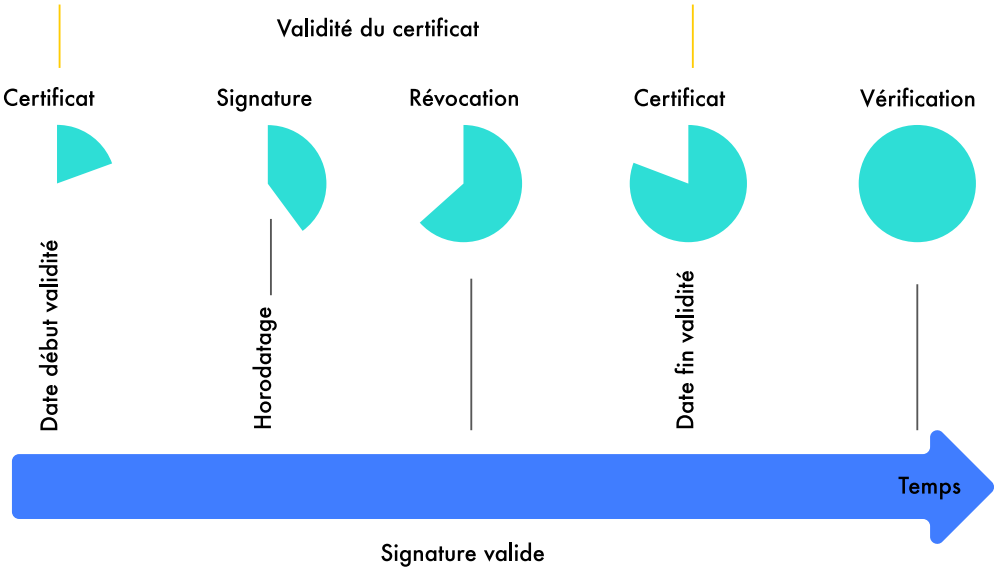
3.1. Formats de signature

Comme évoqué précédemment, la validation des signatures électroniques dépend étroitement du format de la signature et surtout du moment auquel est réalisée la validation. La norme ETSI EN 319 102 -1 définit ainsi 4 classes de signatures décrites succinctement ci-après.

A. **Signature basique :** correspond à une signature qui peut être validée tant que les certificats correspondants ne sont ni révoqués ni expirés.

B. **Signature horodatée :** il s'agit d'une signature qui permet de prouver que la signature existait déjà à un moment donné.

Cette classe de signature peut être utilisée pour valider une signature lorsqu'un certificat a été révoqué après la création de la signature. Voir schéma ci-dessous



C. **Signature avec éléments de validation à long terme ou signature LTV (long term validation) :** cette signature assure la disponibilité à long terme des éléments de validation en incorporant tout le nécessaire ou les références aux éléments requis pour valider la signature.

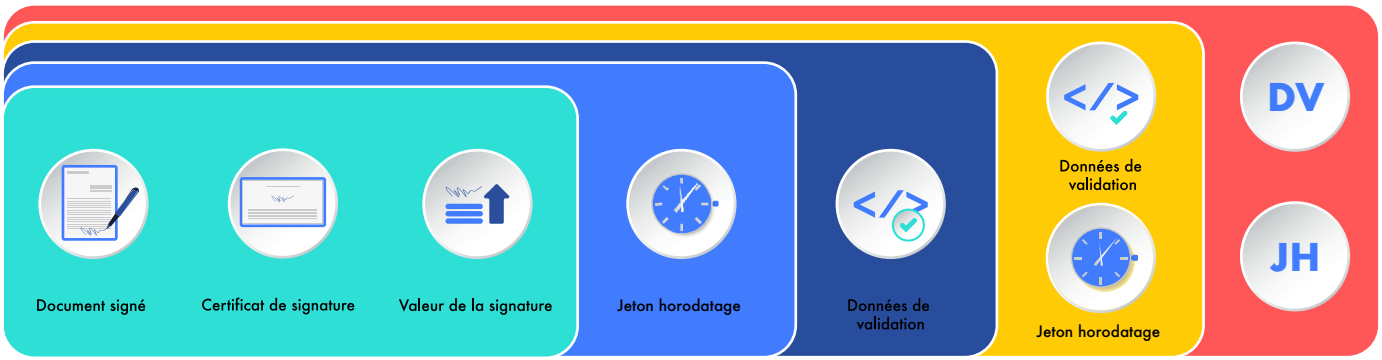
Dans la mesure où il est n'est pas certain que les données de validation soient toujours disponibles en ligne ou que certains vérificateurs ne puissent pas accéder à ces données, il est nécessaire de saisir ces données directement dans la signature. C'est l'objet des signatures de classe 3 qui peuvent ainsi encore être validées lorsque les certificats expirent ou sont révoqués, et également lorsque la sécurité des algorithmes appliqués devient douteuse ou que les tailles de clé utilisées ne sont plus à la pointe de la technologie.

