Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Archivage électronique sécurisé

ÉTAT DE L'ART

Version du 29 novembre 2006

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)

avec le concours

de la Direction des Archives de France (DAF)
du ministère de la Culture et de la communication

et de la Direction générale pour la modernisation de l'État (DGME)
du ministère de l'Économie, des finances et de l'industrie

sur la base d'une prestation de CAPRIOLI & ASSOCIES et JMR CONSULTANTS

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

conseil.dcssi@sgdn.pm.gouv.fr

Historique des modifications

Version	Objet de la modification	Statut
07/02/2006	Création du document sur la base d'un marché public (N°CO05000012 du 20 juin 2005, sur la fourniture d'une étude relative à la sécurité globale des services d'archivage)	Version de travail
21/06/2006	Finalisation	Validé
29/11/2006	Intégration de compléments relatifs aux éditeurs	Validé

Table des matières

1 Partie juridique

1.1 Objet

Cette partie a pour objet de répertorier et présenter les textes les plus pertinents ayant une incidence sur l'archivage électronique et adoptés aux niveaux international, communautaire et national.

Les textes et normes qui suivent permettent d'appréhender à la fois le contexte juridique à prendre en compte ainsi que les principes de base qui sont traités dans le cadre de documents pratiques (normes, guides).

1.2 Textes et normes internationaux

Les textes mentionnés ci-après n'ont pas de caractère contraignant dès lors qu'ils n'ont pas été transposés dans un texte national. Il en va de même pour les normes internationales et les recommandations qui n'auront un impact direct sur l'archivage électronique que si la personne qui en est chargée décide de s'y conformer. Toutefois, si le respect de ces dispositions est facultatif, il est recommandé de les prendre en compte dans la mesure où bien souvent elles posent les bases de « l'état de l'art »[1].

- **Loi-type de la Commission des Nations Unies pour le Droit du Commerce International (C.N.U.D.C.I.) sur le commerce électronique** (Résolution 51/162 de l'assemblée générale du 16 décembre 1996, www.uncitral.org). Ces dispositions fixent les exigences liées à la conservation juridique des documents électroniques notamment par le biais de tiers archiveurs. L'article 9-2 fait référence à la conservation, s'agissant de la force probante des messages de données, en prévoyant que « *l'information prenant la forme d'un message de données se voit dûment accorder force probante. Cette force probante s'apprécie eu égard à la fiabilité du mode de création, de conservation ou de communication du message, à la fiabilité du mode de préservation de l'intégrité de l'information, à la manière dont l'expéditeur a été identifié et à toute autre considération pertinente*. ».
  L'article 10 de la loi-type intitulée « *Conservation des messages de données* » se fonde sur l'intervention d'une personne elle-même ou d'une tierce personne et dispose « *1. Lorsqu'une règle de droit exige que certains documents, enregistrements ou informations soient conservés, cette exigence est satisfaite si ce sont des messages de données qui sont conservés, sous réserve des conditions suivantes :*
  a) *L'information que contient le message de données doit être accessible pour être consultée ultérieurement ;*
  b) *Le message de données doit être conservé sous la forme sous laquelle il a été créé, envoyé, reçu, ou sous une forme dont il peut être démontré qu'elle représente avec précision les informations créées, envoyées ou reçues ;*
  c) *Les informations qui permettent de déterminer l'origine et la destination du message de données, ainsi que les indications de date et d'heure de l'envoi ou de la réception, doivent être conservées si elles existent.*
  2. L'obligation de conserver des documents, enregistrements ou informations conformément au §1 ci-dessus ne s'étend pas aux informations qui n'ont d'autre objet que de permettre l'envoi ou la réception du message de données.
  3. L'exigence visée au §1 ci-dessus peut être satisfaite par recours aux services d'une autre personne, sous réserve que soient remplies les conditions fixées aux alinéas a, b, c, de ce §. ».

[1] Une norme est définie par l'Organisation internationale de normalisation (ISO) et la Commission Électrotechnique Internationale (CEI) comme étant un « *document, établi par le consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné.* ». Il a ainsi été jugé que l'existence d'une norme permet de représenter un état de l'art dans le domaine auquel elle se rapporte (Cass. Civ. 3ème ch. du 4 février 1976, Bull. civ. III, n°49).

- **« Le commerce électronique : considérations juridiques »**, étude établie par le secrétariat de la CNUCED (Conférence des Nations Unies sur le Commerce Et le Développement), UNCTAD/SDTE/BFB/1, du 15 mai 1998.

- **Loi-type de la C.N.U.D.C.I. sur les signatures électroniques** (Résolution 56/80 de l'assemblée générale du 12 décembre 2001, www.uncitral.org).

- **Convention du Conseil de l'Europe sur la cybercriminalité** du 23 novembre 2001, disponible à l'adresse : http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm. Le titre 2 de la Convention intitulé « *Conservation rapide de données informatiques stockées* » dispose dans son article 16 que « *1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.*
2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver une donnée stockée spécifiée se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et protéger l'intégrité desdits données pendant une durée aussi longue que nécessaire, jusqu'à maximum 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.
3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre des dites procédures pendant la durée prévue par son droit interne. (…). ». **La loi française n° 2005-493 du 19 mai 2005** a ratifié cette convention qui est donc désormais applicable sur le territoire national (Loi autorisant l'approbation de la convention sur la cybercriminalité et du protocole additionnel à cette convention relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques J.O. du 20 mai 2005, p. 8729 et s.).

- **Recommandation Rec.(95)11 relative à la sélection, au traitement, à la présentation et à l'archivage des décisions judiciaires dans les systèmes de documentation juridique automatisés** (adoptée par le Conseil des Ministres le 11 septembre 1995).

- **Recommandation Rec.(2000)13 du Comité des Ministres aux États membres sur une politique européenne en matière de communication des archives** (adoptée par le Conseil des Ministres le 13 juillet 2000).

- **Recommandation Rec.(2002)2 du Comité des Ministres aux États membres sur l'accès aux documents publics** (adoptée par le Conseil des Ministres le 21 février 2002).

- **Recommandation Rec.(2003)14 du Comité des Ministres aux États membres sur l'interopérabilité des systèmes d'information dans le secteur de la justice** (adoptée par le Conseil des Ministres le 9 septembre 2003).

- **Recommandation Rec.(2003)15 du Comité des Ministres aux États membres sur l'archivage des documents électroniques dans le secteur juridique** (adoptée par le Conseil des Ministres le 9 septembre 2003). Cette recommandation constitue l'aboutissement des recommandations citées précédemment et vise spécifiquement le domaine de la justice. Elle définit différentes notions et procède à une distinction entre la conservation initiale tenant à la valeur probante des documents et l'archivage ultérieur tenant à la valeur patrimoniale des documents. Ainsi, **« *l'archivage* *signifie la conservation des documents durant les délais prescrit par la législation et les règlements applicables des États membres comprenant les stades suivants : i. "conservation initiale" : la conservation tenant aux finalités primaires pour lesquelles les documents ont été produits en vue de leur valeur probante ;* ii. "*l'archivage ultérieur*" *: la conservation tenant à la valeur patrimoniale des documents, au-delà de leurs finalités primaires.*». La notion de **« *documents électroniques* »** vise quant à elle « *des documents, tant les textes que les images audio et vidéo sous forme numérique, qui ont vocation à créer des droits, une valeur probante et sont susceptibles d'être remis à un dépositaire public.* ».

- **Norme OAIS (Open Archival Information System)** de la Consultative Comittee for Space Data System. C'est un modèle de référence pour l'implantation technique de systèmes de gestion des documents d'archives de toute nature, dans un but de préservation à long terme. Cette norme propose une classification des types de migrations et des différents modes d'interopérabilité entre archives**.**

- **Norme ISO 15489 « *Record Management* »,** norme internationale générale, qui propose des procédures d'archivage, depuis la création du document jusqu'à ce qu'il n'ait plus d'intérêt pour l'entreprise. Selon la norme ISO 15489-1, le Record Management est un « *champ de l'organisation et de la gestion en charge d'un contrôle efficace et systématique de la création, de la réception, de la conservation, de l'utilisation et du sort final des documents, y compris des méthodes de fixation et de préservation de la preuve et de l'information liée à la forme des documents.* ».

- **Norme internationale DTD-EAD de description des documents d'archive** (Définition Type de Document - Encoded Archive Description). L'EAD est un outil informatique et le DTD permet de structurer en XML les instruments de recherche de type archivistique : inventaires, répertoires, catalogues de collections.

- **Les normes comptables IFRS** (International Financial Reporting Standard) s'applique aux sociétés européennes faisant appel public à l'épargne, lesquelles doivent désormais se conformer à ce référentiel comptable international dont l'établissement par l'IASB (International Accounting Standards Board) visait notamment à améliorer la fiabilité des données comptables.

- **Title 21 Code of Federam Regulation Part 11**, cette section des règles et règlements recommandation de la Food and Drug Administration concerne les enregistrements électroniques, la traçabilité de l'information et la signature électronique. Elle a vocation à s'appliquer à toutes les sociétés exportant ou souhaitant exporter des produits pharmaceutiques vers les États-Unis.

1.3 Textes communautaires et normes européennes

L'ensemble des directives et textes ci-dessous référencés est susceptible d'avoir un impact sur les règles applicables à l'archivage électronique au niveau national, soit parce que les dispositions visées ont déjà été transposées en droit national, soit parce qu'elles sont appelées à l'être dans des délais plus ou moins brefs (les textes de transposition sont référencés au niveau des textes nationaux).

- **Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995** relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données (J.OC.E., n° L. 281 du 23 novembre 1995, p. 31).
  → ***Impact sur la conservation des données à caractère personnel***.

- **Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996** relative à la protection des bases de données (J.O.C.E., n° L. 77 du 27 mars 1996, p. 20).
  → ***Impact sur la conservation des bases de données*.**

- **Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999** sur un cadre communautaire pour les signatures électroniques (J.O.C.E., n° L 013 du 19 janvier 2000, p. 12 et s.).
  → ***Impact sur l'archivage électronique dans la mesure où ce texte traite des signatures électroniques et de l'archivage des certificats électroniques qui sont étroitement liés à la reconnaissance juridique des écrits sous forme électronique*.**
  Son annexe II dispose que les prestataires doivent « *enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par voie électronique* » et doivent « *utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable de sorte que :*
  - *seules les personnes autorisées puissent introduire et modifier des données ;*

- *l'information puisse être contrôlée quant à son authenticité ;*
- *les certificats ne soient pas disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement et*
- *toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur.* ».

- **Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000** relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« *directive sur le commerce électronique* ») (J.O.C.E., n° L 178 du 17 juillet 2000, p. 1 et s.).
  → ***Impact sur la reconnaissance juridique de la validité des contrats électronique incluant leur archivage***.
  Considérant 34 : « *Chaque État membre doit ajuster sa législation qui contient des exigences, notamment de forme, susceptibles de gêner le recours à des contrats par voie électronique. Il convient que l'examen des législations nécessitant cet ajustement se fasse systématiquement et porte sur l'ensemble des étapes et des actes nécessaires au processus contractuel, y compris l'archivage du contrat.* ».

- **Directive 2001/115/CE du Conseil du 20 décembre 2001** modifiant la directive 77/388/CEE en vue de simplifier, moderniser et harmoniser les conditions imposées à la facturation en matière de taxe sur la valeur ajoutée (J.O.C.E. n° L 15 du 17 janvier 2002, p. 24 et s.). Cette directive constitue le cadre juridique communautaire permettant la dématérialisation des factures et prévoyant les modalités de leur conservation.
  → ***Impact sur la conservation des factures électroniques***.
  L'article 2 e) définit notamment **la notion de transmission et de stockage d'une facture par voie électronique** comme étant « *une transmission ou une mise à disposition du destinataire et un stockage effectués au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et en utilisant le fil, la radio, les moyens optiques ou d'autres moyens électromagnétiques.* ».

- **Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002** concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, (dite « *directive vie privée et communications électroniques* ») (J.O.C.E., n° L. 201 du 31 juillet 2002, p. 37).
  → ***Impact sur la conservation des données à caractère personnel***.

- **Directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002** concernant la commercialisation à distance de services financiers auprès des consommateurs et modifiant les directives 90/619/CEE du Conseil, 97/7/CE et 98/27/CE (J.O.C.E. n° L. 271 du 9 octobre 2002, p. 17 et s).
  → ***Cette directive définit la notion de support durable*** comme étant « *tout instrument permettant au consommateur de stocker des informations qui lui sont adressées personnellement d'une manière permettant de s'y reporter aisément à l'avenir pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées.* ». Le considérant 20 précise que les supports durables « *incluent notamment les disquettes informatiques, les CD-ROM, les DVD et le disque dur de l'ordinateur du consommateur sur lequel le courrier électronique est stocké, mais ils ne comprennent pas les sites Internet, sauf ceux qui satisfont aux critères spécifiés dans la définition des supports durables.* ».

- **Directive 2003/58/CE du Parlement européen et du Conseil du 15 juillet 2003** modifiant la directive 68/151/CE du Conseil en ce qui concerne les obligations de publicité de certaines formes de société (J.O.C.E. n° L. 221 du 4 septembre 2003, p. 13 et s). Cette directive a pour objectif l'adaptation de la législation relative aux obligations de publicité de certaines sociétés à l'évolution des technologies en offrant la possibilité de procéder à ces obligations par voie électronique. En ce sens le point 8 de l'article 1er qui modifie la directive 68/151/CEE du Conseil du 9 mars 1968 dispose que « *aux fins du présent article, on entend par « voie électronique » que l'information est envoyée à l'origine et reçue à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et entièrement transmise, acheminée et reçue par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques selon des modalités définies par les États membres.* ».

- **Directive 2003/511/CE du Parlement européen et du Conseil du 14 juillet 2003** relative à la publication des numéros de référence de normes généralement admises pour les produits de signatures électroniques conformément à la directive 1999/511/CE du Parlement et du Conseil (J.O.C.E., n° L. 175 du 15 juillet 2003, p. 45).

- **Directive 2004/18/CE du Parlement européen et du Conseil du 31 mars 2004** relative à la coordination des procédures de passation des marchés publics de travaux, de fournitures, de services (J.O.U.E. n° L 134 du 30 avril 2004, p. 114 et s.) et de la **directive 2004/17/CE du 31 mars 2004** portant coordination des procédures de passation des marchés dans le secteur de l'eau, de l'énergie, des transports et des services postaux (J.O.U.E. du 30 avril 2004, p. 1).
  → Impact sur la dématérialisation des procédures de passation des marchés publics.
  Ces directives maintiennent pour l'essentiel, les principes propres aux modalités de la dématérialisation des procédures de passation des marchés publics et préconisent l'utilisation de la signature électronique avancée, sans l'imposer.

- **Projet de décision-cadre sur la rétention de données traitées et stockées** en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection et la poursuite de délits et d'infractions pénales, y compris du terrorisme**,** du Conseil de l'Union européenne, en date du 28 avril 2004. → ***Cette décision-cadre porte notamment sur la rétention de données de connexion et non sur les conditions de stockage.***
  Ainsi, « *il y a lieu de retenir certains types de données, qui sont déjà traitées et stockées à des fins de facturation, des fins commerciales ou toute autre fin légitime, pendant un laps de temps supplémentaire en prévision du fait que ces données pourraient s'avérer nécessaires à l'avenir en cas d'enquête ou de poursuites judiciaires* ». Le but est de favoriser la coopération judiciaire dans le domaine pénal par une harmonisation des législations des États membres. L'article 4 dispose que « *Chaque État membre prend les mesures nécessaires afin de veiller à ce que les données soient retenues pendant une période d'au moins douze mois et de maximum 36 mois après leur création. (…)* ». L'article 7 relatif à la sécurité des données énonce les principes minimums devant être respectés, à savoir, « *a) les données retenues sont de la même qualité que les données sur le réseau ;*
  b) les données font l'objet de mesures techniques et d'organisation appropriées pour les protéger contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, ainsi que contre toute autre forme de traitement illicite ;
  c) toutes les données sont détruites à la fin de la période de rétention, à l'exception des données ayant fait l'objet d'un accès et qui ont été conservées ;
  d) il appartient à chaque État membre de définir dans son droit national la procédure à suivre pour avoir accès aux données retenues et pour conserver les données ayant fait l'objet d'un accès. ».

- **Norme : le modèle européen MoReq (Model Requirements for the Management of Electronic Records).** Établi par un groupe d'États européens, ce modèle vise à mettre en place un système qui soit en mesure de gérer les documents électroniques, aux degrés de confidentialité et d'intégrité voulus, en combinant les avantages de la gestion électronique à ceux de la méthode classique d'archivage. Il convient de rappeler que ***les normes n'ont pas, de droit, de caractère contraignant. Toutefois, si le respect de ces dispositions est facultatif, il est recommandé de les prendre en compte dans la mesure où bien souvent elles posent les bases de « l'état de l'art ».***

1.4 Textes et normes au niveau national

Il est important de rappeler le principe de hiérarchie des textes juridiques. Les textes édictés par les pouvoirs législatif et réglementaire constituent ainsi un ensemble hiérarchisé dans lequel la norme juridique de rang supérieur l'emporte sur celles de rang inférieur. Cet ordre est le suivant :

- ***la constitution ;***
- ***les lois organiques ;***
- ***les lois ;***
- ***les ordonnances qui lorsqu'elles font d'une loi de ratification acquièrent la valeur juridique d'une loi ;***
- ***les décrets ;***
- ***les arrêtés ;***

- ***les circulaires.***

En cas de contradiction entre ces textes, c'est toujours la disposition de la norme juridique la plus élevée dans la hiérarchie qui s'appliquera.

De plus, compte tenu de l'inflation des textes législatifs et réglementaires adoptés, il est apparu opportun de les présenter selon les domaines juridiques concernés. Néanmoins, les cloisons entre les différents domaines définis ne sont pas nécessairement hermétiques et certains textes ont des effets plus larges qu'il n'y paraît. Par ailleurs, seuls les textes ayant un impact sur l'archivage électronique font l'objet de précisions. Les autres textes forment le contexte général dans lequel s'inscrit l'archivage électronique et dont on ne saurait faire abstraction ; étant précisé que la liste qui suit ne prétend pas à l'exhaustivité mais référence les textes les plus pertinents.

1.4.1 Droit privé

- **Loi n° 2000-230 du 13 mars 2000** portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (J.O. du 14 mars 2000, p. 3968) : cf. notamment les articles 1316 à 1316-4 introduits par la loi dans le code civil et relatifs aux écrits et signatures électroniques. Le législateur y a redéfini la preuve littérale afin d'intégrer dans le système probatoire français les écrits sous forme électronique.
  → ***Impact sur les conditions d'établissement et de conservation d'un écrit électronique à titre de preuve***.

- **Loi n° 2003-706 du 1er août 2003** de sécurité financière (J.O. du 2 août 2003 p. 13220 et s.). Cette loi reprend les principes issus du **Sarbanes Oxley Act américain de juillet 2002** ; étant noté que la loi américaine est applicable aux sociétés, notamment françaises, qui émettent des titres enregistrés auprès de la SEC ou placés sur le marché américain. Ces textes imposent aux entreprises, parallèlement à la mise en place de procédures de contrôle interne, **l'organisation d'un système d'archivage permettant d'obtenir rapidement des informations sur l'historique financier de l'entreprise**.
  → ***Impact direct sur l'archivage électronique dans la mesure où l'archivage constitue un moyen de vérifier que les informations comptables, financières et de gestion communiquées aux organes sociaux de la société reflètent avec sincérité l'activité et la situation de la société.*** A ce titre, la législation américaine va jusqu'à imposer la conservation des messages électroniques.

