CLUSIF

LES DOSSIERS TECHNIQUES

La Signature Électronique

Juin 2018

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris

Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88

clusif@clusif.fr – www.clusif.fr

Table des matières

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Les responsables du groupe de travail :

Grégoire	**SANDRÉ**	*Econocom Digital Security*
Jean-Paul	**JOANANY**	*Generali Vie*

Les contributeurs :

Bruno	**GUIOT**	*EDF*
Garance	**MATHIAS**	*MATHIAS AVOCATS*
Stéphane	**JOURDOIS**	*Digital Security*
Matthieu	**GUILLAUME**	*Wavestone*
Jean-François	**DEMESTEERE**	*Imprimerie Nationale*
Annabelle	**TRAVERS-VIAUD**	*Airbus Defence & Space - Cybersecurity*
Sébastien	**MAUPTIT**	*AG2R La Mondiale*
Oumar	**DIAO**	*EVA Group*
David	**OPTER**	*Pôle Emploi*
José	**NDELE**	*Technospheris*
Abdelaziz	**TALEB**	*Modis*

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture de ce document.

I. Introduction

I.1. Contexte et périmètre

De nombreux projets de signature électronique sont aujourd'hui arrivés à leurs termes, et d'autres, après parfois une très longue période d'hésitation, sont sur le point d'être lancés. Pourtant des incertitudes demeurent quant à leurs réussites, tant il semble difficile pour les acteurs d'appréhender l'ensemble des aspects juridiques, techniques, ou organisationnels de ce type de projets.

Dans une période où nombre d'entreprises se lancent dans des projets de dématérialisation, la signature électronique apparait comme un élément important de cette transformation digitale à laquelle toutes aspirent. Le besoin de sécurisation des projets de signature électronique revêt donc un caractère essentiel.

Tous les retours d'expériences concernant les problèmes rencontrés, les facteurs de succès ou autres bonnes pratiques seront dans ces conditions des apports précieux pour tous ceux qui aujourd'hui se trouvent impliqués dans de tels projets.

Il n'est ni dans les intentions du CLUSIF, ni dans celles de ce groupe de travail de remettre en cause ou de discuter de la pertinence ou non d'utiliser la signature électronique. Il s'agit plutôt d'essayer de fournir les outils permettant d'aplanir les difficultés inhérentes à ce type de projets, en particulier le déploiement d'une Infrastructure de Gestion de Clés (IGC) ou Public Key Infrastructure (PKI) qui peut pour beaucoup, représenter l'un des principaux freins à l'adoption de la signature électronique.

Dans ce document les notions de cryptologie et de PKI sont effleurées. Ces notions pourront être approfondies avec des documents traitant spécifiquement de ces sujets.

I.2. Objectifs du document

Le principal objectif de ce document est de fournir des éléments pragmatiques aux chefs de projets et personnes qui ont ou auront la responsabilité de conduire des projets intégrant la signature électronique, afin que leurs projets soient couronnés de succès.

Dans ce document, seuls seront traités les cas de signature électronique s'adossant à une IGC. Des processus de signature électronique ne s'y adossant pas existent, toutefois ces usages ont été considérés trop spécifiques par le groupe de travail pour être traités dans ce document qui se veut généraliste.

Ne seront pas traités dans ce document les utilisations de certificats numériques pour des signatures techniques (signature de code, signature de révocation, etc.)

I.3. A qui s'adresse ce document ?

Le document s'adresse à tous types de sociétés, qu'elles aient ou non fait le choix de gérer la signature électronique en interne ou qu'elles aient préféré faire appel à un prestataire externe.

Il s'adresse ainsi à toutes personnes/sociétés qui souhaitent déployer ou sont en charge d'intégrer la signature électronique au sein de leurs processus d'entreprise, qu'elles aient fait le choix de gérer cette

signature en interne ou qu'elles aient préféré faire appel à un prestataire externe. Parmi les acteurs probables de ce type de projet il faut citer :

- Les architectes des systèmes d'information,
- Les chefs de projet,
- Les responsables des processus métiers,
- Les responsables d'exploitation informatique,
- Les juristes d'entreprise,
- Les responsables de la Sécurité de Systèmes d'Information (RSSI),
- Les directions financières,
- Etc.

II. Valeur juridique

II.1. Contexte législatif

Depuis toujours, la signature est nécessaire à la perfection d'un acte juridique. Elle remplit deux fonctions : elle permet, d'une part, d'identifier « celui qui l'appose » et, d'autre part, de concrétiser le consentement de celui-ci. Dans sa forme traditionnelle, la signature est manuscrite et non raturée. Elle est placée sur *l'instrumentum*, c'est-à-dire le support de l'acte juridique. Dans le cas d'un acte juridique électronique, l'apposition d'une signature traditionnelle est impossible, le support du contrat n'étant pas matérialisé, d'où la nécessité de recourir à une définition de la signature électronique.

La **signature électronique** est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier (*Cf. Wikipédia – La Signature numérique*).

La signature, la signature électronique[1] font l'objet de deux principales définitions juridiques, le Code civil et le Règlement européen n°910/214 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (dit eIDAS), à savoir :

- L'article. 1367 du Code civil donne la définition suivante :

  « *La signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.*
  Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. 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'État. ».

Cet article est précisé par le décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique, qui prévoit que la fiabilité d'un procédé de la signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée

Ce décret reprend les termes du Règlement eIDAS, qui abroge la directive 159 1999/93/CE.

L'article 3 du Règlement définit la signature électronique comme : « Des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer ».

L'apport majeur de ce règlement est la reconnaissance de l'effet juridique de la signature électronique qualifiée. En effet, selon l'article 25 « 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

[1] Les textes tant nationaux qu'européens reposent sur le principe de neutralité technologique. Toutefois, à ce jour, la technologie la plus répandue et fiable pour générer des signatures électroniques est l'utilisation des procédés de cryptographie.

une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée. »

Et d'ajouter « l'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite. ».

Enfin cet article pose également le principe « qu'une signature électronique qualifiée qui repose sur un certificat qualifié délivré dans un État membre est reconnue en tant que signature électronique qualifiée dans tous les autres États membres. »

À cette fin, le règlement met en place des procédures relatives au contrôle des services de confiance « service électronique normalement fourni contre rémunération qui consiste »

a) En la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services ; ou

b) En la création, en la vérification et en la validation de certificats pour l'authentification de site internet ; ou

c) En la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services. »

Le texte réglemente également les prestataires de services de confiance (ou PSCo) qui peuvent être qualifiés ou non-qualifiés.

En France, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) joue un rôle prépondérant dans ces processus de qualifications et de contrôles.

Ces conditions de fiabilité présumée sont décrites dans l'article 2 du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique[2].

Dans son chapitre 4, le règlement définit la signature électronique qualifiée. « Est une signature électronique qualifiée une **signature électronique avancée**, conforme à l'article 26 du règlement susvisé et **créée à l'aide d'un dispositif de création de signature électronique qualifié** répondant aux exigences de l'article 29 dudit règlement, **qui repose sur un certificat qualifié de signature électronique** répondant aux exigences de l'article 28 de ce règlement.

Il est important de noter que l'utilisation d'un certificat électronique qualifié nécessite le recours à un prestataire de service de confiance électronique lui-même qualifié.

Ce cadre est d'autant plus nécessaire que contrairement à la signature manuscrite, la signature électronique n'est pas intelligible par l'homme, et il ne peut donc pas la vérifier sans un outillage.

Même si la correspondance n'est pas formelle, le Référentiel Général de Sécurité (RGS) à destination des administrations françaises, délivré par l'ANSSI, fournit une aide technique graduée (*, **, ***) permettant d'atteindre ces niveaux de signature en déterminant la qualité des certificats et des prestataires de services électroniques. Toutefois, il convient de ne pas oublier que tout écrit disposant d'une signature électronique simple reste admissible devant les Tribunaux au même titre qu'un écrit disposant d'une signature électronique qualifiée bénéficiant de la présomption de fiabilité sous

[2] Ce décret serait abrogé par Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique.

réserve de rapporter la preuve que les exigences de fiabilité sont respectées. En outre, en cas de contentieux, le juge appréciera toujours souverainement la hiérarchie des preuves[3].

Ces services sont assurés par des Prestataires de services de confiance (PSCo) qui peuvent être qualifiés (par l'ANSSI) ou par un prestataire accrédité par la COFRAC qui deviennent PSCe ou non. Dans le cadre de Prestataires de services de confiance qualifiés, il y a un renversement de la charge de la preuve, car ils apportent une présomption de responsabilité.

Indépendamment des enjeux juridiques liés à la signature électronique, la dématérialisation implique de prendre en compte le cycle de vie du document (et de la signature) dans sa globalité : de sa création, à son archivage, voire à sa destruction. Les aspects liés à la sécurité ainsi qu'à la protection des données à caractère personnel (notamment dans le cadre de l'application du RGPD - Règlement Général sur la Protection des Données 2016/679 UE) devront également être abordés dans le cadre des projets et de la négociation des contrats.

II.2. Identification du besoin

La signature permet aux parties impliquées dans une transaction de s'engager sur les termes de cet accord. Un projet de signature électronique répond au besoin principal d'authentifier un ou plusieurs signataires pour un acte donné. Ce besoin peut être plus ou moins fort, selon qu'il s'agit de signer un acte authentique, des achats publics, des contrats en ligne, des vérifications de l'état civil…

Une analyse de risques permettra d'identifier la solution la plus adaptée au besoin, en couvrant au mieux les objectifs de sécurité tout en apportant une réponse circonstanciée aux événements redoutés par le métier.

Selon les résultats de cette analyse de risques, le projet s'orientera vers des solutions tenant compte du niveau de qualité de la signature, de la présomption de fiabilité, du délai de conservation, etc.

Le Règlement eIDAS introduit une innovation, le cachet électronique permettant à une personne morale de créer une signature électronique qui se distingue de celle de la personne physique. Ce cachet qui se définit de la façon suivante (art. 3), « *des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières* », peut servir à authentifier les biens numériques d'une personne morale.

II.3. Preuve numérique

Notre système juridique a laissé une marge d'appréciation importante au juge quant à la validité de la preuve.

Ainsi, l'article 1368 du Code civil dispose que « *A défaut de dispositions ou de conventions contraires, le juge règle les conflits de preuve par écrit en déterminant par tout moyen le titre le plus vraisemblable* ». L'article 287 du Code de procédure civile dispose également que « *Si l'une des parties dénie l'écriture qui lui est attribuée ou déclare ne pas reconnaître celle qui est attribuée à son auteur,*

[3] L'article 288-1 du Code de procédure civile dispose que « lorsque la signature électronique bénéficie d'une présomption de fiabilité, il appartient au juge de dire si les éléments dont il dispose justifient le renversement de cette présomption » et l'article 1368 du code civil dispose « (...) qu'à défaut de dispositions ou de conventions contraires, le juge règle les conflits de preuve par écrit en déterminant par tout moyen le titre le plus vraisemblable ».

le juge vérifie l'écrit contesté à moins qu'il ne puisse statuer sans en tenir compte. Si l'écrit contesté n'est relatif qu'à certains chefs de la demande, il peut être statué sur les autres.

Si la dénégation ou le refus de reconnaissance porte sur un écrit ou une signature électronique, le juge vérifie si les conditions mises par les articles 1366 et 1367 du code civil à la validité de l'écrit ou de la signature électronique sont satisfaites. ».

Le juge sera donc libre de vérifier par exemple l'imputabilité à une personne physique ou morale. Le cycle de vie du document sera donc analysé et ce même de nombreuses années après la signature du document. Ainsi, les contrats qui seront signés avec les Prestataires de services de confiance concernant l'horodatage, l'archivage devront donner lieu à des négociations afin de s'assurer des modalités de conservation des documents (notamment clause d'audit, documentation de la conformité, etc.). Les Parties seront aussi libres d'insérer des conventions sur la preuve.

II.4. Durée de vie de la signature et du document associé

Une confusion souvent rencontrée en matière de signature électronique consiste à penser que la validité d'une signature dépend de celle du certificat avec lequel elle a été produite. Si tel était le cas, alors cela signifierait que la validité de la signature s'achève en même temps que le certificat expire, ce qui n'est évidemment pas le cas. La validité d'une signature dépend de la validité du certificat au moment de la génération de la signature. C'est la raison pour laquelle il est primordial de conserver tous les éléments (horodatage, liste de révocations, etc.) qui ont permis d'établir la validité de la signature au moment de sa création.

L'algorithme utilisé lors de la signature peut au moment de sa vérification (quelquefois plusieurs années plus tard) être devenu vulnérable, ce qui pourrait laisser planer un doute sur la validité de la signature et l'intégrité du document, c'est pourquoi il est conseillé de faire appel à des solutions ou des services d'archivage légal à valeur probante.

III. Fondements technologiques

Bien que la règlementation ne le précise pas (contrairement au RGS et le RFC 3279), la signature électronique sécurisée est étroitement liée aux technologies de cryptographie à clé publique ou cryptographie asymétrique. La connaissance de ces concepts est donc indispensable à quiconque est responsable ou impliqué dans un projet faisant appel à la signature électronique.

La **cryptologie** est composée des deux branches cryptographie et cryptanalyse.

La **cryptographie** s'attache à la protection de messages ou données en concevant des procédés ou algorithmes de chiffrement utilisant des secrets ou clés, assurant ainsi confidentialité, authenticité et intégrité.

Les clés, qui ne sont ni plus ni moins qu'une suite d'octets, possèdent des caractéristiques spécifiques à l'algorithme auquel elles se rapportent. Aussi il est très dangereux de vouloir mesurer la force d'un algorithme à la seule longueur des clés qu'il utilise.

La **cryptanalyse** qui analyse des textes chiffrés pour retrouver les informations dissimulées, est la composante complémentaire à la cryptographie. Ainsi les cryptographes qui possèdent les clés font du chiffrement ou du déchiffrement, alors que les crypto-analystes qui n'ont pas accès aux clés font du décryptage (ou décryptement[4]).