Néanmoins cela n'est possible qu'associé à une vigilance permanente destinée :

- soit à conserver la signature dans un environnement de confiance permettant de garantir dans le temps la disponibilité et l'intégrité de l'ensemble de la signature ;
- soit à renforcer régulièrement la signature d'origine au moyen d'un nouvel horodatage (objet de la classe 4 ci-après).

Ces deux derniers points constituent l'essentiel des exigences en matière de conservation des signature électronique, objet de l'article 34 du règlement eIDAS précisant la mise en œuvre des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques au-delà de la période de validité technologique.

D. **Signature assurant la disponibilité et l'intégrité à long terme des éléments de validation :** permet de valider la signature au-delà des nombreux événements qui limitent sa validité (par exemple, la faiblesse des algorithmes cryptographiques utilisés ou l'expiration des données de validation)



Les signatures de classe 4 répondent en fait à la deuxième option du point de vigilance lié à la classe 3, destiné à renforcer régulièrement la signature d'origine au moyen d'un nouvel horodatage.

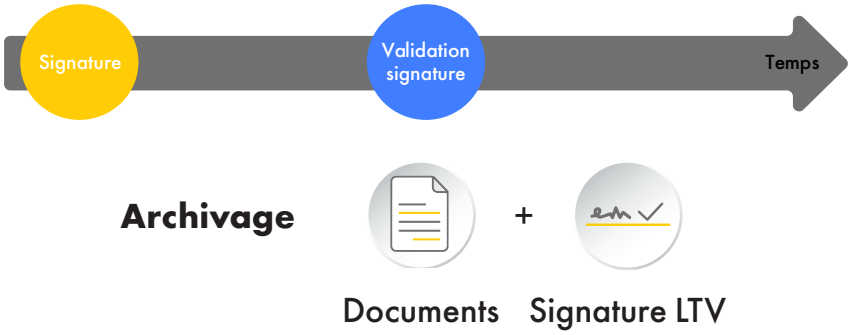
3.2 Scénarios retenus de validation des signatures électroniques

D'après ce qui précède plusieurs scénarios sont dès lors possibles afin de valider/ conserver une signature électronique. Nous présentons trois scénarios qui nous paraissent les principaux.

1.Scénario 1

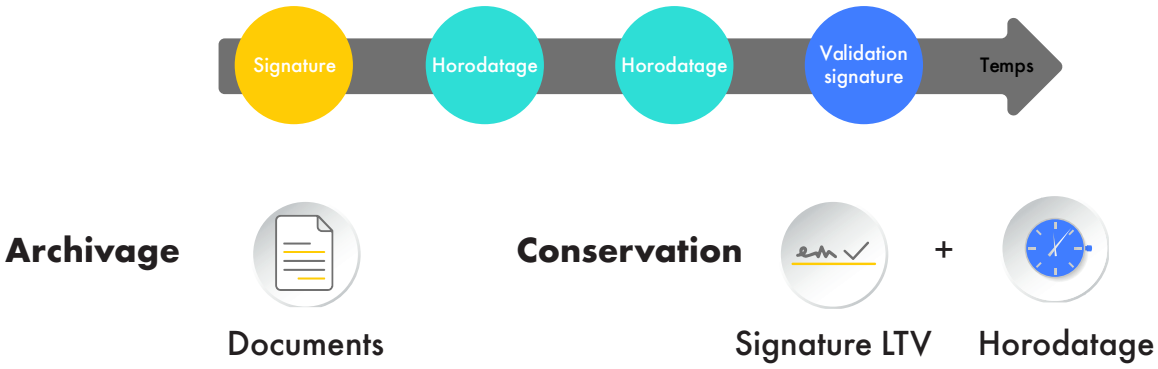
Réaliser (ou faire réaliser par un prestataire de services de confiance dument qualifié à cet effet) la vérification de la signature le plus tôt possible après apposition de la signature elle-même. Cette validation fait l'objet d'une attestation probante (rapport de validation) qu'il faut conserver dans un environnement de confiance permettant de garantir sa disponibilité et son intégrité dans le temps (jusqu'à extinction du délai de prescription légale concernant le type de document signé).