- **Loi n° 2004-575 du 21 juin 2004** pour la confiance dans l'économie numérique (J.O. du 22 juin 2004, p. 11168 et s.). Ce texte a une portée transversale. L'article 25 de la loi codifiée à l'article 1369-1 du code civil impose aux professionnels de mentionner « *en cas d'archivage du contrat, les modalités de cet archivage par l'auteur de l'offre et les conditions d'accès au contrat archivé.* » dans les conditions générales de vente. Cet article introduit, en outre, l'article 1108-1 du code civil qui traite de la validité des actes juridiques conclus sous forme électronique et dispose que « *lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique dans les conditions prévues aux articles 1316-1 et 1316-2 et, lorsqu'un acte authentique est requis, au second alinéa de l'article 1317*. ». De plus, l'article 27 de la loi insère un article 134-2 au code de la consommation qui impose aux professionnels la conservation des contrats électroniques en garantissant à tout moment l'accès sur demande du cocontractant. Cet article ne précise toutefois pas les modalités de cette conservation.
  → ***Impact direct sur l'archivage électronique et la reconnaissance juridique des actes électroniques***

- **Ordonnance n° 2001-741 du 23 août 2001** portant transposition de directives communautaires et adaptation au droit communautaire en matière de droit de la consommation (J.O. du 25 août 2001 p. 13645 et s.). Cette ordonnance modifie notamment l'article L. 121-19 du code de la consommation qui dispose désormais que « *I- Le consommateur doit recevoir, par écrit ou sur un autre support durable à sa disposition, en temps utile et au plus tard au moment de la livraison :*
  1° Confirmation des informations mentionnées au 1° et 4° de l'article L. 121-18 et de celles qui figurent en outre aux articles L. 111-1 et L. 113-3 ainsi que celles prévues pour l'application de l'article L. 214-1, à moins que le professionnel n'ait satisfait à cette obligation avant la conclusion du contrat ;
  2° Une information sur les conditions et les modalités d'exercice du droit de rétractation ;

3° L'adresse de l'établissement du fournisseur où le consommateur peut présenter ses réclamations ;
4° Les informations relatives au service après vente et aux garanties commerciales ;
5° Les conditions de résiliation du contrat lorsque celui-ci est d'une durée indéterminée ou supérieure à un an.
II. Les dispositions du présent article ne sont pas applicables aux services fournis en une seule fois au moyen d'une technique de communication à distance et facturés par l'opérateur de cette technique à l'exception du 3°. ».
→ ***Impact sur l'archivage électronique de ces informations obligatoires.***

- **Ordonnance n° 2005-648 du 6 juin 2005** relative à la commercialisation à distance de services financiers auprès des consommateurs (J.O. du 7 juin 2005, p. 10002). L'article L. 121-20-11 du code de la consommation introduit par cette loi, dispose « *le consommateur doit recevoir, par écrit ou sur un autre support durable à sa disposition et auquel il a accès en temps utile et avant tout engagement, les conditions contractuelles ainsi que les informations mentionnées à l'article L. 121-20-10. ».* Cette loi qui transpose la directive 2002/65/CE reprend la notion de support durable définie par cette dernière.
→ ***Impact sur l'archivage électronique de ces informations obligatoires.***

- **Ordonnance n° 2005-674 du 16 juin 2005** relative à l'accomplissement de certaines formalités contractuelles par voie électronique (J.O. du 17 juin 2005, p.10342). Cette ordonnance procède à une adaptation du Code civil aux contrats conclus par voie électronique en prévoyant les modalités de l'échange des informations pré-contractuelles, de la remise d'un écrit par voie électronique et l'adaptation de certaines exigences de forme notamment la formalité du double original.
Ainsi l'article 1369-8 inséré dans le code civil dispose, s'agissant des lettres recommandées électroniques, que « *un avis de réception peut être adressé à l'expéditeur par voie électronique ou par tout autre dispositif lui permettant de le conserver* », les **modalités de cette conservation devant faire l'objet d'un décret d'application**. De plus, l'article 1369-11 dispose désormais que « *l'exigence d'un envoi en plusieurs exemplaires est réputée satisfaite sous forme électronique si l'écrit peut être imprimé par le destinataire.* ». De même, l'article 1325 est modifié et précise que « *l'exigence d'une pluralité d'originaux est réputée satisfaite pour les contrats sous forme électronique lorsque l'acte est établi et conservé conformément aux articles 1316-1 et 1316-4 et que le procédé permet à chaque partie de disposer d'un exemplaire ou d'y avoir accès .*».
→ ***Impact sur l'archivage électronique de ces formalités obligatoires remplies par voie 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 (J.O. du 31 mars 2001, p. 5070).
→ ***Les prestataires de services de certification électronique (PSCE) doivent être en mesure de démontrer que les systèmes d'archivage concourant au service de certification qu'ils fournissent, sont fiables****.*
Ainsi, l'article 6 du décret dispose que le PSCE doit « *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*. » et « *faire preuve de la fiabilité des services de certification électronique qu'il fournit*. ». Le décret précise les obligations sans fixer la nature des informations à archiver ni les modalités de leur conservation.

- **Décret n° 2002-535 du 18 avril 2002** relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information (J.O. du 19 avril 2002, p. 6944). Ce texte adopté dans le contexte du dispositif réglementaire relatif aux signatures électroniques a une portée plus large et concerne la certification de la sécurité offerte par des produits ou des systèmes des technologies de l'information, « *au regard notamment de leur aptitude à assurer la disponibilité, l'intégrité ou la confidentialité de l'information traitée face aux menaces dues en particulier à la malveillance* » (alinéa 1er de l'article 1er du décret).
→ ***Impact possible sur la certification de la sécurité offerte par des produits et services en matière d'archivage électronique.***

- **Décret n° 2002-803 du 3 mai 2002** portant application de la troisième partie de la loi n° 2001-420 du 15 mai 2001 relative aux nouvelles régulations économiques (J.O. du 5 mai 2002, p. 8717 et s).

- **Décret n° 2002-1436 du 3 décembre 2002** modifiant le code de l'organisation judiciaire, le code de procédure civile, le nouveau code de procédure civile et le décret n° 96-1080 du 12 décembre 1996 portant tarif des huissiers de justice en matière civile et commerciale (J.O. du 12 décembre 2002, p. 20482 et s.). Ce texte modifie notamment le NCPC en étendant les procédures de vérification en écriture reconnues au juge aux écrits et signatures électroniques.

- **Décret n° 2005- 137 du 16 février 2005** pris pour l'application de l'article L. 134-2 du code de la consommation (J.O. du 18 février 2005, p.2780 et s.). Ce décret précise que l'obligation de conserver les contrats, passés en ligne avec un consommateur, vise les contrats électroniques d'un montant supérieur à 120 € et s'étend sur une durée de 10 ans.
  → ***Impact sur l'archivage électronique des contrats passés par voie électronique avec un consommateur.***

- **Arrêté du 26 juillet 2004** relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation (J.O. du 7 août 2004, p. 10223). Ce texte abroge et remplace l'arrêté du 31 mai 2002 pris en application du décret du 30 mars 2001. Il vient compléter le dispositif réglementaire en définissant le schéma de qualification des PSCE pour que les signatures électroniques bénéficient de la présomption de fiabilité conformément à l'alinéa 2 de l'article 1316-4 du code civil et aux conditions posées dans le décret du 30 mars 2001.

1.4.2 Droit public

- **Loi n° 78-753 du 17 juillet 1978** portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal (J.O. du 18 juillet 1978, p. 2851 et s.) modifiée. Son article 1er modifié par **l'ordonnance n° 2005-650 du 6 juin 2005** relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques (J.O. du 7 juin 2005, p. 10022 et s.) dispose que « *sont considérés comme documents administratifs, au sens des chapitres Ier, III et IV du présent titre, quel que soit le support utilisé pour la saisie, le stockage ou la transmission des informations qui en composent le contenu, les documents élaborés ou détenus par l'État, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées de la gestion d'un service public.* ». L'article 2 précise notamment, que « *le droit de communication ne s'applique qu'à des documents archivés* » et que « *le dépôt aux archives publiques des documents administratifs communicables aux termes du présent chapitre ne fait pas obstacle au droit de communication à tout moment desdits documents.* ». L'article 4 de la loi dispose, quant à lui, que « *L'accès aux documents administratifs s'exerce, au choix du demandeur et dans la limite des possibilités techniques de l'administration :*
  a) Par consultation gratuite sur place, sauf si la préservation du document ne le permet pas ;
  b) Sous réserve que la reproduction ne nuise pas à la conservation du document, par la délivrance d'une copie sur un support identique à celui utilisé par l'administration ou compatible avec celui-ci et aux frais du demandeur, sans que ces frais puissent excéder le coût de cette reproduction, dans des conditions prévues par décret ;
  c) Par courrier électronique et sans frais lorsque le document est disponible sous forme électronique. ».
  → ***Impact sur l'archivage électronique des documents administratifs compte tenu des règles régissant leur communication et par voie de conséquence leur accessibilité.***

- **Loi n° 79-18 du 3 janvier 1979 sur les archives** (J.O. du 5 janvier 1979, p. 43 et s.). Ce texte pose les principes en matière d'archivage et ne vise aucun support spécifique. L'article L. 211-1 du code du patrimoine, au sein duquel la loi du 3 janvier 1979 a été codifiée, **définit la notion d'archives** en disposant que « *les archives sont l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale, et par tout service ou organisme public ou privé, dans l'exercice de leur activité.* ». L'article L. 211-5 du code du patrimoine **définit les archives privées** exclusivement par opposition aux archives publiques, ainsi « *les archives privées sont l'ensemble des documents définis à l'article L. 211-1 qui n'entrent pas dans le champ d'application de l'article L. 211-4.* ». Par ailleurs, l'article L. 211-2 du code du patrimoine,

donne aux archives **une double finalité** en précisant que « *la conservation des archives est organisée dans l'intérêt public tant pour les besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques ou privées, que pour la documentation historique de la recherche.* ». Enfin, le code du patrimoine précise **divers délais de conservation** pour la plupart liés aux délais de prescription.
→ ***Impact sur l'archivage électronique***

- **Loi n° 94-126 du 11 février 1994** relative à l'initiative et à l'entreprise individuelle dite « *loi Madelin* » (J.O. du 13 février 1994, p. 2493).

- **Loi n° 2000-321 du 12 avril 2000** relative aux droits des citoyens dans leurs relations avec les administrations (J.O. du 13 avril 2000, p. 5646 et s.). Voir notamment l'article 16 de ce texte (procédé homologué de datation électronique qui devrait être modifié par l'ordonnance prise en application de l'article 3 de la loi du 9 décembre 2004 de simplification du droit). Cette loi a été modifiée par l'ordonnance n° 2005-1516 du 8 décembre 2005 en ce qui concerne les démarches administratives accomplies par voie électronique qui impose notamment le recours aux accusés de réception. Ainsi, l'administration sera considérée comme régulièrement saisie si le courrier électronique qui lui est adressé est assortie d'un accusé de réception.
→ ***Impact sur l'archivage électronique.***

- **Loi n° 2001-1246 du 21 décembre 2001 de financement de la sécurité sociale pour 2002** (J.O. du 26 décembre 2001, p. 20552). Ses articles 28 et 73 prévoient la transmission par voie électronique des documents nécessaires au remboursement ou à la prise en charge ainsi qu'à l'accomplissement de déclarations sociales par voie électronique. Est visé le groupement d'intérêt public dit « *de modernisation des déclarations sociales* » (GIP MDS), organisme centralisateur crée par l'ACOSS, l'AGIRC, l'ARRCO, la CNAV et l'UNEDIC et regroupant également les principaux autres régimes obligatoires (dont la CNAM), des organismes de prévoyance collective et les organisations patronales.
→ ***Impact sur l'archivage électronique de ces documents et téléprocédures.***

- **Loi n° 2002-276 du 27 février 2002** relative à la démocratie de proximité (J.O. du 28 février 2002, p. 3808 et s.). V. notamment l'article 6-VII de ce texte (publication des délibérations en ligne par les collectivités locales à titre non exclusif).
→ ***Impact sur l'archivage électronique de ces documents.***

- **Loi n° 2003-591 du 2 juillet 2003** habilitant le Gouvernement à simplifier le droit (J.O. du 3 juillet 2003, p. 11192 et s.). Ce texte habilite le Gouvernement à prendre un certain nombre d'ordonnances dans des domaines déterminés afin de simplifier le droit (du point de vue des formalités et des modalités des démarches auprès des administrations et organismes assimilés notamment). Au titre des ordonnances adoptées, cf. par exemple **l'ordonnance n° 2003-1213 du 18 décembre 2003** relative aux mesures de simplification des formalités concernant les entreprises, les travailleurs indépendants, les associations et les particuliers employeurs (J.O. du 20 décembre 2003, p. 21806) ; étant noté que des décrets d'application ont également été adoptés.
→ ***Impact sur l'archivage électronique des formalités et documents établis par voie électronique sur la base de ces textes. Cet archivage concernant tant les administrations que les usagers (entreprises ou autres).***

- **Loi n° 2004-809 du 13 août 2004** relative aux libertés et responsabilités locales (J.O. du 17 août 2004, p. 14545). Les articles 124 (attributions de moyens informatiques aux élus par les collectivités locales) et 139 (contrôle de légalité) notamment introduisent les technologies de l'information dans le Code général des collectivités territoriales. V. également la circulaire générale d'application du 10 septembre 2004 (NOR/LBL/B/04/10074/C).
→ ***Impact sur l'archivage électronique notamment pour les actes transmis au contrôle de légalité et le respect de cette procédure par voie électronique.***

- **Loi n° 2004-1343 du 9 décembre 2004** de simplification du droit (J.O. du 10 décembre 2004, p. 20857). Ce texte habilite le gouvernement à adopter des ordonnances afin de simplifier le droit, étant noté que la dématérialisation des échanges y occupe une place prépondérante (cf. notamment article 3 de la loi).

→ ***L'ordonnance n° 2005-1516 du 8 décembre 2005 prise en application de l'article 3 de la loi du 9 décembre 2004 prévoit diverses dispositions qui ont un impact sur l'archivage électronique à des niveaux différents*, et ce, notamment aux référentiels qui seront adoptés.**

- **Ordonnance n° 2004-164 du 20 février 2004** relative aux modalités et effets de la publication des lois et de certains actes administratifs (J.O. du 21 février 2004, p. 3514). L'article 3 de cette ordonnance dispose « *La publication des actes mentionnés à l'article 2 (les lois, les ordonnances accompagnées d'un rapport de présentation, les décrets et, lorsqu'une loi ou un décret le prévoit, les autres actes administratifs) est assurée, le même jour, dans des conditions de nature à garantir leur authenticité, sur papier et sous forme électronique. Le Journal officiel de la République française est mis à la disposition du public sous forme électronique de manière permanente et gratuite*. ». Il s'agit, en l'espèce, du dépôt légal électronique et non d'archivage électronique lequel est du ressort de la Bibliothèque Nationale de France.
  → ***Impact sur l'archivage électronique de ces documents.***

- **Ordonnance n° 2004-178 du 20 février 2004** relative à la partie législative du code du patrimoine (J.O. du 24 février 2004, p. 37048 et s.). Le livre II du code du Patrimoine issu de cette ordonnance est dédié aux archives. Il dispose d'un régime général des archives publiques comme privées et du régime spécifique des archives audiovisuelles de la justice. L'article L. 212-6 du code du patrimoine dispose que « *les collectivités territoriales sont propriétaires de leurs archives. Elles en assurent elles-mêmes la conservation et la mise en valeur.* », ce qui exclut tout recours à l'externalisation de la part de ces dernières.
  → ***Impact sur l'archivage électronique et son régime juridique (notamment / externalisation pour les collectivités territoriales)***

- **Ordonnance n° 2005-650 du 6 juin 2005** relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques (J.O. du 7 juin 2005, p. 10022 et s.). L'article 7 de cette ordonnance insère à l'article 6 de la loi du 17 juillet 1978 un III qui dispose que « *lorsque la demande porte sur un document comportant des mentions qui ne sont pas communicables en application du présent article mais qu'il est possible d'occulter ou de disjoindre, le document est communiqué au demandeur après occultation ou disjonction de ces mentions.* ».
  → ***Impact sur l'archivage électronique des documents administratifs compte tenu des règles régissant leur communication et par voie de conséquence leur accessibilité.***

- **Ordonnance n° 2005-1516 du 8 décembre 2005** relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (J.O. du 9 décembre 2005, p. 18986). Cette ordonnance prise en application de la loi n° 2004-1434 du 9 décembre 2004 de simplification du droit modifie notamment la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec l'administration. L'article 1 définit notamment les termes de « *système d'information* » comme étant « *tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives* » et de « *produit de sécurité* » qui désigne « *tout dispositif, matériel ou logiciel, mettant en œuvre des fonctions qui contribuent à la sécurité des informations échangées par voie électronique* ». Le chapitre 2 de cette loi a pour but d'encadrer les démarches administratives accomplies par voie électronique. En substance, il dispose que l'administration « *peut* » répondre par voie électronique aux usagers lorsque ceux-ci ont initié la demande d'information par cette voie. Ainsi, le recours aux courriers électroniques est une faculté pour les autorités administratives. Toutefois, un courrier électronique adressé par un usager lie l'administration qui doit considérer être régulièrement saisie dès lors qu'un accusé de réception ou un accusé d'enregistrement a été valablement émis. Un décret en Conseil d'État viendra préciser cette disposition. Le chapitre 3 de cette loi est relatif à la signature électronique des actes administratifs et dispose qu'à cette fin, l'administration doit se conformer au référentiel général de sécurité dont dispose également l'ordonnance. De plus, l'ordonnance précise que cette signature doit reposer sur un procédé qui « *permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte* ». De plus, l'usager, pourra avoir recours à un dispositif de stockage mis à sa disposition par des autorités administratives et des organismes privés agréés afin de faciliter ses démarches administratives.

Le chapitre 4 vise le référentiel général de sécurité précité. A ce titre, l'article 9 de l'ordonnance dispose qu'un « *référentiel général de sécurité fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique telles que les fonctions d'identification, de signature électronique, de confidentialité et d'horodatage.* ». Ainsi, lorsqu'une autorité administrative met en place un système d'information, elle doit préalablement déterminer les fonctions de sécurité nécessaires pour protéger ce système eu égard au référentiel général de sécurité et aux différents niveaux de sécurité prévus. Enfin, cette ordonnance traite de l'interopérabilité des services offerts par voie électronique en précisant qu'un référentiel général d'interopérabilité fixe les règles techniques à cet effet. Ainsi, l'article 11 dispose que le référentiel général d'interopérabilité « *détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives* ». Qu'il s'agisse du référentiel général de sécurité ou de celui d'interopérabilité, un décret viendra en préciser les conditions d'élaboration, d'approbation, de modification et de publication. Il convient cependant de préciser que les systèmes d'informations traitant d'informations relevant du secret de la défense nationale n'entrent pas dans le champ d'application de cette ordonnance.

→ ***Impact sur l'archivage électronique des documents administratifs compte tenu des règles régissant désormais leur communication par voie électronique et par voie de conséquence leur accessibilité. De plus, création d'un référentiel général de sécurité et d'un référentiel général d'intéropérabilité auquel les autorités administratives devront se conformer dans la mise en œuvre de tous systèmes d'information. Ce texte impacte donc directement les archives publiques et l'archivage électronique.***

- **Décret n° 79-1037 du 3 décembre 1979** relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques (J.O.R.F. du 5 décembre 1979)
  Ce décret complète la loi en fixant les grands principes d'organisation de l'archivage entre les producteurs et les services d'archives. Il s'agit notamment des principes de durée d'utilité administrative (DUA), de détermination du sort final des documents, des visas d'élimination, de la sélection et du tri, du rôle et des responsabilités des différents services d'archive et de la règle des trois âges de l'archive (courante, intermédiaire, définitive),…
  → ***Impact sur l'archivage électronique.***

- **Décret n° 79-1038 du 3 janvier 1979** relatif à la communicabilité des documents d'archives publiques (J.O. du 5 décembre 1979, p. 3058) qui énonce les documents ne pouvant faire l'objet d'une communication qu'après un délai de soixante ans.

