LA SIGNATURE ÉLECTRONIQUE II

Validation et Archivage

fntc

QUI SOMMES-NOUS ?

CR2PA

Le CR2PA, club de l'archivage managérial, est une association regroupant une quarantaine de membres issus d'organismes publics et du monde de l'entreprise.

Indépendant des acteurs du marché, le CR2PA est un lieu d'échange et de partage entre pairs du métier de l'archivage.

FnTC

Créée en 2001, la **Fédération des Tiers de Confiance du Numérique** opère avec pertinence la fusion de la technologie avec le droit et le « chiffre », ses membres offrent au **marché du Numérique** un inestimable gisement de compétences dans les domaines historiques de la **digitalisation** : signature électronique, archivage électronique, identité numérique, facture électronique, vote électroniques, e-finance, e-santé, ... Mais également dans ses domaines montants : Blockchain, KYC, Cachet électronique visible (CEV), ...

Nous contacter

CR2PA

75 rue de Lourmel
75015 PARIS
contact@cr2pa.fr

FNTC

Délégation Générale
43 rue de Douai
75009 PARIS
infos@fntc-numerique.com

INTRODUCTION

Début février 2020, dans une table ronde organisée par le CR2PA à laquelle participaient des experts de la FnTC, les échanges avec l'assistance avaient mis en avant l'intérêt que beaucoup portaient au thème de la signature électronique. Quelques semaines plus tard arrivait la crise sanitaire, et avec elle, la généralisation du télétravail et des échanges dématérialisés qui ont mené à une explosion des usages de cet outil.

Bien utiliser un outil nécessite de bien en comprendre le fonctionnement. Le CR2PA, club de l'archivage managérial, porteur des attentes et des enjeux des utilisateurs, et les experts de la FnTC, au meilleur de la maîtrise des solutions et de leur cadre réglementaire et juridique, ont noué un dialogue fécond pour en expliquer les rouages et en dégager les points-clés.

Le 1er fascicule a cherché à répondre aux questions « comment ça marche ? » et « quel niveau de signature choisir pour quel cas d'usage ? ».

Mais l'histoire ne s'arrête pas là. La signature électronique est, par nature, destinée à fournir une preuve, celle du consentement du signataire au contenu du document signé. En ce sens, elle rentre dans le domaine de la conservation à vocation probatoire, autant dire : de l'archivage.

L'objectif de ce 2ème fascicule est de faciliter les choix et le dialogue entre utilisateurs et prestataires, en détaillant les finalités et le contenu des différentes étapes du cycle de vie « après la signature ».

La prise en compte de la durée en est un facteur indispensable ; le records manager le sait bien, lui qui est dans l'entreprise le porteur de l'objectif de pérennité du patrimoine d'information de valeur.

Le mouvement de remplacement du support papier par le numérique, s'il a des avantages évidents dans le domaine de la production et de la transmission, voire du stockage et de la recherche, présente des faiblesses dans celui de la conservation, en premier lieu la vulnérabilité des solutions à l'obsolescence technologique.

INTRODUCTION

Il est donc important de retenir des solutions qui donnent le moins de prise possible à ce risque, en enregistrant au plus tôt la preuve de la validation technologique, plutôt qu'en misant sur la capacité à rejouer cette validation dans un futur incertain.

Dans l'étape suivante, comme toujours dans le domaine de l'archivage, la capture des éléments de contexte est au moins aussi importante que l'enregistrement du contenu de l'archive. C'est l'objet de la collecte des éléments de preuve.

La dernière étape est celle de l'archivage, et là nous retrouvons les fondamentaux qui le caractérisent.

Relativisons cependant les certitudes en rappelant deux principes importants :

- Le juge progresse lui aussi dans sa compréhension des nouvelles technologies. Il faut donc rester attentifs aux évolutions de la jurisprudence et aux indications qu'elles donnent sur ce qu'un tribunal va attendre en matière d'éléments de preuve.
- Comprendre en détail les technologies ne doit pas nous empêcher de conserver un recul critique. Comme dans tous les domaines de la sécurité, il faut commencer par évaluer le niveau du risque auquel on veut répondre, et sur cette base choisir le niveau de solution correspondant.

Merci aux acteurs du groupe de travail qui n'ont pas ménagé leur temps pour produire ce document. Et merci par avance aux lecteurs qui nous feront part de leurs remarques, car nous sommes loin d'avoir épuisé toute la matière de ce sujet.

Bruno Lalande,
Président CR2PA

SOMMAIRE

GLOSSAIRE

Validation

Le processus de vérification et de confirmation de la validité d'une signature ou d'un cachet électronique.

Données de validation

Les données qui servant à valider une signature électronique ou un cachet électronique.

Consentement

Le consentement peut se définir comme la volonté d'engager sa personne ou ses biens, ou les deux à la fois. On engage les biens d'autrui lorsque l'on agit en exécution d'un mandat, dit aussi « procuration » délivré par le mandant.

Enrôlement (également appelé enregistrement)

Quel que soit le mode de réalisation d'une signature électronique, cette dernière doit identifier celui qui la réalise.

La première étape est donc l'enrôlement : comment établir une identification numérique fiable pour une personne. L'enregistrement doit porter sur :

- L'identité de la personne
- Son moyen d'authentification a posteriori

Par exemple : le prénom et le nom de la personne + son numéro de téléphone mobile.
Les éléments relatifs à l'enrôlement sont des pièces maîtresses du dossier de preuves.

Politiques

Elles servent à détailler les modalités techniques et/ou d'organisation pour chaque domaine concerné mis en œuvre :

- Politique de gestion des identités et des droits ;
- Politique de certification pour la délivrance des certificats ;
- Politique de signature électronique ;
- Politique de traçabilité et de gestion de preuve ;
- Politique de confidentialité et de mise en œuvre du RGPD (analyse d'impact et registre de traitement).

