Projet ICare

Archivage électronique (2) :

La pratique de l'archivage électronique

Référence : ICARE/CAB/TPC/DOC_4/v1
Type : Note de travail
Diffusion : Publique

Date : 06/05/2002
Titre : **ICare – Archivage électronique (2) : La pratique de l'archivage électronique**

Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
Ce document décrit une pratique de l'archivage électronique conforme aux exigences de la conservation juridique.

Table des matières

1 Préambule

Une étude précédente contenue dans un document " *Archivage électronique (1) : les principes de la conservation juridique"* de référence ICARE/CAB TPC/DOC_4/v1 rapprochait les enjeux et exposait les besoins de l'archivage technique et de la conservation juridique. Le présent document décrit une pratique de l'archivage électronique conforme aux exigences de la conservation juridique.

Selon le rapport du Conseil d'Etat : prétexter la forme électronique d'un acte ne permettra pas de le répudier. La preuve sera administrée à partir de la fourniture du message électronique et de sa signature électronique préalablement archivés. L'archivage devra se dérouler dans de bonnes conditions de fiabilité "certifiées" par un Tiers spécialisé : "*si le document électronique est accompagné d'un certificat répondant à certaines exigences, délivré par une autorité de certification accréditée, la fiabilité de la signature et la conservation durable du document signé (si le certificat a aussi cet objet) sont présumés*".

L'hypothèse traitée dans la présente étude est celle des écrits sous forme électronique, formes dématérialisées d'actes sous seing privés. La préparation de l'archivage électronique supposerait naturellement une étape préalable de dématérialisation documentaire si les actes considérés étaient originellement sur support papier[1].

En pratique, l'archivage électronique aux fins de conservation juridique présente quatre phases décrits dans les développements ci-dessous :
- la mise en archive où sera identifié et préparé ce qu'il convient d'archiver (1.),
- l'éventuelle intervention d'un tiers archiveur (2.),
- le stockage à proprement parler (3.),
- la restitution des archives.

1. La mise en archive

L'archivage intervient dans une phase dite *post-transactionnelle*. Le message signé passe alors concrètement à l'étape de l'archivage électronique, de telle façon qu'il devra être possible ultérieurement de le ressortir, on dira de le *désarchiver*, et de "rejouer" la signature électronique afin d'en vérifier la valeur juridique au moment où l'utilisateur l'avait en mains. A noter que l'archivage peut être le fait d'au moins deux utilisateurs, le destinataire du message ou l'émetteur signataire.

1.1 La détermination des éléments à archiver

Curieuse question que celle de dresser la liste des éléments à archiver. Après tout, il s'agit d'archiver un message électronique. Le fait qu'il soit signé nécessite cependant qu'on envisage l'éventualité d'archiver de concert d'autres éléments.

1.1.1. L'archivage de l'écrit électronique et de sa signature

Le rapport du Conseil d'Etat montrait dans le rapport précité comment signature, archivage et preuve sont liés. Le Conseil envisageait le dispositif suivant : "*lorsqu'un document électronique assorti d'une signature électronique est présenté pour établir la preuve d'un acte, il ne saurait être contesté au seul motif qu'il se présente sous forme électronique ; il tient lieu d'acte sous seing privé dès lors qu'il est assorti d'une signature*

[1] La norme NF Z42-013 envisage également l'archivage électronique des documents dont la version initiale est sur support papier et qui ont été numérisés, dans son paragraphe 7.2. : *Les procédures pour l'enregistrement, le stockage et la gestion des documents doivent être écrites dans le dossier technique et comprendre un certain nombre d'informations précises. Le manuel utilisateur doit comporter toutes les informations concernant les modifications autorisées avant le stockage de ces messages, en particulier les opérations destinées à transformer le document dans un des formats prévus par la norme. Dans le cas des documents électroniques, les contrôles doivent porter au moins sur la quantité de documents produits aux reçus, leur conformité aux formats prévus dans la norme, l'existence des codifications dans des fichiers contenus dans le système parce que les messages comparent des codifications.*

fiable et qu'il est conservé avec celle-ci de façon durable". L'écrit sous forme électronique, hypothèse de travail dans lequel nous nous sommes placés, montre des garanties d'identification et d'intégrité. Dans la grande majorité des cas, l'acte sous seing privé électronique comportera une signature électronique, sécurisée ou non, qui assurera d'office l'identification et l'intégrité recherchées. Aussi faudra-t-il archiver l'écrit électronique et sa signature. Ce qui ne devrait pas poser de difficulté en pratique si on s'en remet aux protocoles techniques qui réunissent dans un même fichier le message électronique et sa signature[2].