- **Décret n° 79-1040 du 3 décembre 1979 relatif à la sauvegarde des archives privées présentant du point de vue de l'Histoire un intérêt public (**J.O. du 5 décembre 1979, p. 3059)**.**

- **Décret n° 99-68 du 2 septembre 1999** relatif à la mise en ligne des formulaires administratifs (J.O. du 4 septembre 1999, p. 1775).

- **Décret n° 2000-318 du 7 avril 2000** relatif à la partie Réglementaire du code général des collectivités territoriales (J.O. du 9 avril 2000, p. 5769 et s.). Ce décret codifie dans la partie réglementaire du code général des collectivités territoriales les dispositions issues du décret n° 88-849 du 28 juillet 1988, les article R. 317.1 à R. 317-4 du code des communes et les articles 6, 7 et 8 du décret n° 79-1037 du 3 décembre 1979 et abroge ces derniers.

- **Décret n° 2001-492 du 6 juin 2001** pris pour l'application du chapitre II du titre II de la loi n° 2000-321 du 12 avril 2000 et relatif à l'accusé de réception des demandes présentées aux autorités administratives (J.O. du 10 juin 2001, p. 9246 et s.). Ce décret a des impacts quant à l'identification des agents dans les échanges par voie électronique.

- **Décret n° 2001-493 du 6 juin 2001** pris pour l'application de l'article 4 de la loi n° 78-753 du 17 juillet 1978 et relatif aux modalités de communication des documents administratifs (J.O. du 10 juin 2001, p. 9246 et s.). L'article 1er du décret dispose que « *toute personne demandant copie d'un document administratif dans les conditions prévues à l'article 4 de la loi du 17 juillet 1978 peut obtenir cette copie :*
  - *soit sur un support papier ;*

- *soit sur un support informatique identique à celui utilisé par l'administration ;*
- *soit par messagerie électronique.*

Le demandeur souhaitant obtenir copie d'un document sur support informatique ou par messagerie électronique est avisé du système et du logiciel utilisé par l'administration. ».

→ *Impact sur l'archivage électronique des documents administratifs compte tenu des règles régissant leur communication et par voie de conséquence leur accessibilité.*

- **Décret n° 2001-846 du 18 septembre 2001** pris en application du 3° de l'article 56 du code des marchés publics et relatifs aux enchères électroniques (J.O. du 19 septembre 2001, p. 14847 et s.). Ce texte pris en application de l'ancienne version de l'article 56 du code des marchés publics (décret n° 2001-210 du 7 mars 2001 portant code des marchés publics) demeure applicable et concerne l'achat de fournitures courantes.
  → Impact sur la traçabilité des opérations et de la procédure et par voie de conséquence sur l'archivage des éléments pertinents.

- **Décret n° 2002-535 du 18 avril 2002** relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information (J.O. du 19 avril 2002, p. 6944). Ce texte adopté dans le contexte du dispositif réglementaire relatif aux signatures électroniques a une portée plus large et concerne la certification de la sécurité offerte par des produits ou des systèmes des technologies de l'information, « *au regard notamment de leur aptitude à assurer la disponibilité, l'intégrité ou la confidentialité de l'information traitée face aux menaces dues en particulier à la malveillance* » (alinéa 1er de l'article 1er du décret). Étant noté qu'il est précisé « *Les administrations de l'État recourent, dans la mesure du possible et en fonction de leurs besoins de sécurité, à des produits ou des systèmes des technologies de l'information certifiés suivant la procédure prévue au présent décret* » (alinéa 2 de l'article 1er du décret).
  → *Impact possible sur la certification de la sécurité offerte par des produits et services en matière d'archivage électronique.*

- **Décret n° 2002-692 du 30 avril 2002** pris en application du 1° et du 2° de l'article 56 du code des marchés publics et relatifs à la dématérialisation des procédures de passation des marchés publics (J.O. du 3 mai 2002, p. 8064). Ce texte pris en application de l'ancienne version de l'article 56 du code des marchés publics (décret n° 2001-210 du 7 mars 2001 portant code des marchés publics) demeure applicable. L'article 2 dispose notamment que « *Quelle que soit la procédure, les personnes intéressées doivent pouvoir consulter et archiver sur leur ordinateur le règlement de la consultation. Les personnes intéressées, dans le cadre d'un appel d'offre ouvert, et les candidats invités à présenter une offre, dans le cadre d'une mise en concurrence simplifiée, d'un appel d'offres restreint ou d'une procédure négociée, doivent pouvoir également consulter et archiver sur leur ordinateur le cahier des charges, les documents et renseignements complémentaires.* ».
  → *Impact sur l'archivage électronique des procédures de passation des marchés publics par voie électronique*

- **Code des marchés publics issu du décret n° 2004-15 du 7 janvier 2004** (J.O. du 8 janvier 2004, p. 37003). Son **article 56** traite spécifiquement de la dématérialisation des procédures. Toutefois, c'est l'ensemble des dispositions du code des marchés publics qui doit être pris en compte, et ce, notamment compte tenu du dernier alinéa de l'article 56 qui dispose : « *Les dispositions du présent code qui font référence à des écrits ne font pas obstacle au remplacement de ceux-ci par un support ou un échange électronique.* ».
  → *En matière de marchés publics, la question relative à l'archivage est essentielle. Il en va de la preuve de la légalité du marché passé (procédure de passation, contrat). Les contrôles a posteriori qui doivent être exercés par les autorités compétentes doivent également être pris en compte*.
  Les précisions relatives aux documents devant être archivés par la personne publique et les durées de conservation sont mentionnées dans le vade-mecum du MINEFI et le Guide établi par la Mission pour l'Économie Numérique (cf. infra).

- **Décret n° 2004-617 du 29 juin 2004** relatif aux modalités et effets de la publication sous forme électronique de certains actes administratifs au Journal officiel de la République française (J.O. du 30 juin 2004). Ce décret qui permet la publication sous forme électronique de certains actes au journal officiel, et autorise qui plus est que cette publication soit effectuée exclusivement par voie électronique concernant les décisions individuelles et l'ensemble des

autres actes dépourvus de valeur réglementaire relevant de matières déterminées (article 2), implique la conservation de ces actes.
→ ***Impact direct sur l'archivage électronique***

- **Décret n° 2004-114 du 26 octobre 2004** relatif à l'exécution des marchés publics par carte d'achat (J.O. du 29 octobre 2004, p. 18259 et s.).

- **Décret n° 2004-1298 du 26 novembre 2004** relatif à diverses dispositions concernant les marchés de l'État et des collectivités territoriales (J.O. du 30 novembre 2004, p. 20310 et s.). L'article 1er modifie le code des marchés publics et ajoute à l'article 40 – IV un second alinéa ainsi rédigé « *Lorsque la direction des Journaux officiels est dans l'impossibilité de publier l'édition du Bulletin officiel des annonces des marchés publics dans sa version imprimée, elle peut se borner à la publier, à titre temporaire, sous sa forme électronique. Dans ce cas, elle avertit immédiatement les abonnés à la version imprimée de ce bulletin de l'interruption temporaire de sa parution.* ».
→ ***Cette disposition implique que les annonces ainsi publiées soient conservées sous leur forme électronique.***

- **Décret n° 2004-459 du 28 mai 2004** fixant les catégories d'actes individuels ne pouvant faire l'objet d'une publication sous forme électronique au Journal Officiel de la République française (J.O. du 29 mai 2004, p. 9583).

- **Décret n° 2005-324 du 7 avril 2005** relatif à la transmission par voie électronique des actes des collectivités territoriales soumis au contrôle de légalité et modifiant la partie réglementaire du code général des collectivités territoriales (J.O. du 8 avril 2005, p. 6340). Ce décret a été pris en application de l'article 139 de la loi n° 2004-809 du 13 août 2004 relative aux libertés et responsabilités locales. Il prévoit une procédure d'homologation du dispositif de télétransmission dont les modalités seront fixées par arrêté du ministre de l'intérieur ainsi qu'une convention comprenant la référence du dispositif homologué devant être conclue entre le responsable de l'exécutif local et le préfet.
→ ***Impact sur l'archivage électronique des actes et sur la traçabilité des échanges.***

- **Décret n° 2005-222 du 10 mars 2005** relatif à l'expérimentation de l'introduction et de la communication des requêtes et mémoires et de la notification des décisions par voie électronique (J.O. du 11 mars 2005, p. 4212 et s.). Ce décret détermine les caractéristiques essentielles que doit revêtir la procédure électronique de transmission utilisée pour cette expérimentation et précise qu'un arrêté du garde des Sceaux, définit ces caractéristiques, ainsi que les exigences imposées aux parties ou à leur mandataire pour qu'un document soit valablement transmis.
→ ***Impact sur l'archivage électronique des actes et sur la traçabilité des échanges.***

- **Décret n°2005-972 du 10 août 2005** modifiant le décret n°56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice, (J.O. du 11 août 2005, p. 13095) et **décret n°2005-973 du 10 août 2005** modifiant le décret n°71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, (J.O. du 11 août 2005, p. 13096). Ces deux décrets sectoriels pris en application de l'article 1317 alinéa 2 du code civil fixent les conditions d'établissement, de transmission et de conservation des actes authentiques électroniques qu'il s'agisse d'originaux ou de copies.
→ ***Impact sur l'archivage électronique des actes authentiques électroniques.***

- **Arrêté du 18 avril 2005** relatif aux conditions de protection du secret et des informations concernant la défense nationale et la sûreté de l'État dans les contrats (J.O. du 20 avril 2005, p. 6914). Cet arrêté s'applique à certaines catégories de marchés publics.

- **Arrêté du 26 octobre 2005** portant approbation d'un cahier des charges des dispositifs de télétransmission des actes soumis au contrôle de légalité et fixant une procédure d'homologation de ces dispositifs (J.O. du 3 novembre 2005, p. 17289).

- **Circulaire du 2 novembre 2001 relative à la gestion des archives dans les services et établissements publics de l'État** (PRMX0105139C). Cette circulaire précise les principes régissant la gestion des archives intermédiaires dans les services et établissements publics de l'État tant en termes d'identification des responsables que de moyens à mettre en œuvre

pour permettre cette gestion ainsi que le cadre du contrôle de la gestion des archives intermédiaires. A ce titre, les **archives intermédiaires** sont définies comme étant « *dans le cycle des archives, les documents qui, n'étant plus d'usage courant, doivent néanmoins être conservés temporairement à proximité des services d'origine pour les besoins administratifs ou juridiques.* ». Ces archives intermédiaires se distinguent des **archives définitives** « *(ou archives historiques) : dans le cycle de vie des archives ce sont les documents qui sont conservés indéfiniment, pour les besoins de la gestion et de la justification des droits des personnes et pour la documentation historique de la recherche. Ces archives définitives sont constituées, après tri et élimination, à partir des archives intermédiaires.* » et des **archives courantes** définies comme « *les documents utilisés pour le traitement quotidien des affaires et dont la conservation est assurée dans le service d'origine* ».
Spécifiquement en matière d'archives électroniques, la circulaire dispose que les agents chargés de la gestion des intermédiaires « *doivent notamment s'assurer, dans le respect de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, que la conception des traitements informatiques mis en œuvre permettra de conserver durablement les données dans les délais fixés par les instructions relatives à la durée d'utilité administrative et au sort final des documents. Ils s'assurent que les documents numériques à verser présentent toutes les garanties d'authenticité et sont accompagnés de l'ensemble des métadonnées indispensables à l'exploitation ultérieure des données.* ».
D'une manière générale, cette circulaire entend que la conservation et l'organisation des archives intermédiaires soient effectuées dans les locaux des services producteurs en coordination et sous le contrôle des services d'archives publics.
→ ***Impact sur l'archivage électronique des archives publiques.***

- **Circulaires du 21 janvier 2002** définissant le cadre d'interopérabilité des systèmes d'information publics communs aux administrations de l'État.

- **Circulaire du 4 décembre 2002** du Premier ministre, précisant les conditions de la mise en œuvre du cadre commun d'interopérabilité définit par le circulaire du 21 janvier 2002 (version 2), l'environnement et les conditions de mise en œuvre et d'utilisation opérationnels d'interopérabilité ; les conditions de réutilisation des logiciels et des ressources numériques de l'administration de l'État ; et invitant les collectivités territoriales à y participer**.**

- **Circulaire du 7 janvier 2004** portant manuel d'application du code des marchés publics (J.O. du 8 janvier 2004, p. 37031 et s.) modifiée par la **circulaire du 16 décembre 2004** (J.O. du 1er janvier 2004, p. 12813 et s.).

- **Instruction du 14 janvier 2005 relative aux modalités de délivrance du visa d'élimination des documents papier transférés sur support numérique ou micrographique** (DITN/DPACI/RES/2005/001). Cette instruction vise les opérations tendant à reproduire les documents papier avant l'expiration de leur durée d'utilité administrative sur des supports électroniques pour ensuite détruire ces documents papier. Elle rappelle que la destruction des documents papier reste soumise au visa de l'administration des archives même s'ils ont fait l'objet d'une copie sur un autre support lequel peut toutefois être accordé avant l'expiration du délai d'utilité administrative. Puis, l'instruction envisage la valeur juridique de ces copies et relève à ce titre que « *Au total s'il semble possible d'envisager l'élimination, après reproduction, des pièces justificatives ou des copies, souvent très abondantes dans les dossiers individuels, l'élimination d'originaux émanant de l'administration et engageant celle-ci doit, en revanche, être envisagée avec plus de prudence.* ».
→ ***Impact sur l'archivage électronique dans la mesure où ce texte permet notamment de différencier les règles applicables à l'élimination lorsque les documents concernés sont des documents numérisés et non des documents électroniques « originaux ». Ainsi un document numérisé est une copie et n'acquière pas la qualité d'original.***

- **Instruction du 3 mars 2005 relative aux actions entreprises par la direction des archives de France en matière d'archivage électronique dans le cadre du développement de l'administration électronique** (DITN/RES/2005/002).

- **Recommandations du 29 mars 2005 relatives à la gravure, à la conservation et à l'évaluation des CD-R** (DITN/RES/2005/004).

1.4.3 Droit fiscal

- **Loi n° 90-1169 du 29 décembre 1990 de finances rectificative pour 1990** (J.O. du 30 décembre 1990). Ce texte permet le recours à des factures « *E.D.I* ».

- **Loi n° 99-1173 de finances rectificative pour 1999 du 30 décembre 1999** (J.O. du 31 décembre 1999, p. 19968). Cette loi impose aux entreprises dont le chiffre d'affaire hors taxes réalisé au titre de l'exercice précédent est supérieur à 100 millions de francs de souscrire par voie électronique leurs déclarations d'impôt sur les sociétés à compter du 31 décembre 2000 et de souscrire et d'acquitter la TVA dont elles sont redevables, par voie électronique, à compter du 1er mai 2001.
  → ***Impact sur l'archivage électronique des déclarations.***

- **Loi n° 2002-1576 du 30 décembre 2002** de finances rectificatives pour 2002 (J.O. du 31 décembre 2002, p. 22070 et s.). Ce texte transpose la directive 2001/115/CE et reconnaît les factures transmises par voie électronique pour la déduction de la TVA, sous réserve du respect des conditions posées. L'article 17 pose le principe du recours à des factures électroniques signées à la condition qu'un contrat soit conclu entre l'émetteur et le destinataire de la facture.
  → ***Impact sur l'archivage électronique de ces documents et leur contrôle par les administrations compétentes.***

- **Décret n° 2003-632 du 7 juillet 2003** relatif aux obligations de facturation en matière de taxe sur la valeur ajoutée et modifiant l'annexe II du code général des impôts et la deuxième partie du livre des procédures fiscales (J.O. du 9 juillet 2003, p. 11617 et s.). Texte pris en application de la loi n° 2002-1576.
  → ***Impact sur l'archivage électronique de ces documents et leur contrôle par les administrations compétentes.***

- **Décret n° 2003-659 du 18 juillet 2003** relatif aux obligations de facturation en matière de taxe sur la valeur ajoutée et modifiant l'annexe III du code général des impôts et la deuxième partie du livre des procédures fiscales (J.O. du 20 juillet 2003, p. 12272 et s.).

- **Arrêté du 28 février 2001** (J.O. du 6 mars 2001, p.3488). Cet arrêté autorise la mise en œuvre par la Direction Générale des Impôts du traitement informatisé de la transmission, par voie électronique, des éléments déclaratifs en matière d'impôt sur le revenu et porte conventions types relatives à ces opérations.

- **Instruction fiscale du 12 juillet 1999** précisant les modalités d'application de l'arrêté du 3 mai 1999 relatif aux factures transmises par voie électronique. Cette instruction fiscale indique que le système de télétransmission doit assurer les fonctions suivantes au titre de l'archivage :
  - *constitution quotidienne et archivage d'une liste récapitulative séquentielle et exhaustive des messages émis et/ou reçus et des anomalies éventuelles détectées lors de contrôles ;*
  - *archivage des factures émises et reçues ;*
  - *les informations émises et reçues doivent être conservées dans leur contenu originel, pendant un délai de six ans ;*
  - *le support informatique sur lequel sont conservés les messages factures doit être alimenté automatiquement par le système des informations qui en sont directement issues ;*
  - *l'obligation de conservation porte sur l'intégralité du message émis ou reçu ;*
  - *la liste récapitulative et un fichier des partenaires avec lesquelles l'entreprise échange des factures par télétransmission doit être conservée dans les mêmes conditions ;*
  - *possibilité de restituer les documents en langage clair à la demande de l'administration ;*
  - *la restitution doit pouvoir être opérée de manière sélective*.

  Ainsi, l'archivage constitue l'un des éléments des fonctionnalités assurées par le système de télétransmission de factures dont il est indissociable.
  → ***Impact sur l'archivage électronique de ces documents et leur contrôle par les administrations compétentes.***

- **Instruction fiscale de la Direction Générale des Impôts du 7 août 2003** – Taxe sur la valeur ajoutée. Obligations des assujettis. Obligations relatives à l'établissement des factures (Bulletin officiel des impôts, n° spécial, 3 C.A., n° 136 du 7 août 2003).
  → ***Impact sur l'archivage électronique de ces documents et leur contrôle par les administrations compétentes.***

1.4.4 Sécurité

- **Loi nº 2004-669 du 9 juillet 2004** relative aux communications électroniques et aux services de communication audiovisuelle (J.O. du 10 juillet 2004, p. 12483 et s.). Cette loi, qui a remplacé le code des postes et télécommunications par le code des postes et des communications électronique (CPCE), fixe notamment, le régime juridique applicable à la conservation des données de connexion (article L. 34-1 du CPCE). Cette disposition, qui a pour objet de faciliter la lutte contre la cybercriminalité, entre pleinement dans une logique de renforcement de la sécurité et vise l'ensemble des prestataires techniques au sens de l'article 6-I-1 de la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004 (c'est-à-dire « *les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne (…).* »).

- **Loi n° 2001-1062 du 15 novembre 2001** relative à la sécurité quotidienne (J.O. du 16 novembre 2001, p. 18215).

- **Loi n° 2003-239 du 18 mars 2003** pour la sécurité intérieure (J.O. du 19 mars 2003, p. 4761).

- **Loi n° 2004-204 du 9 mars 2004** portant adaptation de la justice aux évolutions de la criminalité (J.O. du 10 mars 2004, p. 4567).

- **La loi n° 2004-575 du 21 juin 2004** pour la confiance dans l'économie numérique dite LCEN (J.O. du 22 juin 2004, p. 11168). Les articles 29 à 40 de la loi traitent de la sécurité et plus particulièrement de la cryptologie. Cette loi a abrogé l'article 28 de la loi n° 90-1170 du 29 décembre 1990 modifiée (J.O. du 30 décembre 1990, p. 16439). Les textes d'application doivent être adoptés.

- **Décret n° 96-67 du 29 janvier 1996** modifié relatif aux compétences du S.G.D.N. dans le domaine de la sécurité des systèmes d'information (J.O. du 30 janvier 1996, p. 1443).

