La signature électronique III

Conservation à long terme des documents signés

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 », et 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 électronique, 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
14 rue de Bruxelles
75009 PARIS
infos@fntc-numerique.com

INTRODUCTION

Dans nos deux premiers guides consacrés à la signature électronique, nous avons pu nous familiariser avec cette notion.

Le premier de ces guides nous a permis d'en maîtriser les rouages en posant la définition et le cadre réglementaire, en détaillant les différents niveaux de signature et leurs caractéristiques, enfin en développant les principaux cas d'usage.

Armés de ces bases, nous étions parés pour aborder sereinement le deuxième guide qui nous donnait les clés de la conservation de nos documents/données et de leurs signatures en précisant l'importance de l'acte de vérification, en décrivant les éléments constitutifs de la preuve et de sa gestion et en énumérant les bonnes pratiques à observer pour leur archivage dans les règles de l'art.

Tout était dit, semble-t-il, si nos documents/données n'étaient confrontés à ce que nous pourrions appeler « le paradoxe des durées de vie ». A savoir l'incompatibilité des durées de conservation longues, voire très longues, de nos informations numériques alors qu'elles reposent sur des technologies et des supports en perpétuelle évolution et d'obsolescence rapide.

Il nous a donc paru indispensable de vous offrir ce troisième volet dédié spécifiquement à la conservation long terme. Son objectif est simple : vous y exposer les pièges que cache ce paradoxe et vous proposer des solutions pour les éviter afin que documents et données demeurent pérennes et conservent leur intégrité et leur lisibilité aussi longtemps que les activités auxquelles ils se rattachent le nécessitent.

François Delion,
CR2PA

SOMMAIRE

GLOSSAIRE

SAE

Système d'archivage électronique.

PSCO

Prestataire de services de confiance.

eIDAS

electronic IDentification, Authentication and trust Services. « Le règlement [européen] eIDAS [...] instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique numérique. Il couvre notamment le sujet de la signature électronique, et abroge la directive 1999/93/CE. L'ANSSI est l'un des organismes nationaux chargés de la mise en oeuvre de ce règlement. » Source : ANSSI – Le règlement eIDAS.

OAIS

Open Archival Information System (Système ouvert d'archivage d'information). Modèle conceptuel destiné à la gestion, à l'archivage et à la préservation à long terme de documents numériques. L'OAIS est une norme internationale ISO enregistrée sous la référence 14721.

RSA

Du nom de ses inventeurs (Ronald Rivest, Adi Shamir et Leonard Adleman), le chiffrement RSA est un algorithme de cryptographie asymétrique.

PKI

Public Key Infrastructure ou infrastructure à clés publiques (ICP) en français. Infrastructure composée de procédures, outils et logiciels destinée à gérer des clés publiques et à les lier à des identités (comme des noms d'utilisateurs ou d'organisations).

RGPD

Règlement général sur la protection des données. Reglement europeen 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Il abroge la directive 95/46/CE.

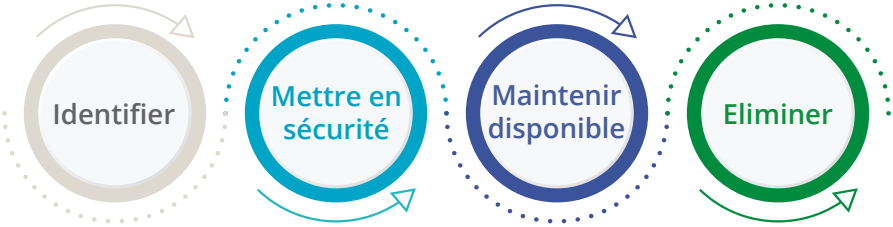
OS

Operating system, système d'exploitation en français (exemple : Windows, Mac OS, Linux, etc.).

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

QU'EST-CE QUE LA CONSERVATION À LONG TERME ?