Par contre, après une période plus ou moins longue d'archivage, lorsqu'il sera désarchivé, l'acte électronique ne pourra servir de preuve que si la signature électronique est valide[3]. Il faudra alors vérifier la signature, ce qui nécessite l'emploi du certificat électronique[4]. Le certificat sera plus facilement disponible... s'il a été, par la même occasion, archivé[5] !

1.1.2. L'archivage du certificat électronique

Placé au centre de la garantie d'identification, le certificat fait l'objet de mesures de conservation spécifiques pendant toutes les étapes de son cycle de vie. Le certificateur[6] le diffuse dès sa création tout en gardant une copie. Créé pour une certaine durée de temps, de l'ordre de 16 à 24 mois, le certificat doit être conservé non seulement jusqu'à la fin de sa durée de validité, mais encore à l'issue de cette période, jusqu'à la fin du cycle de vie du message signé, c'est-à-dire pendant la durée de conservation légale. Sujet à conservation, le certificat est l'aboutissement d'une série de traitements électroniques de certification.

Le 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 pose dans son article 6.II une obligation pour le certificateur d'établir un système de conservation dont l'utilité est précisée par le point l) de l'article précité. Le certificateur doit utiliser des systèmes de conservation des certificats électroniques garantissant que *:*

> - *l'introduction et la modification des données sont réservées aux seules personnes autorisées à cet effet par le prestataire ;*
> - *l'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;*
> - *toute modification de nature à compromettre la sécurité du système peut être détectée".*

De façon plus générale, le point k) de l'article stipule qu'un prestataire de services de certification doit satisfaire à certaines exigences comme "*conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique*". Parmi les informations à conserver en priorité pour un système qui est le point central du dispositif d'identification, celles qui correspondent à l'identité des personnes ainsi que les pièces justificatives présentées. Le point m) de l'article le rappelle : *vérifier [...] la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité*".

1.1.3. Le non-archivage de la clé privée

Enfin pour élargir le débat, conserver le certificat électronique, c'est conserver la clé publique qui y est contenue. Par opposition, la clé privée ne doit pas être conservée… par quelqu'un d'autre que son propriétaire. Parmi les

---

[2] C'est ce qui est prévu par le protocole PKCS #7 de l'IETF.

[3] Naturellement la validité de la signature électronique s'apprécie au jour de son "apposition" sur le message électronique et non au jour du désarchivage.

[4] Il est rappelé que la signature électronique est chiffrée et que sa vérification nécessite un déchiffrement préalable (le tout étant réalisé par un "dispositif de vérification de signature"). Le déchiffrement est opérée grâce à la clé cryptographique publique contenue dans le certificat électronique. Un prestataire de service de certification a attesté par ce certificat que la clé publique est celle du signataire.

[5] Au risque de complexifier les choses, on peut ajouter qu'il faudrait conserver également la Politique de Certification (cf. partie 1) sans laquelle il est n'est possible de savoir dans quelles conditions, selon quelles modalités et à qui le certificat a été délivré. En ce sens, "Comprendre la différence entre signature électronique et numérique" par PINKAS Denis. Le texte a été diffusé sur le Web et par écrit (par exemple, Actes de la conférence Trusting Electronic Trade'99 à Marseille).

[6] L'appellation correcte est *prestataire de service de certification électronique* (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.

critères qui caractérisent la *signature électronique sécurisée* dans le décret d'application de l'article 1316-4, on lit que la signature est "*créée par des moyens que le signataire puisse garder sous son contrôle exclusif*[7]". Le considérant 18 de la directive européenne du 19 décembre 1999 rappelait le principe : "*le stockage et la copie de données afférentes à la création d'une signature* [c'est-à-dire la clé privée] *risquent de compromettre la validité juridique des signatures électroniques*".

Le risque est potentiel si parmi les différentes options possibles, le signataire a choisi de faire tirer le bi-clé par le certificateur. Le certificateur dispose ainsi immédiatement de la clé publique et acquiert la certitude qu'elle correspond à la clé privée. La clé privée doit être transmise par le certificateur, qui ne doit pas en garder copie, au signataire par une voie sécurisée. En réponse à cela, le décret d'application de l'article 1316-4 établit que "*dans le cas où il fournit au signataire des données de création de signature électronique, garantir la confidentialité de ces données lors de leur création et s'abstenir de conserver ou de reproduire ces données*[8]".