- **Décret n° 98-102 du 24 février 1998** modifié (J.O. du 25 février 1998, p. 2915). Ce décret définit les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui les conventions secrètes de cryptologie. Néanmoins, l'article 28 de la loi n° 90-1170 du 29 décembre 1990 sur la réglementation de la télécommunication ayant été abrogée par la LCEN, on peut s'interroger sur l'applicabilité de ce texte depuis le 22 juin 2004.

- **Décret n° 99-199 du 17 mars 1999** définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle de l'autorisation (J.O. du 19 mars 1999, p. 4050). Néanmoins, l'article 28 de la loi n° 90-1170 du 29 décembre 1990 sur la réglementation de la télécommunication ayant été abrogée par la LCEN, on peut s'interroger sur l'applicabilité de ce texte depuis le 22 juin 2004.

- **Décret n° 99-200 du 17 mars 1999** définissant les catégories de moyens et de prestations de cryptologie dispensés de toute formalité préalable (J.O. du 19 mars 1999, p. 4051). Néanmoins, l'article 28 de la loi n° 90-1170 du 29 décembre 1990 sur la réglementation de la télécommunication ayant été abrogée par la LCEN, on peut s'interroger sur l'applicabilité de ce texte depuis le 22 juin 2004.

- **Décret n° 2001-693 du 31 juillet 2001** créant au S.G.D.N. une Direction Centrale de la Sécurité des Systèmes d'Information (J.O. du 2 août 2001, p. 12496).

- **Décret 2001-1192 du 13 décembre 2001** relatif au contrôle à l'exportation, à l'importation et au transfert de biens et technologies à double usage (J.O. du 15 décembre 2001, p. 19905). Ce décret assure l'adaptation du droit national au règlement du Conseil n°1334/2000 du 22 juin 2000 instituant un régime communautaire de contrôle des exportations de biens et technologies à double usage (J.O.C.E. L. 159 du 30 juin 2000, p.1 ; ce règlement a été

modifié par les règlements n° 2289/2000 du Conseil du 22 décembre 2000 (J.O.C.E. L. 336 du 30 décembre 2000, p.14) et n° 458/2001 du 6 mars 2001). De plus, il convient de signaler les annexes définissant notamment les conditions d'utilisation de l'autorisation générale communautaire d'exportation n° EU001 (modifiées en dernier lieu par le règlement du Conseil n° 1504/2004 du 19 juillet 2004 portant modification et mise à jour du règlement CE n° 1334/2000, J.O.U.E. L. 281 du 31 août 2004, p.1).

- **Décret n° 2002-535 du 18 avril 2002** relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information (J.O. du 19 avril 2002, p. 6944). Ce texte adopté dans le contexte du dispositif réglementaire relatif aux signatures électroniques a une portée plus large et concerne la certification de la sécurité offerte par des produits ou des systèmes des technologies de l'information, « *au regard notamment de leur aptitude à assurer la disponibilité, l'intégrité ou la confidentialité de l'information traitée face aux menaces dues en particulier à la malveillance* » (alinéa 1er de l'article 1er du décret). Étant noté qu'il est précisé « *Les administrations de l'État recourent, dans la mesure du possible et en fonction de leurs besoins de sécurité, à des produits ou des systèmes des technologies de l'information certifiés suivant la procédure prévue au présent décret* » (alinéa 2 de l'article 1er du décret).
  → *Impact possible sur la certification de la sécurité offerte par des produits et services en matière d'archivage électronique.*

- **Décret n° 2002-997 du 16 juillet 2002** relatif à l'obligation mise à la charge des fournisseurs de prestations de cryptologie en application de l'article 11-1 de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications (J.O. du 18 juillet 2002, p.12255).

- **Arrêté du 15 mars 2002** portant organisation de la direction centrale de la sécurité des systèmes d'information (J.O. du 17 mars 2002, p. 4838).

- **Arrêté du 18 avril 2005** relatif aux conditions de protection du secret et des informations concernant la défense nationale et la sûreté de l'État dans ses contrats (J.O. du 20 avril 2005, p. 6914 et s.).

1.4.5 Données à caractère personnel

Ces textes sont mentionnés dans la mesure où les règles de conservation des données à caractère personnel sont spécifiques. Elles doivent être prises en compte dans le cadre de l'archivage électronique le cas échéant.

- **Loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés (J.O. du 7 janvier 1978, p. 7 et s.).

- **Loi n° 2004-801 du 6 août 2004** relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (J.O. du 7 août 2004, p. 14063 et s.).

- **Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie (J.O. du 17 août 2004, p 14598 et s.).** Cette loi a introduit un article L. 161-36-1 A du code de la sécurité sociale qui dispose dans son I alinéa 4 : « *Afin de garantir la confidentialité des informations médicales mentionnées aux alinéas précédents, leur conservation sur support informatique comme leur transmission par voie électronique entre professionnels, sont soumises à des règles définies par décret en Conseil d'État pris après avis public et motivé de la Commission Nationale de l'Informatique et des Libertés.* ».

- **Décret n° 2005-1309 du 20 octobre 2005** pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-80 du 6 août 2004 (J.O. du 22 octobre 2005).

1.4.6 Les normes et guides

1.4.6.1 Les principales normes nationales

Rappel : Une norme est définie par l'Organisation internationale de normalisation (ISO) et la Commission Électrotechnique Internationale (CEI) comme étant un « *document, établi par le consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné.* ». Il a ainsi été jugé que l'existence d'une norme permet de représenter un état de l'art dans le domaine auquel elle se rapporte (Cass. Civ. 3ème ch. du 4 février 1976, Bull. civ. III, n°49), même si elle n'a pas, de droit, de caractère contraignant.

C'est pourquoi, les normes n'auront un impact direct sur l'archivage électronique que si elles sont directement intégrées dans un texte réglementaire national, ce qui n'est pas le cas actuellement, ou si la personne chargée de l'archivage choisit officiellement de s'y conformer.

Néanmoins, ***les normes en matières d'archivage électronique présentent l'intérêt de déterminer des procédures d'organisation qui permettent, dans une certaine mesure, d'encadrer le processus d'archivage***.

- **La norme AFNOR Z 42-01317** « *Archivage électronique – Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes* », homologuée en décembre 2001. Cette norme fournit un ensemble de spécifications concernant les mesures techniques et organisationnelles à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques afin d'assurer la conservation et l'intégrité de ceux-ci. Pour atteindre l'objectif d'intégrité, cette norme préconise de stocker les documents sur des supports non réinscriptibles de type WORM (Write Once Read Many) ou équivalents, gérés, du point de vue fichiers et volumes, conformément aux standards ISO 13490 ou 13346. Cette norme est en cours de modification.

- **Le projet de norme ISO/WD 15809-1, Electronic archival storage.** Ce projet de norme reprend au plan international la norme française AFNOR Z 42-013. Il vise notamment, a établir les références pour la conception et l'exploitation de systèmes informatiques destinés à la conservation des documents.

- **Norme Z 43-100.** Cette norme a pour objet de préciser, s'agissant de l'emploi de supports micrographiques, les conditions dans lesquelles la conservation des documents doit être effectuée, notamment dans l'hypothèse d'une conservation de longue durée. Cependant, l'impression micrographique ne consiste pas à proprement parler en une conservation électronique dans la mesure où les informations sont matérialisées. Cette solution n'est envisageable que si le document électronique à conserver possède une représentation visuelle imprimable.

1.4.6.2 Les principaux guides et documents de référence

Les guides et autres documents de référence qui suivent constituent des recommandations, qui à l'heure actuelle, n'ont pas de caractère contraignant (ce qui est susceptible d'évoluer notamment pour les PRIS). Sans s'imposer, ces documents sont à prendre en compte dans la réflexion dans la mesure où ***ils contribuent à poser les bases de l'état de l'art, en matière d'archivage électronique, et ce, notamment dans la sphère publique***.

- **Le guide « *Conservation des informations et des documents numériques pour les téléprocédures, les intranets et les sites internet : format, support, métadonnées, organisation, XML et normalisation* »** de l'Agence pour les Technologies de l'Information et de la Communication dans l'Administration (ATICA) repris par l'Agence pour le Développement de l'Administration Électronique (ADAE). Ce guide est destiné en premier lieu aux maîtres d'ouvrage de téléprocédures et aux maîtres d'ouvrage qui ont la charge des sites Intranet et internet. Il fournit des recommandations pour la mise en œuvre de l'archivage et décrit les formats, les métadonnées, les supports et l'organisation qui permettent de déterminer les conditions de conservation des documents numériques produits et/ou reçus.

- **Politique de Référencement Intersectoriel de Sécurité (PRIS) - V1 -** relative à la mise en place d'un référentiel documentaire identifiant des niveaux croissants de sécurité s'appliquant à différents services de confiance et disponible sur le site www.adae.gouv.fr . Les politiques de Référencement Intersectorielle Section A et B Entreprise**/Individu** - Authentification** - Signature** prévoient s'agissant de l'archivage que « *les données à archiver sont au moins les suivantes :*
  - *les fichiers de configuration des équipements informatiques,*
  - *les PC,*
  - *les DPC,*
  - *les agréments contractuels avec d'autres AC,*
  - *les certificats et les LCR tels qu'émis ou publiés,*
  - *les récépissés ou notifications (à titre informatif),*
  - *les justificatifs d'identité des porteurs,*
  - *les journaux d'évènements de l'AC et l'AE.*

  Pendant tout le temps de leur conservation, les archives doivent :
  - *être protégées en intégrité,*
  - *être accessibles aux personnes autorisées (48 heures ouvrées pour les archives papier et conformément au plan de reprise après incident pour les archives électroniques),*
  - *pouvoir être lues et exploitées.*

  L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver les pièces en toute sécurité. »

  De plus, « *tout dossier de demande de certificat accepté doit être archivé pendant au moins cinq ans, comptés au maximum à partir de l'acceptation du certificat par son porteur. Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées. Ce dossier, complété par les mentions consignées par l'AC doit permettre de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.* ». De même, « *les certificats de clés de signature ainsi que les LCR produites doivent être archivés pendant au moins cinq ans après l'expiration des clés. L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver les éléments en toute sécurité.* ». Au même titre « *les journaux d'événements de l'AC (et éventuellement ceux de l'AE) seront archivés pendant cinq ans après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage devront offrir le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements devra être garantie tout au long de leur cycle de vie.* ».

  Par ailleurs, la politique de certification pour les AC – authentification avec imputabilité - Individu comme Entreprise dispose, concernant les archives, que « *l'AC archive toutes les données qui pourraient être utiles à la preuve de la certification d'un UF. Ces données à archiver, et documentées sont les suivantes :*
  - *accords contractuels ou conventions avec d'autres IGC*
  - *certificats de l'UF et de composantes*
  - *CRL*
  - *Demandes de révocation et leurs résultats*
  - *Données d'identifications personnelles de l'UF (y compris quand cela est utilisé le lien entre un signataire et son certificat qualifié) dont le numéro de référence et les limitations de validité et d'usage des pièces d'identité officielles utilisées lors de l'enregistrement.*
  - *Journaux d'événement des entités de l'IGC en relation avec les opérations propres aux certificats et le cas échéant aux bi-clés cryptographiques.*
  - *Logiciels et fichiers de configuration des différentes composantes*
  - *Récépissé des communications internes et externes de l'IGC*
  - *Ensemble de tous les éléments utiles à l'enregistrement d'un UF demandé dans la demande de certificat et pour son authentification.*
  - *Nature des documents présentés par le demandeur.*
  - *Emplacement où sont conservées les copies des formulaires remplis par le demandeur, y compris le document manifestant l'adhésion et l'acceptation du demandeur aux conditions d'utilisation et du contenu du certificat.*
  - *Identité de la personne morale au nom de laquelle a lieu la demande.*
  - *Méthode utilisée pour validée les documents d'identité.* ».

  S'agissant de la période de rétention des archives il est précisé que cette dernière « *résulte d'un compromis entre le besoin et les contraintes de moyens de conservation. La durée de conservation des informations relative à la certification de l'UF dépend des obligations légales de conservation de preuves pour les transactions sécurisées à l'aide du certificat qualifié de*

l'UF et de besoins pour faire la preuve de la certification de l'UF. Dans la plupart des cas des clauses limitant la période de contestation possible de la transaction sont susceptibles de déterminer la durée minimale de conservation des informations. ».
En outre, « *les archives doivent être protégées en intégrité et en disponibilité. La définition de la sensibilité des journaux d'événement dépend de la nature des informations traitées et du métier. Elle doit être définie au cas par cas. Elle peut causer un besoin de protection en confidentialité.* ». Enfin, « *il est recommandé que l'AC définisse dans sa DPC la précision de l'horloge pour dater les événements enregistrés ou archivés et comment elle atteint cette précision.* ».

- **Politique de Référencement Intersectoriel de Sécurité (PRIS) – V2,** en matière d'archivage, la PC Type – Authentification, reprend les exigences de la PRIS V1 mentionnées ci-dessus.

- **Le cadre commun d'interopérabilité des systèmes d'information publics (version 2)**, publié par l'A.D.A.E. en février 2003, disponible à l'adresse : www.adae.gouv.fr.

- **Standard d'échange de données pour l'archivage électronique – versement – communication - élimination**, établi par l'A.D.A.E. et la Direction des Archives de France. Le standard d'échange fait actuellement l'objet d'un appel à commentaires et sera, en principe, stabilisé au cours du premier trimestre 2006. Ce standard dont l'objectif vise à permettre une interopérabilité entre les systèmes d'information entre services producteurs, services d'archives et tierces entités, porte sur la normalisation des schémas de données intervenant dans le versement et la communication de documents électroniques. Il a vocation à être intégré au référentiel général d'interopérabilité prévu par l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (J.O. du 9 décembre 2005, p. 18986).

- **Vade-mecum juridique sur la dématérialisation des marchés publics** établi par la Direction juridique du MINEFI disponible sur le site : www.minefi.gouv.fr. Selon ce vade-mecum « *les dispositions du code du patrimoine relatives aux archives s'appliquent aux documents quel que soit leur support matériel donc y compris aux documents électroniques. En particulier, la décision d'archiver et le choix des documents reviennent en ce qui concerne les marchés publics à l'autorité publique chargée de leur passation et/ou de leur exécution, en collaboration avec l'administration des archives.* ».
  Il est ajouté que « *la fiabilité des documents archivés quel que soit leur support réside dans la confiance accordée à la personne publique. (…) Dans le cas d'un marché sous la forme d'un dossier électronique, c'est la signature électronique de ce marché par la personne publique qui lui conférera le caractère de seul exemplaire de référence. Pour les autres pièces relatives aux marchés publics destinées à être archivées, une attestation ou un certificat de nature administrative délivré par la personne responsable du marché qui pourrait être un document électronique, leur conférera fiabilité préalablement à leur archivage.* ».
  « *Quant à la pérennité, elle s'apprécie dans la conservation des documents, l'obsolescence rapide des matériels, logiciels, périphériques pouvant entraîner une non-lisibilité des informations dans des délais relativement courts (compris entre 5 et 10 ans).* ».
  « *Ces différentes opérations ne remettent pas en cause à terme la valeur probante de ces documents qui doit toujours être appréciée au regard des règles juridiques contemporaines à leur formation.* ».
  De même, les concepts généraux de l'archivage, la nature et la durée de conservation des documents électroniques des marchés y sont étudiés.

- **Archivage électronique**, guide rédigé par un groupe d'étude du Conseil supérieur de l'ordre des experts comptables présidé par G. Rouquette, 1998, publié aux éditions Expert Comptable Media.

- **Guide de l'archivage électronique sécurisé, Recommandations pour la mise en œuvre d'un système d'archivage interne ou externe utilisant des techniques de scellement aux fins de garantir l'intégrité, la pérennité et la restitution des informations,** de juillet 2000, disponible sur le site : www.edificas.org.

- **Les archives électroniques,** Manuel pratique publié par la Direction des archives de France, Catherine Dhérent, 2002, disponible sur commande à l'adresse suivante :

http://larecherche.servicepublic.fr/df/oxide?criteriaContent=dherent&page=resultsdfB&action=launchsearch&DynRubrique=Catalogue&DynCorpus=&DynDomain=Catalogue

- **Charte des principes juridiques pour un archivage électronique sécurisé et de confiance,** Fédération Nationale des Tiers de Confiance, 2002.

- **Guide de l'horodatage,** Fédération Nationale des Tiers de Confiance, 2005, disponible à l'adresse : www.fntc.org.

- **La conservation de la signature électronique : Perspectives archivistiques,** Jean-François Blanchette, Rapport remis à la Direction des Archives de France, Ministère de la Culture, septembre 2004, disponible à partir du site des archives de France (www.archivesdefrance.culture.gouv.fr) Ce rapport prend en considération l'entrée en vigueur de la loi du 13 mars 2000 et de ses décrets d'application du point de vue de l'archivage et de la valeur probante des documents. Après avoir décrit les technologies de signature numérique, l'auteur s'attache à définir le cadre juridique de cette signature puis les stratégies techniques permettant sa conservation. Enfin, un état des lieux des solutions adoptées par des grandes institutions d'archivage étrangères est dressé.

- **Guide technique de la sécurité de la dématérialisation des achats publics** du 20 avril 2005 réalisé par la Mission pour l'économie numérique et disponible à l'adresse : www.men.minefi.gouv.fr/webmen/themes/adm/recommandations.doc. L'annexe 8 de ce guide est relative à l'archivage. Elle précise notamment eu égard à la longue durée de conservation des documents relatifs à la procédure de marchés publics que l'on peut « *se contenter dans un premier temps, d'archiver les fichiers afférents à la procédure sur un CD-ROM, avec la signature qui est apposée, pour ceux qui sont signés, et en précisant alors que leur signature était valable au moment où elle a été apposée ; si la PRM dispose d'un certificat, il est utile qu'elle signe elle-même ces archives ; sinon elle doit prendre les précautions nécessaires pour que ces archives ne puissent être contestées.* ».

- Manuel « **Archivage des documents bureautique** », réalisé par J. Poivre et la Direction des Archives de France, 2004, paru à la Documentation Française, à commander à l'adresse : www.ladocumentationfrançaise.fr.

- Guide « **Comprendre et pratiquer le Record Management** : **Analyse de la norme ISO 15489 au regard des pratiques archivistiques françaises** », par le groupe Métiers de l' A.A.F. (Association des Archivistes Français) et de l'A.D.B.S. (Association des Professionnels de l'Information et de la Documentation), 2005, disponible à l'adresse : www.adbs.fr/site/publications/rm/evalnorme_iso15486.pdf.

- Recommandation du Forum des Droits de l'Internet relative à la **Conservation électronique des documents** (secteur privé), publié le 1er décembre 2005 en partenariat avec la Mission pour l'Économie Numérique et disponible à l'adresse : www.foruminternet.org/telechargement/documents/reco-archivage-20051201.pdf. Ce document appréhende la problématique de l'archivage électronique dans la sphère privée et tente d'apporter certains éléments de réponse.

2 Partie technique

2.1 Éviter les confusions

Plutôt que d'élaborer un glossaire nous préférons remettre un ensemble de termes dans leur contexte et expliquer les différences qui peuvent exister ou les erreurs à ne pas commettre. Ce qui suit ne se veut pas exhaustif mais traite de la majorité des cas pouvant être rencontrés.

Limites :

Il est également important de préciser les limites de notre analyse dans la mesure où de façon générique les documents électroniques peuvent, soit résulter d'un processus de numérisation, soit être produits directement par un processus informatique. Seul ce dernier cas sera pris en considération ce qui explique que nous ne nous intéresserons pas, par la suite, à tout ce qui concerne l'aspect numérisation ainsi qu'aux procédures et matériels associés. L'autre point important relève de la prise en compte de l'archivage vu sous son côté légal c'est à dire le traitement des documents à valeur probante ce qui élimine du champ ne serait-ce que l'ensemble des données à caractère patrimonial.