Sauvegarde / Back-up

Opération technique consistant à dupliquer des données ou des documents, et à les stocker dans un lieu distant, dans le but de prévenir une faille du système ou une disparition accidentelle des originaux.

En cas de survenance d'un incident, les données font l'objet d'une restauration.

Ce glossaire est une aide précieuse pour vous accompagner dans la lecture de ce livret.

GLOSSAIRE

Conservation (sens 1) / Rétention

Obligation légale ou réglementaire de garder à disposition des autorités, voire de la collectivité certains documents traçant les activités d'une entreprise ou d'un organisme dans divers domaines règlementés : gestion financière, santé, environnement, patrimoine historique, etc.

NB : le mot conservation possède aussi en français le sens de maintenance matérielle des documents, correspondant au terme anglais *preservation*.

Conservation (sens 2) / Préservation

Ensemble des opérations techniques qui permettent de maintenir dans le temps des objets documentaires (quel que soit leur support), de préserver leur intégrité et de garantir l'accès à leur contenu.

NB : le mot conservation possède aussi en français le sens d'obligation réglementaire de garder les documents sous son contrôle, correspondant au terme anglais *retention*.

Stock / Back-log

Ensemble des documents produits, archivés ou simplement conservés dans le passé et dont les conditions de stockage, d'identification, d'accessibilité et de sécurité ne sont peut-être pas conformes à ce qu'elles devraient être au regard des risques de non-disponibilité et de sur-conservation.

Le stock s'oppose au flux des documents nouvellement créés et non encore archivés.

Archivage / Records management

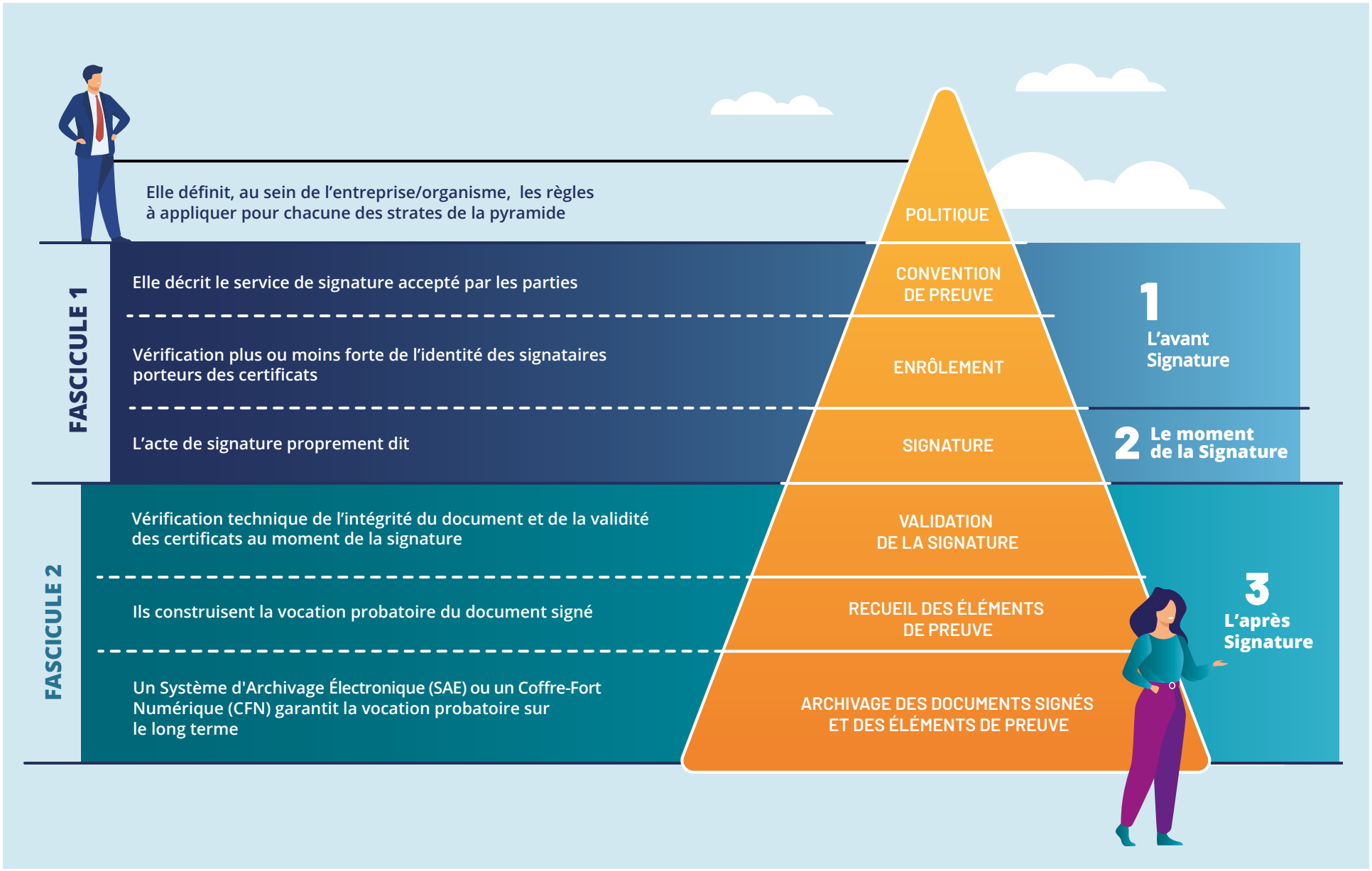
Démarche d'organisation qui a pour objectif d'identifier, de mettre en sécurité et de maintenir disponibles l'ensemble des documents qui engagent une entreprise ou un organisme vis-à-vis de tiers ou de son activité future et dont le défaut représenterait un risque.