2. *Scénario 2*



Utiliser la classe 3 de la signature LTV afin d'embarquer l'ensemble des éléments permettant de la vérifier dans le temps et la conserver dans un environnement de confiance dédié et répondant ainsi à l'article 34 du règlement eIDAS sur la « Conservation des signature électroniques qualifiées » destiné à mettre en œuvre des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques au-delà de la période de validité technologique.

3. *Scénario 3*



Il s'agit d'une variante du scénario précédent consistant à utiliser une signature de classe 4 destinée à la protéger dans le temps par un nouvel horodatage régulier. Ce scénario répond également à l'article 34 du règlement eIDAS sur la conservation des signatures.

Quelle que soit le scénario retenu, il est recommandé que le PSCO assure la conservation du document faisant l'objet de la signature ou du cachet électronique, dans les mêmes conditions de protection en intégrité, notamment pour pallier le risque d'affaiblissement de la fonction de calcul d'empreinte liant le document et la signature ou le cachet[3].

[3] Recommandation de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) concernant « les services de conservation qualifiés des signatures et des cachets électroniques qualifiés - Critères d'évaluation de la conformité au règlement eIDAS »

3.3 Autres éléments de validité

Au-delà de la validation proprement dite des signature électroniques, il est également important de pouvoir disposer d'autres éléments destinés à apporter toutes les précisions nécessaires tant juridiques qu'organisationnels et techniques concernant l'ensemble du processus ayant abouti à la signature électronique dont il est nécessaire de démontrer la valeur probante.

1. Dossier de preuve

Ce document constitue un des éléments importants à fournir en cas de contentieux. Il sera en effet essentiel de pouvoir démontrer la qualité du processus mis en œuvre en cas de contestation et surtout sa conformité aux lois et règlementations.

Le dossier de preuve est ainsi constitué de deux grandes parties :

- Une première partie, explicative et didactique, doit permettre aux juristes de bien comprendre la façon dont le processus mis en œuvre fonctionne et respecte bien l'ensemble des exigences légale et réglementaires et surtout de le démontrer, notamment en termes de fidélité et d'authentification des documents produits.

- Une deuxième partie plus détaillée sera d'avantage destinée aux experts, et vient compléter la première partie afin de parfaitement comprendre le déroulement des différentes étapes du processus (voir § 1.6 « Le cycle de vie de la signature électronique ») en rappelant les engagements et obligations de chacune des parties prenantes concernées.

Le dossier de preuve précise entre autres :

- La façon dont se déroule l'enrôlement du signataire,
- Le niveau du certificat revendiqué,
- La manière dont le signataire est authentifié au moment de signer,
- La façon dont le signataire donne son consentement,
- La nature des éléments archivés et comment cet archivage est réalisé (en particulier les traces).

2. Fichier des éléments techniques de preuve

Dans la mesure où la signature est souvent réalisée sur une plateforme tierce, il est néanmoins important de pouvoir disposer de la preuve du déroulé du processus. C'est justement l'objet du fichier des éléments techniques de preuve, souvent appelé « fichier de preuve », ce qui peut apparaître comme un raccourci dangereux. Quoiqu'il en soit ce fichier est constitué de l'ensemble des éléments et évènements qui interviennent pendant la réalisation de la signature. Ce fichier doit lui-même être protégé par l'opérateur qui le réalise, ce qui est en général obtenu grâce au cachet électronique de cet opérateur.

4. Importance de l'archivage électronique

À la lecture de ce qui précède, la notion d'archivage revient très régulièrement. En effet, la façon dont sont gérés tous les éléments nécessaires à prouver la recevabilité d'un document signé doit absolument prendre en compte leur archivage. La qualité de ce dernier est en effet indispensable pour disposer d'un ensemble fiable d'un point de vue légal et règlementaire.

Nous avons également fait plusieurs fois référence à l'article 34 du règlement eIDAS sur la « *Conservation des signature électroniques qualifiées* » destiné à mettre en œuvre des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques au-delà de la période de validité technologique. Le titre de cet article est assez trompeur car contrairement à ce que l'on pourrait croire il ne s'agit pas d'un archivage électronique au sens classique du terme.