Données, document, fichier, information, objet :

Pour simplifier nous retiendrons que les données servent de base à la constitution d'un fichier, que un ou plusieurs fichiers constituent un document et que un document ou un ensemble de documents représentent de l'information. Le terme fichier a plus une connotation informatique alors que document est déjà plus proche du contenu au sens informationnel.
Les données peuvent être de toute nature : texte, images, vidéo…
La notion d'objet représente plus un terme générique dont la signification est à rapprocher de l'un des termes évoqués précédemment en fonction du contexte.

Intégrité :

Ce terme a son importance dans la mesure où sa signification peut être différente suivant que l'on se place d'un côté technique ou juridique. Globalement la garantie d'intégrité consiste à préserver l'objet dans son état d'origine, sans altération aucune. Techniquement cela se vérifie entre autre grâce à des algorithmes de hashage qui détectent la moindre modification ne serait ce que d'un seul bit à l'intérieur d'un fichier. A l'inverse, d'un point de vue juridique, l'intégrité concerne l'information quel que soit le format du support de cette information tant logique que physique. Il est ainsi tout à fait possible de modifier l'intégrité technique des fichiers (suite à un processus de migration par exemple) sans altérer l'intégrité de l'information.

Stockage, conservation, archivage :

Ces trois termes sont parfaitement complémentaires et s'imbriquent les uns dans les autres du fait de leurs fonctionnalités respectives. Ainsi la conservation consiste en une action destinée à préserver, et surtout à maintenir intact l'objet conservé, en utilisant différents types de stockage pour ce même objet.
L'archivage revient à prendre en compte, en plus de la conservation, les opérations qui entourent cette dernière comme le fait de recueillir, de classer et de permettre l'interrogation dans le temps des objets concernés.

Archivage, sauvegarde :

Ces deux termes sont plutôt à comparer suivant leurs finalités respectives lesquelles sont totalement différentes. En effet la sauvegarde, tout comme l'archivage revient à conserver de l'information et comprend les opérations permettant d'atteindre cet objectif.
Par contre la finalité de la sauvegarde est uniquement de permettre une copie des données d'origine dite copie de sécurité afin d'éviter de les perdre en cas de dysfonctionnement du dispositif sur lequel elles sont enregistrées. De ce fait, la durée de conservation est relativement limitée mais surtout les données concernées doivent être mises à jour très régulièrement pour ne pas dire en permanence. A l'inverse l'archivage doit permettre une conservation qui peut être beaucoup plus longue, voire *ad vitam eternam*. De même l'archivage autorise une interrogation aisée, même si elle est contrôlée, des objets conservés. Contrairement à la sauvegarde, les données archivées sont considérées comme figées, c'est-à-dire non modifiables.

Rétention :

Ce mot est à bannir du vocabulaire dans un contexte d'archivage. En effet, il provient d'une mauvaise traduction de son équivalent anglais « retention » dont la signification est tout autre dans la mesure où elle indique une durée de conservation.

Gestion des archives, records management :

La principale différence entre le records management et la gestion des archives est la nécessité de capter les documents à la source, dès la fixation des données et la validation du document. En effet, si l'on attend un mois ou un an pour archiver ou sécuriser des données comment être sûr de l'intégrité du document lors de sa restitution ? Si l'on se réfère aux trois étapes retenues pour le cycle de vie de l'archive, à savoir : courante, intermédiaire et patrimoniale, le records management ne concerne que les deux premières étapes. Précisons également que l'archive intermédiaire est définie comme la durée pendant laquelle les données possèdent une quelconque utilité pour l'organisme producteur.

GED ou GEID, SAE :

La GED (Gestion Électronique de Documents) ou GEIDE (Gestion Électronique d'Informations et de Documents Existants), pour reprendre la définition donnée par l'APROGED (Association des Professionnels de la GEIDE) représente un ensemble d'outils et de techniques qui permettent de dématérialiser, classer, gérer et stocker des documents à partir d'applications informatiques dans le cadre normal des activités de l'entreprise.

S'agissant de stockage, la différence est importante avec un SAE (Système d'Archivage Électronique) dont le rôle est de conserver des documents électroniques. De même la majorité de l'activité GED est basée sur la notion de numérisation de document existant, opération que nous avons a priori éliminée de notre champ d'investigation. Néanmoins, pour une meilleure compréhension de l'ensemble de la problématique relative à l'archivage électronique nous reproduisons ci-dessous un tableau comparatif des deux approches, tiré du document décrivant les spécifications MoReq.

Un système de GED	**Un système d'archivage électronique**
• permet la modification des documents et la production de plusieurs versions ;	• interdit la modification des documents ;
• peut permettre la destruction des documents par leurs auteurs ;	• interdit la destruction de documents en dehors d'un contrôle strict ;
• peut comporter la gestion de durées de conservation ;	• comprend obligatoirement un contrôle rigoureux des durées de conservation ;
• peut comprendre une structure organisée de stockage, sous le contrôle des utilisateurs ;	• comprend obligatoirement une structure rigoureuse de classement (le plan de classement), gérée et contrôlée par l'administrateur ;
• est *a priori* dédié à la gestion quotidienne des documents pour la conduite des affaires.	• peut faciliter les tâches quotidiennes mais est aussi destiné à la constitution d'un fonds sécurisé des documents probants de l'entreprise.

ASP, SSP, TTP, TA :

Ces acronymes nous permettent d'aborder une notion importante liée à l'archivage qui est celle du service offert par des tiers. Ainsi l'ASP ou Service Application Provider en est le nom générique. Typiquement l'ASP fournit à son client un traitement à distance, plus ou moins spécialisé comme par exemple pour les plus connus les ISP (Internet Service Provider), traduit par FAI (Fournisseur d'Accès Internet) ou encore les SSP (Storage Service Provider). Plus proche de nous, se trouvent les TTP (Trusted Third Party) ou tiers de confiance qui sont apparu en même temps que le développement de la signature électronique dont celui qui nous intéresse tout particulièrement est tiers archiveur (TA).

2.2 Les contraintes

Les objectifs auxquels doit répondre tout système d'archivage électronique sont multiples et ne pourront être atteints qu'en respectant un ensemble de mesures dont une grande partie repose sur des aspects purement techniques. Il en est ainsi de l'intégrité, de la sécurité et de la pérennité des données pour lesquelles il faudra savoir gérer et anticiper le principe de l'obsolescence technologique récurrente tout en facilitant leur accès.

Les contraintes technologiques sont d'autant plus importantes qu'une fois en place, un système d'archivage inefficace aura beaucoup de mal à être corrigé compte tenu du volume d'information à traiter.

Nous allons maintenant aborder un peu plus en détail les différentes contraintes rencontrées.

2.2.1 Format logique

Les différents formats logiques disponibles pour un document dépendent du type de document. C'est ainsi qu'il existe des formats spécifiques pour les images, les textes sans mise en forme, les textes avec mise en forme, les pages prêtes à l'impression, etc.

Formats images :

- JPEG Joint Photographic Expert Group ;
- PNG Portable Network Graphics ;
- SVG Scalable Vector Graphics ;
- GIF Graphic Interchange Format ;
- TIFF Tagged Image File Format;
- PNG Portable Network Graphics ;
- BMP ;
- PCX.

Formats textes sans mise en forme :

- ASCII, souvent indiqué comme TXT.

Formats textes avec mise en forme :

- HTML Hyper Text Markup Language;
- RTF Rich Text Format ;
- Open Document Format for Office Application, la version v1.0 de ces spécifications a été approuvée par l'OASIS (Organization for the Advancement of Structured Information Standards) en mai 2005 ;
- DOC.

Formats pages prêtes à l'impression :

- PDF Portable Document Format. Signalons que le format PDF/A (A pour archive) vient d'être normalisé sous la référence ISO 19005-1 : Format de fichier des documents électroniques pour une conservation à long terme - Partie 1: Utilisation du PDF 1.4 (PDF/A-1) ;
- PS PostScript.

XML (eXtensible Markup Language) :

XML a été mis au point par le XML Working Group sous l'égide du World Wide Web Consortium (W3C) dès 1996. Depuis le 10 février 1998, les spécifications XML 1.0 ont été reconnues comme recommandations par le W3C, ce qui en fait un langage reconnu. (Tous les documents liés à la norme XML sont consultables et téléchargeables sur le site web du W3C, http://www.w3.org/XML/).

Les principaux atouts de XML sont les suivants :

- XML est un standard ouvert, gratuit, libre de droits ;
- Les fichiers XML sont au format texte, ils sont facilement lisibles et compréhensibles ;
- Un document XML est auto descriptif : il contient d'une part la structure des données et d'autre part les données elles-mêmes ;
- Le langage XML est un métalangage, il est extensible à souhait : il permet de créer ses propres balises ;
- Sa structure arborescente permet de modéliser la majorité des problèmes informatiques ;
- Il est universel et portable : le format texte qui tient compte des différents jeux de caractères est compréhensible par tous les systèmes d'exploitation ;
- Il est déployable : il peut être facilement distribué par n'importe quels protocoles à même de transporter du texte, comme HTTP ;
- Il a un niveau élevé d'intégrabilité : un document XML est utilisable par toute application pourvue d'un parser (c'est-à-dire un logiciel permettant d'analyser un code XML)

Ainsi, XML est particulièrement adapté à l'échange de données et de documents.

L'utilisation de ce format dans le standard de métadonnées garantit la lisibilité et l'intelligibilité de ces métadonnées sur une longue durée. En effet, des techniques de rafraîchissement et de migration existent et pourront être employées sans difficulté avec les documents en formats structurés XML, car ces documents ne contiennent que du « texte pur »

Le choix parmi tel ou tel format devra se faire en fonction de divers critères dont le premier est incontestablement celui de la pérennité, la capacité à être migré ou encore converti, ceci sans oublier le facteur économique.

Il faut également distinguer les notions de formats ouverts, fermés ou propriétaires. Le format ouvert est par définition facilement accessible quant à ses spécifications tant pour les aspects techniques que légaux. A l'inverse, un format fermé ne permet pas cette accessibilité. En ce qui concerne les formats propriétaires, en général liés aux fournisseurs, ils peuvent être soit ouverts soit fermés.

À titre complémentaire nous citerons également l'EAD, format de métadonnées spécifique pour la description des documents d'archives.

Il est clair qu'il faudra privilégier l'utilisation d'un format qui permette l'intelligibilité, soit en lecture directe (exemple du TXT voire de l'XML), soit par utilisation d'un interpréteur relativement facile à écrire en cas de besoin (cas du PDF et plus particulièrement du PDF/A). On aura par contre soin d'éliminer tous types de formats propriétaires issus de traitements ou de logiciels dont la pérennité ne peut être assurée. En ce qui concerne le choix en matière de format on pourra avantageusement se référer au cadre commun d'interopérabilité sur cette question : **Cadre commun d'interopérabilité des systèmes d'information publics Version 2.1** accessible à l'adresse http://www.adae.gouv.fr/article.php3?id_article=219

2.2.2 Format physique ou type de support

Aujourd'hui, un grand nombre de types de supports est disponible pour l'archivage. On distingue généralement deux grandes familles : les supports magnétiques et les supports optiques.

S'agissant des supports magnétiques nous distinguerons les bandes magnétiques, des disques magnétiques et des nouvelles technologies qui en sont issues. En ce qui concerne les supports optiques nous citerons successivement les CD, puis les DVD et enfin les disques magnéto-optiques. Néanmoins avant de décrire ces dispositifs, il est nécessaire de bien préciser une notion pour la moins importante : celle du WORM ou « write once, read many ».

2.2.2.1 La notion de WORM

Nous donnons ci-après une définition élargie du WORM, extraite du projet de norme ISO 18509, évolution de la norme NF Z42-013. Le WORM fait ainsi référence à une méthode d'enregistrement dont la propriété intrinsèque est d'être non effaçable, non réinscriptible et non modifiable.

Trois types particuliers ont été définis:

- Type A: transformation permanente du support, principe des disques optiques avec modification du substrat ;
- Type B: utilisation d'un micro-code WORM inclue dans le support au moment de sa fabrication, reconnu par le lecteur ou le contrôleur et protégé de l'effacement et de la ré-écriture dans des conditions normales d'utilisation, principe des disques magnéto-optiques ou des bandes équivalentes ;
- Type C: génération d'un micro code enregistré avec l'information et destiné à traiter cet enregistrement comme un enregistrement de type WORM par le logiciel de gestion du support, le protégeant du même coup de l'effacement et de la ré-écriture dans des conditions normales d'utilisation, principe des disques magnétiques. Dans certain cas la protection de type WORM peut être limitée à une durée de conservation associée aux données à protéger.

2.2.2.2 Les supports magnétiques

La bande magnétique

Loin d'être obsolètes, les bandes magnétiques sont encore utilisées comme supports d'archivage alors que les temps d'accès sont plutôt médiocres comparés aux autres supports de

stockage optiques ou magnétiques et que leur pérennité est largement contestée. Ceci certainement en raison de leurs coûts très attractifs. Les évolutions technologiques ont cependant été nombreuses dans ce domaine puisque de 1995 à 2003, 19 nouvelles technologies de bandes correspondant à de nouveaux formats ont été mises sur le marché. Durant la seule année 1998, six nouveaux formats ont fait leur apparition. Enfin l'avènement de la notion de WORM logique a largement contribué à leur utilisation dans les processus d'archivage.

Le disque dur magnétique

Quoique le concept ne soit pas nouveau, l'utilisation du disque magnétique comme support d'archivage repose sur la réunion d'au moins trois éléments importants en plus de leur évolution au niveau de WORM logique. Tout d'abord un aspect économique bien sûr avec l'arrivée de l'interface SATA (Serial Advanced Technology Attachment), évolution de la norme ATA (8.3 Mo/s) utilisée pour l'accès aux disques durs et offrant désormais un débit de 150 Mo/s avec une connectique simplifiée ayant pour conséquence de réduire de manière drastique le coût du gigaoctet de stockage sur les disques durs. Ensuite le fait que pour bon nombre d'organisations, les volumes d'informations augmentent sans cesse et que les temps d'archivage s'allongent en conséquence impose l'utilisation de supports de plus en plus rapides. Enfin, le troisième élément est directement lié au mécontentement des utilisateurs qui reprochent fréquemment à leurs équipements leur manque de rapidité et de fiabilité essentiellement lorsqu'il s'agit d'effectuer des interrogations et des restitutions.

2.2.2.3 Les supports optiques

Les CD (Compact Disc) et les DVD (Digital Versatile Disc) sont les deux principaux formats optiques. Conçues à l'origine pour constituer un support audio de haute qualité, les spécifications du CD ont ensuite évoluées afin de permettre le stockage des données numériques.

La grande différence du support optique par rapport aux supports magnétiques réside dans sa fiabilité et surtout dans sa pérennité, bien plus élevée car non soumise à des phénomènes physiques naturels dus entre autre au seul caractère magnétique par exemple de la bande qui peut à long terme provoquer un phénomène de « *collage* ». Même si certains constructeurs de disques optiques n'hésitent pas à annoncer des durées de garanties très longues pour leurs supports il y a lieu de modérer une telle information du seul fait qu'au bout de toutes ces années il y a fort à parier que les lecteurs n'existeront plus dans ce format et qu'en conséquence on se retrouvera avec un disque que l'on sera incapable de relire. Par ailleurs, l'information est stockée d'une façon permanente par modification du substrat, d'où l'origine de la notion de WORM (Write Once Read Many) physique. C'est pourquoi, les supports optiques ont encore tendance à être largement privilégiés lorsqu'il s'agit d'archivage. L'inconvénient majeur étant, cette fois, son prix par rapport à celui de la bande magnétique. La solution pourrait bien venir des nouvelles technologies basées sur le disque magnétique telles que présentées ci-après.

2.2.2.4 Les Juke Box

Afin d'augmenter les capacités directement adressables en ligne mais surtout afin de simplifier les manipulations, signalons que tant pour les bandes que pour les disques optiques existe, ce que l'on a coutume d'appeler, des librairies (ou juke box) lesquelles peuvent contenir une multitude de cartouches ou de disques optiques, accessibles via des systèmes robotisés, autorisant ainsi des capacités de stockage extrêmement importantes pouvant atteindre le téraoctet (To) voire le pétaoctet (Po).

Même si dans l'absolu le support idéal existait, ce qui est loin d'être le cas, encore ne faudrait-il pas oublier de prendre en considération les aspects économiques de façon globale. En effet sur ce dernier point il est nécessaire de raisonner non pas sur l'achat ponctuel de tel ou tel support ou technologie mais sur une exploitation simulée de plusieurs années afin de prendre en compte l'ensemble des paramètres : administration, maintenance, remplacement… Quoiqu'il en soit, le type de support sera avant tout choisi en fonction de critères précis comme la durée de conservation, la criticité des données à conserver, l'accessibilité, la volumétrie et le coût. Nous pouvons également ajouter comme exigences vis-à-vis des supports qu'ils aient les qualités suivantes :
- Stabilité intrinsèque du support et robustesse ;
- Large diffusion de la technologie et offre multi-constructeurs ou reposant sur des normes publiques ;
- Existence d'outils de contrôle des supports ;
- Chemin d'accès aux données protégé ;
- Simplicité des opérations de recopie ;
- Protection contre l'effacement accidentel.

2.2.3 Système d'accès et performance

Dans le cas d'un système d'indexation classique rappelons qu'une base de données, si performante soit-elle, pourra se trouver relativement vite limitée en termes de performances en fonction de l'augmentation des volumes à gérer. D'où la nécessité, avant d'opter pour une technologie, de pouvoir apprécier les performances du système à pleine charge et non pas seulement sur un test, en général non significatif. Il faut également faire attention au fait que si certains critères de recherche ont été oubliés à l'origine, il sera toujours délicat voire très difficile de les ajouter ensuite. Par ailleurs, un moteur de recherche, pourtant séduisant sur son principe, peut se révéler totalement inefficace à cause du phénomène de bruits parasites renvoyant systématiquement une multitude de réponses inexploitables. Dans ces deux cas, à savoir critères d'indexation incomplets ou bruits parasites, l'information archivée deviendrait ainsi quasi inaccessible et serait pour ainsi dire perdue.

2.2.4 Évolutivité

Dans la mise en place de tout système d'archivage il est notamment important de prévoir l'évolution de la volumétrie des données à conserver afin d'anticiper les augmentations de capacité des différents matériels et plates-formes, voire d'envisager certaines migrations. La prise en compte de cette évolutivité est en effet fondamentale quant au choix des technologies à utiliser.

2.2.5 Migration

Pour diverses raisons dont celle de l'évolutivité, il peut être nécessaire de prévoir des migrations tant au niveau du format logique que des supports physiques. Dans ce cas, il faudra particulièrement veiller au type de migration concernée afin d'en évaluer aussi précisément que possible les tenants et les aboutissants en matière de coûts, en matière de temps nécessaire et de risque d'indisponibilité temporaire d'accéder à l'information. Le modèle OAIS que nous aborderons au chapitre suivant relève quatre types de migrations :

- rafraîchissement de support : migration numérique dans laquelle un support est remplacé par un support du même type par copie bit à bit ;
- duplication : migration numérique dans laquelle il n'y a pas de changement de l'information transférée vers un support de même type ou plus vraisemblablement vers un autre support dans la mesure où ce type de migration est en général utilisé pour faciliter la migration vers de nouveaux types de support avec une automatisation maximum et un faible risque de perte d'informations ;
- ré-empaquetage : migration numérique qui produit quelques changements au niveau de l'information d'empaquetage. Cette dernière permet de relier et d'identifier les composants d'un document, par exemple les informations de volume et de répertoire. Ainsi au cours d'un transfert vers d'autres supports, il se peut que l'organisation des répertoires contenant les documents transférés, soit amenée à changer. Il y aura donc bien modification des informations d'empaquetage de ces documents sachant que le contenu de ces deniers ne sera absolument pas altéré ;
- transformation : migration numérique qui produit quelques changements dans les bits du contenu d'information mais vise à conserver l'intégralité du contenu d'information. L'information de représentation joue un rôle clé dans les transformations. Deux types de transformations peuvent être définies : la transformation réversible et la transformation irréversible. A titre d'exemple de transformation réversible, l'on peut envisager le remplacement d'une représentation qui utilise le jeu de caractères ASCII par une représentation utilisant le jeu de caractères UNICODE UTF-16. Pour illustrer une transformation irréversible nous pouvons citer le remplacement d'un nombre représenté en virgule flottante IBM 7094 par un nombre représenté en virgule flottante IEEE.