III.1. La cryptographie asymétrique

Il est question de cryptographie asymétrique lorsque deux clés (ou bi-clé) sont utilisées ; l'une est dite ***publique*** car connue et accessible par tout le monde, l'autre est dite ***privée*** car elle n'est connue et accessible que par son seul propriétaire.

Bien qu'étroitement liées à l'identité de l'utilisateur, les deux clés utilisées doivent être aléatoires, décorrélées (la connaissance de la clé publique ne permet pas de déduire la clé privée[5]), pouvoir être facilement générées, mais néanmoins être reliées entre elles (toute donnée chiffrée par l'une des clés n'est déchiffrable qu'avec l'autre clé). Comme son nom l'indique la clé publique a vocation à être librement partagée, tandis que la clé privée ne doit être accessible que par son seul propriétaire.

Le principe des systèmes asymétriques est basé sur la complexité de résolution de certains problèmes mathématiques comme la factorisation d'un nombre entier formé de deux facteurs premiers[6] comme l'algorithme RSA, ou de logarithme discret[7] sur un corps fini comme l'algorithme de Diffie-Hellman.

Les utilisations qui sont faites de la cryptographie asymétrique ont d'abord pour objectif le chiffrement de données. Dans la figure ci-dessous, un document est envoyé en toute confidentialité à Alice en se

[4] Synonyme de décryptage : Restitution du sens d'un message

[5] La connaissance de la clé privée permet généralement (aussi bien en DSA qu'en RSA) de déduire la clé publique

[6] La factorisation consiste à retrouver la décomposition en facteurs premiers d'un entier donné, obtenu de manière secrète par multiplication de deux nombres premiers, généralement de taille comparable. Un tel nombre composé est classiquement appelé « module »

[7] Le problème dit « du logarithme discret » est fondé sur la difficulté d'inverser l'opération d'exponentiation dans un groupe mathématique.

servant de sa clé publique pour chiffrer le document, lequel pourra uniquement être déchiffré par Alice grâce à sa clé privée.

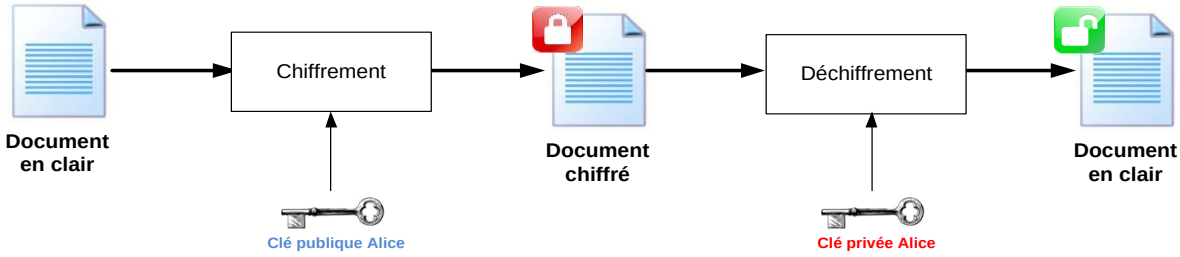


Figure 1 - Principe du chiffrement asymétrique

Mais une des caractéristiques essentielles des systèmes asymétriques est leur capacité à implémenter la signature électronique illustrée par la Figure 2. A l'inverse du chiffrement, la signature est réalisée en utilisant la clé privée du signataire, toutes ses contreparties pouvant alors vérifier sa signature en utilisant sa clé publique.

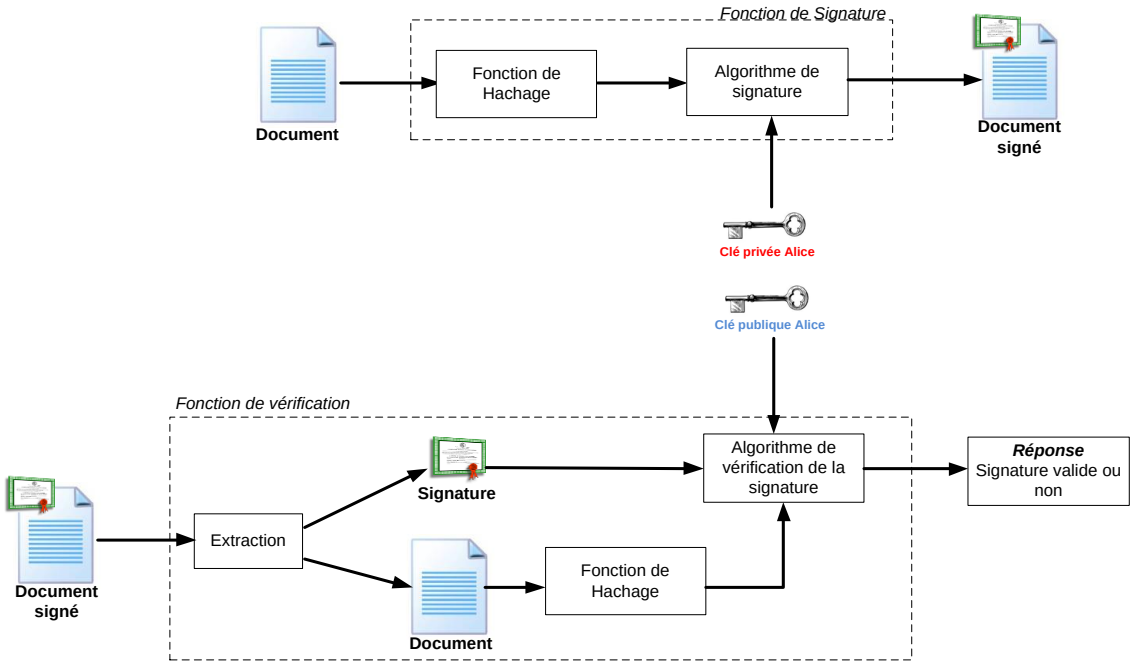


Figure 2 - Processus de Signature

La cryptographie asymétrique connaît deux limitations principales **[1]**. Les données que peuvent accepter des algorithmes comme RSA sont limitées à la taille de la bi-clé (pour un document, il faut le découper). Ensuite les performances de la cryptographie asymétrique sont assez mauvaises. Pour le chiffrement, la solution apportée est une utilisation conjointe de la cryptographie symétrique. Pour la signature électronique, la solution apportée consiste à employer les fonctions de hachage (Cf. § Les fonctions de hachage) comme décrit dans la Figure 2.

III.2. La cryptographie symétrique

A la différence de la cryptographie asymétrique, dans les systèmes symétriques une seule et même clé est partagée entre l'émetteur et le récepteur. Les algorithmes utilisent des combinaisons d'opérations

très simples comme des permutations, rotations, expansions, réductions qui combinent des caractères du texte en clair et ceux de la clé.

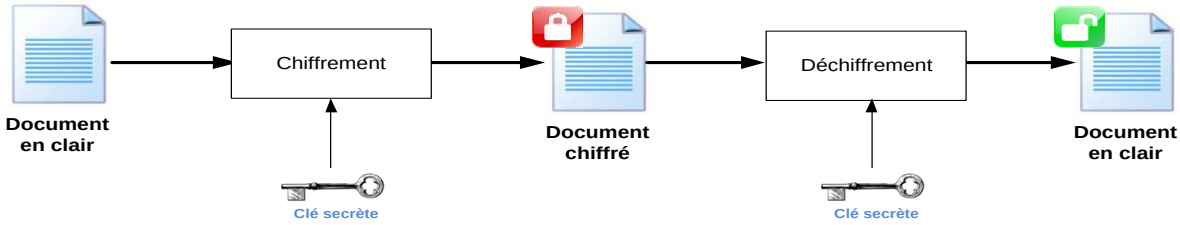


Figure 3 - Principe du chiffrement symétrique

Principalement utilisés pour assurer la confidentialité de données échangées, les systèmes symétriques peuvent également être utilisés dans des protocoles d'authentification de partenaires ou de vérification d'intégrité.

La principale limitation d'utilisation de le cryptographie symétrique réside dans la problématique de la transmission en toute confidentialité de la clé secrète.

III.3. Les fonctions de hachage

Une fonction de hachage transforme un document de taille quelconque en une chaîne de caractères de longueur fixe relativement petite par rapport au document d'entrée. Cette chaîne de caractères est communément appelée le *haché*, *condensat* ou encore *empreinte*. Comme illustré dans la Figure 2, les fonctions de hachage sont des éléments essentiels des procédés de signature électronique.

Le haché d'un document doit être non prédictible de sorte que tout changement, même minime, du document, entraine un haché différent, garantissant ainsi l'intégrité du document.

D'un point de vue cryptographique, une fonction de hachage est un traitement mathématique à sens unique et irréversible. Cette irréversibilité entraine qu'à partir du haché on ne puisse pas retrouver le document initial (*résistance à la préimage*).

Une autre caractéristique essentielle aux fonctions de hachage voudrait que si deux documents ont le même haché, alors ces documents sont obligatoirement identiques (permettant d'assurer ainsi l'unicité). C'est ce que l'on désigne par la *résistance aux collisions.*

Une dernière propriété attendue des fonctions de hachage est leur *résistance à la seconde préimage* qui assure que pour un document connu, il est pratiquement (utilisation d'une quantité raisonnable de ressources dans une durée de temps raisonnable) impossible de créer un second document donnant le même haché.

Les fonctions de hachage permettent ainsi non seulement de gagner de la performance, mais surtout elles permettent de détecter la falsification d'une signature, protégeant ainsi l'intégrité d'un texte.

III.4. Recommandations sur la taille des clés

Le niveau de sécurité, pour un algorithme choisi, dépend non seulement de la taille de la clé, mais également de sa durée de validité. La taille de la clé doit être régulièrement revue à la hausse afin de suivre l'accroissement de la puissance des ordinateurs.

Les recommandations de l'ANSSI **[5]** se basent par exemple sur une hypothèse purement calculatoire supposant que de nouvelles attaques n'ont pas vu le jour, que la cryptanalyse par informatique quantique n'est pas sortie de son stade de laboratoire, et que la paire de clés n'est pas prématurément révocable.

Ainsi le choix de la taille des clés (en bits) dépendra non seulement de l'algorithme utilisé, mais aussi de la durée pendant laquelle on souhaite que l'opération cryptographique soit valide. Le tableau ci-dessous reprend ainsi les principales recommandations de l'ANSSI également disponibles sur le site : *https://www.keylength.com/fr/5/*.

	Types d'algorithmes						
Période de validité	**Symétrique**	**Factorisation** ***Module***	**Logarithme discret**		**Courbe elliptique**		**Hash**
			Clef	***Groupe***	***GF(p)***	***GF(2^n)***	
2014 – 2020	100	2048	200	2048	200	200	200
2021- 2030	128	2048	200	2048	256	256	256
> 2030	128	3072	200	3072	256	256	256

IV. Les infrastructures de gestion de clés

Disposer d'une paire de clés cryptographiques est suffisant pour techniquement apposer une signature sur un document et ensuite la vérifier (Cf. Figure 2). Mais la signature doit sans ambiguïté permettre d'identifier celui qui l'appose. Le récepteur d'un document signé utilisera la clé publique de l'émetteur pour vérifier la signature, mais il devra auparavant s'être posé les questions : *« à qui appartient cette clé publique ? »* et *« pour quels usages peut-on l'utiliser ?».*

La clé publique doit donc être accompagnée d'informations descriptives concernant notamment son propriétaire et les usages auxquels cette clé est destinée. L'ensemble de ces informations sont conservées dans des **certificats numériques**, fichiers de données à la structure normalisée, créés et délivrés par des Infrastructures de Gestion de Clés (IGC). Ces autorités de confiance, comme elles sont communément appelées, garantissent le lien entre la clé publique et l'identité du signataire engageant ainsi leur responsabilité.

Version du certificat
Numéro de série
Description de l'algorithme de signature du certificat
Nom de l'Autorité de certification ayant émis/signé le certificat
Période de validité
Nom du détenteur du certificat
Clé publique du détenteur du certificat
Identité de l'autorité de certification (optionnel)
Identité du détenteur du certificat (optionnel)
Extensions (optionnel)
Signature de l'Autorité de Certification

Figure 4 - Structure simplifiée d'un certificat numérique

Les IGC remplissent principalement les rôles d'Autorité de Certification, d'Autorité d'Enregistrement ou de Service de publication, mais elles peuvent aussi délivrer des services complémentaires.

Une personne physique ou morale qui voudra que son identité soit associée de manière certaine à une paire de clés cryptographiques, devra donc demander à une Autorité de Certification de lui délivrer un certificat pour attester de cette relation.

IV.1. Autorité de Certification

L'Autorité de Certification (AC) est donc la source de la confiance que l'on peut accorder aux certificats. Elle garantit que les certificats qu'elle délivre sont conformes à sa Politique de Certification (PC)[8] qui définit à la fois les types de certificats qu'elle émet, à qui elle peut les délivrer, ainsi que les procédures de production et de gestion associées. L'AC signe tous les certificats qu'elle émet, ces informations

[8] Le RGS v2.0 propose dans son annexe A2 des politiques de certifications types utilisables pour des certificats de signature.

(nom, signature) sont disponibles dans les données du certificat (Cf. Figure 4).

Certaines AC peuvent délivrer des certificats à d'autres AC créant ainsi une hiérarchie de certificats. Ainsi lors de la vérification d'un certificat, il est nécessaire non seulement de vérifier la période de validité du certificat, mais aussi celles de tous les certificats de la hiérarchie des AC impliquées dans son émission. On parle alors de chemin de certification pour cette série d'AC.