1.2 Les modalités : archivage interne ou externe

A l'issue d'un envoi de messages sécurisés dans la phase transactionnelle, on ne peut faire moins que de procéder à un archivage sécurisé. Archiver en interne semble la solution la plus évidente est aussi la plus discutable. En effet, en cas de problème interne ou de litige avec les partenaires aux échanges électroniques, comment s'assurer que le message sur lequel on raisonne est bien le message considéré et non une version dérivée ou rectifiée ? Comme le message est resté sous son contrôle de l'utilisateur, l'utilisateur a tout loisir de le modifier. A moins qu'on ait pris une sorte d'instantané du message qui puisse donner toutes les garanties lorsque c'est nécessaire.

Pour alléger les systèmes d'information chargés de messages électroniques post-transactionnels et pour renforcer la confiance et la sécurité, on pourra envisager de faire intervenir un archiveur distant, encore appelé t*iers archiveur*. La distance entre l'utilisateur et l'archiveur entraîne de nouveau l'emploi ou la poursuite des échanges électroniques. L'idée consiste à faire appel à un tiers archiveur extérieur ou à un prestataire à valeur ajoutée offrant une fonction d'archivage en liaison avec la certification électronique. Dans ce cas, l'utilisateur réunit tous les éléments à archiver, messages électroniques, signatures électroniques, clés de chiffrement s'il y a lieu, certificats électroniques et les expédie via des moyens de télécommunications à l'archiveur. Celui-ci à réception effectue plusieurs traitements pour vérifier la permanence des garanties de sécurité pendant le transport électronique entre son client et lui :

- il vérifie que l'émetteur est un client,
- il contrôle que les éléments télétransmis sont arrivés à bon port et en bon état,
- il accuse réception au client des éléments susceptibles d'être archivés en l'état.

A noter que l'entité qu'on appelle par commodité *tiers archiveur* n'est pas réellement un "tiers" au sens de la certification électronique comme on verra ci-dessous, mais plutôt un archiveur distant. Il est à son tour un utilisateur de la certification.

La pratique précédente semble la plus évidente en théorie. Le Tiers Archiveur intervient dans un processus d'échanges électroniques qui se poursuivent vers lui après que la phase transactionnelle des messages électroniques soit terminée. L'inconvénient est qu'il équivaut à transférer par voie de télécommunications un volume important de données, générateur de risques techniques et de coûts non négligeables. D'où la tentation de revenir à un archivage en interne mais faisant appel à une certification externe. L'utilisateur se protégera en faisant appel à un témoin sur lequel il n'a pas de prise directe : le certificateur. Lorsque les archives sont chez l'utilisateur final, émetteur ou destinataire des éléments électroniques archivés, le risque existe que, volontaire ou involontairement, les éléments archivés soient modifiés, corrigés, altérés ou détruits. Au moment de l'archivage, les messages électroniques et les autres éléments ont terminé leur cycle d'utilisation normale. C'est le contenu du message à ce *moment t* qu'il faut retenir comme archive. Ici apparaît la notion de temps. Tout changement de contenu qui surviendrait après ce moment de leur cycle de vie ne serait que manipulation des archives. L'idée consiste dans ce cas à faire reconnaître l'état des messages à un moment déterminé par un tiers objectif qui dans ce cas est... un *tiers horodateur*[9].

[7] On rappelle que la clé privée est qualifiée par le décret (art.1) de *données de création de signature électronique.*

[8] article 6-II-i du Décret.

[9] L'*horodatage sécurisé* est actuellement étudié par un groupe de travail de même type (entre l'association IALTA et le Conseil Supérieur de l'Ordre des Experts-Comptables) que celui qui a publié le Guide de l'archivage sécurisé (voir INFRA).

Cette dernière constatation est intéressante au niveau de la théorie de la certification. Il semble nécessaire de distinguer besoin et service. Tel besoin de l'utilisateur n'est pas rempli forcément par le service de même dénomination chez un tiers de confiance. Comme on le voit:

- le besoin d'archivage de l'utilisateur peut être satisfait en externe grâce au service d'un tiers archiveur ;
- le besoin d'archivage de l'utilisateur peut être satisfait en interne grâce au service d'un tiers horodateur.

2. L'éventuelle transmission à un archiveur distant

A proprement parler, le Tiers Archiveur n'est pas une *Tierce Partie de Confiance*, il ne participe pas aux procédures de certification, il est comme l'émetteur ou le destinataire du message, un utilisateur de signature électronique. En effet, l'ensemble des éléments à archiver doit lui être envoyé dans des conditions telles que le niveau de sécurité des échanges électroniques soit maintenu.