2.2.6 Sécurité/sauvegarde

La notion de sécurité doit être omniprésente dans le cadre de la mise en place d'un système d'archivage notamment au niveau des accès qui doivent être parfaitement maîtrisés et contrôlés du point de vue des droits à l'information archivée. Citons également en matière de dispositif sécuritaire la mise en place de procédures *ad hoc* destinées à garantir tant la confidentialité que l'intégrité des données. Afin de renforcer la notion de preuve il est également nécessaire de prévoir un système de traçabilité permettant de conserver l'ensemble des opérations effectuées sur le système quelles qu'elles soient. Enfin il ne faut surtout pas oublier un élément fondamental de sécurité : la sauvegarde de l'information ou tout autre système de redondance des données qui doit permettre en cas de sinistre de ne pas perdre l'information.

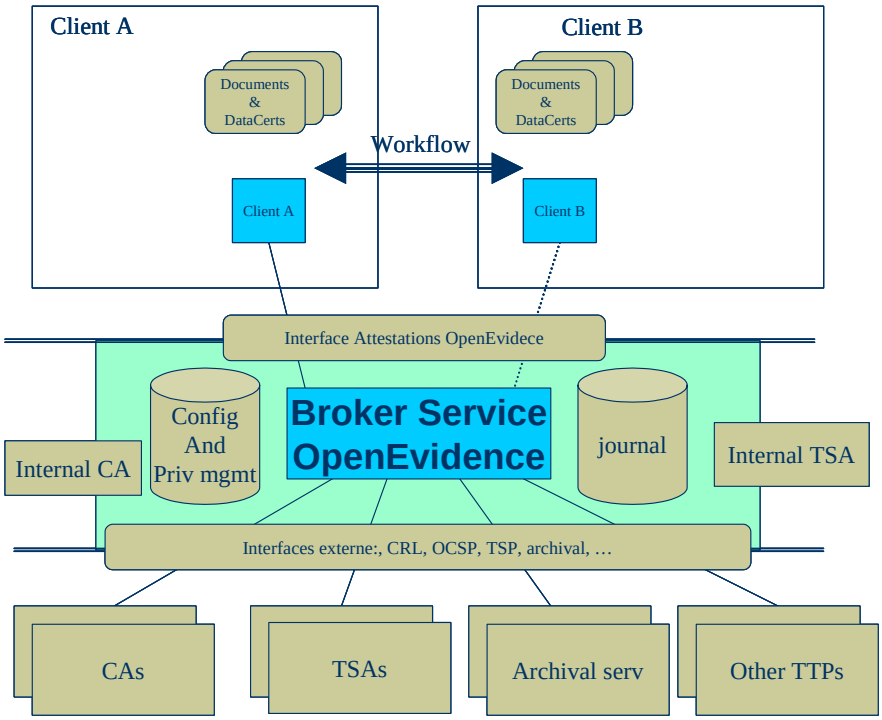
2.2.7 Prise en compte de la signature électronique

La reconnaissance juridique des échanges électroniques est en principe conditionnée par l'apposition d'une signature électronique. Ce qui ne va pas sans poser certains problèmes en matière d'archivage. En effet, de par la présence même d'un système cryptographique ce dernier n'échappe pas au fait que potentiellement le risque existe qu'il soit craqué un jour. Il faut donc absolument en tenir compte et faire en sorte de pouvoir substituer très rapidement un système par un nouveau plus performant. Afin d'anticiper ce phénomène de craquage il est également possible de mettre en place certaines procédures comme celle consistant à re-signer les documents régulièrement soit, a minima de les horodater afin d'éviter tout risque de falsification. Il est clair qu'il est préférable d'avoir prévu ce type de traitement dès l'origine si l'on veut s'éviter de fortes déconvenues lors de sa restitution, comme la remise en cause d'une information quant à son identification ou son intégrité, lui retirant du même coup toute sa valeur de preuve.

Pour éviter ce type de déboires deux solutions sont envisageables. La première consiste à partir du principe que l'on devra être capable de vérifier la signature d'un document électronique au moment de son utilisation. Ceci impose de conserver avec les documents archivés l'ensemble des éléments (listes de révocation, certificats des autorités concernées) qui permettront le moment venu de vérifier leur signature. Quoiqu'il en soit et en fonction du délai de conservation cette vérification deviendra de plus en plus aléatoire à cause de la disparition possible de telle ou telle autorité de certification. D'où la deuxième solution proposée qui revient à valider la signature au moment de l'intégration du document correspondant au système d'archivage. Là encore deux options sont possibles, la première laisse au système d'archivage le soin de cette validation et la deuxième option prévoit l'intervention d'un tiers de confiance qui aurait qualité pour effectuer cette validation.

Attestation de preuve :

Dans ce dernier cas, le tiers en question générerait l'équivalent d'une attestation électronique, assimilable à un jeton d'horodatage qui devrait être conservée en même temps que le document signé. Il s'agirait en fait d'une véritable attestation de preuve dans laquelle l'on pourrait retrouver outre les éléments de la validation de signature, un horodatage ainsi que la localisation du document archivé. Ce principe est la base même du projet OpenEvidence (http://www.openevidence.org/) dont nous reproduisons le schéma global ci-dessous.



Les deux solutions présentées ne sont en réalité pas exclusives l'une de l'autre. C'est ainsi que nous recommandons dans tous les cas de conserver des métadonnées relatives à la signature électronique et de vérifier la signature au moment de l'archivage sans omettre d'enregistrer le résultat de cette vérification.

3 Partie organisation

3.1 Normes existantes en matière d'archivage électronique

Nous abordons ici les différentes normes utiles dans le cadre de l'archivage électronique appréhendées essentiellement sous un angle organisationnel.

3.1.1 Modèle OAIS (Open Archival Information System)

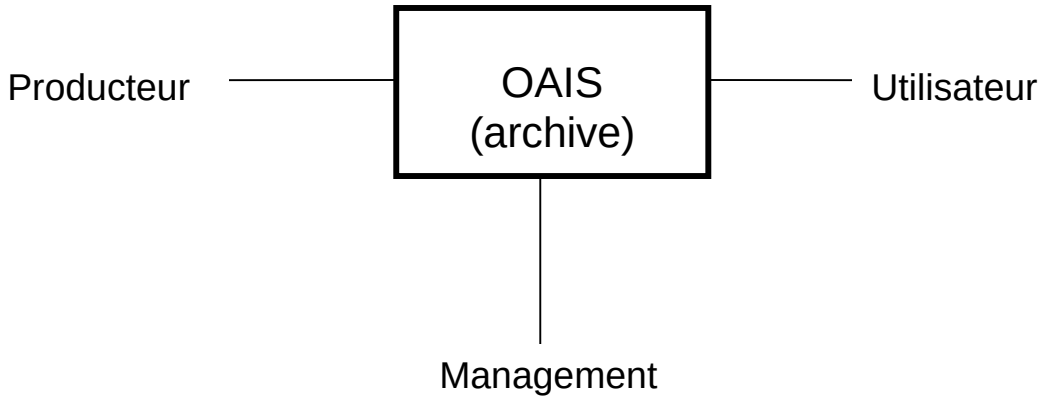
La norme ISO 14721:2003 (Systèmes de transfert des informations et données spatiales -- Système ouvert d'archivage de l'information -- Modèle de référence), plus connue sous le nom de modèle OAIS (Open Archival Information System) est consultable à l'adresse suivante : http://www.ccsds.org/CCSDS/documents/650x0b1.pdf.

Une traduction française, en cours de normalisation, est accessible à l'adresse suivante : http://vds.cnes.fr/pin/documents/projet_norme_oais_version_francaise.pdf.

Cette norme conceptuelle, mise au point par les principaux centres d'études spatiales du monde dont le CNES (Centre National d'Etudes Spatiales), définit les objets d'information, les métadonnées nécessaires à leur préservation et l'organisation à mettre en place pour leur archivage, leur conservation et leur communication, définit un vocabulaire et un ensemble de concepts permettant d'appréhender de façon globale et complète, la question de l'archivage long terme de données sous forme numérique. Elle définit deux modèles complémentaires : un modèle d'information et un modèle fonctionnel détaillé dont les fonctions de base sont le versement (projet de norme ISO relatif à l'interface entre le producteur et le service d'archives), la gestion des données, le stockage et l'accès. Elle propose également une classification des types de migration et des différents modes de coopération possibles entre archives. La mise en œuvre de cette norme permet d'affirmer que les documents archivés le seront convenablement et par conséquent permettront de s'assurer de leur fiabilité. OAIS traite aussi bien des documents à valeur juridique que patrimoniale.

L'objet de cette norme est de présenter un système d'archivage à la fois pour les données numériques et les données sur supports physiques. Un OAIS est un centre d'archive constitué de personnes et de systèmes, dont la responsabilité est de conserver des informations et de les rendre accessibles à une Communauté d'utilisateurs cible.

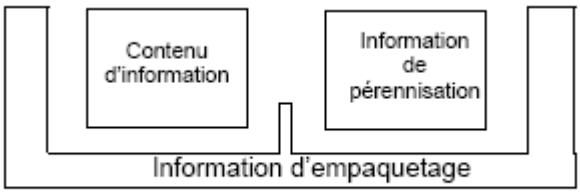
Le modèle OAIS se présente comme une interface entre les producteurs d'information, les utilisateurs et le management qui n'a ici qu'un rôle de définition de politique globale d'archivage, la gestion au quotidien étant laissée à l'administration.



Modèle d'environnement d'un OAIS

3.1.1.1 Paquet d'informations

L'OAIS fournit la définition du concept de Paquet d'informations constitué de deux types d'informations appelés Contenu d'information et Information de pérennisation (PDI : Preservation Description Information), encapsulés par une Information d'empaquetage.



Paquet 1

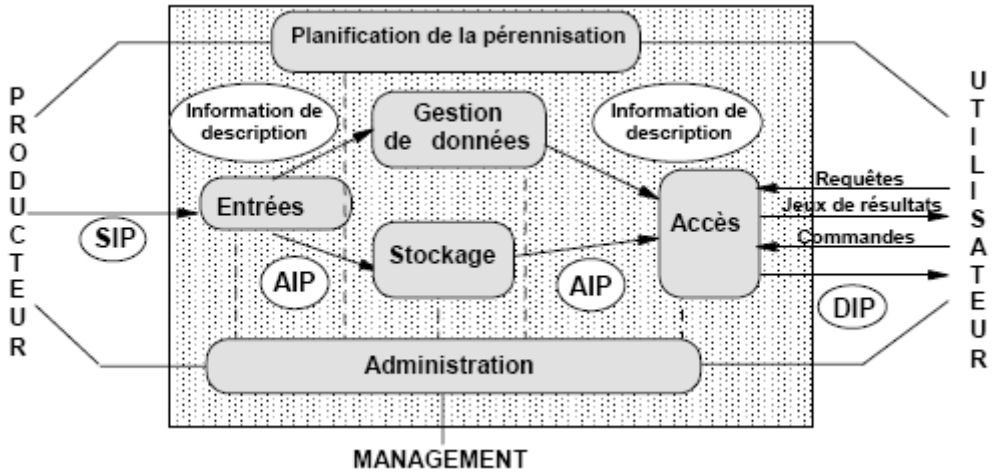
Le contenu d'information comprend, outre l'information objet de la conservation, les informations de représentation nécessaires à sa compréhension.

L'Information de pérennisation se subdivise en quatre catégories d'informations :

- la **provenance** décrit l'origine du Contenu d'information, identifie les personnes qui en ont eu la charge depuis sa création, ainsi que son historique (y compris l'historique des traitements subis).
- le **contexte** décrit les relations existant entre le Contenu d'information et d'autres informations situées hors du Paquet d'informations. Par exemple, il peut expliquer pourquoi le Contenu d'information a été produit, et inclure une description de la façon dont ce Contenu est relié à un autre Objet contenu d'information existant.
- l'**identification** fournit un ou plusieurs identificateurs, ou systèmes d'identificateurs, grâce auxquels le Contenu d'information peut être identifié de façon unique. Parmi les exemples, on peut citer le numéro ISBN pour un livre, ou un ensemble d'attributs permettant de différencier les Contenus d'information entre eux.
- l'**intégrité** fournit un mécanisme ou un dispositif protecteur pour prémunir le Contenu d'information contre toute altération non documentée. Par exemple, il peut s'agir d'un checksum sur le Contenu d'information d'un Paquet d'informations numériques.

3.1.1.2 Entités fonctionnelles

Nous donnons ci-après le modèle de référence du système OAIS ainsi que le rôle joué par chacune des entités, extraits du document de référence.



AIP : Archival Information Package (Paquet d'informations archivé)
DIP : Dissemination Information Package (Paquet d'informations diffusé)
SIP : Submission Information Package (Paquet d'informations à verser)

Entité « Entrées » :

Cette entité assure les fonctions et services relatifs à l'acceptation des Paquets d'informations à verser (SIP) provenant des Producteurs (ou d'éléments internes sous le contrôle de l'Entité «Administration »), et à la préparation de leur contenu en vue du stockage et de la gestion des données au sein de l'Archive. Les fonctions de l'Entité « Entrées » comprennent : la réception des SIP, le contrôle d'Assurance Qualité sur ces SIP, la génération d'un Paquet d'informations archivé (AIP) conforme aux normes de documentation et de formatage des données de l'Archive, l'extraction de l'Information de description des AIP pour l'inclure dans la base de données de l'Archive et la coordination des mises à jour à effectuer au niveau des Entités « Stockage » et « Gestion de données ».

Entité « Stockage » :

Cette entité assure les fonctions et services relatifs au stockage, à la maintenance et à la récupération des AIP. Les fonctions de l'Entité « Stockage » comprennent notamment : la réception des AIP en provenance de l'Entité « Entrées » et leur insertion dans l'espace de stockage permanent, la gestion de la hiérarchie du stockage, le renouvellement des supports sur lesquels les fonds de l'Archive sont stockés, les contrôles d'erreurs spécifiques et de routine, la fourniture des moyens de sauvegarde, la mise en œuvre des plans de reprise d'activité, et la transmission des AIP à l'Entité « Accès » en réponse aux commandes.

Entité « Gestion de données » :

Cette entité assure les fonctions et services relatifs à l'enrichissement, la conservation et l'accès à l'Information de description (qui identifie et documente les fonds de l'Archive) et aux données administratives utilisées pour gérer l'Archive. Les fonctions de l'Entité « Gestion de données » comprennent : l'administration des fonctions de la base de données de l'Archive (conserver et tenir à jour les schémas, les définitions de vues et l'intégrité référentielle), les mises à jour de la base de données (chargement de nouvelles Informations de description ou de nouvelles données administratives de l'Archive), la recherche d'éléments de l'Entité « Gestion de données » pour générer des jeux de résultats, et la production de rapports à partir de ces résultats.

Entité « Administration » :

Cette entité assure les fonctions et services relatifs à l'exploitation d'ensemble du système d'archivage. Les fonctions de l'Entité « Administration » incluent : la proposition et la négociation des Protocoles de versement avec les Producteurs, la vérification des versements pour s'assurer de leur conformité aux normes d'archivage ainsi que la gestion de la configuration du matériel et des logiciels du système. Elle fournit aussi les moyens techniques pour contrôler et améliorer l'exploitation de l'Archive, ainsi que pour inventorier, rendre compte et migrer/mettre à jour les contenus de l'Archive. Elle est également responsable de l'établissement et du maintien des normes et règles applicables à l'Archive, de l'aide à l'Utilisateur et de l'activation des requêtes enregistrées.

Entité « Planification de la pérennisation » :

Cette entité assure les fonctions et services relatifs à la surveillance de l'environnement de l'OAIS et à la production de recommandations visant à ce que les informations stockées dans l'OAIS restent accessibles sur le long terme à la Communauté d'utilisateurs cible, même si l'environnement informatique d'origine devient obsolète. Les fonctions de l'Entité « Planification de la pérennisation » incluent l'évaluation du contenu de l'Archive et la recommandation périodique de mises à jour de l'information archivée pour migrer les fonds courants, le développement de recommandations dans le domaine des normes et règles d'archivage, la surveillance des évolutions à la fois de l'environnement technologique et des exigences de service de la Communauté d'utilisateurs cible, et enfin de sa Base de connaissance. Cette entité conçoit aussi des modèles de Paquets d'informations et accompagne la conception et la validation de ces modèles appliqués à des SIP ou des AIP, pour les adapter à des versements spécifiques. L'Entité « *Planification de la pérennisation* » développe aussi des plans détaillés de migration, des prototypes de logiciels et des plans de test pour répondre aux objectifs de migration de l'Entité « *Administration* ».

Entité « Accès » :

Cette entité assure les fonctions et services qui aident l'Utilisateur à déterminer si une information existe ou non dans un OAIS, à trouver sa description, son emplacement si elle est disponible, et à demander et recevoir des produits d'information. Les fonctions de l'Entité « *Accès »* incluent : la communication avec les Utilisateurs pour recevoir leurs demandes, les contrôles d'accès à l'information bénéficiant d'une protection particulière, la coordination du traitement des demandes jusqu'à leur exécution finale, la génération des réponses (Paquets d'informations diffusés, Jeux de résultats, rapports) et leur transmission aux Utilisateurs.

En plus des entités décrites ci-dessus, différents Services de base sont censés être disponibles. On considère que ces services constituent une autre entité fonctionnelle dans ce modèle. Mais cette entité est tellement omniprésente que, par souci de clarté, elle n'est pas représentée dans le schéma.

3.1.2 Norme ISO15489 Records management associée à la méthodologie DIRKS

L'ISO 15489-1: 2001, est une norme internationale pour le Records management qui fournit des règles et des conseils sur la gestion des documents utiles dans la conduite des activités d'une organisation. Elle est accompagnée du rapport technique ISO/TR 15489-2 : 2001 qui sert à décrire une méthode pour les mettre en œuvre.

Les informations que nous indiquons ci-après sont pour l'essentiel issues d'une analyse effectuée sur la norme ISO 15489 au regard des pratiques archivistiques françaises par le Groupe métiers « Records management », commun à l'Association des archivistes français (AAF) et à l'Association des professionnels de l'information et de la documentation (ADBS). Il s'agit de la version 2, datée d'avril 2005.
http://www.archivistes.org/article.php?id=1117294358

3.1.2.1 Précisions

Au sein d'une organisation, le records management ne gère pas nécessairement tous les documents produits ou reçus de façon exhaustive. La couverture du records management peut, en effet, être restreinte conformément à la politique d'archivage définie. Le records management a ainsi pour objet l'ensemble des documents « *à archiver* », c'est-à-dire les documents que l'organisation aura décidé de préserver à titre de preuve ou en raison de leur valeur informationnelle, il s'agit des documents essentiels ou utiles dans la conduite de ses activités

La norme précise de façon formelle que les archives définitives (documents préservés in fine pour le citoyen après qu'ils aient cessé d'être utiles pour l'organisation) ne sont pas l'objet du records management.

Enfin le records management prend en compte le document dans une version finie (non modifiable, validée et signée si besoin).

3.1.2.2 Objectif

Le records management a pour finalité de permettre à l'organisation de disposer à tout instant du document dont elle a besoin pour conduire ses activités, répondre aux exigences légales et réglementaires, et se protéger en cas de contentieux. Cet objectif se traduit par le fait de garantir que le document existe, qu'on sait où le trouver, qu'il est accessible, traçable, authentique, fiable, intègre et exploitable.
Ceci implique que l'organisme se dote d'un « *système de records management* » ayant les fonctions principales suivantes :

- veiller à ce que le document essentiel à l'organisme existe ;
- prendre en charge le document depuis sa création jusqu'à son sort final (destruction ou versement aux archives définitives) ;
- conserver le document dans son contexte ou en lien avec lui ;
- garantir la conservation des documents et leur restitution dans des délais et sur des supports adaptés ;
- assurer la traçabilité du document ;
- communiquer le document selon les droits d'accès associés.