IV.2. Autorité d'Enregistrement

L'Autorité d'Enregistrement[9] (AE) dépend au moins d'une AC et effectue tout ou partie des fonctions administratives telles que :

- Vérifier l'identité du demandeur en obtenant les pièces justificatives correspondant à la Politique de Certification sous laquelle le certificat doit être émis
- Valider que le demandeur est habilité à obtenir les droits ou qualités qui seront mentionnés dans le certificat
- Obtenir la clé publique du demandeur
- Vérifier que le demandeur est en possession de la clé privée associée à la clé publique
- Soumettre les demandes de génération de certificat à l'autorité de certification émettrice du certificat
- Recevoir et traiter les demandes de révocation, de suspension ou de réactivation des certificats

Le rôle de l'AE est primordial. En effet une fois généré le certificat devient infalsifiable car signé avec la clé privée de l'AC. C'est pendant la phase d'enregistrement que peuvent survenir des tentatives de fraudes visant à usurper l'identité du propriétaire légitime du certificat. **Une faille dans la procédure d'enregistrement de l'identité du porteur du certificat peut remettre en cause la confiance dans tous les certificats délivrés par l'AC**.

La fonction d'autorité d'enregistrement est le plus souvent remplie par l'autorité de certification mais, selon la politique de certification attachée aux certificats numériques, cette fonction peut être déléguée. C'est le schéma que l'on retrouve le plus couramment lorsqu'une entreprise fait appel à un prestataire pour lui fournir des certificats, que ceux-ci soient destinés à ses clients ou à ses collaborateurs.

Une autre fonction essentielle assurée généralement par l'Autorité d'Enregistrement concerne la gestion des demandes de révocation ou de suspension des certificats. Les demandes de révocation pour des raisons qui peuvent être une suspicion de compromission de la clé privée, des modifications des informations contenues dans le certificat, ou autres, sont transmises à l'AC pour la réalisation du traitement, après que l'identité du demandeur ait été vérifiée.

[9] D'après le RFC3647 de l'IETF.

IV.3. Service de publication

Le service de publication permet de diffuser les certificats émis par l'AC à l'ensemble des utilisateurs. Il publie également la liste des certificats et des listes de révocation des certificats (LCR ou CRL - Certificate Revocation List).

Toute signature effectuée avec un certificat après sa date de révocation doit être considérée comme invalide. La révocation d'un certificat peut jeter un doute sur l'ensemble des signatures effectuées avec ce certificat, car il est souvent difficile d'assurer que la date de révocation est bien antérieure à la compromission (ou tout autre raison) ayant entrainé la révocation.

IV.4. Autorité de validation

Avant d'utiliser un certificat, et dans le cas de la signature électronique, la clé publique qu'il contient, il est nécessaire de vérifier sa validité. Il s'agit d'un processus comprenant des opérations visant entre autres à contrôler :

- L'intégrité du certificat,
- Sa validité,
- Sa politique d'usage.

Devant la complexité que peut revêtir un tel processus (notamment s'il est question de hiérarchie de certificats), il est courant de faire appel à une Autorité de Validation (AV) qui, ayant collecté les listes de révocation produites par les autorités de certification, sera en mesure de rendre ce service.

IV.5. Autorité d'Horodatage

L'Autorité d'Horodatage (AH) qui peut être une composante d'une IGC permet d'attester qu'une donnée existe à un moment précis en assurant l'association de la donnée et du temps, et en signant une structure (jeton d'horodatage) permettant cette association.

Une Autorité d'Horodatage peut faire fonctionner plusieurs unités d'horodatage chacune ayant son certificat et sa clé privée. Le certificat de signature et les documents signés par le porteur d'une clé de signature sont des informations que peut signer une unité d'horodatage dans le cadre de la signature électronique.

IV.6. Processus de délivrance d'un certificat

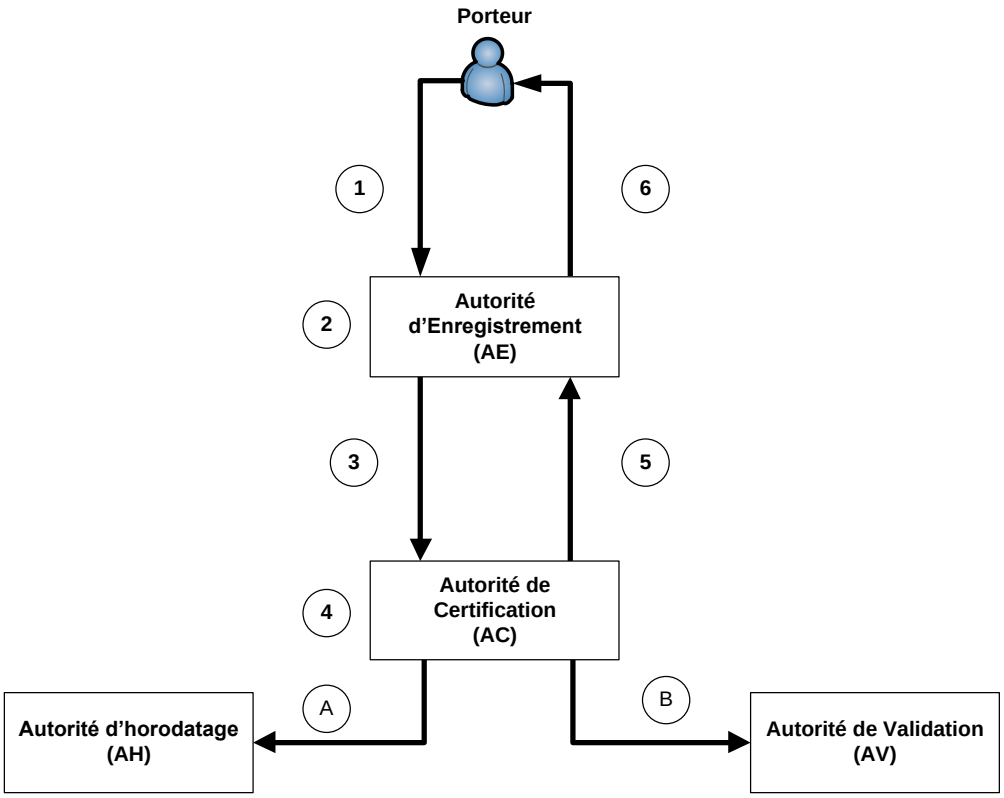
La figure ci-après illustre de façon très schématique le processus de délivrance d'un certificat :

1. Le porteur (ou son représentant) fait une demande de certificat.

   La génération de la bi-clé peut être réalisée directement par le porteur, par l'autorité d'enregistrement (avec généralement la remise d'un support physique) ou par l'autorité de certification.

2. L'autorité d'enregistrement procède à la vérification de l'identité du porteur
3. La demande est transmise à l'autorité de certification

4. L'autorité de certification génère le certificat
5. Le certificat est transmis à l'autorité d'enregistrement afin d'être remis au porteur
6. Le certificat est remis au porteur (ou éventuellement à son représentant)



La signature électronique va de plus faire intervenir les deux autorités non impliquées dans la délivrance du certificat :

A. L'autorité d'horodatage sera sollicitée lors de la signature d'un document
B. La liste de révocation des certificats est récupérée par l'autorité de validation et peut être sollicitée lorsqu'il sera nécessaire de vérifier la validité de la signature d'un document avant ou après qu'elle ait été générée.

   Remarque : Dans de nombreux cas, la signature sera vérifiée par un logiciel utilisé par le vérifieur qui va consulter le statut de révocation (via liste de révocation ou service associé).

IV.7. Les certifications des services d'une IGC

Le niveau de confiance que l'on peut accorder aux AC repose sur la rigueur avec laquelle ses politiques de certification sont appliquées. Cela englobe aussi la politique d'enregistrement qui, comme précisé auparavant, garantit l'identité du propriétaire du certificat.

Cette rigueur peut être évaluée et certifiée par des organismes externes[10]. Ce processus de qualification aboutira, s'il est couronné de succès, à ce que l'IGC soit certifiée comme Prestataire de Services de Confiance auprès des autorités.

IV.7.1. Niveaux de signature

Une signature électronique est équivalente à une signature manuscrite dans l'Union Européenne (eIDAS article 25). Une signature électronique ne peut pas être refusée comme preuve en justice au seul motif qu'elle est électronique ou non électronique qualifiée (eIDAS article 25).

Le règlement eIDAS ne définit que la « signature électronique avancée » et la « signature électronique qualifiée ». Le terme « signature simple » est généralement utilisé pour désigner les autres niveaux de signature sans définition règlementaire.

	Signature Simple	Signature Avancee	Signature qualifiee	
Niveau de signature	Simple	Avancé	Qualifié	
Niveau de certificat	Certificat simple	Certificat provenant d'une chaîne de certification avancée - sur support logiciel	Certificat qualifié sur support matériel	
			Clé USB ou carte à puce	Serveur qualifié
Bénéfice	Intégrité	Intégrité et non-répudiation	Intégrité et non répudiation	
Exemple de besoins par niveau de signature	Notes de frais, promesse d'embauche	Contrat de travail (RH)	Acte notarié, contrat de crédit	
Exigence enrôlement	Pas d'exigence	Identité vérifiée à distance	Présence physique du demandeur obligatoire et dispositif qualifié	

Tableau 1- Signature par une personne physique

	Cachet Simple	Cachet Avance	Cachet qualifiee
Niveau de signature	Simple	Avancé	Qualifié
Niveau de certificat	Certificat simple	Certificat avancé	Certificat qualifié sur dispositif cryptographique qualifié (HSM)
Bénéfice	Intégrité	Intégrité et non répudiation	Intégrité et non répudiation
Exigence enrôlement	Pas d'exigence	Pas d'exigence	Respect des règles d'enrôlement du dispositif cryptographique qualifié

Tableau 2 - Cachet serveur

La signature électronique avancée doit répondre aux exigences de l'article 26 de ce règlement :

[10] LSTI est en France le seul organisme certificateur des PSCo, en tant que tel il est accrédité par la COFRAC qui représente l'État français.

a) *Être liée au signataire de manière univoque ;*

b) *Permettre d'identifier le signataire ;*

c) *Avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; et*

d) *Être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.*

La « signature électronique qualifiée » est définie comme : « une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique ».

Un « certificat de signature qualifié » en plus des exigences de contenu énoncées dans le règlement doit être délivré par un « prestataire de service de confiance qualifié » tel que défini dans le règlement.

La notion de « prestataire de service de confiance qualifié » remplace les notions de « Prestataires de services de certification électronique (PSCE) qualifiés » et « prestataires de services d'horodatage électronique (PSHE) qualifiés » introduites par le RGS.

Exemple de signature avancée : lettre recommandée électronique.

Exemple de signature qualifiée : signature chez le notaire.

IV.7.2. Normes et standards

Les différents composants d'une IGC ont été définis par le groupe PKIX11 de l'IETF et tout particulièrement par le RFC 5280 qui s'appuie sur le format de certificat le plus courant défini par ISO/IEC/ITU-T X509 version 3 pour le certificat et version 2 pour les CRL.

L'IETF, l'ISO, l'IEC et l'ITU se coordonnent pour définir les documents de normes et standards sur les IGC et les certificats.

L'ensemble des normes et références s'appliquant à la signature électronique et liées à eIDAS ou les documents qu'il remplace ou complète est indexé dans le document de l'ETSI TR 119 000. On y retrouvera tout particulièrement les références pour les différents formats AdES (CAdES EN 319 122, ...) et les politiques de signatures (TS 119 172).

En France pour ce qui concerne la signature électronique, le RGS[12], publié par l'ANSSI, définit les standards cryptologiques à utiliser, des modèles de politiques à utiliser pour les IGC et les exigences pour leurs différents niveaux de certification et celles des prestataires de confiance. Il complète les documents de l'ETSI en attendant qu'ils soient tous publiés.

IV.8. Type de certificats

On distingue plusieurs types de certificats selon l'usage qu'il est en fait :

- Certificat de chiffrement :

[11] Les documents principalement RFC publiés par ce groupe se trouvent à https://tools.ietf.org/wg/pkix/

[12] En 2017, le RGS n'est pas aligné sur eIDAS pour ce qui concerne les prestataires de confiance.

Il est utilisé afin de protéger la confidentialité des données en les chiffrant avec la clé publique de l'utilisateur qu'il s'agisse d'une personne physique ou d'une personne morale (certificat serveur TLS).

- Certificat de signature :
  Utilisé pour signer des données, on peut en distinguer deux sortes :
  1. Certificat de signature des clés : il est détenu par des sous-autorités de certification et il permet uniquement de signer les clés privées/publiques d'un utilisateur final
  2. Certificat de signature de documents : il est détenu par le porteur et permet de signer des documents. Quand le porteur est non humain, le RGS comme eIDAS utilise le terme de cachet ou cachet serveur au lieu de signature.
- Certificat d'horodatage :
  Il permet d'horodater des données. On peut les classer comme sous-catégorie des certificats de signature. Ce certificat est généralement détenu par une Autorité d'horodatage.
- Certificat d'authentification

  Les certificats d'authentification sont de véritables cartes d'identité de son porteur ou d'une entité lorsqu'il s'agit d'une personne morale.

Il est important d'utiliser un certificat pour un usage déterminé. Autrement dit, pour réduire la surface d'attaques il est préférable de ne pas utiliser un seul certificat pour plusieurs usages (chiffrer, signer et/ou horodater). En effet, la compromission d'un tel certificat donnerait beaucoup de pouvoir à un éventuel attaquant.

IV.9. Les supports des certificats

Les certificats numériques se présentent sous la forme de fichiers informatiques. La clé privée qui leur est associée doit absolument être protégée dans un support (container) sécurisé. Une erreur fréquemment commise est de conserver le certificat dans le même dispositif que la clé privée. En effet le format de fichier le plus couramment utilisé (PKCS12, fichiers P12 ou PFX) est un format « container » regroupant à la fois le certificat et la clé privée.

Ce genre de méprise peut conduire à la compromission de l'intégrité de la clé privée. Dans le cas d'échange de certificats pour une communication sécurisée en S/MIME, l'une des parties peut transmettre le container contenant le certificat ET la clé privée plutôt que le seul certificat.

IV.9.1. Les HSM (Hardware Security Module)

Un HSM est un dispositif matériel considéré comme d'un haut niveau de confiance doté de fonctions cryptographiques et offrant des services de sécurité qui consistent à générer, stocker et protéger des clés cryptographiques. Ce matériel peut se présenter sous la forme d'une carte électronique enfichable sur un ordinateur ou d'un boîtier externe (appliance).