D'ailleurs le site de la commission européenne (https://ec.europa.eu/) précise bien :
« Le règlement eIDAS fixe des règles pour la conservation des signatures électroniques, des cachets électroniques ou des certificats liés aux services de confiance. La conservation est différente de l'archivage électronique (qui n'est PAS un service de confiance dans le cadre d'eIDAS). Les objectifs et les cibles du processus doivent faire une distinction entre les deux activités :

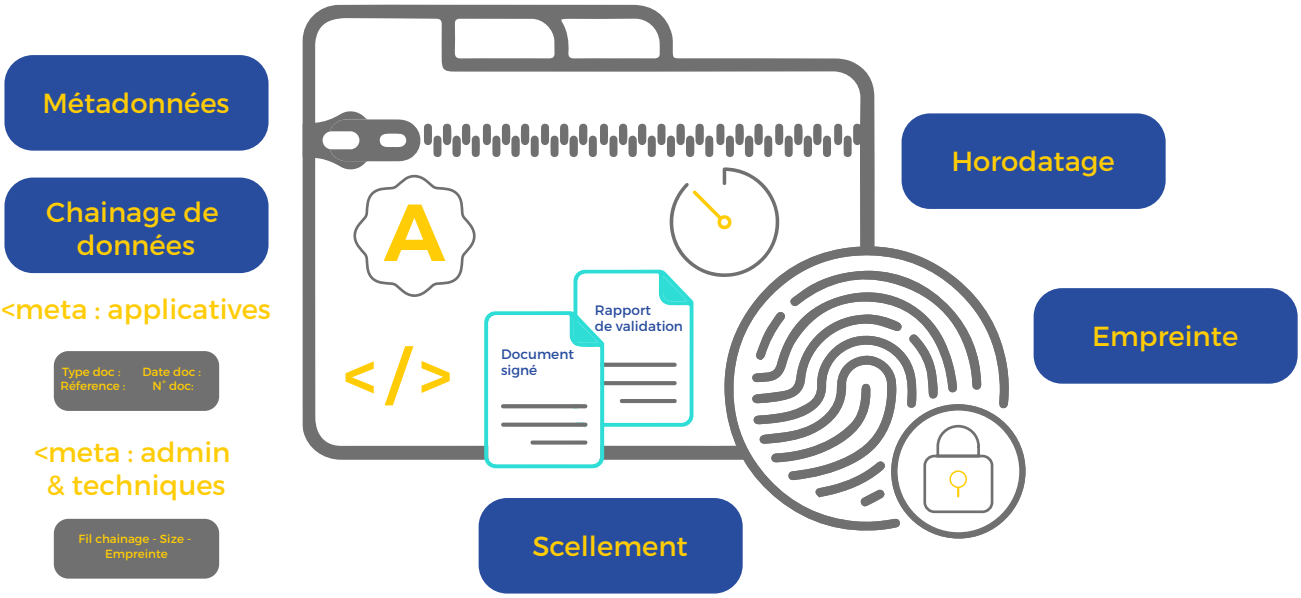
- *La conservation dans le cadre d'eIDAS vise à garantir la fiabilité d'une signature électronique qualifiée ou d'un cachet électronique qualifié dans le temps. La technologie qui sous-tend ce service de confiance vise donc la signature ou le cachet électronique ;*

- *L'archivage électronique vise à garantir qu'un document est conservé afin de garantir son intégrité (et d'autres caractéristiques juridiques). La technologie qui sous-tend l'archivage électronique vise donc le document. L'archivage électronique reste de la compétence des États membres.*

En d'autres termes, l'archivage électronique des documents et la conservation des signatures électroniques et des cachets électroniques sont de nature différente, reposent sur des solutions techniques différentes (jointes au document ou à la signature électronique/cachet électronique) et diffèrent dans leur finalité (conservation du document vs conservation de la signature électronique/conservation électronique). »

Néanmoins, une des voies possibles pour la conservation des signatures électroniques est d'avoir justement recours à l'archivage électronique en utilisant une signature de classe 3 dite LTV embarquant les éléments nécessaires à sa validation dans le temps.

Les deux premiers scénarios de validation proposés au chapitre précédent font ainsi pleinement appel à un système d'archivage électronique tant pour le document signé que pour l'attestation de validation dans le scénario 1 ou la signature au format LTV dans le scénario 2.



Finalement, seul le scénario 3 peut se passer partiellement d'un archivage électronique mais uniquement pour la partie signature, le document signé lui-même ainsi que les autres éléments de preuve devant absolument être conservés via un système d'archivage électronique à l'état de l'art technique et bénéficiant d'une certification réalisée à partir d'un référentiel reconnu répondant à toutes les exigences légales et règlementaires correspondantes.