La majorité des définitions ci-contre sont issues du « Nouveau glossaire de l'archivage » 2010 Glossaire de l'archivage - Arcateg, méthode d'archivage par catégorie »(Archives 17).

Pour aller plus loin

- Le CR2PA appelle également archivage managérial la démarche d'archivage (mise en sécurité des informations dans le temps) basée sur une évaluation du risque pour l'entreprise ou l'organisation propriétaire des informations reçues ou émises. Il se prévoit dès la création de l'information dès lors qu'elle engage la responsabilité de son émetteur/récepteur pour une certaine durée ou qu'elle participe au patrimoine de l'entreprise ou de l'organisation.

LA PYRAMIDE DE LA SIGNATURE ELECTRONIQUE



LA VALIDATION DES SIGNATURES

1

1.1 La validation : pourquoi vérifier ?

Qu'est-ce que la validation ?

Il s'agit de l'étape intervenant après la signature et visant à vérifier :

- L'empreinte de la signature = vérification de l'intégrité du document signé
- La validité du certificat au moment de la signature = vérification de l'authenticité

Quel est l'enjeu de la validation ?

- L'enjeu est de s'assurer de la validité de la signature et du certificat au moment de la signature.
- Le risque lié à cette vérification porte sur sa réalisation après expiration du certificat.
- (voir tableau ci-contre).

Est-ce obligatoire ?

Certains textes l'imposent comme l'indique quelques exemples ci-dessous :

La validation est également appelée vérification.

Textes	Validation sur niveau de signature particulier	Validation sur une typologie de document
eIDAS (article 32 et 33)	Signature électronique qualifiée	
Articles 96F bis du CGI		Factures électroniques signées
Article 5 de l'arrêté du 22 mars 2019 relatif à la signature électronique des contrats de la commande publique	Signature électronique qualifiée.	

Exemples non exhaustifs

1.2 En quoi consiste la validation des signatures et cachets électroniques ?

La validation est un acte d'après signature.

C'est un « *processus de vérification et de confirmation de la validité d'une signature ou d'un cachet électronique (Règlement eIDAS, article 3 Définitions, alinéa 41).* »

L'acte de validation comporte 2 types de vérification :

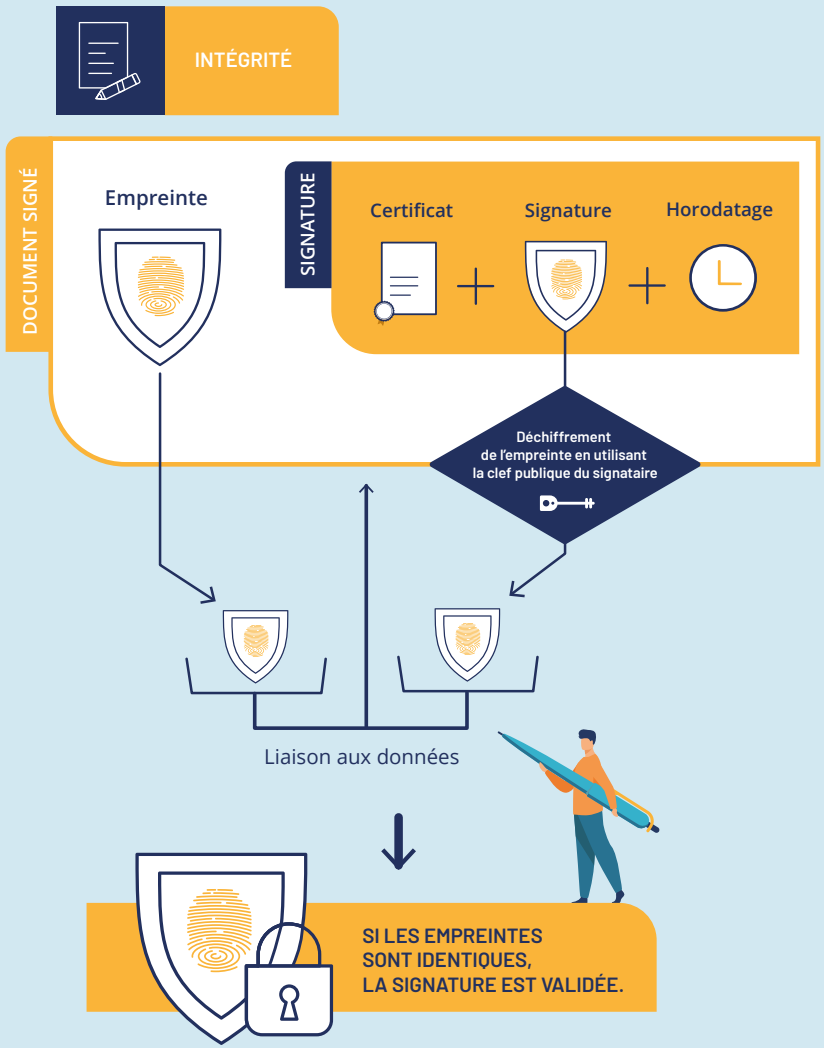
- **Une vérification technique** : on utilise les informations contenues dans le certificat pour vérifier l'intégrité du document d'une part (clé publique pour le calcul de l'empreinte – cf. Schéma) et d'autre part, la validité et la non-révocation du certificat électronique au moment de la signature.
- **Une vérification du niveau de confiance (ou chaîne de confiance)** : lorsqu'une Autorité de Certification (AC) délivre un certificat, elle le signe à l'aide d'un certificat qu'elle a obtenu auprès d'une AC tierce qui elle aussi a fait appel à une autre AC et ainsi de suite, jusqu'à identifier ce que l'on appelle l'AC racine.
- La vérification assure la confiance que l'on peut accorder à toute la chaîne des certificats qui ont été utilisés pour créer finalement la signature électronique qualifiée du document.