1



1.1 Les éléments de définition

La conservation à long terme va de pair avec les objectifs et la définition de l'archivage et du 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». (Nouveau Glossaire de l'archivage, Marie-Anne Chabin, 2010)

- La mise en place de cette notion, qui se concentre sur la valeur de l'information à conserver et sur le cycle de vie à lui associer, a également pour objectif de permettre sa mise à disponibilité pour une capitalisation des connaissances, une transmission, une réutilisation, une traçabilité.
- Les principes de l'archivage induisent ainsi la notion de durée nécessaire pour la rétention de l'information. Ce qui amène à adopter une démarche de pérennisation au gré des changements technologiques.
  En effet, qui dit (très) long terme veut dire nouveau cycle technologique et donc des changements potentiels.

  En dehors de la durée, l'enjeu pour l'archiviste est de garantir que les données/documents conservés soient intègres, lisibles et pérennes. Ainsi, ses actions se centrent sur la préservation du patrimoine informationnel créé en se reposant sur les standards existants, le cadre réglementaire et leurs évolutions pour garantir la disponibilité de ces actifs.

« En dehors de la durée, l'enjeu pour l'archiviste est de garantir que les données/documents conservés soient intègres, lisibles et pérennes. »

- Dans le modèle OAIS, le long terme est défini comme une période suffisamment longue pour être soumise à l'impact des changements technologiques, y compris à la prise en compte de nouveaux supports et nouveaux formats de données ou à des changements de la communauté d'utilisateurs. Le long terme peut se poursuivre indéfiniment.
- Pérennisation et préservation apparaissent ainsi comme un même concept : permettre de faire face à la perte d'informations d'identification ainsi qu'à l'obsolescence des supports et des logiciels. L'objectif est d'identifier et de conserver des documents et des données pour les rendre accessibles sur le moyen (10 ans et plus) et le long terme (50 ans et plus).
- Les enjeux sont donc les suivants : assurer la sécurité, l'intégrité, la lisibilité, la gestion des accès et la durée de conservation des documents engageants et vitaux pour une organisation.
- Il faut donc aboutir à une conservation électronique pérenne et adaptée aux besoins spécifiques de maintien dans le temps des informations autour du processus de signature.

1.2 Quels sont les enjeux et les risques technologiques d'une conservation à long terme ?

Un document signé électroniquement répond à plusieurs objectifs des « utilisateurs » du document. Qu'ils soient émetteurs, destinataires initiaux ou destinataires tiers, chacun exige que l'objet électronique soit intègre, lisible et que son imputabilité à l'émetteur s'appuie sur des moyens de traçabilité. Si les outils de cryptographie moderne, comme la signature asymétrique RSA ou les architectures de type PKI proposent des moyens fiables et éprouvés, ils restent cependant exposés à différents risques parfaitement connus et pour lesquels des moyens complémentaires de gestion des documents permettent de réduire ces risques conformément aux principes de la gestion des risques exposés dans ce livret.

Détaillons les trois risques exposant un document signé sur la durée de sa vie opérationnelle (la durée de vie d'un document est expliquée dans le focus sur la notion de durée d'archivage) :

1. L'obsolescence technologique

Elle est la conséquence de l'accroissement de la capacité de calcul informatique et qui conduit à rendre possible le contournement de certains algorithmes de signature.

Pour les plus aguerris: les clefs de signature de type RSA sont progressivement passées de 1024 à 2048 bits et les recommandations récentes de l'ANSSI visent à des clefs de 4096 bits pour les prochaines générations de signature (source: « IGC/A - Politique de certification concernant les autorités de certification racines gouvernementales» Anssi - v2.2 https://www.ssi.gouv.fr/uploads/2014/11/igca_pc_v2-2.pdf)

L'accroissement de la capacité de calcul s'apprécie selon deux axes :

- l'évolution des technologies conduisant à la puissance de calcul des nouveaux composants électroniques (processeurs de calcul utilisés par exemple pour le minage des bitcoins).
- l'axe « organisationnel » permettant de faire travailler des milliers d'ordinateurs pour aboutir à un même objectif.