Ce haut niveau de résistance aux attaques permet de garantir l'intégrité de l'Autorité de Certification vis-à-vis de ses Politiques de Sécurité[13].

[13] Wikipedia : https://fr.wikipedia.org/wiki/Hardware_Security_Module

IV.9.2. Carte à puce

Comme le HSM les cartes à puce disposent de fonctions cryptographiques et permettent de stocker les certificats et des clés privées avec un haut niveau de confiance. Cependant ces supports ont des inconvénients non négligeables, notamment dans le cadre de la mobilité :

- Imposent des contraintes au niveau du terminal (lecteur de cartes, pilotes dont la disponibilité peine à suivre l'accélération des changements de versions d'OS)
- Ont des coûts pouvant rapidement être dissuasifs,
- Requièrent une logistique importante (acquisition/stockage/distribution…)

IV.9.3. Token PKI USB, calculette :

Même capacité que les cartes à puce avec l'avantage de ne pas nécessiter de lecteur spécifique.

IV.9.4. Puce TPM (Trusted Platform Module)

La puce TPM est un **microprocesseur cryptographique** généralement intégré sur la carte-mère d'un ordinateur.
Elle permet :

- De générer, stocker et contrôler l'usage des clés cryptographiques et des certificats,
- D'authentifier l'équipement,
- D'assurer l'intégrité de l'équipement.

Ce composant matériel offre un niveau de protection raisonnable aux informations cryptographiques qui y sont stockées. La protection offerte par un TPM est inférieure à celle que peut fournir une carte à puce. A noter qu'il est possible de réinitialiser le contenu de la puce TPM.

La puce TPM est supportée de façon standard par les principaux systèmes d'exploitation (Windows, Linux, Unix, ...)

IV.10. Formats de signature

On trouve les signatures sous plusieurs formats dont :

- Binaires : PKCS #7 / CMS / CAdES
- XML : XML-Sig / XML-DSig / XAdES
- PDF : PAdES

Les formats de signature les plus courants organisent le stockage de la signature et du contenu signé sur l'un des trois modes suivants :

- Signature enveloppée ou encapsulée : les données signées sont contenues dans la signature ;
- Signature enveloppante : la signature est contenue dans la structure des données signées ;
- Signature détachée : la signature et les données sont contenues dans deux structures différentes.

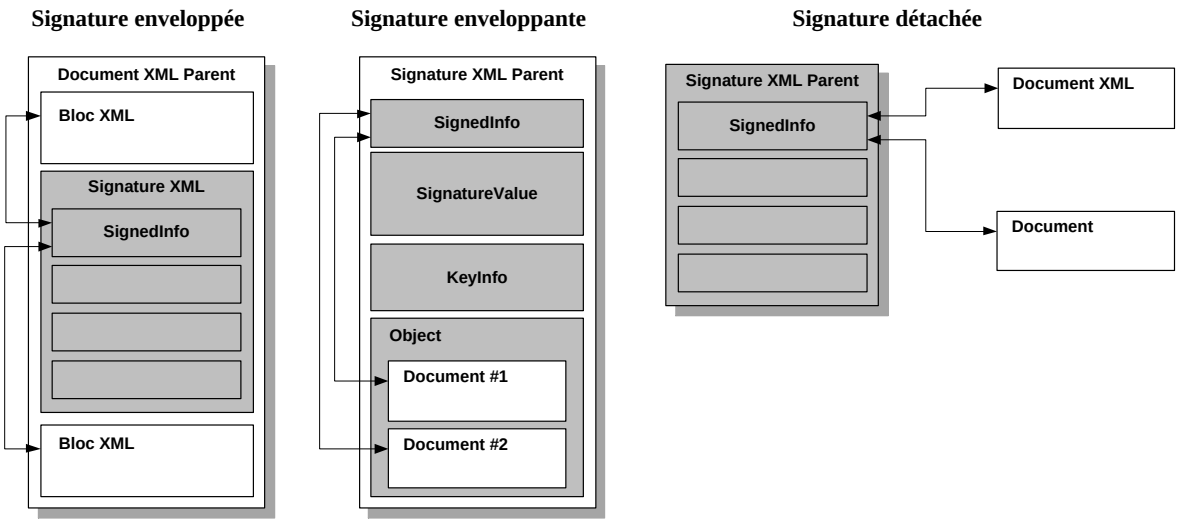


Figure 7 – Différentes formes de signature appliquées au format XML

Dans le cadre de la famille AdES, des extensions complémentaires peuvent être ajoutées au format de signature XAdES. Ces extensions permettent d'étendre la durée de vie de la signature :

- XAdES : format de base
- XAdES-T : en complément des données ajoutées par le XAdES, cette extension inclut une date, un timestamp à l'intérieur de la signature qui peut être délivré par une *autorité d'horodatage* (AH)
- XAdES-C : en complément des données ajoutées par le XAdES-T, cette extension inclut les données de validation complètes (chemins de certification et informations sur le statut de révocation du certificat)
- XAdES-X : en complément des données ajoutées par le XAdES-C, cette extension inclut les données de validation étendues (date des références aux données de validation)
- XAdES-XL : en complément des données ajoutées par le XAdES-X, cette extension inclut des données de validation étendues pour le long terme (valeurs des certificats, valeurs des états de révocation)
- XAdES-A : en complément des données ajoutées par le XAdES-XL, cette extension inclut des données de validation pour l'archivage (dates de l'archivage des signatures afin de les protéger au cas où les données cryptographiques deviendraient vulnérables).

Le choix de la forme et du format dépend de plusieurs facteurs :

- Le contexte (signature personne physique, personne morale, signature unitaire, signature faite par une application métier, etc.)
- Le type de données à signer (PDF, XML, etc.).

La durée de vie de la signature et le processus de vérification : les outils disponibles pour vérifier la signature vont permettre de choisir la forme et le format de signature.

V. Les usages

Choisir quels processus tireraient avantage à utiliser la signature électronique, repose la question de savoir quels objectifs sont recherchés lorsque l'on demande à un individu ou une entité de signer un document[14]. La signature électronique permettant notamment la détection de la perte d'intégrité d'un document dans le temps et d'apporter d'autres informations inaltérables sur le document signé (date, lieu, validité du document, etc.), il est donc attendu, et sans que ce soit explicite, que le signataire ne puisse contester qu'il est l'auteur du document considéré ou qu'il en ait approuvé le contenu.

Les quelques questions suivantes peuvent aider à faire un choix :

- Est-ce qu'il est important de pouvoir vérifier que le document n'a pas été altéré dans le temps ?
- Est-ce que le document doit être validé par une ou plusieurs personnes ?
- Est-ce qu'il est important que les identités des signataires soient établies ?
- Est-ce qu'il est important que les signataires ne puissent pas contester leurs signatures sur le document ?

Outre ces besoins, la signature électronique fait partie de l'éventail des outils à disposition des entreprises pour atteindre leurs objectifs en matière de dématérialisation, tels que :

- Fluidifier la circulation des informations au sein d'un processus ;
- Réduire la durée de traitement d'un processus ;
- Réduire les frais inhérents au traitement des documents papiers.

Comme tout projet, la mise en place de la signature électronique nécessite des investissements, tant matériels qu'organisationnels. Il faut donc bien peser les gains qu'elle apportera, et comme pour tout projet le calcul du retour sur investissement doit avoir été établi.

V.1. Procédés de signature

Les certificats numériques étant le gage de l'identité de son porteur, à l'instar de la carte d'identité ou du passeport, la même « rigueur » devait donc être apportée à sa délivrance pour qu'il puisse inspirer la même confiance. Les procédures de délivrance demandaient donc presque toujours de faire appel à une Autorité d'Enregistrement avec une rencontre en face-à-face avec le futur signataire auquel il était remis un token (carte à puce le plus souvent). Ce token qui contenait le certificat était demandé au moment où l'utilisateur devait signer un document.

Il pouvait cependant se passer beaucoup de temps entre le moment où le certificat était délivré et celui où il serait effectivement utilisé. La plupart des utilisateurs avaient en général perdu le token, ou

[14] Les documents papiers ou électroniques ne sont bien entendu pas les seuls objets qu'il est possible de signer. Il est par exemple également possible de signer une œuvre d'art (peinture, sculpture), sans oublier le fait qu'une signature n'est pas seulement un paraphe, mais peut être aussi un mode opératoire ou une façon de faire, voire une suite d'indices ou de symptômes.

s'il s'agissait d'un fichier, ne savaient plus où il était stocké sur son ordinateur (quand celui-ci n'avait pas été remplacé). Nous avons tous en tête les premières déclarations d'impôts qu'il fallait signer avec un certificat délivré par le Ministère des Finances.

C'est ainsi qu'est née l'idée de ne délivrer un certificat qu'au moment de son utilisation, et qu'il a été question de signature à la volée et de signature durable.

V.1.1. Signature à la volée

Plutôt que de parler de signature à la volée, il est plus approprié de parler d'émission de certificat de signature à la volée. Celui-ci n'est en effet délivré qu'au moment de son utilisation et n'a en général qu'une durée de vie très courte (1 minute à 1 semaine). La clé privée est le plus souvent générée par l'autorité de certification qui la détruit une fois la signature réalisée.

Ce type de certificat est surtout utilisé pour des transactions à distance, ce qui jusqu'à aujourd'hui a limité son usage à des cas ne présentant que peu de risques de contestation du fait que l'identité du signataire est plus difficile à établir et à démontrer.

Un code OTP[15] envoyé sur le téléphone portable du signataire est couramment employé pour enrichir les éléments permettant de prouver l'identité du porteur. Cette limitation pourrait être abrogée sous réserve d'être validée par le législateur avec l'apport de nouvelles technologies comme la reconnaissance faciale que des sociétés proposent d'utiliser pour apporter davantage de fiabilité au processus d'établissement de l'identité du signataire.

L'acceptation du SMS comme authentifiant par le législateur est purement spéculative et improbable. Purement théoriques jusqu'à il y'a peu, les attaques via SS7 sont aujourd'hui utilisées par les criminels[16]. Si des moyens d'authentification « renforcés » supportés par les ordiphones sont concevables, l'utilisation des SMS est aujourd'hui explicitement découragée par le NIST[17].

V.1.2. Signature durable ou autonome

Comme pour la signature à la volée, le terme de signature durable se rapporte davantage au certificat utilisé pour réaliser la signature qu'à l'acte de signature lui-même. Il s'agit essentiellement de certificats délivrés dans un processus incluant une rencontre physique qui garantit l'identité.

La « lourdeur » toute relative de ce processus pour l'obtention du certificat entraîne, par souci d'économie de temps et d'argent, que ces certificats aient à la fois une durée de vie plus longue et, en dépit des problèmes que cela peut engendrer, qu'ils soient utilisés pour différents usages (Identité, Signature ou Chiffrement).

V.2. La mise en œuvre technique

Les chapitres précédents ont permis de se familiariser avec les concepts techniques et juridiques inhérents à la signature électronique. La Figure 2 en a décrit le principe, mais il reste que sa déclinaison opérationnelle est à expliciter. Dans les faits le futur signataire devra notamment :

[15] One-Time Password – Mot de passe à usage unique

[16] https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/

[17] https://threatpost.com/nist-recommends-sms-two-factor-authentication-deprecation/119507/

- Accéder et visualiser le document à signer,
- Signer ce document en utilisant un « instrument de signature » qui aura été mis à sa disposition.

Dans la méthode manuscrite « traditionnelle », le signataire devait, pour signer, utiliser un stylo et exécuter un geste (sa signature) que lui seul, dans une certaine mesure, maîtrise permettant en cela de prouver son identité.

Pour la signature électronique, le principe est le même. L'application de signature remplace le stylo et le geste correspond à l'information (mot de passe, code OTP, etc.) renseignée par le signataire pour à la fois attester de son consentement et de son identité, et surtout permettre d'accéder à la clé privée

Le processus de signature numérique nécessitant une datation fiable, il peut être décomposé en trois sous-processus :

1. La signature du document,
2. L'horodatage du document,
3. La vérification.

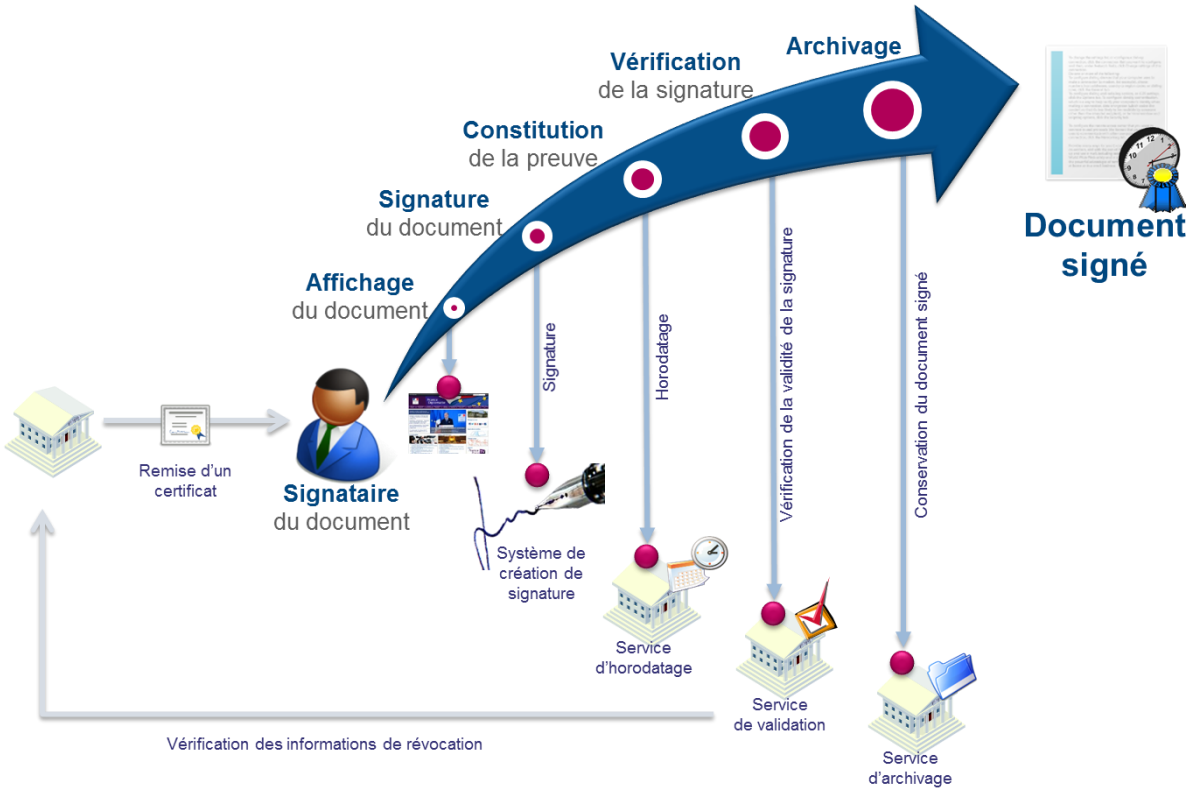


Figure 8 – Modèle de cinématique de signature

Selon les outils et application utilisés, ces étapes sont plus ou moins transparentes pour l'utilisateur.