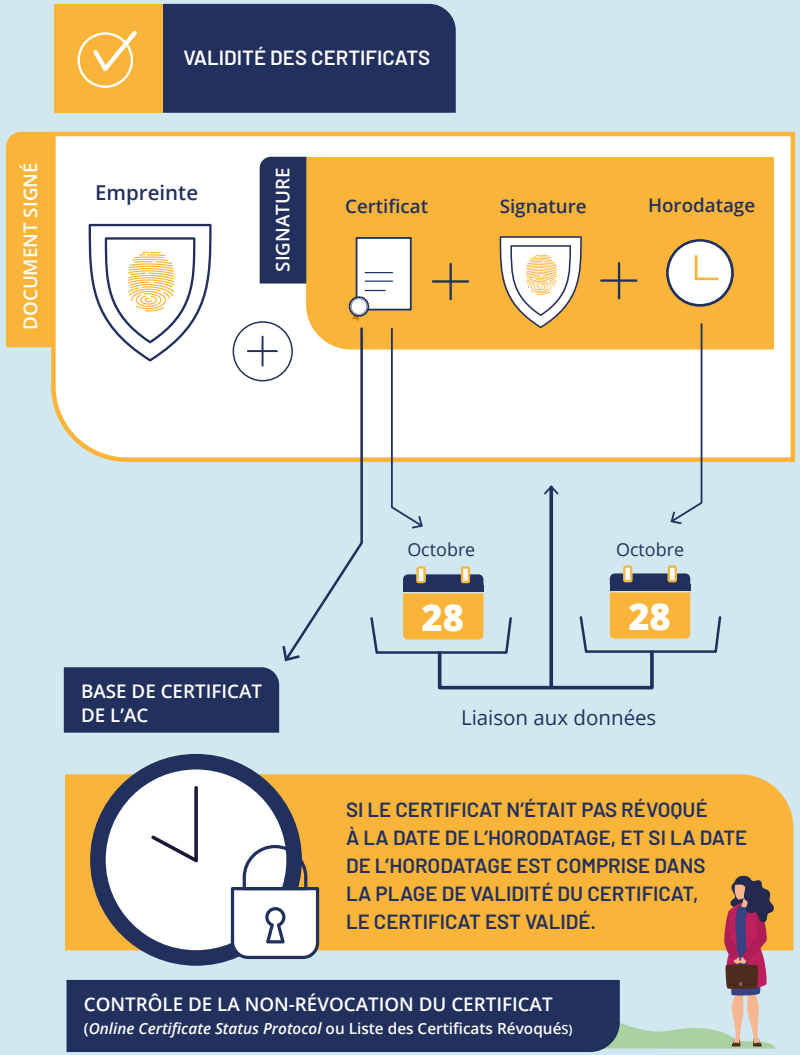
Le résultat de la validation des signatures/cachets électroniques est fourni sous la forme d'un rapport intelligible attestant l'intégrité du document et la non révocation du certificat.

Ce rapport est aussi appelé « rapport de validation ».

Un service de confiance qualifié (règlement eIDAS) de validation existe pour les signatures et cachets qualifiés. Dans ce cas-là, il ne peut être opéré que par un prestataire dûment qualifié au sens dudit règlement.

SCHÉMA DE VALIDATION TECHNIQUE





1.4 Quand doit-on procéder à la validation ?

Rappelons ici que les certificats électroniques ont une durée limitée de validité. De manière générale, les certificats sont valides durant 2 ou 3 ans mais certains, appelés certificats à la volée, sont valides pour une durée beaucoup plus courte (se comptant en heures ou jours), voire à usage unique.

Or, la validation comporte un volet visant à vérifier la validité du certificat au moment de la signature. Si le certificat est encore valide lors de la vérification, cela ne pose aucun problème mais s'il est caduc les choses se compliquent :

- Il sera alors nécessaire de vérifier l'horodatage apposé au moment de la signature pour ensuite vérifier la validité du certificat à la date et heure figurant dans l'horodatage. Bien entendu, cela s'applique lorsqu'un horodatage a été apposé et que celui-ci est valide : *l'horodatage repose lui aussi sur un certificat à durée de validité limitée.*
- Puis il faudra vérifier auprès de l'Autorité de Certification, la validité du certificat. Le risque serait ici que l'autorité ne puisse effectuer cette vérification pour diverses raisons : *la fermeture de son activité par exemple.*

Les prestataires « qualifiés » sont soumis à une obligation de Plan de Continuité du service pour éviter ces désagréments.

Recommandation FnTC-CR2PA

- Il semble donc logique de procéder le plus tôt après l'acte de signature à la validation dans le but d'éviter ces possibles complications.

Niveau de signature/ cachet	Validation encadrée par l'eIDAS	Qui peut procéder à la validation ?	Avec quel outil valider ?	Quand procéder à la validation ?
Qualifié	Oui	PSCQ	-	Au besoin
Avancé ou Simple	-	Tout le monde	La solution de signature ou un outil en ligne ou la solution de conservation (si la fonctionnalité existe)	Au plus tôt après la signature

1

GESTION DE LA PREUVE

2

Un peu d'histoire juridique...