2. L'obsolescence algorithmique

Elle est la conséquence de la recherche fondamentale en terme de rupture d'algorithme. Le SAE permet de reconstituer les signatures en cas de rupture algorithmique. Il offre lui aussi une couverture pour pallier à cette défaillance.

3. La perte de confiance dans le PSCO

Il y a un cas d'école de perte de confiance dans le PSCO à l'origine des identités et signatures.
En 2011, la confiance dans le PSCO DigiNotar créé en 1998 est rompue suite à une faille de sécurité avérée. En quelques jours, la confiance dans les certificats de l'entreprise s'évapore, non seulement pour l'avenir mais aussi pour les certificats déjà émis.
Les procédures de supervision ont considérablement évolué et le risque est maintenant réduit d'avoir un tel incident. Mais l'analyse de risques et la mise en place de procédures appropriées permettront une réaction rapide à ce type d'incident et à ses conséquences.

Il est donc important, comme toujours, de bien choisir son Autorité de Certification ou prestataire de signature et de veiller à ce qu'ils proposent un niveau de confiance suffisant notamment au travers de certifications : ANSSI RGS et/ou eIDAS, entre autres.

EP: éléments de preuve
RV: rapport de validation

1.3 Quels sont les enjeux et les risques juridiques d'une conservation à long terme ?

L'un des risques majeurs a trait à la qualité de la preuve dans le temps. La signature électronique s'appuie sur des certificats dont la validité peut varier dans le temps. Mais aucun certificat n'est a priori valide au-delà de trois ou quatre ans, en tous les cas jusqu'au terme d'un délai de conservation commercial (ex : 10 ans). A défaut (ex : certificat dont la validité n'aurait pas été vérifiée au moment de la signature ou ne pourrait plus l'être si la vérification a lieu au moment de la contestation), le contrat signé pourrait être considéré comme n'ayant jamais existé ou ne valoir que comme commencement de preuve. Il serait alors à corroborer avec d'autres indices.

Le risque est-il le même tout au long de la vie du contrat ? Non. En général, l'occurrence du risque est plus importante dans les premières années qui sont souvent celles où les litiges adviennent (ex : crédit à la consommation). Mais ce crible du risque est avant tout lié au type de document signé et à leur cycle de vie (que ce soit papier ou électronique). Une analyse de risques est donc à prévoir par type de document.

Points de vigilance :

A quoi faut-il penser quand on sait que l'on part sur du long terme ?
Avant tout, il faut prévoir une documentation portant sur la conservation des documents signés sur le long terme (politique d'archivage, conditions d'utilisation, etc.).
Ensuite, il faut déterminer en amont quels seront les éléments et informations qui seront conservés et sous quelle forme, notamment si le document signé est compris dans un fichier de preuve. Il sera primordial dans cette optique de pouvoir faire le lien entre l'identité du signataire et le document signé (ex : fourniture d'une pièce d'identité).
Enfin, les conditions d'accès aux documents signés doivent être claires, transparentes et pérennes dans le temps. Voir fascicule n°2 « Validation et archivage » chapitre 2 Gestion de la preuve fntc_signatureelectronique_ii.pdf (fntc-numerique.com)

POURQUOI RÉALISER LA CONSERVATION À LONG TERME DANS UN SAE ?

2.1 Pour respecter la réglementation actuelle et anticiper la règlementation future :

Une proposition de modification du Règlement eIDAS est en cours au sein de la Commission Européenne. Cette proposition modifiera le périmètre des services de confiance en intégrant la définition suivante concernant le service d'archivage électronique : « a service ensuring long term electronic storage and preservation of electronic document » .
Cette proposition devrait déboucher en 2023 mais le texte peut encore être amené à évoluer. Ainsi, les documents électroniques conservés dans ce service qualifié bénéficieront d'une présomption d'intégrité pendant toute la durée de conservation.