Affichage du document :

- Visualisation du document à signer si possible en mode WYSIWYS[18],

[18] What You See Is What You Sign

- Authentification permettant d'assurer la non répudiation,
- Demande de signature.

Signature du document :

- Récupération de la bi-clé et du certificat du signataire,
- Signature du document avec la clé privée du signataire,

Vérification de la signature :

- Récupération de la CRL [19]et d'un jeton d'horodatage,
- Apposition d'un cachet serveur (horodatage).

Archivage (fonction connexe à la signature électronique) :

- Conservation des documents, des signatures et des preuves,
- Visualisation des documents et des preuves.

Prérequis :

a) Disposer d'une application de signature,

b) Détenir la clé privée associée à son certificat de signature valide,

c) Récupérer tous les certificats de la chaîne de certification (clé privée),

d) Récupérer le certificat de l'autorité d'horodatage,

e) Avoir un moyen ou une application permettant de vérifier la signature sur le document signé.

Les différentes opérations techniques effectuées pour l'horodatage, la signature d'un document et la vérification du document signé sont décrites au chapitre « ANNEXE : processus technique de signature d'un document ».

V.3. Signature d'un contrat d'assurance

La Figure 9 décrit schématiquement le processus de souscription d'un contrat d'assurance vie. Celui-ci faisait traditionnellement intervenir les acteurs que sont le client, l'intermédiaire (agent, courtier) et la compagnie d'assurance. La signature électronique, si elle permet une réduction du délai de transmission des documents entre l'intermédiaire et l'assureur, fait maintenant entrer les prestataires de services de confiance dans la relation. Leur rôle est déterminant pour assurer la validité et la pérennité de la transaction ainsi effectuée.

À noter que dans ce cas précis il y a une rencontre physique (face à face) entre le client et l'intermédiaire, ce dernier jouant ainsi en plus le rôle d'Autorité d'Enregistrement déléguée avec la lourde charge de garantir l'identité du client.

[19] Certificateur Revocation List

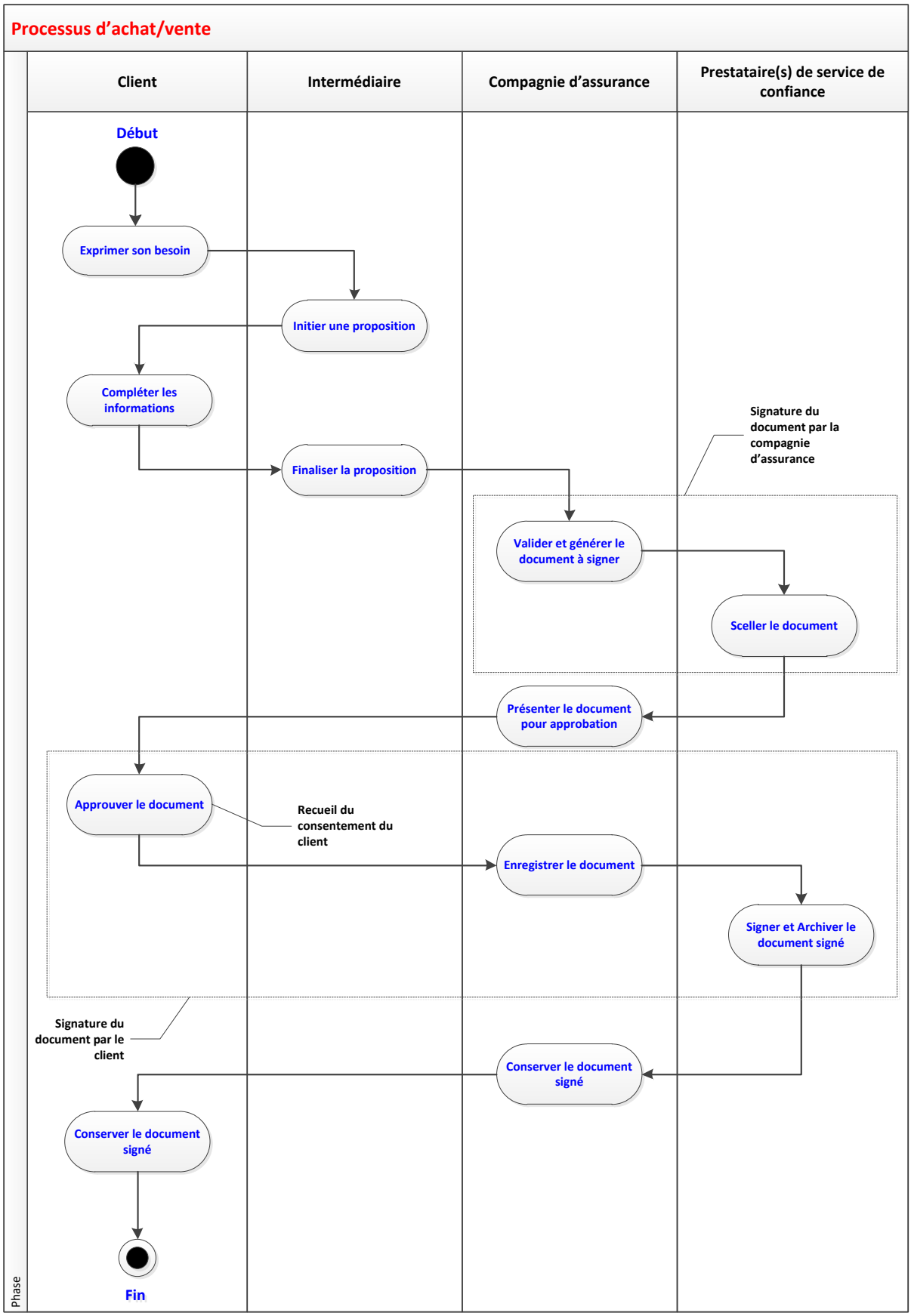


Figure 9 - Exemple de processus utilisant la signature électronique

V.4. Lettre recommandée électronique

L'article L100 du Code des Postes et Communications Electroniques stipule que *« l'envoi recommandé électronique est équivalent à l'envoi par lettre recommandée, dès lors qu'il satisfait aux exigences de l'article 44 du 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 »*.

De plus l'article L122-15 du Code des Relations entre le Public et l'Administration précise que *« Lorsqu'une personne doit adresser un document à l'administration par lettre recommandée, cette formalité peut être accomplie par l'utilisation d'un téléservice au sens de l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, d'un envoi recommandé électronique au sens de l'article L. 100 du code des postes et des communications électroniques ou d'un procédé électronique, accepté par cette administration, permettant de désigner l'expéditeur et d'établir si le document lui a été remis.*

Lorsque l'administration doit notifier un document à une personne par lettre recommandée, cette formalité peut être accomplie par l'utilisation d'un envoi recommandé électronique au sens du même article L. 100 ou d'un procédé électronique permettant de désigner l'expéditeur, de garantir l'identité du destinataire et d'établir si le document a été remis. L'accord exprès de l'intéressé doit être préalablement recueilli ».

Le règlement eIDAS exige par ailleurs que « *l'envoi et la réception de données sont sécurisés par une signature électronique avancée ou par un cachet électronique avancé d'un prestataire de services de confiance qualifié, de manière à exclure toute possibilité de modification indétectable des données »*

La lettre recommandée électronique (LRE) est donc un parfait exemple d'application de la signature électronique dont le cadre juridique vient très récemment d'être clarifié.

<u>Cas d'usage d'une résiliation d'un contrat d'assurance</u>

Dans le cadre de la mise en place de l'article L 113-15-2 du code des Assurances découlant de la loi sur la consommation dite « loi Hamon » et visant les résiliations de contrats d'assurance des particuliers, le nouvel assureur a l'obligation d'informer le précédent assureur en lui indiquant certains éléments relatifs à l'assuré et à son ancien contrat.

Ces informations sont actuellement envoyées par lettres recommandées papier ce qui engendre à la fois un coût financier qui peut s'avérer important, mais aussi des longueurs dans le traitement de ces « mobilités » de clients qui iraient à l'encontre d'un des objectifs de la loi Hamon qui est de fluidifier/faciliter la concurrence.

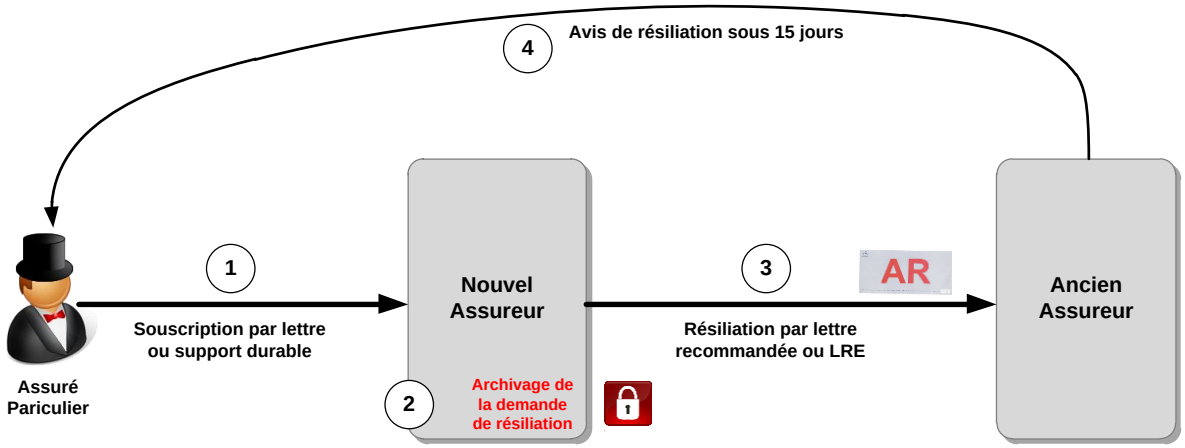


Figure 10 : Processus de résiliation d'un contrat

Dans cette relation entre assureurs vient s'immiscer le *Transmetteur* qui, à l'instar de La Poste dans le cas du courrier papier, va acheminer la lettre recommandée électronique du nouvel assureur vers l'ancien assuré. La signature va être utilisée par l'un pour signer la demande de résiliation et par l'autre pour signer l'accusé de réception.

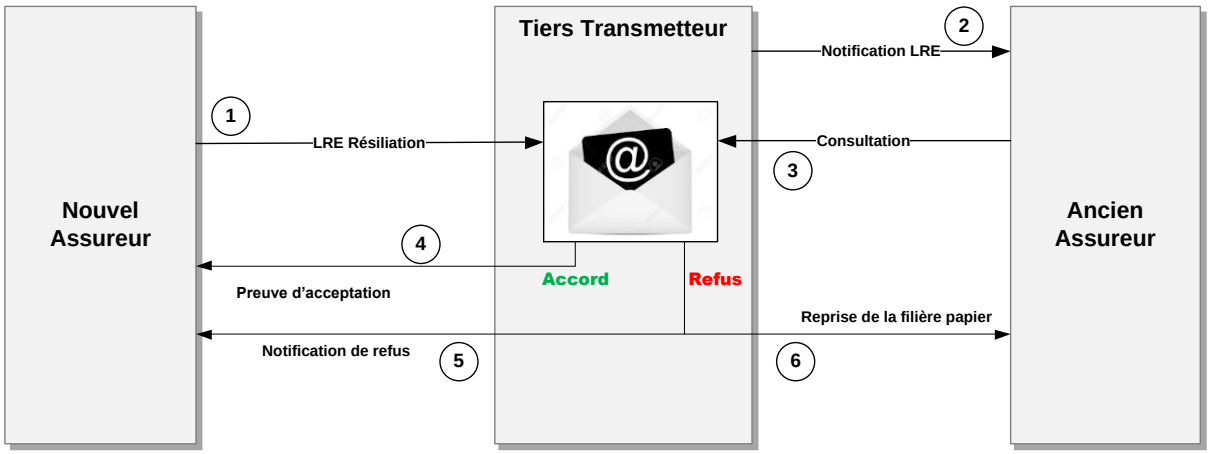


Figure 11 : Schéma de principe d'une résiliation par LRE

Tous les flux échangés entre les parties sont signés (cachet serveur) par les émetteurs pour éviter toute contestation. Le tiers transmetteur peut être également l'opérateur de confiance ayant délivré les certificats de signature aux protagonistes.

V.5. Signature de courrier électronique

La signature des messages électroniques repose sur l'utilisation du standard S/MIME[20] qui permet également de chiffrer le contenu des messages, car si les signatures électroniques veillent à l'intégrité des données, elles n'en assurent pas la confidentialité. Les messages qui ne sont que signés électroniquement, sans ajouter de chiffrement, sont envoyés en clair et peuvent donc être lus par des tiers

[20] Extension sécurisée de MIME, voir RFC2633 et ses évolutions.