La norme Z 42-013 indique que les réseaux de télécommunications peuvent être utilisés. Mais *parce que le transfert des documents entre le prestataire et l'organisme en entreprise s'effectue par le moyen de lignes de télécommunication publique, il est obligatoire de prévoir des mécanismes d'authentification et de sécurité*[10]. On retrouve ici le même couple de garanties sécuritaires que dans la signature électronique : authentification et intégrité. Mais alors que dans la signature, l'authentification prenait le pas sur l'intégrité, dans l'archivage, c'est l'intégrité qui est prioritaire.

2.1. Le Guide de l'archivage sécurisé et le tiers archiveur

Les conditions et modalités de l'archivage technique ne sont pas neutres au regard des effets juridiques. Cette constatation avait déjà été faite par le Conseil Supérieur de l'Ordre des experts comptables dans un rapport publié en 1998 sur *L'Archivage Electronique*[11]. Pour étendre cette réflexion aux échanges électroniques sécurisés par des signatures électroniques, l'association IALTA France et le Conseil Supérieur ont créé un groupe de travail commun qui a publié en juillet 2000 un *Guide de l'Archivage électronique sécurisé*. Les travaux du Groupe de travail ont été grandement confortés par les membres de l'Association des Professionnels de la Gestion électronique des documents (APROGED) permettant d'implémenter dans le processus la norme Z 42-013 sur l'archivage électronique.

Les recommandations finales du groupe de travail commun, outre IALTA France, le Conseil Supérieur (OEC) et l'Aproged, sont parrainées par Edificas (organisation EDI des experts comptables), le Conseil National des Greffiers des Tribunaux de Commerce, la Chambre Nationale des Huissiers de Justice, le Conseil supérieur du Notariat, le CIGREF, la Caisse Nationale d'Assurance maladie, l'Association française de l'audit et du conseil informatique et la Compagnie Nationale des Commissaires aux Comptes[12].

Dans la phase précédente, l'utilisateur a préparé la mise en archive. A cette fin, il a récupéré dans le système de stockage, le message à archiver et sa signature électronique. En principe, la signature électronique devrait figurer dans le message ; on se souviendra néanmoins que la signature peut avoir voyagé indépendamment du message auquel elle se rapporte. Enfin il faut nécessairement archiver le certificat électronique qui apporte simultanément la clé publique nécessaire au rejeu de la vérification et la garantie du certificateur que la clé publique appartient à un bénéficiaire, porteur par ailleurs, de la clé privée correspondante et qui a servi à chiffrer la signature. Ces éléments forment au sens du Guide un *lot* qui peut alors être envoyé à l'archiveur.

Le lot à archiver sera envoyé dans des conditions telles que le niveau de sécurité des échanges électroniques perdure. L'archiveur qui recevra les éléments devra pouvoir identifier son client, besoin d'authentification. La mission de l'archiveur est de conserver les informations dans l'état où il les a reçues pour pouvoir les restituer à l'identique ultérieurement. Ce qui suppose en amont qu'il ait bien reçu les informations que l'utilisateur a voulu lui confier, d'où un besoin renforcé d'intégrité des informations. En un mot, le lot des éléments à archiver fera l'objet d'une signature électronique. Il doit cependant être bien entendu que cette signature n'est apposé qu'à titre purement technique uniquement pour sécuriser l'envoi électronique.

---

[10] Cf. Chapitre 10 de la norme.

[11] Rapport disponible aux éditions du Conseil Supérieur de l'Ordre des Experts-Comptables, Paris.

[12] Le rapport est en téléchargement libre sur les sites Web des organisations ci-dessus citées.

2.2. Les règles professionnelles du tiers archiveur

Le droit interne encadre-t-il la profession de tiers archiveur ? On peut se demander si les tiers archiveurs sont touchés par la législation sur la signature électronique. En effet, le décret d'application de l'article 1316-4 définit le *prestataire de service de certification électronique* dans son article 1 comme "*toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique"*. Le tiers archiveur ne délivre pas de certificats, il les utilise. Par contre, il fournit un service. Mais en "matière" de signature électronique ou en "liaison[13]" avec la signature électronique ?

A défaut de base légale claire et de dispositions précises, la norme Z 42-013 préconise la voie contractuelle en identifiant dans son chapitre 10 les principes à contractualiser en matière de contrat client-archiveur, de contrat de sous-traitance et d'agréments d'un prestataire de service.

2.3. La nécessité de maintenir l'intégrité pendant le transfert de l'archive

Comme il a été exposé plus haut, l'archivage qui se prétend *sécurisé*[14] doit assurer en priorité un niveau optimal d'intégrité de l'écrit électronique pendant les différentes étapes de son cycle de vie sans négliger d'identification de la source du document.