Le respect de la règlementation actuelle permet d'assurer une pertinence juridique face à une pertinence technique : L'article 1366 du Code Civil indique « 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 [c'est le rôle souvent confié à la signature électronique] et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité [c'est le rôle de l'archivage] ».
Il est donc nécessaire d'archiver les documents signés. Car ne pas le faire contrevient à la lecture habituelle (littérale) de cet article et induit des risques probatoires. Les juges ont désormais l'habitude d'analyser les documents électroniques signés et ont développé des réflexes pour appréhender la fiabilité d'une signature électronique.

2.2 Parce que je suis le seul responsable de mes archives et que je dois veiller à ce qu'elles répondent à l'état de l'art (NF Z42-013) en matière d'archivage à long terme

Je dois donc, en tant que propriétaire de mes archives, m'assurer que l'archivage respecte :

- La durée de conservation établie.
- Le maintien de l'intégrité de mes archives : journaux, cycle de vie et traçabilité.
- Le maintien de la disponibilité, de l'accessibilité et de la lisibilité de mes archives.

2.3 Pour m'assurer de la correcte réversibilité de mes données :

La réversibilité est le principe d'extraction d'un système de stockage de tout ou partie des documents qui y sont conservés ainsi que de toutes les métadonnées associées. Elle permet d'éviter la dépendance par rapport à un système en permettant de migrer l'ensemble des documents d'un système vers un autre.

La réversibilité des contenus signés et archivés dans le SAE ne consiste pas simplement à restituer le fichier, mais aussi tous les éléments nécessaires au maintien de la vocation probatoire et de la traçabilité :

- Les preuves archivées avec le document : preuves de validation, authentification, etc.
  (voir fascicule 2 : §2.3 Les constituants de la preuve p.19)
- Les preuves liées à l'archivage : journaux de cycle de vie et des évènements.
- Les attestations liées à l'archivage afin de démontrer par exemple l'élimination d'un document archivé.

Points de vigilance : les solutions de signatures proposent de conserver les documents signés. Le responsable des archives doit absolument s'assurer des points suivants :

- Qui archive quoi ?
- Qu'est-ce qui est conservé ?
- Comment cela est-il conservé ?
- Combien de temps ? (cf. fascicule 2 chapitre 3)

Comment gérer la durée de conservation face aux règlement eIDAS vs RGPD ?

Tant qu'**une durée de conservation est justifiée**, et ce même si celle-ci s'étend au-delà de ce que préconise le RGPD (par exemple des données de facturation conservées 10 ans), **cette durée pourrait être considérée comme conforme aux finalités probatoires reconnues par les deux règlements** (sous réserve de respecter les exigences de la CNIL).

COMMENT CONSERVER SUR LE LONG TERME ?

Dans un projet d'archivage électronique, la pérennité des documents est un des points importants à prendre en compte.
Les formats des fichiers qu'un système d'archivage électronique accepte doivent donc être analysés précisément pour satisfaire ce critère : le contenu du document doit être accessible et lisible pendant toute la durée de conservation.

Le format est un moyen d'obtenir notre triptyque gagnant : pérennité, accessibilité et lisibilité.

L'orientation vers l'utilisation de formats ouverts et standardisés s'impose. Mais la multitude de formats existants et la diffusion de formats propriétaires ne facilitent pas la tâche. La politique d'archivage de l'entreprise doit prendre en compte ces situations spécifiques liées à ses activités et à son environnement.

3.1 Le rôle du format de l'archive :

Qu'est-ce qu'un format ? Le format de fichier désigne la nature d'un document informatique qui permet de déterminer le logiciel correspondant à sa lecture. Ce principe permet ainsi d'échanger des données entre différents logiciels informatiques.

Un fichier dispose d'une extension en 3 lettres en général indiquant le format. Dans un projet d'archivage électronique, dont l'un des objectifs est la pérennité de l'information et sa lisibilité dans le temps, la question de la préservation du format d'origine et la capacité de relecture des données sont centrales.