La signature et la preuve électronique tendent à se répandre dans les prétoires au fur et à mesure de la digitalisation progressive de chaque pan du Droit. Confrontés à des concepts encore peu étudiés, les juges ont cherché à caler des concepts figurant dans les articles 1316-1 et 1316-4 puis 1366 et 1367 du Code civil à des objets techniques qui leur étaient présentés (souvent en appel). On voit se dessiner une jurisprudence foisonnante en la matière :

- L'analyse du contenu des éléments de preuves est de plus en plus fouillée.
- Au fil du temps, le juge approfondit sa doctrine sur les éléments de preuves attendus et sur leur complétude. Le justiciable doit donc lui aussi être prudent et respecter au mieux les prescriptions de la jurisprudence.

ÉVOLUTION AU FIL DU TEMPS DE LA TERMINOLOGIE ET DES ÉLÉMENTS PRODUITS DANS LA JURISPRUDENCE

2

CA Nancy, 14 février 2013 (une première)

Appel de la décision du TI Epinal du 12 décembre 2011. le fichier de preuve de la transaction, produit aux débats, a été émis par l'autorité de certification.

> Démonstration en justice du mode de fonctionnement et production d'une attestation de l'AC.

> « *la mention du numéro de l'avenant sur le fichier de preuves permet de vérifier que c'est bien cet avenant qui a été signé électroniquement par Monsieur X* ».

Action en paiement non forclose pour la Banque.

2013

Preuves présentées :

Fichier de preuves
Attestation de l'autorité de Certification

Cour d'Appel de Chambéry, 25 janvier 2018

Admission de la fiabilité du procédé de signature électronique d'un contrat de crédit à la consommation, en se fondant sur le fichier de preuves fourni par un prestataire de service de confiance.

Une synthèse de fichier de preuves de la transaction :
« *Q0IPPERS - PQSPASS - 50972441639001-2015. 5.5-8.18.41.1194, émanant de la société KEYNECTIS ayant la qualité de prestataire de service de gestion de preuve, qui atteste de la signature électronique le 05/05/2014 à 08:18:47 du document référencé par monsieur Sammy Y* », dont elle précise l'adresse mail et qui mentionne le code d'identité du certificat électronique.

2018

Preuves présentées :

Synthèse du fichier de preuves
Adresse mail
Code d'identité du certificat

Cour d'appel, Paris, Pôle 4, chambre 9, 15 Avril 2021

La banque fournit la synthèse du fichier de preuves de la transaction qui décrit le protocole de consentement entre les parties via le concessionnaire / intervenant, en sa qualité d'IOBSP, la fiche d'informations « IOBSP/IOA » portant mandat de l'intéressé, et son attestation de formation signée par le directeur général de la banque.

Le PSCE atteste du consentement des signataires ayant apposé leurs signatures électroniques sur le document contenu dans le fichier de preuves (il y est indiqué que le signataire s'est identifié sur la page de consentement en saisissant un code qui lui a été transmis par la banque).

La banque produit aussi une attestation de fiabilité des pratiques du prestaire de service de confiance couvrant la date de contractualisation.

Les conditions générales d'utilisation du service de signature électronique prévoyaient que pour accéder au service, le client devait s'identifier auprès du mandataire de la banque (qualité de IOBSP) en fournissant l'original de sa carte d'identité ainsi qu'une copie de ce document.

Une « enveloppe de preuve » électronique est fournie avec le fichier de preuves, contenant le fichier de preuves référencé de façon spécifique, avec des lettres et des chiffres, créé par le PSCE pour les besoins de la banque. Dans ce document, figurent le nom du client, la date de signature du contrat ainsi que les modalités de vérification de la signature électronique.

2021

Preuves présentées :

Synthèse du fichier de preuves / Consentement
Code transmis / Attestation de fiabilité
Mode d'identification / Enveloppe de preuve

Une jurisprudence fournie vient traiter la question de la preuve des documents signés électroniquement. Les cas traités sont intéressants mais ne sauraient embrasser la totalité des situations rencontrées par le Juge.

2.1 Les éléments de preuve

Le concept de preuve est bien connu par les prestataires. Cependant le vocabulaire utilisé peut être différents d'un prestataire à l'autre.

Ainsi, lorsque l'on cherche aujourd'hui une solution de signature, on peut être confronté aux termes suivants : fichier de preuves, chemin de preuves, déroulé de preuves, dossier de preuves, attestation de preuves, dossier de réalisation, enveloppe de preuve, etc.

Cette jungle terminologique peut porter à confusion bien qu'il ne s'agisse que d'un choix marketing de la part des prestataires.

Aucune définition officielle ou règlementaire ne fixe le terme à employer à ce jour.

En tout état de cause, quel que soit le terme employé, l'important est ce que le document contient, à savoir les constituants de la preuve.

Les preuves de la validation de la signature pourront être présentées avec le document signé lors d'un litige. Leur recevabilité est laissée à l'appréciation souveraine du juge.

2.2 Les besoins de preuve

Le besoin de vérification des signatures existe déjà dans le monde papier, voici ce qui change lorsque la signature est électronique :

Ce que l'on doit prouver	Comment le prouver
Que le signataire est bien qui il prétend.	Grâce au processus d'enrôlement avant la signature et d'authentification au moment de la signature.
Que le processus de signature a permis de recueillir le consentement.	Grâce au processus de consentement au moment de la signature, dont les traces se retrouvent dans les éléments de preuves.
Que le document n'a pas été modifié et que la signature est bien liée au document.	Grâce aux processus de garantie de l'intégrité du document signé : • Le rapport de validation permet de démontrer la validité de la signature et l'intégrité du document. • Une des fonctionnalités d'un système d'archivage électronique ou d'un coffre-fort numérique est de pouvoir produire un rapport intelligible à partir de ses différents journaux démontrant l'intégrité des archives tout au long de leur vie.
Que le document a été conservé dans des conditions qui font foi et qu'il est toujours lisible.	Grâce à la capacité de maintenir la lisibilité du document via, par exemple, un logiciel de visualisation interne ou externe à la solution d'archivage.