Pour assurer la confidentialité de messages il faut utiliser les fonctions de chiffrement du standard S/MIME. Dans ce cas, une clé secrète symétrique, dite clé de session, est générée pour chaque message. Cette clé est utilisée pour chiffrer le contenu du message avec un algorithme symétrique. Enfin, une copie de cette clé est chiffrée pour chaque destinataire (avec sa clé publique de chiffrement) et copiée en entête du message. Ainsi, seuls les destinataires peuvent déchiffrer leur copie de la clé de session et l'utiliser pour lire le message.

Remarque

Les messages peuvent être envoyés en mode « texte clair » ou en mode « opaque ». Dans ce cas de figure ils sont préalablement encodés en base 64, mais ils restent interprétables pour un tiers, il est donc nécessaire de chiffrer le message si la confidentialité est un facteur important.

La Figure permet d'illustrer les étapes de signature d'un message qui ne diffère pas d'un processus de signature classique d'un document.

Figure 12 : Schéma de principe d'une signature d'un message électronique

1. Le message est capturé (en clair ou encodé en Base64).
2. La clé privée de l'expéditeur est récupérée.
3. L'opération de signature est effectuée sur le message à l'aide de la clé privée. Une signature électronique est produite.
4. La signature électronique (au format PKCS#7) est ajoutée au message.
5. Le message est envoyé.

Lorsque le destinataire ouvre un message électronique signé, la signature électronique doit être vérifiée. La figure suivante illustre les étapes de cette vérification

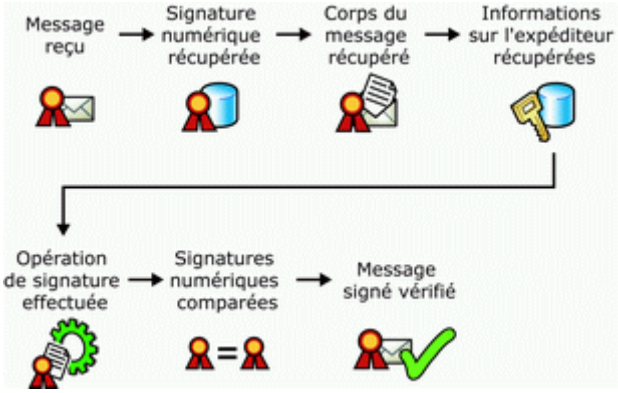


Figure 13 : Schéma de principe de réception des messages électroniques.

1. Le message est reçu.
2. La signature électronique est extraite du message.
3. Le message est récupéré.
4. La clé publique de l'expéditeur est récupérée.
5. Une opération de signature est effectuée sur le message.

6. La signature numérique incluse avec le message est comparée à la signature numérique produite lors de la réception.
7. Si les signatures correspondent, le message est valide.

VI. La conduite du projet

VI.1. Rôles et Acteurs

Un projet de mise en œuvre de signature électronique nécessite, en plus des traditionnels acteurs d'un projet d'entreprise, de faire appel à des acteurs supplémentaires :

Chacun de ces acteurs est porteur de missions, rôles et responsabilités spécifiques :

Organisme mettant en place la signature électronique	
Responsabilités	**Rôles fonctionnels associés**
Missions : En charge de la définition des Politiques de Signature, et notamment : - Définition des **niveaux de garantie et de conformité réglementaires** attendus vis-à-vis des signatures électroniques ; - Définition des **conditions d'acceptation des certificats signataires**, et/ou de la délivrance des certificats signataires aux populations d'utilisateurs cibles ; - Modalités de **conservation des signatures électroniques** produites, avec maintien de	Définition des besoins liés à la signature électronique, et de la limitation des responsabilités associées portées par l'organisme : • MOA, • Représentant des Métiers • Direction générale • Direction juridique • RSSI • MOE / DSI

Organisme mettant en place la signature électronique	
Responsabilités	**Rôles fonctionnels associés**
la force probante dans le temps, et/ou appel à des tiers de confiance spécialisés ; En charge de l'intégration fonctionnelle et technique dans les workflows Métier **<u>Responsabilités :</u>** Porteur des responsabilités associées : - A la conformité de la signature vis-à-vis des règlements et standards, en vue de sa **force probante**. Sélection des partenaires (éditeurs, tiers de confiance) selon ce critère ; - A la protection des données personnelles, notamment des signataires.	<u>Pour la délivrance des certificats signataires :</u> Gestionnaire référentiel des identités Ressources humaines (si les signataires font partie du personnel de l'organisme)

Utilisateur signataire	
Responsabilité	**Rôles fonctionnels associés**
<u>Missions :</u> Conservation de façon sûre de ses clés privées de signature, que celles-ci lui aient été remises sur support matériel ou logiciel, sauf dans le cas d'une signature à la volée. Utilisation de la fonction de signature selon les conditions d'emploi qui lui ont été communiquées. **<u>Responsabilités :</u>** Porteur d'engagement vis-à-vis des signatures qu'il produit, et de l'utilisation de ses moyens de signature. Porteur d'engagements liés aux signatures produites (valeur d'engagement définie selon les Politiques de signature, acceptées, tacitement ou non, par le signataire).	L'utilisateur signataire peut être, par exemple : - Une personne physique individuelle (un « Particulier »), - Une personne physique en tant que personnel d'une entité, - Le représentant légal, ou le délégué, d'une entité morale, - Une personne morale (cachet serveur) L'utilisateur peut ou non faire partie de l'organisme mettant en place la fonction de signature

Tiers de confiance	
Responsabilité	**Rôles fonctionnels associés**
<u>Périmètre d'intervention</u> : L'organisme souhaitant mettre en œuvre un processus de signature électronique peut faire	<u>Définition des services, engagements et responsabilités portées par l'entité (et leurs limitations) :</u> Direction générale et Direction juridique

Tiers de confiance	
Responsabilité	**Rôles fonctionnels associés**
appel à un ou plusieurs tiers de confiance, en mesure de fournir : - Des certificats de signatures destinés aux signataires ; - Des jetons d'horodatage devant « enrichir » la signature ; - Des certificats de signatures destinés aux Unités d'Horodatage ; - L'archivage longue durée de la validité des signatures, avec maintien de leur valeur probante dans le temps si besoin. **Missions :** Suivant les services fournis, élaboration et communication aux clients des : - Politiques de certification ; - Politiques d'Horodatage ; - Politiques d'Archivage long terme, etc. Initialisation des clés de signature des Autorités de confiance (Autorités de Certification, Autorités d'Horodatage), lors d'une « Cérémonie des Clés ». Opérations des plates-formes associées aux services de tiers de confiance, et notamment disponibilité des fonctions suivantes, nécessaires à l'établissement et/ou à la vérification des signatures : - D'horodatage ; - De mise à disposition des CRL ; - D'archivage des éléments de traçabilité associés à l'ensemble du cycle de vie ; - De maintien des éventuelles qualifications de conformité. **Responsabilités :** Porteur d'engagement de responsabilité légale vis-à-vis des services qu'il fournit, visant à la fois : - La conformité aux standards et règlements prévus ; - La disponibilité des services critiques listés ci-dessus, et notamment sur une longue durée (plusieurs années, suivant date d'expiration des différents certificats impliqués dans le processus).	Porteurs de l'offre/Métiers MOE / DSI /RSSI Gestion des secrets d'initialisation des services de confiance : - Via la Cérémonie des clés et la détention des secrets associés. Maitre de cérémonie Huissier / Témoin Détenteurs des secrets (ou « Porteur de secrets ») Opérations des plates-formes hébergeant les services de confiance : Responsable des plates-formes Opérateurs et Administrateurs système, réseau, applicatif Auditeur et contrôleur des plates-formes. Délivrance de certificats : Administrateur habilitations Gestionnaire identités Opérateur d'enregistrement Opérateur HelpDesk / révocation

Editeur de la solution électronique	
Responsabilité	**Rôles fonctionnels associés**
Missions : Élabore et met à disposition la solution de signature Assure le support à l'intégration et le MCO/MCS (Maintien en Conditions Opérationnelles / de Sécurité). Peut inclure notamment le suivi de la conformité de la solution vis-à-vis de la réglementation. **Responsabilités :** Porteur de responsabilité liée à la conformité des signatures produites par rapport aux spécifications et aux conformités (réglementaires, standards) revendiquées[21]. Notamment en termes d'interopérabilité avec d'autres offres du marché, comme des solutions de vérification de signature d'horodatage, etc. *À noter : Non-porteur de responsabilités quant à l'utilisation de sa solution (tant que conforme aux spécifications d'usage) ou des signatures produites, étant donné qu'il n'intervient pas dans le processus de génération et d'émission de la signature proprement dit.*	MOE / DSI Expert fonctionnel en signature électronique et services de confiance Architecte technique/applicatif Développeurs Chef de projet d'intégration

VI.2. Le choix d'une IGC.

Au lancement d'un projet de signature électronique se posera la question du choix de l'autorité de certification et de la pertinence pour l'entreprise d'utiliser sa propre IGC ou de recourir à un tiers de confiance. Le choix dépend du contexte et des objectifs du projet mais le tableau ci-dessous permet d'orienter rapidement la réflexion en fonction de critères basiques.

	Interne	Externe	Commentaire
Reconnaissance auprès de tiers		+	Du fait du fonctionnement d'une IGC, le choix d'utiliser une IGC externe d'un tiers reconnu sur le marché et dans les divers types de logiciels utilisant des certificats (tels que les navigateurs, lecteurs de documents, etc.), permet de faire reconnaitre rapidement les opérations effectuées à l'aide des certificats.

[21] Certification aux Critères Communs par exemple, ou ANSSI. Processus de qualification des outils (RGS)

	Interne	Externe	Commentaire
Facilité de déploiement		+	Le recours à un tiers externe reconnu permet d'obtenir rapidement une infrastructure d'IGC prête à délivrer des certificats répondant aux standards du marché.
Certification		+	La certification d'une IGC ou la qualification d'offre de certificat sont des projets très coûteux et très longs, il est donc souvent recommandé de faire appel à un prestataire déjà certifié *(cf. § Normes et standards).*
Volumétrie de certificats à délivrer	+	+	Il convient de se poser la question de la volumétrie de certificats nécessaires à la réalisation du projet. Cela aura naturellement un impact sur le choix de l'architecture de l'IGC.
Coût	+	+	Le coût de déploiement et de maintenance d'une IGC n'est pas anodin. Les besoins en termes de volumétrie, d'usages, de niveau de sécurité permettent d'orienter le choix d'IGC interne ou externe.
Délai de mise à disposition		+	Dans le cas d'un prestataire, le service est tout de suite disponible avec cependant des adaptations à prévoir notamment concernant la politique de certification. C'est l'incontournable phase de paramétrage de l'IGC qui est plus ou moins longue.
Facilité de tester ou de démonstration	+		La maîtrise complète de l'IGC permettra, dans la majorité des cas, d'être plus réactif et d'être plus libre sur les interfaces de l'IGC. D'une autre manière, le recours à des tiers reconnus permettra de tester plus rapidement et dans un contexte cible (reconnaissance des certificats, standard des certificats, standard des interfaces IGC, etc.)
Extension à d'autres usages	+		La maîtrise des IGC et de la configuration des gabarits ou modèles de certificats permet, plus souplement, de créer, ajouter ou supprimer des usages sur certaines offres de certificats. Attention cependant aux modifications de configuration qui remettent en cause la qualification ou la certification d'une offre.
Disponibilité des compétences		+	Un projet d'IGC peut être très complexe et dans tous les cas nécessiter des compétences notamment en termes de droits, de cryptographie, de gestion d'une autorité de certification, etc. La durée de vie d'une autorité de certification excède généralement les 10 ans et pour certaines

	Interne	Externe	Commentaire
			atteint les 30 ans. Il convient donc de s'entourer de compétences reconnues dès le début du projet pour construire une architecture viable et pérenne.
Maintenabilité		+	Le service étant le cœur de métier du prestataire, il devrait avoir tout mis en œuvre pour que celui-ci soit pérenne. Néanmoins une clause de réversibilité dans le contrat de prestation constituerait également une bonne assurance.
Pérennité	+	+	Au vu des durées de vie habituellement pratiquées dans des projets de signature, la pérennité de l'IGC est un facteur important à prendre en compte dès le début. Si un tiers de confiance a été choisi, il est important de prendre des dispositions prévoyant la cessation d'activité du tiers, si une IGC interne est déployée, il faut s'assurer de pouvoir la maintenir et la faire évoluer pour qu'elle suive les besoins métiers tout au long de la vie du service de signature.
Contraintes Réglementaires		+	*RGS (1.0 & 2.0), eIDAS, ETSI*
Possibilité de délégation		+	C'est une des raisons pour laquelle il est fait appel à un prestataire.
Accessibilité de l'IGC	+	+	La disponibilité d'une IGC externe est à priori plus grande lorsqu'elle est opérée par un prestataire, mais ce n'est qu'une affaire de moyens.
Disponibilité de l'IGC		Contrat de service possible.	Focus sur les fonctions critiques de la PKI (révocation) et sur les niveaux de services qui doivent être en adéquation avec les contraintes réglementaires et les besoins du métier.
Vérification de la signature		+	Le recours à un tiers de confiance faisant déjà partie des autorités de confiance déployées dans les solutions de vérification de signature permet de simplifier ce processus. Pour un usage interne il est tout aussi aisé de procéder à la vérification de signature avec une IGC interne.
Disponibilité de la technologie	+	+	La certification ou la qualification d'une offre d'IGC impose l'utilisation de certaines solutions logicielles ou matérielles. Il convient de s'assurer que les technologies nécessaires à l'élaboration de son projet sont disponibles et autorisées par les lois des pays dans lequel le service sera utilisé.

VI.3. Évaluation des risques

L'utilisation de signature électronique dans le cadre d'un projet implique la mise à disposition d'acteurs très divers et non spécialistes d'un outil technique généralement utilisé au fin fond de processus automatisés. Il en découle des scénarios de risques qui vont apparaître avec des impacts côté métier alors qu'ils sont généralement perçus du côté des équipes IT.