Contrôle des formats en entrée :
« Le SAE peut contrôler ou pas les formats des archives versées. Si un contrôle est effectué et si le format identifié ne fait pas partie de la liste établie, Il y a trois possibilités :

- Le versement est refusé
- Le format est soumis à approbation
- Le fichier est automatiquement transformé dans un format pérenne. La mise en place de ce dernier cas est délicate dans le sens où le SAE prend la responsabilité de la transformation. Or l'intégrité du document n'est pas conservée au sens informatique du terme (le fichier en entrée et le fichier transformé n'ont pas la même « empreinte », ils sont différents).

Si aucun contrôle n'est effectué, il y a risque, lors de la restitution, de ne pas pouvoir accéder au contenu. Toutes ces décisions relèvent de décisions d'entreprise prenant en compte les situations spécifiques liées aux types d'activités. » (Les Mémos du CR2PA, Guide Recommandations les formats d'archivage, 2014)

3.2 La conversion de format durant le cycle de vie :

« Pour des documents dont la durée de conservation est importante (plusieurs dizaines d'années), il n'y a pas de garantie que le format utilisé soit toujours lisible durant toute la conservation du document. Pour se prémunir contre cela, il peut être nécessaire de mettre en place un processus de conversion vers un nouveau format considéré comme plus pérenne. Là encore, l'intégrité, au niveau informatique, n'est pas conservée. » (Les Mémos du CR2PA, Guide Recommandations les formats d'archivage, 2014)

La norme NF Z42-013, au paragraphe « 6.4.3 Conversion des formats des documents durant la conservation » exige que « L'évènement de conversion de format doit être journalisé » et recommande que l'événement journalisé intègre « l'empreinte de l'objet numérique converti ainsi que la référence de l'objet numérique dont il est issu. »
« Les fichiers au format d'origine et au format converti doivent être conservés. L'OAIS (ISO 14721:2012) parle de migration/transformation/émulation [de formats] pour garantir la continuité d'accès au contenu. » (Les Mémos du CR2PA, Guide Recommandations les formats d'archivage, 2014)

Quelques suggestions pour débuter :

- Conserver le format source et les ressources de lecture du format source (l'OS et le logiciel qui tourne dans l'OS + les licences d'utilisation). L'accès aux données d'un fichier peut s'avérer impossible si son format n'est pas adapté au logiciel, au système d'exploitation et à l'ordinateur. Conserver également les preuves liées à l'archivage : journaux de cycle de vie et des évènements.
- Convertir dans des formats pérennes (normes, standards) : un fichier au format .doc ou .xls a une durée de vie moyenne de 5 ans. Au-delà, le format devra être converti afin de garantir la lisibilité des données car le cycle de vie des supports et formats électroniques ne coïncide pas avec les durées légales d'archivage des documents.
- Toutes les opérations de conversion (dans un autre format) et de migration (vers un autre support/serveur) doivent être notifiées dans les journaux afin de garantir l'intégrité des archives.

Pour aller plus loin, la norme NF Z42-013 vous indiquera les bonnes pratiques à mettre en place.

Comment qualifier et piloter l'outil de migration ? S'assurer de son bon paramétrage ? Il faut auditer le contrat passé avec le Tiers Archiveur et déterminer comment est garantie la pérennité des supports de conservation. Le tiers archiveur doit disposer des expertises et des moyens technologiques pour éliminer le risque d'une perte ou d'une corruption de données.

Conclusion

L'obsolescence des formats est un danger parfaitement maîtrisable à condition d'être mesuré et anticipé. Le Système d'Archivage Electronique à vocation probatoire apparaît comme la solution la plus sûre pour répondre à cette problématique et concilier sur le long terme intégrité, authenticité et fiabilité des documents archivés.