2.3 Les constituants de la preuve

Les éléments de preuve sont un ensemble de fichiers lisibles que tout un chacun peut s'approprier.

L'objectif est de fournir des preuves auprès du juge. Mais aussi de comprendre le processus chronologique mis en œuvre et le respect des exigences règlementaires.

A minima, les éléments de preuve à apporter sont :

- Le procédé d'identification (enrôlement) utilisé : numéro de téléphone, mail, CNI, face à face, etc.

  Permet de comprendre les moyens utilisés pour identifier les personnes dans le but de leur générer un certificat électronique de signature. Cette preuve est notamment importante dans le cadre des signatures simples pour lesquelles l'identification n'est pas règlementée.

- Le niveau de certificat identifiant les personnes physiques signataires : simple, avancé ou qualifié.

  Permet de présumer le degré de fiabilité dans l'identification de la personne.

- La procédure d'authentification utilisée lors de la signature : OTP, token, etc.

  Permet de comprendre les moyens utilisés pour que le signataire s'authentifie au moment de la signature.

- La procédure de consentement mise en place : case à cocher, obligation de dérouler le document jusqu'à la fin, etc.

  Permet de comprendre les moyens utilisés pour signifier clairement le consentement de chacun des signataires.

- La liste des éléments à archiver et la méthode d'archivage :

  Permet de comprendre les moyens utilisés pour garantir la vocation probatoire des documents signés et des éléments de preuve.

- Les horodatages de chaque action pour prouver le déroulé chronologique de la signature.

  Permet d'assurer la traçabilité des actions composant l'acte de signature.

- Les preuves de la validation : rapport de validation ou preuves de la validation technique.

  Permet de s'assurer de l'intégrité du document et de la non-révocation des certificats des signataires.

La convention de preuve, si elle a été réalisée, permet notamment de fixer les éléments de preuves constituant le dossier de preuves.

La recevabilité des éléments de preuve est toujours à l'appréciation du juge qui peut s'appuyer sur les jurisprudences antérieures.

Légende des acteurs

S : Signataires

AC : Autorité de Certification

PSCQ : Prestataire de Services de Confiance Qualifié

Légende technique

EP : Eléments de Preuve

RV : Rapport de Validation

SE : Signature Electronique

SEA : Signature Electronique Avancée

SEQ : Signature Electronique Qualifiée

2

L'ARCHIVAGE

3

3.1 Pourquoi archiver ?

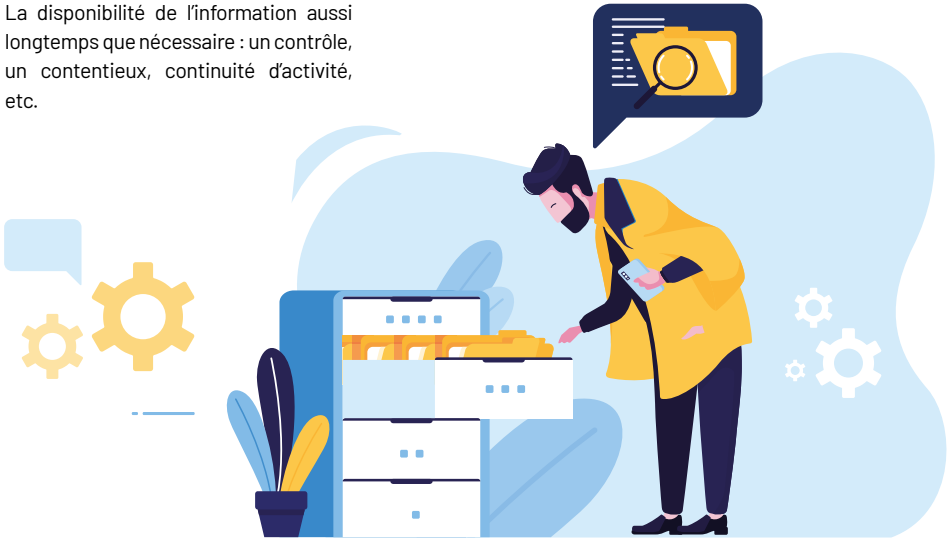
L'archivage du document signé dans une solution à vocation probatoire répondant à l'état de l'art (exemple : normes NF Z42-013 et NF Z42-020) permet de garantir, *a minima*, les préceptes de disponibilité, pérennité, lisibilité et intégrité :

- En conformité avec l'article 1366 du code civil : *"L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »*.
- L'assurance de l'intégrité du document signé mais aussi des éléments de preuve pendant toute leur durée de conservation.
- La disponibilité de l'information aussi longtemps que nécessaire : un contrôle, un contentieux, continuité d'activité, etc.

Flash info

D'un point de vue strictement juridique, il convient de distinguer la conservation et l'archivage.

- La conservation permet de rapporter la preuve des droits (c'est-à-dire des informations contenues dans un document) tandis que l'archivage a trait au support (le document proprement dit) à des fins juridiques.
- Le stockage a une optique purement technique.



3.2 Que doit-on archiver ?

Les documents signés, les signatures et les éléments de preuve.

- **Le document signé** : en tant qu'objet de l'acte de la signature, il doit être archivé de manière intègre pour garantir sa recevabilité en tant que preuve.
- **La signature** : selon les formats de signature utilisés, la signature peut faire partie du document (encapsulée) ou être présentée à part entière. Dans ce cas, il faut l'archiver.
- **Les éléments de preuve** : le seul document et sa signature ne suffisant pas pour prouver la procédure correcte de signature électronique, les éléments de preuve jouent un rôle primordial pour accroître la recevabilité du document en tant que preuve devant le juge.