Les objectifs du records management rejoignent ceux d'une démarche qualité conforme aux normes ISO 9001, Systèmes de management de la qualité et ISO 14001, Systèmes de management environnemental.

3.1.2.3 Outils

Plan de classement des activités :
Ce plan représente l'organisme à travers ses activités.

Référentiel de classement et d'archivage des documents :
Le référentiel de classement et d'archivage s'appuie sur le plan de classement des activités. Il indique pour chacune des activités les catégories documentaires de l'activité et pour chaque catégorie documentaire :

- si elle est à enregistrer dans le système d'archivage ou non,
- sa durée de conservation,
- le sort à appliquer aux documents de cette catégorie à l'issue de la durée de conservation : destruction ou versement aux archives définitives.

Règles d'attribution des identifiants :
Chaque document ou dossier doit porter un identifiant unique qui permettra de le traiter de façon individualisée tout au long de son cycle de vie.

Règles de localisation :
Chaque lieu de stockage et chaque système de gestion documentaire faisant partie du système de records management est identifié de façon univoque.

Règles de description du document :
La norme distingue la description du contexte du document, la description de son contenu et la description de sa structure.

3.1.2.4 Processus

Le records management comprend les trois processus suivants :

- le processus de **conception et de mise en œuvre** du système, avec les étapes suivantes :
  - enquête préliminaire ;
  - analyse des activités de l'organisation ;
  - identification des exigences archivistiques ;
  - évaluation des systèmes existants ;
  - identification de la stratégie pour la satisfaction des exigences archivistiques ;
  - conception du système d'archivage ;
  - mise en œuvre du système d'archivage ;
  - contrôle a posteriori.
- le processus de **gestion des documents** « *records* », comprenant les différentes phases suivantes:
  - analyse et classement du document produit ou reçu ;
  - capture et enregistrement du document dans le système de records management ;
  - analyse et ajout de métadonnées (description du document, de son contexte, de son contenu, de sa structure) ;
  - stockage sécurisé ;
  - prise en compte des évolutions du document ;
  - communication, mise à disposition, accès ;
  - migrations, ou changement de support et/ou de format ;
  - application du sort final (destruction ou transfert de la responsabilité ou de la propriété).
- le processus d'**audit et de contrôle** du système.

3.1.2.5 DIRKS

Il s'agit d'un manuel publié par le gouvernement australien pour Design and Implementation of Recordkeeping Systems, (Conception et déploiement des systèmes archivistiques. Ce manuel présente une approche pour gérer la conservation des documents de façon conforme à la norme AS 4390 - Australian Standard – Records management, publiée en 1996 ainsi qu'à la norme ISO 15489 qu'elle a précédé. Ce qui distingue ce document est avant tout la qualité et l'étendue de ses explications par rapport aux divers aspects à analyser.

La méthode DIRKS propose huit étapes dans la conception d'un système d'archivage :

1. Analyse préliminaire ;
2. Analyse des activités d'affaires ;
3. Identification des exigences archivistiques ;
4. Évaluation des systèmes existants ;
5. Stratégies pour la conservation ;
6. Conception d'un système archivistique ;
7. Implantation d'un système archivistique ;
8. Examen post-implantation.

3.1.3 Moreq (Model requirements for the management of electronic records)

Ce modèle a été élaboré en pensant aux besoins des responsables de l'archivage électronique et traditionnel, et rédigé dans un esprit pragmatique et utilitaire. Les exigences de MoReq visent à mettre en place un système en mesure de gérer les documents électroniques aux degrés de confidentialité et d'intégrité voulus, en combinant les avantages de la gestion électronique et ceux de la théorie classique de l'archivage.

Ces spécifications décrivent les exigences pour l'organisation de l'archivage électronique et insistent principalement sur les exigences fonctionnelles pour disposer d'un archivage électronique à des fins de preuve à l'aide d'un système d'archivage électronique (SAE).

Les spécifications sont rédigées pour être également applicables au secteur public et aux entreprises du secteur privé qui souhaitent mettre en place un SAE, ou qui souhaitent évaluer la capacité de leur système existant au regard de l'archivage électronique.

En outre ces spécifications se limitent délibérément aux fonctionnalités requises pour un logiciel d'archivage électronique.

Nous présentons ci après les différents éléments du modèle MoReq.

Panorama des exigences d'un SAE :

Concepts fondamentaux :

Document d'archives et document d'archives électronique

Le guide du DLM (document lisible par machine) Forum suggère de considérer un document d'archives comme composé de :

- un contenu ;
- une structure ;
- un contexte ;
- une présentation.

Plan de classement :

Le *records management* ordonne les dossiers de manière structurée et les bonnes pratiques veulent que cette structure reflète les activités de l'entreprise ou de l'organisme. La représentation de cet agencement est dénommée « plan de classement ». Le plan de classement est en général hiérarchique, bien qu'il puisse aussi être organisé par un thésaurus sans arborescence.

- Configuration du plan de classement ;
- Séries et dossiers ;
- Sous-dossiers ;
- Maintenance du plan de classement (seul l'administrateur a la possibilité de modifier le plan de classement).

Contrôles et sécurité :

- Accès (contrôle de l'accès aux documents et à l'information sur les documents archivés ;
- Historique des événements (toute opération ou modification doit être tracée) ;
- Sauvegarde et restauration (documents et métadonnées) ;
- Traçabilité des mouvements ;
- Authenticité ;

- Indices de sécurité et habilitations.

Conservation et sort final :

- Tableaux des durées de conservation : un dossier ou un document peut être rattaché à plusieurs durées de conservation – indication systématique du sort final ;
- Révision : contrôle des documents arrivés à échéance de conservation ;
- Transfert, export et destruction.

La capture des documents :

Les documents créés ou reçus dans l'exercice des activités sont archivés dès qu'ils sont sélectionnés, c'est-à-dire « capturés » dans le SAE. Pendant la capture, les documents sont « classés », c'est-à-dire qu'on leur affecte le code de la rubrique du plan de classement dont ils relèvent et qu'on leur assigne un identifiant unique, ce qui permet au SAE de les gérer.

Un système souple doté de contrôles pertinents pour :

- les documents produits aussi bien en interne qu'à l'extérieur ;
- de formats variés ;
- arrivant via divers canaux de communication (réseau, messagerie, fax, scan) à des fréquences et avec des volumes variables ;
- possibilité d'affectation d'un même document à plusieurs dossiers.

Import en masse

Cas des documents auto-modifiés

Gestion des messages électroniques (capture automatique ou après sélection)

Identification :

Exigence d'un identifiant unique (identifiants uniques pour chaque occurrence de chaque entité), plutôt automatisé

Recherche, repérage et restitution :

- Recherche et repérage : fonctions non classiques du Records management (outils de recherche et de navigation) ;
- Affichage des documents, impression et autres cas de restitution.

Fonctions d'administration :

- Administration générale : gestion des utilisateurs, contrôle de la capacité de stockage, restaurations ;
- Reporting et statistiques : produire tout type d'état statistique à partir de l'historique des événements ;
- Modification, suppression et édition d'extrait des documents archivés.

Autres fonctions :

- Gestion et archivage des documents non électroniques ;
- Conservation et sort final des dossiers mixtes ;
- GED et Workflow (communication des systèmes) ;
- Signature électronique, chiffrement, filigranes numériques, etc. ;
- Interopérabilité et ouverture.

Exigences non fonctionnelles :

- Facilité d'utilisation, performance et extensibilité, disponibilité du système ;
- Normes techniques ;
- Environnement législatif et réglementaire ;
- Externalisation et recours à des tiers (contrat détaillé et récupération à l'identique) ;
- Conservation à long terme (> 10 ans, jusqu'à plusieurs siècles) et obsolescence technologique ;
- (supports, matériels et formats) – possibilité de conversion/migration en masse avec les métadonnées.

Les métadonnées :

Donnent un minimum d'exigences d'ordre générique sous forme de tableau : métadonnée + occurrence + renvoi à l'exigence dans le chapitre correspondant.

Métadonnées distinctes mais coordonnées pour :

- le plan de classement ;
- les séries et dossiers et sous-dossiers ;
- les documents ;
- les extraits de document.

Métadonnées concernant l'utilisateur et les profils :
Personnalisation des métadonnées (cela dépend des entreprises et des organismes).

Un groupe de travail qui vient de se constituer est destiné à fournir une version MoReq2 au modèle.

3.1.4 Norme NF Z42-013

Il s'agit d'une norme française de la famille de l'Archivage électronique correspondant aux « *Recommandations relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes* »

La norme fournit un ensemble de spécifications concernant les mesures techniques et organisationnelles à mettre en œuvre pour l'**enregistrement, le stockage et la restitution** de documents électroniques afin d'assurer la **conservation et l'intégrité** de ceux-ci. Les documents peuvent, soit résulter d'un processus de numérisation à partir de documents sur support papier ou de microformes, soit être produits directement par un processus informatique. La norme couvre ainsi également les **opérations de numérisation** des documents.

Cette norme traite seulement des systèmes utilisant des **disques optiques de type WORM** (Write Once Read Many), non réinscriptible pour le stockage permanent de documents électroniques. Elle ne s'applique pas aux systèmes qui comportent uniquement des équipements de stockage permettant de supprimer ou de modifier des documents a posteriori. Ces supports ont été retenus parce que :

- il n'est pas possible d'effacer une information une fois qu'elle est enregistrée ;
- il n'est pas possible d'enregistrer une autre information à la même place que la précédente ;
- il est aussi impossible d'apporter à l'information enregistrée une quelconque modification ;
- les supports offrent une totale insensibilité aux champs magnétiques.

Les documents sonores, les séquences d'images animées, ainsi que les radiographies médicales n'entrent pas dans le champ d'application de la norme.

Cette norme est destinée :

- aux organismes ou entreprises qui souhaitent mettre en oeuvre des systèmes informatiques dans lesquels ils pourront stocker des images, des documents électroniques de telle façon que leur fidélité et leur intégrité par rapport aux documents d'origine soient assurées ;
- aux sociétés de services informatiques qui désirent concevoir des systèmes devant assurer la fidélité et l'intégrité de documents électroniques ;
- aux entreprises de services assurant le stockage de documents électroniques pour le compte de tiers.

En outre cette norme détail les différents éléments suivants :

- Dossier de description technique du système ;
- Horodatage ;
- Processus de capture des documents ;
- Systèmes pour l'enregistrement des documents ;
- Supports de stockage (détaillés ci-dessous) ;
- Sécurités ;

- Procédures d'exploitation ;
- Suivi des procédures ;
- Audits ;
- Tiers archiveur ;
- Prestataires de services.

Au niveau des supports de stockage la norme présente les éléments suivants (hors options particulières comme celle du chaînage des supports):

Types de supports de stockage admis :

Seuls des supports WORM sont admis pour réaliser les opérations de stockage des documents électroniques. Ces supports doivent comporter dès leur origine un numéro d'identification unique introduit par le fabricant.

Initialisation des supports de stockage :

Chaque support de stockage doit être initialisé en indiquant, préalablement à l'enregistrement du premier document, un certain nombre d'informations comme : le lieu de l'initialisation, l'horodatage de cette initialisation, le nom de l'organisme ou de l'entreprise…

Clôture des supports de stockage :

Quand un support est rempli et après que le dernier enregistrement utilisateur ait été stocké, ce support doit être clôturé. Pour ce faire, certaines informations sont inscrites à la suite des dernières informations de l'utilisateur: le lieu de la clôture, l'horodatage de cette clôture, le nom de l'organisme ou de l'entreprise…

S'il existe encore des secteurs non utilisés sur ces supports, ceux-ci doivent être modifiés de telle manière qu'il ne soit plus possible d'écrire sur le support par la suite.

Conservation des supports de stockage :

L'état des informations enregistrées doit être vérifié à intervalles réguliers. Il est recommandé de copier les informations enregistrées sur de nouveaux disques avant l'expiration de la durée de vie que le fabricant recommande pour le disque d'origine

Impact du changement de système sur les supports de stockage :

Si un système de stockage des documents électroniques doit être remplacé par un nouveau système, tous les documents électroniques stockés dans l'ancien système doivent être copiés dans le nouveau. Deux cas sont à prévoir :

- les nouveaux lecteurs-enregistreurs sont capables de lire les supports exploités par les anciens lecteurs-enregistreurs ; il faut alors contrôler que l'ensemble des supports est bien lisible par les nouveaux lecteurs-enregistreurs avant de procéder à la mise hors service de l'ancien système ;
- les nouveaux lecteurs-enregistreurs ne peuvent lire les supports exploités par les anciens lecteurs-enregistreurs ; il faut alors copier l'ensemble des documents contenus sur les anciens supports sur des nouveaux supports au moyen d'une installation qui comporte temporairement les deux générations de lecteurs-enregistreurs.

Sauvegardes :

Sauvegardes du système : il faut effectuer systématiquement des sauvegardes des documents, des index et de tous les logiciels servant au fonctionnement du système.

Copies de sécurité : à intervalles réguliers, il doit être réalisé des copies de sécurité de tous les documents et les index créés ou modifiés. Ces copies de sécurité doivent être réalisées sur des disques de type WORM.

Supports de stockage illisibles :

Il peut arriver qu'un support de stockage soit illisible. Dans ce cas, outre la nécessité de vérifier complètement les systèmes informatiques ayant servi à écrire ou à lire ce support (afin de s'assurer que ces systèmes ne sont pas en cause), il est nécessaire :

- d'initialiser un nouveau support ;
- de recopier toutes les données en provenance du support de sauvegarde.

Par rapport à ce qui précède, il paraît évident que cette norme est particulièrement lourde à mettre en œuvre et donc coûteuse. Par ailleurs, elle est extrêmement réductrice vis-à-vis des supports de stockage puisque n'acceptant que les supports de type WORM physique, ce qui élimine l'ensemble des nouveaux dispositifs basés sur du disque magnétique tels que décrits précédemment. Enfin, cette norme, dont l'objet est l'archivage des documents numérisés, n'est pas adéquate pour les documents établis directement sous forme électronique, principal objectif d'un archivage électronique à des fins juridiques.

3.1.5 Projet ISO 18509

Il existe actuellement un projet de norme ISO 18509 qui peut être vu comme une évolution à un niveau international de la norme NF Z42-013, élargissant entre autre la notion de WORM à la notion de WORM logique. Néanmoins il semblerait que ce projet ne se concrétise jamais.

3.2 Architecture du Service d'Archivage Électronique (SAE)

Afin de décrire l'ensemble des fonctions canoniques d'un système d'archivage, nous nous appuierons sur le modèle OAIS (présenté précédemment) qui décompose un système d'archivage en plusieurs grandes fonctions ou « entités », dont les quatre principales sont les suivantes :

- Les entrées ou versements ;
- Le stockage ou conservation ;
- La gestion des données descriptives ;
- Les accès ou la consultation.

Après avoir décrit en détail chacune de ces entités, nous nous intéresserons aux autres fonctions que doit nécessairement posséder tout système d'archivage.

3.2.1 Les entités du SAE

3.2.1.1 Entité « Entrées »

L'entité « Entrées » assure les fonctions et services relatifs à l'acceptation des lots d'informations à verser dans le système d'archive, provenant essentiellement des producteurs, voire de l'administration du système. Cette entité consiste également à préparer le contenu des lots d'information en vue du stockage et de la gestion des données au sein du système d'archive.

Les fonctions de l'entité « Entrées » comprennent ainsi :

1. Recevoir un versement c'est-à-dire offrir la capacité de stocker les lots entrants ;
2. Assurer la qualité en validant le transfert comme étant réussi après contrôle d'intégrité et journalisation de l'opération ;
3. Générer un ou des lot(s) d'archive(s) conforme(s) aux normes de documentation et de formatage des données du système d'archive. Cette fonction peut impliquer des conversions de format de fichier, des conversions de représentations des données ou une réorganisation du contenu d'information des lots d'origine ;
4. Générer l'information de description pour l'inclure dans la base de données du système d'archive ;
5. Coordonner les mises à jour à effectuer au niveau des entités « Stockage » et « Gestion de données ». Cette coordination comprend, notamment l'information d'identification du stockage du lot archivé à inclure dans l'information de description.

3.2.1.2 Entité « Stockage »

L'entité « Stockage » assure les fonctions et services relatifs au stockage, à la maintenance et à la récupération des lots d'information à archiver.

Les fonctions de l'entité « Stockage » comprennent notamment :

1. Recevoir des données en provenance de l'entité « Entrées ». Ceci consiste à insérer ces données dans l'espace de stockage permanent et à envoyer un message d'acquittement à l'entité « Entrées » incluant l'identification du stockage ;
2. Gérer la hiérarchie du stockage : revient à inscrire les données sur les supports appropriés (notions de *on line*, *off line*, *near line*) en fonction de la politique de gestion relative au stockage et en fonction des statistiques d'exploitation ou des directives fournies directement par l'entité « Entrées ». Cette fonction respecte également les niveaux de service exigés pour chacun des lots ainsi que les niveaux de sécurité afférents et fournit les statistiques d'exploitation (capacité disponible/différents supports, utilisation) ;
3. Renouveler, remplacer des supports sur lesquels les fonds du système d'archive sont stockés ;
4. Contrôler les erreurs afin de garantir la non corruption des données stockées ;
5. Fournir des moyens de sauvegarde et de mise en œuvre des plans de reprise d'activité, dupliquer les contenus et les stocker dans une installation physiquement séparée ;
6. Transmettre des lots archivés à l'entité « Accès » en réponse aux demandes.

3.2.1.3 Entité « Gestion de données »

L'entité « Gestion de données » assure les fonctions et services relatifs à l'enrichissement, la conservation et l'accès à l'Information de description (qui identifie et documente les fonds du système d'archive) et aux données « *administratives* » utilisées pour gérer le système d'archive.

Les fonctions de l'entité « Gestion de données » comprennent :

1. Administrer les fonctions de la base de données du système d'archive (conserver et tenir à jour les schémas, les définitions de vues et l'intégrité référentielle) ;
2. Exécuter des requêtes en provenance de l'entité « Accès », rechercher les éléments concernés et générer des jeux de résultats ;
3. Produire des rapports suite à une demande ;
4. Mettre à jour la base de données (chargement de nouvelles informations de description ou de nouvelles données administratives du système d'archive).

3.2.1.4 Entité « Accès »

L'entité « Accès » assure les fonctions et services qui aident l'utilisateur à déterminer si une information existe ou non dans le système d'archive, à trouver sa description, son emplacement si elle est disponible, et à demander et recevoir des produits d'information.

L'entité « Accès » inclut :

1. Communiquer avec les utilisateurs pour recevoir leurs demandes d'interrogations, de rapports, de commandes ;
2. Contrôler l'accès à toute information bénéficiant d'une protection particulière ;
3. Coordonner le traitement des demandes jusqu'à leur exécution finale ;
4. Constituer des réponses (paquets d'informations diffusés, jeux de résultats, rapports) ;
5. Transmettre des réponses aux utilisateurs.

À l'ensemble de ces fonctions principales viennent s'ajouter des fonctions transversales comme :

- **l'administration technique et fonctionnelle générale de la plate-forme ;**
- **le pilotage du service d'archives responsable de la plate-forme ;**
- **la gestion de la relation avec les services producteurs ;**
- **la veille technologique et juridique ;**
- **les projets d'évolution et de migration.**

Toujours au vu du modèle OAIS, l'ensemble de ces fonctions se retrouve essentiellement au niveau de deux entités complémentaires décrites ci-après.

3.2.1.5 Entité « Administration »

L'entité « Administration » assure les fonctions et services relatifs à l'exploitation d'ensemble du système d'archivage.