Conclusion

Même si la signature électronique doit être simple à utiliser, il est indispensable de veiller à sa bonne implémentation en s'appuyant sur des prestataires de services de confiance qualifiés qui devront également entourer la signature de toutes les précautions indispensables à sa validité dans le temps.

Il est ainsi particulièrement important de prendre en compte la totalité du cycle de vie de la signature électronique. En effet à quoi servirait un document signé si le moment venu l'on était dans l'incapacité de produire ce document signé objet du contrôle/contentieux, de démontrer son intégrité et de prouver la validité de sa signature parce qu'un seul des éléments nécessaires tels que détaillés dans les pages précédentes, se révélait manquant.

Bien évidemment la validation des signatures électroniques, même si elle est indispensable peut certes paraître compliquée. De ce fait l'on constate à ce jour que l'impasse est souvent faite sur ce sujet, car mal relayé, il faut également le reconnaître.

Le rôle de l'archivage est aussi crucial tant pour les documents signés eux-mêmes que pour tous les éléments de preuve connexes, y compris la signature, voir pour s'en convaincre le chapitre 4. Dans la mesure où l'archivage électronique reste complexe et surtout coûteux à mettre en œuvre, il est souvent plus efficace d'avoir recours à un prestataire de services de confiance. Attention toutefois au fait que le recours à un tiers ne vous décharge pas pour autant de vos responsabilités concernant les documents que vous lui déposerez et dont vous restez propriétaire.

La même logique peut s'appliquer à la validation/conservation des signatures électroniques et le recours à un prestataire de services de confiance tiers si possible qualifié est fortement recommandé. A savoir que certains prestataires d'archivage proposent un tel service permettant de réaliser la validation des signatures juste avant le versement des documents signés dans le système d'archivage électronique répondant ainsi à la logique du premier scénario tel que présenté au § 3.2.

Tout comme pour l'archivage électronique, la validation/conservation des signatures électroniques pourrait-être représentée comme un iceberg dont on ne voit que la petite partie immergée. On ne saurait donc trop conseiller d'avoir recours à des spécialistes du domaine qui, de plus, sauront vous conseiller et prendre les responsabilités qui leur incombent.

Pour répondre pleinement à ces dernières exigences, l'on recherchera de préférence des prestataires qualifiés même pour de la validation/conservation de signatures avancées voire…simples. Pour cela il est possible de se référer à la liste européenne officielle disponible à l'adresse https://webgate.ec.europa.eu/tl-browser/#/ mais attention à la signification des sigles :

- QVal for QESign (qualified validation service for qualified electronic signature),
- QPres for QESign (qualified preservation service for qualified electronic signature),
- QVal for QESeal (qualified validation service for qualified electronic seal),
- QPres for QESeal (qualified preservation service for qualified electronic seal).

5. GLOSSAIRE

AC : Autorité de certification, prestataire de services de confiance responsable de l'émission, du renouvellement, de la révocation et de la gestion des certificats numériques. L'autorité de certification a en charge l'application d'une politique de certification. Elle est responsable de la validité des certificats qu'elle émet et qu'elle signe.

Certificat électronique : Document sous forme électronique attestant du lien entre l'identité du signataire et les données de vérification de signature électronique.

eIDAS : Règlement (UE) 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 intérieur et abrogeant la directive 1999/93/CE

DSA : Digital Signature Algorithm

ECC : Elliptic curve cryptography

Empreinte : L'empreinte électronique d'un document est l'équivalent de l'empreinte digitale ou génétique d'une personne. Elle est le résultat d'un calcul effectué à l'aide d'un algorithme approprié appelé également fonction de hachage. Les propriétés de l'empreinte sont les suivantes :

- si l'on change, ne serait-ce qu'une virgule, dans un document, son empreinte change ;
- la probabilité que deux documents aient la même empreinte est très faible ;
- il n'est pas possible de reconstituer le document à partir de sa seule empreinte.

EN : Normes européennes

ETSI : European Telecommunications Standards Institute

LTV : Long term validation

OCSP : Online Certificate Status Protocol

PSCO : Prestataire de service de confiance

RIPEMD : RACE Integrity Primitives Evaluation Message Digest

RSA : Ronald Rivest, Adi Shamir et Leonard Adleman

SHA : Secure Hash Algorithm

FISAM

CONSULTING · FORMATION

Création graphique : nathanvanstaevel.com