3.3 Les techniques cryptographiques pour maintenir l'intégrité

La conservation à long terme repose également sur le maintien de l'intégrité du document qui se matérialise par une « marque » d'intégrité (signature électronique, cachet électronique, horodatage ou empreinte). Il existe donc différentes méthodes pour garantir l'intégrité dans le temps, celles-ci relèvent essentiellement de la cryptographie. Aujourd'hui, sont principalement utilisées les méthodes de sur-signature et/ou d'archivage. A ce titre, on peut noter d'une part que pour les signatures et cachets qualifiés, le Règlement eIDAS actuel énonce : « Un service de conservation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique. »

L'extension de la fiabilité de la signature est aussi appelée « sur-signature ». Il s'agit d'étendre la fiabilité de la signature en prolongeant la validité du certificat utilisé soit en appliquant une nouvelle signature/cachet ou un horodatage qualifiés.

D'autre part, la norme NF Z42-013 met l'accent sur la journalisation comme moyen d'intégrité : « 4.6.3 Journalisation Objectif : Être en capacité de contrôler et démontrer que les objets numériques sont restés intègres durant tout leur cycle de vie et tracer des opérations essentielles effectuées sur les archives électroniques. § 1 : Le service d'archivage électronique doit démontrer la préservation de l'intégrité des objets numériques contenus. À ce titre, la fonction de journalisation est essentielle dans un SAE. »

Le règlement « eIDAS » évoque la notion de conservation de la signature ou cachet mais pas celle du document. Or, archiver une signature et archiver un document sont deux choses différentes : l'habitude de penser les deux ensemble venant du papier peut être trompeur, les méthodes d'archivage ainsi que les dispositions légales diffèrent. Néanmoins, le SAE permet d'archiver les deux au sein du même système.

Il est d'ailleurs intéressant de constater que la conformité à la norme NF Z42-013 fait partie du référentiel de certification du service de confiance qualifié de conservation des signatures et cachets électroniques qualifiés. Autrement dit, il est possible de faire de la conservation qualifiée au sens eIDAS avec son SAE conforme à la norme ou certifié NF 461. Mais il n'est pas possible pour les prestataires eIDAS utilisant uniquement la technologie de sur-signature de prétendre disposer d'un service d'archivage électronique au sens de la norme française

CONCLUSION

La pratique nous démontre l'importance de l'archivage à vocation probatoire de nos documents non signés. Il est donc logique d'en faire de même pour nos documents signés dans un outil capable à la fois d'archiver le document et de conserver la signature. Aujourd'hui, la nécessité de maintenir l'intégrité des documents numériques dans le temps, soient-ils signés ou non n'est plus à prouver. En pratique, que ce soit avec un SAE en interne ou bien externalisé chez un Tiers-Archiveur, la conservation à long terme pourra être assurée au moyen de la conformité à la norme puisque les dispositions portant sur la conservation dans le règlement eIDAS actuel ne prennent pas encore en compte le triptyque gagnant (pérennité, lisibilité, accessibilité) quel que soit le type de document. Gageons que les modifications du Règlement eIDAS mettront plus en avant ce triptyque dans le cadre du service d'archivage qualifié, trait d'union entre la pratique des archivistes, du juriste et du Tiers-Archiveur.

REMERCIEMENTS

Comité de rédaction :

Agosti Pascal, Cabinet Caprioli.
Bonnefous Jean-Mathieu, Orano.
Delion François, Bouygues Telecom.
Frézier Amélie, Cecurity.com.
Gasch Stéphane, Chambersign.
Jubin Nathalie, Engie.
Pasquier Chantal, Egis.
Pichat Estelle, Systra.
Repiton Dumollard Sophie, Artelia Group.
Vincent Florent, Thales Group.

Délégation Générale
14 rue de Bruxelles
75009 Paris

infos@fntc-numerique.com
fntc-numerique.com

Contact :
75 Rue de Lourmel
75015 PARIS

contact@cr2pa
www.cr2pa.fr

Octobre 2022