2.3.1. L'intégrité et le changement de support

Les grandes étapes du cycle de vie de l'écrit électronique, création - échange - conservation, peuvent se décliner en de nombreuses sous-étapes, en particulier pour des besoins de changement de support technique de l'écrit électronique. Dans ces points d'articulation, le maintien de l'intégrité doit être particulièrement surveillé : elle doit être garantie avant et après le changement de support. Mais le contenu du message ne reste le même que si l'intégrité perdure au moment du changement de support.

2.3.2. L'intégrité et les données de service

Le maintien de l'intégrité suppose qu'aucune donnée ou information nouvelle ne soit adjointe au corps de l'écrit électronique. Cependant il est nécessaire de considérer les données de services adjointes à des fins purement techniques. La question s'est posé au groupe de travail qui a produit le Guide de l'archivage. Le groupe a raisonné à partir de la notion de *lot* regroupant les éléments à archiver. En effet, l'archiveur doit rester neutre par rapport aux informations archivées. Si on considère que le message incorporant sa signature voyage d'un côté, le certificat peut voyager d'un autre. Dans ce cas, l'archiveur ne dispose d'aucun moyen de savoir que le second message est d'une part, un message électronique et d'autre part, qu'il se réfère à un message précédent. Dans le monde réel, l'archivage se réalise par stockage de boites en carton rassemblant les éléments à conserver, sans que l'archiveur sache nécessairement ce qui est dedans. Cette constatation renvoie à un niveau moyen de confidentialité facile à justifier. D'autre part, les informations à archiver ou les lots qui les contiennent peuvent être chiffrés. Le lien entre message signé et certificat doit nécessairement être géré par le client lui-même. Le client devra peut être encore gérer d'autres spécificités. Par exemple, si le lot à archiver comprend plusieurs messages signés. Le Guide de l'archivage décrit toutes les informations de service qu'il sera nécessaire d'ajouter aux lots à ces fins. Aussi les éléments à envoyer à l'archiveur seront regroupés en lot qui seront scellés par une signature électronique pour garantir la sécurité de la transmission.

Au total, il faut considérer que les données techniques et autres données de service lorsqu'elles sont parfaitement documentés et traçables ne remettent pas en cause l'intégrité du de l'écrit électronique.

[13] La Directive européenne définit le certificateur comme "toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques (art.2).

[14] Le précédent technique et juridique de la signature permet de définir la *sécurisation* comme étant la caractéristique d'une chose ou d'une procédure présentant des garanties de sécurité, telles que (selon les cas) l'identification, l'authentification, l'intégrité, la non répudiation, la confidentialité, la mise en œuvre de ces garanties étant favorisée ou fournie par un tiers de confiance spécifique. La loi reconnaît qu'une signature électronique peut être *sécurisée* (décret d'application de l'article 1316-4 du Code Civil).

3. Le stockage de l'archive

3.1. La localisation de l'archivage

Une circonstance de l'opération quelquefois négligée est la localisation de l'archive. Après tout, ce qui est stocké l'est dans une perspective potentielle de stockage et de réexploitation. En conséquence, il faut bien savoir dans quel endroit l'archive repose.

L'archivage a peut être réalisé chez un tiers archiveur. Après réception du lot à archiver et vérification de la signature électronique du lot, le tiers archiveur a pu stocker les éléments. Pour le reste, tout dépend du professionnalisme de l'archiveur, du respect de la déontologie et de l'état de l'art. L'inconnu est dans la manière dont l'archiveur assure concrètement l'intégrité de la conservation. C'est de nouveau vers les normes techniques qu'on peut se tourner pour fournir un cadre d'organisation, la norme Z 42-013 à laquelle s'est référé le groupe de travail du Guide ou la norme ISO 15489 pour faire plus général[15].

Pour l'entreprise qui décide d'archiver elle-même, le lieu sera situé habituellement… dans les locaux de l'entreprise. Cependant il peut en être autrement pour certains documents. La facture qui deviendra électronique par la grâce de la Directive 2001/115 fera l'objet à l'occasion de la transposition dans le droit interne français d'une obligation générale de conservation. La Directive insiste sur cette obligation générale dans son article 2 (3-d) : "*tout assujetti doit veiller à ce que soient stockées des copies des factures émises par lui-même, par son client ou, en son nom et pour son compte, par un tiers, ainsi que toutes les factures qu'il a reçues*". Pour la localisation du stockage, la règle définie par la directive est loin de ce qui nous occupe dans la présente étude, parce qu'elle est de nature géographique et non de nature technique. Mais il s'agit d'un cas de figure qu'on peut rencontrer : une obligation de localisation de la conservation de l'écrit électronique souvent limitée à l'hypothèse d'échanges électroniques transfrontalières. Il en va ainsi dans les cas suivants :

- pour les assujettis ayant choisi un lieu de stockage situé en dehors de leur territoire, l'Etat peut imposer l'obligation de déclarer le lieu de stockage ;
- pour les assujettis du territoire dont le lieu de stockage n'est pas effectué par une voie électronique garantissant un accès complet et en ligne, l'Etat peut imposer l'obligation de stocker à l'intérieur du pays.