L'archivage à vocation probatoire des éléments de preuve, renforce à son tour la recevabilité de ces mêmes preuves. La règlementation nous oblige à garantir l'intégrité de l'écrit électronique (document signé) : il est logique de garantir également l'intégrité des preuves.

Flash info

- Selon le Tiers de Confiance et la solution utilisée, la récupération et/ou l'archivage des éléments de preuve ne sont pas toujours automatiques.

  Il est important de le définir dans le contrat.

En posant ces questions aux prestataires de signatures, vous pourrez mieux définir à qui confier l'archivage.

3.3 Qui archive quoi ?

L'archivage du document signé et de sa signature est ancré dans les pratiques actuelles. Chaque signataire porte la responsabilité d'archiver ses propres éléments (document, signatures et preuves). Cet archivage peut être réalisé par le signataire lui-même ou par le tiers (prestataire de signature/prestataire d' archivage) qu'il aura retenu. Cependant, il est important de poser les **questions suivantes** afin de s'assurer des conditions d'archivage :

Qu'est ce qui est archivé ?

Permet de s'assurer que tous les éléments seront bien archivés (document, signature et preuves).

A quel moment l'archivage est-il réalisé ?

Permet de s'assurer de l'intégrité des éléments archivés depuis leur génération jusqu'à la fin de la durée de conservation.

Qui réalise cet archivage ? Quelles en sont les conditions ?

Permet de s'assurer que tous les éléments sont bien archivés par quelqu'un mais aussi de vérifier les certifications et/ ou conformité à l'état de l'art en matière d'archivage.

Pendant combien de temps ?

Permet de s'assurer que **la durée de conservation** est conforme à celle désirée par les propriétaires des archives (les signataires) selon leur référentiel de conservation.

En savoir plus :
« La durée de conservation »

Il convient de distinguer **la durée d'archivage** de **la durée de rétention**. Cette dernière est la durée pendant laquelle les éléments (document, signature et preuves) sont disponibles dans la solution de signature du prestataire.

Les éléments de preuve sont-ils inclus ?

Permet de vérifier que les éléments de preuves seront maintenus intègres.

Comment accéder aux archives?

Permet de s'assurer de la disponibilité des archives en cas de besoin.

Comment récupérer les archives ?

Permet de s'assurer de **la restitution** de l'ensemble des éléments (document, signature, éléments de preuve), à tout moment.

En savoir plus : « La restitution »

La réversibilité de l'ensemble des éléments, y compris des éléments de preuve est importante pour garantir leur traçabilité et la continuité de leur vocation probatoire.

3

Peu importe qui archive du moment que les règles de l'art de l'archivage à vocation probatoire sont respectées, ou, *a minima* une conformité aux normes NF Z42-013 et/ou NF Z42-020.

3.4 L'archivage en pratique

Comment assurer la passerelle entre un prestataire de signature électronique et un prestataire d'archivage ?

Dans le contexte d'une procédure de signature électronique, l'interopérabilité touche le versement des documents dans la solution d'archivage à vocation probatoire. Il est important ici de ne pas rompre la chaîne de confiance du document. En d'autres termes, comment s'assurer que cette passerelle va engendrer le bon versement des documents dans la solution de conservation ?

Outre les moyens techniques pouvant être mis à disposition par les prestataires (connecteurs, API), il est important de définir cette **passerelle** soit dans un seul contrat (dans le cas où les prestataires seraient partenaires) ou bien dans chacun des 2 contrats via des annexes qui se répondent.

En savoir plus : « Passerelle »

- Quel que soit le **processus de passerelle** utilisé (automatisé ou manuel), il doit être correctement documenté.

Dans quel format les archives doivent-elles être conservées ?

Le format des archives doit être le format original. Celui-ci a tout intérêt d'être lisible, intelligible et pérenne pour être recevable devant un juge.

L'important est de pouvoir démontrer l'intégrité dans le temps et la pérennité mais aussi la lisibilité et l'intelligibilité du contenu du document.

Comment effectuer la gestion de la pérennité et de la lisibilité ?

Pour assurer le gestion de la pérennité et de la lisibilité, des actions de migration de formats peuvent être nécessaires, il est primordial qu'elles soient tracées.

Comment assurer l'interopérabilité entre prestataires (de signatures, de dématérialisation, d'archivage, etc.) se chargeant de l'archivage à vocation probatoire ?

En matière d'archivage, l'interopérabilité se définit comme la capacité à transférer des archives d'un système à un autre selon les normes en vigueur (NF Z42-013 et NF Z42-020) dans le cadre de la réversibilité des archives.

Le prestataire se chargeant de l'archivage qu'il soit le prestataire en charge de la signature électronique ou de l'archivage électronique des documents signés et des éléments de preuves doit donc respecter ce cadre.

Comment gérer la destruction d'un document signé ? Y a-t-il des bonnes pratiques à mettre en place ?

En matière d'archivage, la destruction des archives est pilotée, auditable et sous la responsabilité du propriétaire des archives.

Il existe 2 solutions de destruction des archives :

- Suppression des archives et de toutes leurs métadonnées ;
- Suppression des archives et d'une partie des métadonnées en conservant certaines métadonnées dites témoins (notamment la date de destruction).

Quelle que soit la solution retenue, la destruction est enregistrée dans le journal du cycle de vie des archives et fait l'objet d'une « *attestation d'élimination* ».

La méthode de destruction est à définir par le propriétaire des archives et à inclure dans le contrat qui le lie à son tiers archiveur.