VI.3.1. Risques projets

Le projet en lui-même peut être impacté par :

- La difficulté de trouver du personnel capable de mener correctement ce type de projet. Les spécialistes capables de mener des projets techniques ayant trait à la signature électronique sont rares. Ceux possédant les capacités additionnelles nécessaires pour collaborer avec l'ensemble des parties prenantes non techniques, peuvent être encore plus difficiles à trouver au bon moment, et à conserver.
- La sous-estimation du besoin en compétences juridiques spécifiques pour assurer que la conjugaison des mesures procédurales et techniques mise en place apporte finalement le niveau de garantie juridique attendu.
- La dépendance du projet de signature vis-à-vis de la mise en place d'une IGC. Si le projet requiert la mise en place d'une IGC, ce jalon sera alors critique pour le projet.
- Une sous-estimation du nombre de certificats nécessaires. Cela peut avoir pour conséquence, un sous-dimensionnement de l'architecture et des dysfonctionnements pouvant bloquer la mise à disposition des certificats aux utilisateurs.
- Une sous-estimation des délais de mise à disposition des certificats. Ces délais peuvent être ceux des AC de l'IGC. La difficulté à bien maîtriser les processus de distribution selon le niveau de confiance attendu, peut aussi être sous-estimée.
- Une sous-estimation des efforts à s'assurer de la mise à jour réglementaire. Il est en effet nécessaire d'inclure la signature électronique dans le corpus réglementaire de la société, mais aussi s'assurer que ce corpus reste conforme aux contraintes réglementaires de la société. La mise à jour du corpus réglementaire n'est pas le seul effort documentaire qui peut être sous-estimé. Tous les processus liés à la gestion des certificats doivent être documentés pour assurer qu'ils répondent bien aux objectifs et être auditables.
- Une sous-estimation des efforts nécessaires pour mettre à disposition les ressources nécessaires pour les audits et les coûts associés.
- Un sous-dimensionnement du processus de conduite du changement. Même s'il est possible de matérialiser la signature électronique, celle-ci reste toujours difficile à appréhender et les concepts associés demeurent trop compliqués pour ne pas être teintés de soupçons.
- Un déficit de communication sur les impacts de la numérisation de la signature et qui cible un nombre important d'acteurs très divers impliqués dans ce type de projet.
- Difficulté d'intégration des différents composants. De nombreuses mises en œuvre d'IGC échouent par incompatibilité entre les usages et les capacités d'interconnexion des composants. C'est en particulier vrai pour les capacités de « provisionning automatique »,

indispensables pour certains types de déploiement (authentification de machines notablement) qui fonctionnent mal dans le cadre d'une architecture hétérogène.

VI.3.2. Risques de sécurité

Des risques de sécurité spécifiques sont à prendre en compte pour la solution :

- La possibilité de perte de l'assurance de non-répudiation des signatures qui peut être due à des problèmes procéduraux ou sur l'IGC.
- Une compromission des clés privées de signature due, par exemple, au processus de distribution ou à la gestion de l'IGC.
- Une compromission de tout ou partie de l'IGC, de ses AC ou des listes de révocation.
- La perte d'une certification assurant le niveau de confiance réglementairement requis, par exemple, à la suite de la découverte de non-conformité pendant un audit.
- La perte d'une partie ou de l'intégralité de l'archivage obligatoire et en particulier des preuves.
- La découverte d'une faiblesse sur la cryptologie utilisée.

VI.3.3. Risques juridiques

Comme pour tout processus incluant la signature d'un document, mais augmenté de la spécificité électronique, des risques juridiques sont à prendre en compte :

- La possibilité de contestation de la validité de la signature immédiate ou au bout d'un certain temps, par exemple après l'expiration d'un certificat.
- Les impacts juridiques en cas de perte d'une certification requise.
- Les impacts résultant de l'impossibilité d'utiliser un des outils liés au processus de signature ou de vérification de la signature à la suite de son obsolescence.

VI.4. Conduite de changement

La conduite de changement ne doit pas être négligée dans un processus de dématérialisation en général, et qui plus est dans un projet de signature électronique. Les rôles et responsabilités des acteurs impliqués dans le projet vont pour certains se prolonger au-delà de la fin de celui-ci.

Donc en plus de leur inculquer toutes les notions relatives à la signature électronique, ce qui est l'un des objectifs de ce document, il faudra également les préparer aux impacts que pourrait occasionner l'introduction de la signature électronique dans leur quotidien.

VI.4.1. Les équipes informatiques.

L'impact sur les équipes informatiques sera très varié selon que l'IGC adoptée soit externe ou interne. Cependant quel que soit le choix, les équipes devront sans doute faire évoluer leurs processus.

L'impact sur les équipes variera également avec la nature du projet. L'administration d'un processus de délivrance de certificat numérique pour des collaborateurs (signature de mail) est bien différente de celui de la fourniture de certificats à des clients finaux (signature de contrats).

Autre point crucial pour les équipes ; la cryptographie. Si les outils cryptographiques n'ont jamais été utilisés auparavant dans l'entreprise, la « simple » gestion des clés peut rapidement tourner au cauchemar pour ceux et celles qui n'y auraient pas été préparées.

À titre d'exemple, et pour se conformer à la norme ISO-27002 :2013, la gestion des clés va notamment consister à :

a) *Générer des clés pour différents systèmes cryptographiques et différentes applications ;*
b) *Émettre et obtenir des certificats de clé publique ;*
c) *Distribuer des clés aux entités prévues, y compris comment les clés devraient être activées lorsqu'elles sont reçues ;*
d) *Stocker des clés, y compris en précisant comment les utilisateurs autorisés obtiennent l'accès aux clés ;*
e) *Modifier ou mettre à jour les clés, y compris les règles sur le moment où les clés doivent être changées et comment cela sera fait ;*
f) *Traiter des clés compromises ;*
g) *Révoquer des clés, y compris comment les clés doivent être retirées ou désactivées, par ex. lorsque les clés ont été compromises ou lorsqu'un utilisateur quitte une organisation (dans ce cas, les clés doivent également être archivées) ;*
h) *Récupérer des clés perdues ou corrompues ;*
i) *Sauvegarder ou archiver des clés ;*
j) *Détruire des clés ;*
k) *Logger et auditer les principales activités liées à la gestion*

Dans le cas d'une IGC externalisée, tout ou partie de ces opérations sera assuré par le prestataire. Si ce n'est pas le cas alors les équipes informatiques devront être préparées à les réaliser.

VI.4.2. Les directions métiers

Les processus de gestion métiers peuvent être profondément modifiés. Il y aura notamment lieu de :

- Former les différents utilisateurs à l'utilisation des outils de signature,
- Les sensibiliser à l'importance de certaines étapes comme le recueil du consentement,
- Identifier le signataire selon les procédures définies dans la politique de signature,
- Les aider à définir des indicateurs de productivité,
- etc.

La réussite d'un projet de signature électronique dépend pour beaucoup de l'implication des futurs utilisateurs. Ils doivent donc faire l'objet d'une attention particulière notamment s'ils doivent être responsables de la vérification de l'identité des futurs signataires.

VI.4.3. Les directions support

Les directions supports parmi lesquelles on peut compter le Juridique, la Conformité, les Achats, la Sécurité des Systèmes d'Information ou encore les Ressources Humaines ont de façon plus ou moins importante contribué au projet (cf. § Rôles et Acteurs), mais comme pour les métiers, leurs processus

de gestion peuvent devoir être revisités, d'où la nécessité de préparer/sensibiliser les acteurs de ces (nouveaux) processus.

VI.5. Définition des indicateurs de succès

Dès les prémisses du projet, durant toute sa durée et après son démarrage, il sera important d'apporter la preuve que les investissements consentis ont été profitables. Il faudra également prouver que l'intégration de la signature électronique dans un ou plusieurs processus a été couronnée de succès et que les objectifs visés ont été atteints

VI.5.1. Réalisation des objectifs de plus-values opérationnelles

Ces indicateurs sont plutôt d'ordre qualitatif bien qu'il soit toujours possible de les valoriser. Il s'agira notamment de mesurer la satisfaction des signataires des documents, ainsi que des utilisateurs (destinataires) de ces mêmes documents. Une enquête de satisfaction ad hoc pourrait confirmer les premiers ressentis utilisateurs.

La mesure de la performance, qui peut par exemple se traduire par la durée totale d'une procédure de souscription (Cf. § Signature d'un contrat d'assurance), est aussi un indicateur très pertinent de succès, de même que le serait une diminution du nombre de contestations ou de contentieux.

L'utilisation de la signature oblige souvent à une formalisation et à une documentation des processus. Ce travail bien qu'indispensable est très souvent négligé. Les exigences de conformité vis-à-vis des politiques de signature obligent à une plus grande discipline quant à la tenue à jour de cette documentation.

On peut également ajouter parmi les autres facteurs de succès :

- L'obtention du niveau de certification prévu ou requis pour le processus de signature ;
- La certification et le bon fonctionnement de l'IGC.

VI.5.2. Réalisation des objectifs de maitrise et d'identification des coûts

Des indicateurs sur la réalisation des objectifs de coûts et de gains dans le temps doivent être définis le plus tôt possible dans le projet. Ces objectifs doivent clairement indiquer ce qui doit être pris en compte pour leur calcul, car la plus-value apportée en termes financiers et de coûts est souvent difficile à quantifier.

L'évolution des processus consécutive à la mise en œuvre de la signature électronique peut être importante, et entrainer des effets d'aubaine dont les coûts et gains peuvent dépasser ou diminuer ceux envisagés au départ. Le retour sur investissement (ROI) devra autant que possible être calculé en les éliminant, mais devra prendre en compte l'ensemble des efforts de mise à jour des processus métiers et les coûts liés au déploiement et à l'utilisation de la solution.

Les coûts non techniques pour assurer le maintien en fonctionnement de la solution ne doivent pas être oubliés. Les processus de revues et mises à jour des politiques devant impliquer des dirigeants peuvent aussi se révéler coûteux. De même la nécessité d'effectuer des audits réguliers implique non seulement le coût des auditeurs mais aussi ceux liés à la logistique et à la mobilisation des acteurs audités.

Les gains obtenus par l'optimisation des processus et l'intégration simplifiée dans les SI tant du côté des destinataires que des signataires devront être intégrés. Dans les gains classiques, il y a évidemment la possibilité d'avoir des processus totalement dématérialisés avec les réductions de coûts et les possibilités d'intégration aux SI qui sont liées.

En cas de remplacement non obligatoire d'une solution de signature manuscrite ou autre type de validation, les coûts de maintien de la solution existante devront aussi être intégrés. Dans ce cas le taux de remplacement de la solution existante par la solution intégrant la signature électronique doit être examiné avec attention tout particulièrement pour déterminer les effets et efforts de la conduite du changement et éventuellement déterminer la solution à maintenir.

Les coûts de contentieux sont aussi à prendre en compte et une charge à suivre. Comme évoqué, il y a un risque non négligeable de tentatives de contester la validité des signatures électroniques parce que non matérielles.

VI.6. Définition des indicateurs de suivi opérationnel

Les indicateurs à mettre en place dans les différents tableaux de bords doivent être définis dès les premières étapes du projet.

La mise en place d'une IGC va impliquer que le suivi des indicateurs va commencer avant le déploiement du projet de signature.

Tout particulièrement le suivi des incidents et des indicateurs liés à l'acceptation de l'utilisation de l'IGC est à suivre très tôt afin d'aider à la prévision des efforts sur la conduite du changement.

Les indicateurs à suivre, dans les premiers temps sont :

- Nombre de certificats produits ;
- Nombre de signatures ;
- Ratio entre nombre de signatures et nombre de signatures manuelles (si solution préexistante) ;
- Population utilisant la signature ;
- Nombre de contestations et/ou de réclamations.

Comme pour tout projet, le périmètre de diffusion des tableaux de bord doit être affiné avec le déploiement. Ceci est particulièrement vrai pour un projet de ce type où la perception d'une perturbation (positive ou négative) n'est pas aussi facilement appréhendée que pour un projet plus classique.

Il serait normal qu'une partie des indicateurs du projet soit intégrée dans le suivi qualité étant donné les évolutions et la mise en place de processus nouveaux.

VII. L'exploitation

La mise en œuvre de la signature électronique dans une entreprise a évidemment un impact sur le projet, mais une fois celui-ci terminé, il devient essentiel d'assurer le fonctionnement et le maintien en condition opérationnel et sécurité (MCO et MCS) du dispositif. Si la conduite de changement a convenablement été réalisée (Cf. §Conduite de changement), alors les différents acteurs seront préparés à toutes les nouvelles tâches qui leur incomberont.

VII.1. Suivi Opérationnel

VII.1.1. Maintien de la conformité du dispositif

Selon son niveau (Cf. § Les certifications des services d'une IGC), la valeur juridique et contractuelle que l'on veut donner à la signature, le processus de maintien de la conformité du dispositif vis-à-vis des politiques de certification, horodatage, enregistrement, signature, archivage, etc. peut s'avérer plus ou moins lourd.

De plus selon les organisations, la question de savoir à quelle entité revient la responsabilité du suivi de ces politiques peut s'avérer épineuse. Par leurs aspects techniques, elles pourraient légitimement relever de la DSI ou du RSSI, mais la signature électronique peut concerner des processus métiers, avec des enjeux financiers, juridiques et/ou réglementaires qui justifieraient une implication plus grande d'autres directions supports comme les Achats, le Juridique ou la Conformité.

S'assurer d'être toujours conforme, va nécessiter la réalisation d'audits et ensuite de suivre les éventuels plans de remédiation. Là encore selon la nature des écarts constatés, les acteurs sollicités peuvent aussi bien appartenir à la DSI qu'à une direction métier, notamment s'il s'agit par exemple d'ajuster la procédure d'enregistrement d'un client.

VII.1.2. Veille technologique sur les algorithmes cryptographiques

L'efficacité des algorithmes cryptographiques est dépendante des évolutions technologiques (cf. § Recommandations sur la taille des clés), il est donc primordial d'exercer une veille afin de s'assurer que leur efficience ne soit pas remise en cause, soit par une avancée technologique majeure (exemple : processeur quantique) ou par la découverte d'une vulnérabilité dans l'implémentation utilisée dans les outils de signature.