La directive crée un droit d'accès aux factures stockées par voie électronique dans un autre Etat membre :

> *"lorsqu'un assujetti stocke les factures qu'il émet ou qu'il reçoit par une voie électronique garantissant un accès en ligne aux données et que le lieu de stockage est situé dans un Etat membre autre que celui dans lequel il est établi, les autorités compétentes de l'Etat membre dans lequel il est établi ont (…) un droit d'accès par voie électronique, de téléchargement et d'utilisation en ce qui concerne ces factures dans les limites fixées par la réglementation de l'Etat membre d'établissement de l'assujetti et dans la mesure où cela lui est nécessaire aux fins de contrôle".*

De façon générale, la norme ISO 15489 sur le Records Management développe le thème du suivi de la localisation :

> *"Il est recommandé de documenter les mouvements de documents afin de garantir que les articles puissent toujours être localisés en cas de besoin. Il est admis que les outils de traçabilité révèlent l'identifiant de l'article, son titre, la personne ou l'entité qui le détient et la date du mouvement. Il est recommandé que le système enregistre la sortie des documents, leur communication entre deux personnes et leur retour à leur adresse de « résidence » ou de stockage, de même que leur élimination ou leur versement à une organisation extérieure habilitée à les recevoir, y compris une institution d'archives".*

[15] Les normes Z 42-013 et ISO 14859 sont plus complémentaires que concurrentes. La Z 42-013 ne traite pas des problèmes de gestion des documents (records management). S'il est nécessaire de traiter ces problèmes, par exemple la création d'un plan de classement, elle recommande au concepteur de l'application d'utiliser les spécifications contenues dans la norme ISO - DIS 15489 (records management). Toute la différence entre les deux normes réside dans l'intitulé anglais de "records management". Selon la traduction de l'AFNOR, ces termes désignent les documents considérés dans leur dimension de preuve, par opposition à "documents" (qui ne prend en compte que leur contenu informatif) et à "archives" (qui vise la portée historique).

3.2. Les opérations d'archivage et leur traçage

Selon la norme Z 42-013, une description détaillée des processus d'écriture des éléments à archiver ainsi que des informations nécessaires à l'indexation de ceux-ci doit être incluse dans le dossier de description technique du système d'archivage. L'enregistrement des documents électroniques qui doit se faire de façon purement séquentielle sur les supports de stockage. Aucun espacement enregistré ne doit être laissée entre de documents successifs. Au minimum, le système doit, pour chaque enregistrement de documents :

- *noter la date et lors de l'enregistrement de celui-ci dans l'en-tête du fichier ou à défaut dans l'historique de fonctionnement du système ;*
- *vérifier que l'enregistrement des documents sur le support d'archivage est correct, en particulier grâce aux codes de détection et de correction d'erreurs des dispositifs d'écriture ;*
- *confirmer que le système d'indexation a identifié le nouvel enregistrement.*

La norme qui préconise l'utilisation des disques WORM est particulièrement précise quant au mode opératoire des inscriptions portées sur les disques portées à titre définitif[16] et qui assure ainsi une intégrité non-discutable.

3.3. L'intégrité pendant la conservation du document

Les préconisations des normes techniques tendent à maintenir un niveau d'intégrité maximal pendant l'archivage. Il peut arriver que pour des besoins ou des raisons diverses, les éléments archivés viennent à être modifiés. La modification doit advenir évidemment d'une personne ayant qualité à le faire. Selon ISO 15489, il est nécessaire qu'un document soit protégé contre les altérations abusives : "*les principes et les procédures techniques précisent quels ajouts ou annotations pourront être portés sur* [l'archive] *après sa création, dans quelles circonstances et par qui*". Toute trace d'annotation, d'ajout ou de suppression sur une archive sera enregistrée. Naturellement on peut s'attendre à ce qu'un contrôle d'intégrité entre l'élément entrant et l'élément sortant de l'archivage donne un résultat négatif. C'est bien la traçabilité qui prendra alors le relais pour montrer que l'archivage, éventuellement l'archiveur, n'a pas failli.