3.5 Le rapport d'archivage

Ce rapport est produit par la solution de conservation. Il rassemble l'ensemble des preuves liées à l'archivage des documents telles que définies dans les normes d'archivage à vocation probatoire.

Cet ensemble de preuve permet de démontrer l'intégrité dans le temps des archives (documents signés, signature et éléments de preuves). Il doit, *a minima* contenir :

- **Les enregistrements** : traces générées pour chaque évènement réalisé dans la solution d'archivage.
- **Les journaux** : documents structurés et exploitables consolidant les enregistrements.
- **Les attestations** : les documents attestant de la conformité, de la responsabilité sur les archives électroniques et de la réalisation d'opérations spécifiques (versement, consultation, etc.).

Ce rapport est fourni par le prestataire en charge de l'archivage et viendra compléter les preuves à présenter en cas de litige.

Légende des acteurs :

S : Signataires

AC : Autorité de Certification

PSCQ : Prestataire de Services de Confiance Qualifié

TA : Tiers Archiveur

Légende technique :

EP : Eléments de Preuve

RV : Rapport de Validation

RC : Rapport de Conservation

SE : Signature Electronique

SEA : Signature Electronique Avancée

SEQ : Signature Electronique Qualifiée

SAE : Système d'Archivage Electronique

CFN : Coffre-fort Numérique

LA CHAÎNE DE RESPONSABILITÉ

4

Les contrats avec les Prestataires de Services de Confiance doivent être équilibrés et permettre de décrire les obligations et responsabilités de chaque acteur. Toutefois, certains points doivent être particulièrement étudiés : comment le prestataire garantit-il la conformité de sa solution de signature électronique par rapport au cadre légal et réglementaire ? Sans cela, le client ne s'engagerait pas avec le prestataire : il s'agit d'une obligation essentielle.

Il faut bien comprendre qu'une solution de signature électronique n'est pas un produit informatique comme les autres.

L'ergonomie juridique de la solution doit être assurée : il faut que la solution technique corresponde à des attentes juridiques matérialisées dans un contrat.

Les chaines de responsabilité doivent être prévues contractuellement et définir clairement qui est responsable de quoi.

Cette définition des responsabilités doit être menée par des experts juridiques pour assurer l'équilibre contractuel.

NOTES

Cet espace vous est dédié pour prendre des notes.

4

CONCLUSION

Dans la continuité du fascicule précédent, le présent document vous a permis de rentrer dans la validation, la gestion de preuve et l'archivage de la signature électronique. Il vous a fait appréhender un écosystème particulier articulé autour de principes techniques et juridiques favorisant le déploiement de cette signature électronique.

Mais depuis plusieurs années, face à la complexité de la mise en œuvre de cette signature électronique, il nous est apparu nécessaire de rappeler la nécessité de la conservation.

Cette démarche s'inscrit dans l'expression « archivage managérial » qui insiste sur l'importance de la première étape de l'archivage : se concentrer sur la valeur de l'information à conserver et sur le cycle de vie à lui associer.

Conserver ou détruire est un geste fort, qui engage la responsabilité des dirigeants dès lors que ces documents fondent les droits et supportent les intérêts de l'entreprise et de ceux qui y travaillent.

Il s'avère en effet que la conservation dans le temps des documents signés peut poser problème. Pour pallier à cet inconvénient, la démarche de disposer, à côté du document signé à conserver, d'un fichier de preuves qui contient l'histoire de la signature de ce document devient nécessaire.

La mise en œuvre d'une solution d'archivage permet d'apporter des garanties dans la conservation des différentes pièces décrites dans ce document.

Ce fascicule, nous l'espérons, permettra à chacun au sein de son entreprise ou de son organisme de traduire au quotidien cette notion d'archivage managérial autour des documents signés électroniquement :

- Les dirigeants, et tous les managers, sont responsables de la production des traces de l'activité de leur entreprise, de ce qui est fait et dit au nom de leur entreprise, et qui de fait engage l'avenir ;
- Les décisions à enjeux doivent être documentées, et les actes archivés avec leurs justificatifs, et conservés de manière appropriée ;
- L'information inutile doit être systématiquement détruite ;
- Les documents produits ou gérés au nom de l'entreprise, qui ont valeur de preuve et qui l'engagent, doivent être en permanence sous contrôle.

La signature électronique en fait à présent partie. Elle fait apparaître un besoin nouveau de compétence dans ce domaine pour accompagner les différents métiers souhaitant utiliser ces nouvelles technologies.

Cet accompagnement articulé entre domaine juridique, domaine métier, domaine système d'information, archivistes et prestataires de services de confiance permettra par un travail coopératif d'anticiper et ainsi de maîtriser des risques majeurs d'image de marque, d'abus d'identité et de contentieux dès l'amont en disposant d'une argumentation de défense construite autour des éléments de preuve établis pour chaque document signé.

Bernard OUILLON
RTE, Vice-Président du CR2PA
Membre de la FnTC

REMERCIEMENTS

Comité de rédaction :

Agosti Pascal, Caprioli & Associés, Société d'Avocats
Bobant Alain, président de la FnTC
Bonnefous Jean-Mathieu, Orano
Borghesi Alain, Vice-président FNTC et PDG Cecurity.com
Delion François, Bouygues Telecom
Frezier Amélie, Cecurity.com
Lalande Bruno, Président CR2PA
Ouillon Bernard, RTE France
Pichat Estelle, Systra
Vincent Florent, Thales Group

Septembre 2021

Délégation Générale :
43 rue de Douai
75009 Paris

+33 (0)6 89 84 73 65
infos@fntc-numerique.com

www.fntc.org

Contact :
75 rue de Lourmel
75015 PARIS

contact@cr2pa.fr

www.cr2pa.fr