Ces évolutions doivent tout particulièrement être suivies pour l'archivage légal et confirment le rôle que doit tenir le tiers-archiveur.

A noter qu'en faisant appel à prestataire utilisant des dispositifs qualifiés, cette veille incombera à ce dernier.

VII.1.3. Gestion du cycle de vie des certificats

La gestion des certificats est inhérente à la mise en place ou à l'utilisation d'une IGC, quand bien même celle-ci est opérée par un prestataire.

VII.1.4. Amélioration du dispositif

Comme pour toute nouvelle application ou nouveau processus, une période d'observation devra être mise en place afin de vérifier si les hypothèses prises lors de la phase projet se révèlent exactes. Des ajustements pourraient s'avérer indispensables pour fluidifier des processus métiers ou techniques rendus très complexes par la mise en œuvre de la signature électronique.

VII.1.5. Suivi des indicateurs

Il n'y a rien de particulier dans le suivi des indicateurs. Les tableaux de bords spécifiques à l'ajout de signature dans des processus existants ont vocation à disparaître pour que ne subsistent plus que des indicateurs spécifiques (ex : taux d'acceptation, nombre d'actes signés ou de documents signés électroniquement, etc.) qui s'ajoutent aux suivis qualité ou financier.

VII.2. Suivi contractuel

Nous l'avons vu, la mise en place de la signature électronique peut nécessiter de faire appel à de nouveaux partenaires avec lesquels des engagements contractuels seront pris. Pour les prestations déjà existantes des avenants aux contrats en cours seront probablement à prévoir.

Mais là encore, rien de particulier par rapport à un projet « normal », il conviendra toutefois d'être vigilant sur le :

- Traitement des contentieux,
- Suivi de l'archivage,
- Suivi des contrats de service (notamment la performance dans la délivrance des certificats, ou la signature de documents, ...),
- Cascade des responsabilités dans les contrats,
- Suivi des contrats avec les fournisseurs du service de confiance,
- Veille juridique,
- Etc.

VIII. Conclusion

Dans ce document les membres du groupe de travail ont essayé de regrouper les différents éléments sur la signature électronique nécessaires aux chefs de projet en y mettant le fruit de leurs expériences et de leurs compétences diverses.

Ces éléments spécifiques vont du juridique en passant par l'organisationnel et l'utilisation de techniques de cryptologie. Parce que ne faisant partie de nos objectifs initiaux, nous n'avons pas délivré de conseils quant à l'organisation du projet en lui-même.

Tous les membres du groupe espèrent que vous avez trouvé dans ce document de quoi vous aider à comprendre la complexité spécifique d'un projet de signature électronique ou mieux, de vous aider à mener jusqu'au bout votre projet.

La signature électronique semble avoir trouvé sa vitesse de croisière et de croissance, il est à parier que de très nombreux projets verront le jour dans les années à venir. La vague de digitalisation ou de dématérialisation qui touche à tous les secteurs de l'économie ne va qu'accentuer cette tendance. De plus, si le document n'a évoqué que des solutions « traditionnelles » à base d'IGC, les toutes nouvelles technologies de reconnaissance automatique des individus (visage, voix, démarche, comportement, etc.), ou de BlockChain devraient accélérer l'adoption de la signature électronique, parce qu'elles permettent d'alléger les processus d'enregistrements.

IX. Références

[1] Sécurité de la dématérialisation ; *De la signature électronique au coffre-fort numérique, une démarche de mise en œuvre*
Auteur : Dimitri Mouton,
Edition : Eyrolles – 12 juillet 2012

[2] Sécuriser ses échanges électroniques avec une PKI ; *Solutions techniques et aspects juridiques*
Auteurs : Thierry Autret, Laurent Bellefin, Marie-Laure Oble-Laffaire,
Editions : Eyrolles – 23 janvier 2002

[3] La signature électronique ; *Transaction et confiance sur Internet*
Auteur : Arnaud-F. Fausse,
Editions : Dunod – 9 janvier 2001

[4] Théorie des codes ; *Compression, cryptage, correction*
Auteurs : Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier, Sébastien Varrette, Editions : Dunod – Septembre 2013

[5] Référentiel Général de Sécurité (RGS) version 2.0 : *Annexe B1 : Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques version 2.03 du 21 février 2014*

[6] Règlement européen eIDAS.
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32014R0910

X. Glossaire

Terme	Commentaire
Algorithme	Un algorithme est une suite finie et non ambiguë d'opérations ou d'instructions permettant de résoudre un problème ou d'obtenir un résultat donné. Dans le cas de la cryptographie, les algorithmes sont liés aux types de clés utilisées. Dans le cas de la signature électronique, ce sont des algorithmes de hachage qui sont utilisés associés à des algorithmes de cryptologie asymétrique.
Archivage électronique	Un système d'archivage électronique permet la gestion de documents sur tout son cycle de vie et particulièrement sur le long terme.
CA / AC	*Certification Authority / Autorité de Certification* est le composant d'une PKI / IGC qui signe les certificats ainsi que les listes de révocation.
Cachet serveur	Forme de certificat électronique permettant la signature par une personne morale en opposition à la « signature électronique » qui ne peut être utilisée que par une personne physique selon le RGS
Cérémonie des clés / *Key Ceremony*	La cérémonie des clés correspond à la génération de la bi-clé de l'autorité de certification (AC) et sa mise en service pour permettre la production des certificats.
Certificat	Un certificat électronique est un ensemble de données contenant au moins une clé publique et une signature. Pour être utilisable dans le cas de la signature électronique il doit aussi comporter des éléments d'identification liés à la personne ou l'entité signataire. Le standard le plus utilisé pour la structure des certificats est celui défini par l'IUT : X.509v3.
Chiffrement	Transformation à l'aide d'une clé d'un message en clair (dit texte clair) en un message incompréhensible (dit texte chiffré) pour celui qui ne dispose pas de la clé de déchiffrement *(Cf. Wikipédia).*
Clé	Paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, scellement, signature numérique, vérification de signature), une clé peut se présenter sous plusieurs formes : mots ou phrases, procédure pour préparer une machine de chiffrement (connexions, câblage, etc.), données codées sous une forme binaire (la clé est alors caractérisée par son nombre de bits).

Terme	Commentaire
Clés privées / clés publiques	La cryptographie asymétrique, aussi appelée cryptographie à clé publique, utilise des couples de clé publique (sans enjeu de confidentialité) et privée (qui doit être gardée secrète pour atteindre l'objectif d'usage). Ce principe résout le problème du partage et des risques de compromissions liés de la clé « secrète » utilisée en cryptographie symétrique. En signature électronique, la clé privée sera utilisée pour signer et la clé publique servira à vérifier la signature. Il peut arriver que le terme « clé privée » soit utilisé pour désigner la « clé secrète » utilisée en cryptographie symétrique.
Clés symétriques	La cryptographie symétrique utilise la même clé pour les processus de codage et de décodage. Cette clé « symétrique » est souvent appelée « secrète » car toute la sécurité de l'ensemble est directement liée au fait que cette clé n'est connue que par l'expéditeur et le destinataire.
Courbe elliptique	Les courbes elliptiques sont des courbes algébriques. Une de leurs propriétés est qu'il est possible de définir une addition et une multiplication sur leurs points. La définition complète de ces courbes ne serait-ce que pour leur utilisation en cryptologie dépasse largement le cadre de ce document. En cryptographie, les courbes elliptiques sont des objets mathématiques qui peuvent être utilisées pour des opérations asymétriques. On parle de cryptographie sur les courbes elliptiques ou ECC (du sigle anglais Elliptic Curve Cryptography). La résistance d'un système fondé sur les courbes elliptiques repose sur le problème du logarithme discret dans le groupe correspondant à la courbe elliptique, dont (d'après le RGS V2.0 annexe B1) : **Logarithme discret dans GF(*p*)** Le problème dit « du logarithme discret dans GF(*p*) » est fondé sur des calculs effectués dans le corps fini à p éléments, où p est un nombre premier également appelé « module ». **Logarithme discret dans les courbes elliptiques définies sur GF(*p*) ou binaire GF(2n) :** Il est possible de définir un problème de logarithme discret dans des structures plus complexes pour lesquelles aucun algorithme plus efficace que les méthodes génériques de calcul de logarithme discret n'est connu. C'est en particulier aujourd'hui le cas des courbes elliptiques qui sont définies sur un corps de base pouvant être, en pratique, premier (GF(p)) ou binaire (GF(2n)).
Diffie-Hellmann	L'échange de clés Diffie-Hellman est un protocole d'échange de clés anonyme qui permet à deux pairs, chacun ayant un couple de clé privée/publique d'établir un secret partagé à travers un canal de communication non sécurisé. Ce secret partagé peut être employé directement comme une clé de chiffrement ou être utilisé pour dériver une autre clé qui, à son tour, peut être utilisée pour chiffrer les communications.
Enrôlement	L'enrôlement est le processus qui permet d'inclure un certificat dans une PKI / IGC. Ce service est critique dans la gestion de la PKI /IGC puisque les vérifications qui y sont faites sont à la base de la confiance que l'on peut apporter à la PKI.

Terme	Commentaire
Hash / Condensat / fonction de hachage / hash function	Le résultat d'une fonction de hachage peut être appelé selon le contexte somme de contrôle, empreinte, empreinte numérique, hash, résumé de message, condensé, condensat, signature ou encore empreinte cryptographique. On nomme fonction de hachage, de l'anglais « hash function » une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale.
Horodatage	Mécanisme permettant d'associer une date et une heure à un évènement. Dans le cas de la signature on utilise l'horodatage certifié permettant d'assurer l'existence du document et son contenu à cette date et heure. D'après le règlement eIDAS, ce sont des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant » Pour être qualifié il doit satisfaire aux exigences suivantes : a) Il lie la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données ; b) Il est fondé sur une horloge exacte liée au temps universel coordonné ; et c) Il est signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié, ou par une méthode équivalente.
PKI / IGC / ICP	*Public Key Infrastructure / Infrastructure de Gestion de Clés / Infrastructure à Clés Publiques* est un ensemble de composants matériels, procéduraux et logiciels permettant de gérer des certificats de façon à leur garantir à priori un niveau de confiance.
RA / AE	*Registration authority / Autorité d'Enregistrement*
Révocation	La révocation d'un certificat dans une PKI / IGC consiste principalement à l'inscription de celui-ci dans la liste de révocation (CRL : Certificate Revocation List) publiée par l'autorité de certification. Le but de cette inscription est d'indiquer que le certificat n'est plus valable indépendamment de sa date de validité.
RGS	Le référentiel général de sécurité (RGS) vise à renforcer la confiance des usagers dans les services électroniques proposés par les autorités administratives, notamment lorsque ceux-ci traitent des données personnelles. Il s'applique aux systèmes d'information mis en œuvre par les autorités administratives dans leurs relations entre elles et avec les usagers. Il peut aussi être considéré comme un recueil de bonnes pratiques pour tous les autres organismes. Dans ses annexes, le RGS définit des règles concernant l'utilisation des certificats électroniques et des mécanismes cryptographiques.

Terme	Commentaire
ROI	Return on Investment /Retour sur investissement : ratio entre le gain apporté sur les sommes investies pour l'obtenir.
RSA	Le chiffrement RSA (nommé par les initiales de ses trois inventeurs) est un algorithme de cryptographie asymétrique. Cet algorithme a été décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman. RSA a été breveté par le Massachusetts Institute of Technology (MIT) en 1983 aux États-Unis. Il s'appuie principalement sur la difficulté qu'il y a à factoriser le produit de deux nombres et utilise de grands nombres premiers pour ses clés.
Tiers de confiance / Opérateur de service de confiance	Un tiers de confiance est un garant électronique. En effet, lorsqu'on parle de tiers de confiance, il s'agit d'un organisme agréé chargé de la gestion des clés privées des utilisateurs assurant, grâce au chiffrement, la confidentialité des messages électroniques et qui permet de certifier l'authenticité des transactions effectuées sur Internet. Le règlement européen eIDAS du 23 juillet 2014 remplace la notion française de « Tiers de confiance » par « prestataire de service de confiance ».

XI. ANNEXE : processus technique de signature d'un document

Les activités ci-dessous décrivent les différentes étapes techniques nécessaires à l'horodatage, la signature d'un document et la vérification de la signature. Ces opérations sont effectuées par les logiciels, elles ne sont exposées ici que pour éclairer et démystifier la complexité des opérations faites même si elles reposent sur des théories mathématiques difficilement accessibles.

Horodatage d'un document électronique (facultatif) :

1. Hacher le document à horodater ;
2. Signer le haché avec sa clé privée permettant à l'autorité d'horodatage de l'identifier ;
3. Chiffrer le haché ainsi signé et l'envoyer à l'autorité d'horodatage ;
4. L'autorité d'horodatage appose une date au haché et d'autres informations d'identification et signe l'ensemble de ces informations avec sa clé privée pour obtenir un certificat d'horodatage ;
5. L'autorité d'horodatage renvoie le certificat d'horodatage au propriétaire du document ;
6. Le propriétaire vérifie la signature et récupère la date.

Signature d'un document électronique :

1. Hacher le document à signer ;
2. Signer avec sa clé privée l'ensemble composé du haché, du document et de la date (éventuellement délivrée par l'autorité d'horodatage) ;
3. Envoyer la signature et le document à notre interlocuteur.

Vérification de la signature et de la non modification du document :

1. Le destinataire sépare le document et la signature ;
2. Il vérifie que le certificat de signature appartient bien au signataire et qu'il n'a pas été révoqué, et ce faisant il vérifie le certificat de l'émetteur et toute la chaîne de certificats jusqu'au certificat racine
3. Il récupère ainsi et sépare le haché et la date du document ;
4. Il hache le document original ;
5. Il compare son haché avec le haché envoyé par le signataire ;
6. Il peut vérifier la datation en demandant au signataire le certificat d'horodatage envoyé par l'autorité d'horodatage.