3.4. La destruction de l'archive

Dire qu'un écrit électronique change de support n'est qu'une vision de l'esprit. La réalité technique montre que dans la plupart des cas, l'écrit électronique est dupliqué sur le nouveau support et devient l'*écrit actualisé*, tandis que l'exemplaire (la copie ?) précédente subsiste et dépérit. Le procédé aboutit à la multiplication à l'envi des copies d'un même écrit électronique. D'où la tentation de procéder à un utile nettoyage des supports et moyens de stockage en détruisant les copies (les *originaux* ?). Ce qui constitue, bien évidement une attente importante autant que définitive à l'intégrité.

Au plan juridique, on ne peut pas ne pas gérer le cas de la destruction de l'écrit électronique ou de son archive. La norme française Z 42-013 considère avec attention cette problématique pour les écrits électroniques dans son point 8.5. et réclame une attestation de destruction[17] : pour les documents électroniques[18], produits par numérisation ou directement produits sous forme électronique[19] et, "*après autorisation du propriétaire de ceux-*

[16] Ainsi la norme précise que : *une protection logicielle doit être mis en vente afin d'éviter tout risque dans dédommagement des documents déjà stockés au moment de l'écriture de nouveaux documents sur les supports. Pour réaliser des opérations de stockage des documents électroniques, seuls des supports WORM sont admis (...) Les procédures décrites ci-dessus doivent s'accompagner d'attestation lors de la mise en œuvre. Celles-ci doivent être conservés pendant la même durée que les documents qu'elles attestent, soit sur support papier, soit sur support optique de type WORM.*

[17] *Destruction : action d'éliminer ou de supprimer des documents, de façon irréversible (Définition ISO 15489).*

[18] *Selon cette norme, un "document" est un "ensemble composé d'un support et des informations enregistrées sur ce support" et un "document électronique" "un document qui peut résulter soit d'un processus de numérisation de l'information initialement sur papier, sur micro-forme, soit d'un processus informatique*.

19 En tant que norme de l'archivage de Gestion Electronique de Documents (GED), la norme Z42-013 s'intéresse également à la numérisation de document sur papier (par scanage) et à la substitution des fichiers électroniques. Dans le cas des documents sur support papier, après autorisation du propriétaire de ceux-ci et après constatation de la fidélité des images numériques par rapport aux documents originaux correspondants, l'opérateur, qui réalise la destruction de ces documents doit produire une attestation de destruction de documents, après la destruction de ceux-ci.

ci, l'opérateur qui réalise la destruction de ses enregistrements électroniques, doit produire une attestation de destruction d'enregistrement électronique, après la destruction de ceux-ci".

La destruction peut encore être totale si passant du simple nettoyage des ressources de stockage, elle vise à la disparition totale et définitive de l'archive. C'est la question du *sort final* abondamment traitée dans la norme ISO 15489. Le sort final des archives et leur retrait du système opérationnel doivent être mises en œuvre sur la base d'une procédure systématique et régulière :

> *Il convient qu'aucune élimination ou aucun transfert n'ait lieu sans l'assurance que le document n'est plus utile, qu'aucun travail relatif à ce document n'est en cours, et qu'aucun contentieux ou aucune enquête ne sont en cours qui pourraient nécessiter la production de ce document comme preuve".*

Il est admis que le sort final vise :
- la destruction physique immédiate, y compris l'écrasement ou la suppression des données ;
- la conservation pendant un nouveau laps de temps au sein de l'entité productrice ;
- le versement dans un lieu de stockage approprié ou le transfert sur un nouveau support, sous le contrôle du producteur ;
- le versement à une autre organisation en charge de l'activité et responsable de l'archivage à la suite d'une restructuration, d'une vente ou d'une privatisation ;
- le versement dans un lieu de stockage géré pour le compte du producteur par un prestataire indépendant sur la base de dispositions contractuelles pertinentes ;
- le transfert de la responsabilité de gestion à une autorité compétente sans transfert physique des documents ;
- le versement à un service d'archives ; ou
- le versement ou dépôt dans une institution archivistique externe.

Toujours teintée de juridisme, la norme décline les aspects physiques du sort final :
- la destruction doit toujours avoir été autorisée ;
- les archives relatives à un contentieux ou à une enquête en cours ou non-clos ne doivent pas être détruites ;
- la destruction d'archives, une fois autorisée, doit être exécutée d'une façon qui garantisse la confidentialité des informations qui s'y trouvent ;
- toutes les copies visées par l'élimination, y compris les copies de sécurité, les copies de conservation et les sauvegardes, doivent être détruites.

On doit naturellement tirer toutes les conséquences juridiques de la destruction de l'original, surtout s'il est sur support papier, et de la substitution d'une forme électronique. C'est sur la dernière forme électronique que reposeront toutes les exigences probatoires, lesquelles devraient être satisfaites si la chaîne de l'intégrité a été maintenue.

4. Le désarchivage

La restitution des documents électroniques conservés dans un système d'archivage électronique est définie comme étant l'opération qui vise à les présenter sous une forme exploitable pour le bénéficiaire de cette restitution. La restitution ainsi définie ne doit pas être confondue avec le retour ou la transmission d'archives, en totalité ou en partie, vers leurs propriétaires ou un tiers mandaté à cet effet.

4.1. Le retour d'archives

Lorsque le besoin de récupérer les archives se fera sentir, une demande de restitution sera présentée par le client ou tout autre organisme habilité au tiers archiveur. Après déstockage du lot demandé, l'archiveur le préparera pour expédition au demandeur. Dans cette phase qui poursuivra les flux électroniques, il importe que l'intégrité soit préservée sans négliger le fait que le client doit être assuré que c'est l'archiveur qui lui renvoie ses informations. Ces opérations, qui peuvent faire appel à des méthodes de sécurisation des transferts ne sont pas

décrites dans la norme, sciemment[20]. Le Guide de l'Archivage préconise de sécuriser l'envoi par l'utilisation d'une nouvelle signature électronique[21].

4.2. La restitution d'archives

L'opération de restitution pourra être constituée soit par l'affichage sur l'écran d'un système informatique, soit par l'impression d'une copie sur papier ou sur un film. La vertu qu'on recherche dans cette phase est la fidélité de l'archive par rapport à l'écrit électronique d'origine. Cette fidélité est obtenue par l'efficacité de la chaîne d'intégrité. L'archive sera fidèle à l'écrit d'origine, si les copies successives restent intègres :

- lors de la préparation de l'archive (garanties assurées par les procédures préconisées par les normes, comme l'ISO 15489),
- lors de son acheminement électronique et surtout de sa réception par l'archiveur (garanti par la signature électronique de sécurisation),
- lors de son stockage chez l'archiveur (garanties assurées par les procédures préconisées par les normes, comme la Z 42-013),
- lors de son acheminement électronique et surtout de sa réception par son propriétaire (garanti par la signature électronique de sécurisation).

Attention qu'in fine, l'intégrité ne soit atteinte. Aussi aucun traitement sur le contenu de l'archive ne doit être autorisé lors de la restitution. La norme Z 42-013 ne reconnaît comme exceptions que les traitements de décompression et les adaptations aux caractéristiques physiques ou logiciels des dispositifs de restitution.

La norme Z 42-013 s'intéresse aux difficultés pratiques de restitution des archives correspondant à des documents primitivement sur support papier. Par exemple, il importe de pouvoir restituer même si le logiciel de restitution correspondant au logiciel de mise en archive a disparu. Il doit y avoir indépendance entre les deux types de logiciels. Priorité sera donnée aux logiciels susceptibles de reconnaître la méthode qui a été employé pour numériser le document d'origine et d'opérer la restitution dans des conditions en garantissant la fidélité. La norme traite également la question du fond de page :

> *"si lors de la numérisation des documents, il a été utilisé le logiciel d'élimination de fond de page de tout autre élément fixe, la restitution fidèle exige de reconstituer le document en additionnant les éléments fixes (fonds de pages) aux éléments variables. Le système doit permettre de s'assurer que la version de fonds de page aux des éléments fixes utilisés bien celle qui a été extraite lors de la numérisation".*

4.3. Le désarchivage en interne

Si au contraire, l'archivage a été réalisé en interne, le désarchivage sera plus facilement réalisé et on ne parlera pas de restitution. L'utilisateur devra alors vérifier par lui-même si les archives sont bien dans l'état originel. Cette vérification pourra procéder par degré, toujours par rapport à une référence, le certificat de l'horodatage[22] :

- d'abord, les fichiers chronologiques de son système d'information démontreront que les archives et le certificat sont de la même génération,
- puis, comme le certificat d'horodatage inclut un condensé du texte des archives, il est possible de relancer l'algorithme de hasch-coding pour produire un condensé des éléments désactivés,
- enfin, on pourra se tourner vers le tiers horodateur pour comparer le certificat de l'entreprise et celui qu'il a émis.

[20] Cf. paragraphe 5.7. de la norme.

[21] Comme précédemment, cette signature qui ne vise qu'à sécuriser l'envoi ne rentre pas dans le cadre de l'article 1316-4. Cependant ce moyen électronique ne pourrait être déclaré irrecevable en cas de litige au sens de la Directive européenne sur la signature électronique (article 5.2.)

[22] Dans le langage technique, le certificat de l'horodatage s'appelle *jeton temporel*.