L'entité « Administration » inclut :

1. Négocier les protocoles de versement avec les producteurs ;
2. Gérer la configuration du matériel et des logiciels du système ;
3. Mettre à jour l'information archivée ;
4. Contrôler l'accès physique ;
5. Élaborer et maintenir des standards et règles applicables au système d'archive, normes sur les formats et sur la documentation, procédures à suivre pendant l'opération de versement, standards et objectifs de migration, règles en matière de gestion de stockage, aspect hiérarchisation et règles en matière de migration afin d'anticiper l'obsolescence des formats de stockage, règles d'administration des fonctions de la base de données, règles de plan de reprise d'activité, règles de sécurité pour protéger les données dans le système d'archive ;
6. Auditer un versement afin de vérifier sa conformité aux spécifications du protocole de versement ;
7. Activer les requêtes en attente de l'ensemble des données requises ;
8. Gérer le service « clients » notamment en tenant les comptes utilisateurs.

3.2.1.6 Entité « Planification de la pérennisation »

L'entité « Planification de la pérennisation » assure les fonctions et services relatifs à la surveillance de l'environnement du système d'archivage et à la production de recommandations visant

à ce que les informations stockées restent accessibles sur le long terme aux utilisateurs cibles, même si l'environnement informatique d'origine devient obsolète.

L'entité « Planification de la pérennisation » inclut :

1. Suivre les évolutions des exigences de service des utilisateurs cibles (formats, supports, progiciels, plates-formes informatiques) ;
2. Effectuer une veille technologique ;
3. Suivre le développement des recommandations dans le domaine des normes et règles d'archivage ;
4. Développer les stratégies et les standards de pérennisation ;
5. Développer des modèles d'empaquetage, des plans de migration, des prototypes de logiciels et des plans de test pour répondre aux objectifs de migration de l'entité « Administration ».

Enfin, un certain nombre de services de base vient s'ajouter à l'ensemble de ces fonctions tels que la communication interprocessus, les services de nommage, l'affectation d'espace de stockage provisoire, le traitement d'exceptions, la sécurité et les services d'annuaires nécessaires au fonctionnement du système d'archivage.

3.2.2 Services de base du SAE

Comme exemples de services de base du SAE nous pouvons citer :

- Les **services du système d'exploitation** qui fournissent les services fondamentaux nécessaires pour exploiter et administrer la plate-forme d'application et fournir une interface entre le logiciel applicatif et la plate-forme ;
- Les **services réseau** qui fournissent les moyens et les mécanismes pour les applications distribuées qui exigent l'accès aux données et l'interopérabilité des applications dans des environnements hétérogènes en réseau ;
- Les **services de sécurité** qui fournissent des moyens et des mécanismes de protection de l'information sensible et des traitements dans le système d'information. La détermination du niveau de protection approprié se base sur la valeur des informations pour les utilisateurs finaux de l'application et sur la perception des risques. Au nombre de ces services nous pouvons lister :
  - **Le service d'identification/authentification** destiné à confirmer l'identité des personnes qui demandent à utiliser les ressources du système d'information. L'authentification doit également s'appliquer aux fournisseurs de données. Le service d'authentification peut intervenir au début ou au cours d'une session.
  - **Le service de contrôle d'accès** empêche l'usage non autorisé des ressources du système d'information. Ce service empêche également que des ressources soient utilisées de manière non autorisée. Il peut être appliqué à différents aspects de l'accès à une ressource (par exemple accès aux communications avec la ressource, accès en lecture, droit d'écriture ou de suppression d'une ressource d'information/de données, exécution d'une ressource de traitement) ou à tous les accès à une ressource.
  - **Le service d'intégrité des données** s'assure que les données ne sont pas modifiées ou détruites sans autorisation. Ce service s'applique aux données figurant dans des espaces permanents de stockage et aux données présentes dans des messages de communication.
  - **Le service de confidentialité des données** s'assure que les données ne sont pas mises à la disposition ou communiquées à des personnes ou des traitements informatiques non autorisés. Ce service est appliqué aux périphériques qui permettent une interaction entre l'homme et le système d'information. En outre, ce service rend impossible tout espionnage des modalités d'utilisation des ressources de communication.
  - **Le service de « non répudiation »** s'assure que les entités qui s'engagent dans un échange d'informations ne peuvent pas contester leur implication. Ce service peut revêtir l'une ou les deux formes suivantes: premièrement, le destinataire des données reçoit une preuve de l'origine des données, ce qui prévient toute tentative de la part de l'expéditeur de nier avoir transmis les données (ou leur contenu) ; deuxièmement, l'expéditeur des données reçoit une preuve de la livraison des données, ce qui prévient toute tentative ultérieure de la part du destinataire de nier avoir reçu les données (voire leur contenu).

3.2.2.1 Accès

D'une façon générale il faut contrôler l'accès aux archives. Il est ainsi nécessaire de restreindre ou d'ouvrir l'accès à certains documents ou dossiers pour les utilisateurs ou groupes d'utilisateurs. En cas d'enjeu de sécurité important, il faut aussi prendre en considération les niveaux d'habilitation des utilisateurs. L'attribution de ces droits d'accès doit être réservée à certains profils. **Toutefois, l'administrateur ne fait que gérer dans le système les droits définis par la direction.** Ces décisions sont notamment basées sur la législation et la réglementation en vigueur (voir Partie 1 du présent livrable).

De manière plus détaillée :

- Le système d'archivage doit permettre à l'administrateur de réserver l'accès aux documents archivés, aux dossiers et aux métadonnées à des utilisateurs ou à des groupes d'utilisateurs identifiés ;
- Seul l'administrateur du système d'archivage doit avoir la possibilité de créer et de modifier des profils d'utilisateurs et d'affilier les utilisateurs à des groupes ;
- Seuls les administrateurs du système d'archivage doivent avoir la possibilité de changer les paramètres de sécurité pour les groupes et les utilisateurs (droits d'accès, niveau de sécurité, privilèges, attribution de mots de passe et gestion) ;
- Le système d'archivage doit permettre à l'administrateur de paramétrer les profils d'utilisateurs selon les fonctions, les types de métadonnées, les documents et les dossiers auxquels l'utilisateur a accès. Ce paramétrage devra :
    - interdire l'accès au système d'archivage sans procédé d'authentification du profil utilisateur ;
    - restreindre l'accès à des dossiers ou documents précis ;
    - restreindre l'accès au niveau d'habilitation de l'utilisateur ;
    - restreindre l'accès à des fonctions particulières (par exemple lecture, mise à jour et/ou destruction de métadonnées précises) ;
    - refuser l'accès après une certaine date ;
    - affilier l'utilisateur à un ou plusieurs groupes.
- Le système d'archivage doit être en mesure de fournir les mêmes fonctions de contrôle pour les profils et pour les utilisateurs ;
- Le système d'archivage doit être en mesure de constituer des groupes avec les utilisateurs qui travaillent sur les mêmes dossiers ;
- Le système d'archivage doit permettre à un utilisateur d'être membre de plusieurs groupes ;
- Si un utilisateur recherche ou veut accéder à un document archivé, un sous-dossier ou un dossier pour lequel il n'a pas de droits d'accès, le système d'archivage doit donner une des réponses suivantes (à choisir lors de la configuration) :
    - niveau sécurité minimal : afficher le titre et les métadonnées ;
    - signaler l'existence du dossier ou du document (c'est-à-dire afficher son identifiant) sans donner son titre ou d'autres métadonnées ;
    - niveau sécurité maximal : ne délivrer aucune information sur le document, même son existence.
- Si un utilisateur effectue une recherche en texte intégral, le système d'archivage ne doit en aucun cas faire figurer dans les résultats des documents auxquels l'utilisateur n'a pas accès.

Ainsi l'accès vise à contrôler qui a accès aux archives, dans quelles circonstances, prévoir des restrictions d'accès, définir des règles d'affectation des niveaux de sécurité aux documents et des niveaux d'habilitation des utilisateurs potentiels, définir également des règles de gestion de cette confidentialité dans le temps, etc.

3.2.2.2 Historique des événements

Un historique des événements consiste en l'enregistrement systématique des opérations qui touchent le système d'archivage. Cela comprend les opérations faites par les utilisateurs ou les administrateurs et les opérations initiées automatiquement par le système d'archivage en fonction des paramètres du système. Le système d'archivage doit être capable de gérer et de contrôler les documents électroniques en respectant les normes visant à la satisfaction des exigences légales de traçabilité et de sécurité, et doivent être en mesure de démontrer leur conformité à ces exigences. L'historique est un facteur clé dans la satisfaction de ces exigences car il procure un enregistrement complet de toutes les opérations effectuées sur chaque document.

L'historique peut produire un volume de données important si toutes les opérations sont contrôlées. C'est pourquoi, dans certaines implémentations, la direction peut décider que certaines opérations n'ont pas besoin d'être contrôlées. Par ailleurs, l'historique en ligne est en général périodiquement transféré hors-ligne, et peut être détruit quand les documents correspondants sont eux-mêmes détruits. **C'est une question d'exigences légales ou réglementaires et/ou de politique managériale.**

Ainsi de façon plus détaillée :

- Le système d'archivage doit contenir un historique inaltérable (les données de l'historique ne peuvent être modifiées en aucune façon, ni détruites par qui que ce soit) des événements. Cet historique doit permettre de capturer et de stocker automatiquement toute information relative à :
    - toute opération effectuée sur un document ou un dossier électronique;
    - l'utilisateur qui prend l'initiative et/ou exécute cette opération ;
    - la date et l'heure de l'opération.
- L'historique peut être réorganisé et recopié sur un support amovible pour des raisons logicielles par exemple, dès lors que son contenu reste inchangé ;
- Le système d'archivage doit fournir un historique de tous les changements de paramètres administratifs, par exemple, si l'administrateur change les droits d'accès d'un utilisateur.
- Le système d'archivage doit être en mesure de capturer et stocker dans l'historique les informations relatives aux opérations suivantes :
    - la date et l'heure du versement de tous les documents électroniques ;
    - toute modification de la durée de conservation d'un dossier électronique ;
    - toute modification des métadonnées ;
    - les modifications de droits d'accès touchant un dossier électronique, un document électronique, ou un utilisateur ;
    - l'export ou le transfert d'un dossier électronique ;
    - la date et l'heure des restitutions ;
    - les migrations de supports et de formats ;
    - les opérations d'élimination / destruction de dossiers ou documents électroniques.
- Le système d'archivage doit être capable de tracer et de conserver les tentatives de violation du système (c'est-à-dire les tentatives d'accès à des documents, sous-dossiers ou dossiers non autorisés).

En conséquence, tout accès aux archives et toutes opérations qui les mettent en cause ou qui touchent aux documents et données associés doivent être tracés dans un historique des événements afin de garantir la traçabilité et l'accès aux données.

3.2.2.3 Sauvegarde et restauration

La conduite des affaires et la réglementation requièrent l'une et l'autre que le système d'archivage soit doté d'un dispositif complet de sauvegarde régulière des documents et des métadonnées, afin de restituer rapidement des documents perdus par suite de défaillance du système, d'accident, de violation de la sécurité, etc. En pratique, les fonctions de sauvegarde et de restauration peuvent être partagées entre les administrateurs du système d'archivage et les responsables des technologies de l'information.

De manière plus précise :

- Le système d'archivage doit fournir des procédures de sauvegarde et de restauration automatique pour la sauvegarde régulière de la totalité ou d'une sélection des dossiers, documents et métadonnées conservés dans le système d'archivage, avec leurs règles de gestion ;
- Le système d'archivage doit permettre à l'administrateur de programmer des sauvegardes :
    - en fonction de la fréquence voulue ;
    - selon un choix de dossiers ou documents à sauvegarder ;
    - selon les supports de stockage, le système ou la localisation des fichiers sauvegardés (par ex. : stockage hors ligne, système distinct, site distant).
- Seul l'administrateur du système d'archivage doit avoir la possibilité de restaurer les sauvegardes.

Ainsi**,** la sécurité des documents archivés inclut également leur protection contre une faille du système par le biais de sauvegardes et la possibilité de restaurer les données à partir de ces sauvegardes.

3.2.2.4 Traçabilité des mouvements

Au cours de leur vie, les dossiers et leurs métadonnées peuvent être transférés sur un autre support ou dans un autre lieu, notamment si leur actualité décroît et/ou que leur utilisation change de nature (par ex. finalité juridique/patrimoniale). Ce transfert peut se faire localement : near-line (par ex. sur un support amovible dans un dispositif automatisé, tel qu'un CD-R dans un juke-box), hors-ligne (par ex. dans une zone de stockage locale ou distante), ou dans un autre centre d'archivage. La traçabilité de ces changements de localisation doit être assurée à la fois pour satisfaire aux exigences réglementaires et pour faciliter l'accès.

Le système d'archivage doit ainsi fournir un dispositif de contrôle pour assurer la traçabilité de la localisation et des mouvements des dossiers. Cette fonction doit enregistrer toute information relative aux mouvements, à savoir :

- identifiant unique du dossier ou des documents ;
- localisation courante ainsi que l'indication des localisations précédentes (en principe définies par les utilisateurs) ;
- date d'envoi ou de changement de localisation ;
- date de réception (pour les transferts) ;
- utilisateur responsable du mouvement (le cas échéant).

3.2.2.5 Intégrité

Il est capital qu'après le versement, aucune composante du document, ni sa structure ni les métadonnées nécessaires pour établir et garantir son intégrité et son origine, ne soient altérées. Les documents doivent être conservés dans une forme non modifiable et protégés contre des changements intentionnels ou accidentels de leur contenu, voire de leur contexte, de leur structure ou de leur apparence et ce durant toute leur vie afin de maintenir leur intégrité. Néanmoins il y a lieu de modérer ces propos en regard des modifications de formats qui peuvent être rendues nécessaires pour une conservation à moyen et long terme. Dans ce cas on aura soin de contrôler l'intégrité de l'information par rapport à son contenu et non plus seulement au sens informatique pour lequel l'information est vue comme une simple suite d'octets. Les processus mis en œuvre à l'occasion de telles migrations de formats devront évidemment garantir cette intégrité de l'information.

Ainsi le système d'archivage doit restreindre l'accès aux fonctions du système, en fonction des profils utilisateurs et des contrôles administratifs. Ceci est nécessaire pour préserver l'intégrité des archives électroniques. De plus le système d'archivage devrait fournir une alerte sur les tentatives de prendre en compte un document incomplet ou dont l'état compromettrait l'intégrité dans le futur ou d'un document dont il serait impossible de vérifier ultérieurement l'intégrité.

3.2.2.6 Indices de sécurité

Dans certains cas, notamment quand la sécurité nationale est en cause, il est nécessaire de limiter l'accès à l'aide d'indices de sécurité et de niveaux d'habilitations. Ces habilitations priment sur tout droit d'accès reposant sur les critères définis précédemment quant aux accès. Il s'agit ainsi d'attribuer un ou plusieurs « indices de sécurité » aux dossiers et documents. Le terme « indice de sécurité » est utilisé ici pour désigner « *une ou plusieurs données associées à un document pour préciser les règles et conditions d'accès* ».

Les utilisateurs se voient alors attribuer un ou plusieurs niveaux d'habilitations qui empêchent l'accès aux dossiers et/ou documents dotés d'indices plus élevés. Les indices de sécurité peuvent être divisés en catégories qui sont soit de nature hiérarchique, soit organisées en fonction d'autres critères spécifiques à une entreprise ou à un domaine d'activité.

Ainsi, le système d'archivage doit permettre d'affecter des indices de sécurité aux documents archivés et de procéder à un des choix suivants au moment de la configuration :

- indices de sécurité affectés aux dossiers et sous-dossiers ;
- ou dossiers et sous-dossiers électroniques sans indice de sécurité.

Par ailleurs, il est fondamental que ce qui apparaît comme le sous-système de sécurité du système d'archivage soit compatible avec les outils de sécurité générale de l'organisation.

Au-delà de ces aspects sécuritaires qui correspondent plus à des notions logiques, immatérielles nous donnons ci-après un dernier complément relatif plutôt aux aspects physiques et à l'organisation générale de la sécurité d'un système d'archivage.

3.2.3 Aspects physiques et organisation générale de la sécurité du SAE

3.2.3.1 Administration et organisation de la sécurité

On doit disposer d'une structure de sécurité qui garantit la bonne exécution des mesures de sécurité. Cette structure de sécurité doit être de préférence disjointe de celle qui a en charge l'exploitation des systèmes informatiques ou de télécommunication. Son organisation et son administration doivent être parfaitement définies et connues de tout le personnel.

3.2.3.2 Sécurité physique

Des mesures de sécurité physique doivent être prises pour empêcher l'accès non autorisé aux matériels, aux systèmes de télécommunication, aux supports amovibles contenant les informations ou leurs sauvegardes.

3.2.3.3 Locaux

Il convient, afin de réduire les risques, d'avoir plusieurs locaux sécurisés, de manière à répartir sur plusieurs sites les supports contenant les informations. Pendant l'absence du personnel, les locaux doivent être fermés à clé. Ils doivent disposer de dispositifs anti-intrusion et être équipés de dispositifs d'alarme. Ceux-ci doivent être systématiquement vérifiés et testés. La définition et la connaissance des procédures de mise en service et d'arrêt des dispositifs d'alarme ne doivent être le fait que d'un nombre restreint de personnes dûment accréditées. Les procédures de réaction aux alarmes doivent être définies et testées périodiquement. Tous les équipements doivent être de préférence situés le plus loin possible du domaine public.

3.2.3.4 Contrôle d'accès des personnels aux matériels

En l'absence des personnels, les différentes clés des locaux, des armoires à protéger ou des systèmes informatiques doivent être tenues dans un endroit lui-même protégé, accessible aux seules personnes autorisées. Toute sortie de clé doit être contrôlée.

3.2.3.5 Contrôle de l'accès des personnels aux bâtiments

Les zones particulièrement sensibles doivent comporter des moyens spécifiques de contrôle. L'usage de systèmes reposant sur des cartes à mémoire est recommandé. Il faut également prévoir des procédures selon les catégories de personnes. En particulier, il convient de prévoir des consignes particulières pour les personnels de nettoyage et de maintenance.

3.2.3.6 Sécurité en matière de personnel

L'autorité responsable doit définir et contrôler les droits d'accès aux informations. Elle doit dresser la liste nominative des personnes ayant accès à ces informations, ainsi que leurs droits sur celles-ci (écriture, lecture, modification, suppression). Tout personnel de l'organisme ou de l'entreprise travaillant sur le système doit au préalable avoir signé un document d'engagement de sa responsabilité. L'utilisation des postes de travail en dehors des heures ouvrables doit être contrôlée par l'autorité responsable. Les procédures de sécurité doivent être connues de tout le personnel. L'autorité responsable doit s'en assurer régulièrement, en particulier lorsqu'elles ont été modifiées ou supprimées.

3.2.3.7 Sécurité des matériels

Les dispositifs de sécurité des matériels et des logiciels contribuent, séparément ou conjointement, à la sécurité des systèmes informatiques en permettant comme cela a déjà été mentionné : l'identification et l'authentification des périphériques, des supports et des utilisateurs ; un contrôle d'accès et de détection ; des contrôles ; si nécessaire le chiffrement des informations.

Ainsi, l'aspect sécurité doit être intégré lors du choix des équipements, de leur installation et de leur exploitation.

3.2.3.8 Logiciels et progiciels

Les logiciels et les progiciels font partie intégrante de la configuration du système ; ils doivent en conséquence être soumis aux mêmes règles de sécurité que les matériels. Parmi les systèmes d'exploitation et les progiciels, doivent être retenus en priorité ceux qui permettent :

- une protection renforcée des outils de contrôle d'accès ;

- une protection contre les intrusions et les logiciels parasites ;
- un contrôle d'intégrité.

Le développement des logiciels doit s'appuyer sur des méthodologies rigoureuses, dont le choix et le contrôle du bon usage sont de la responsabilité du responsable de l'application. Avant d'être mis en exploitation, les progiciels et les logiciels doivent avoir été suffisamment testés sur une machine autre que celle qui est exploitée pour la production courante. Les logiciels et les progiciels doivent être particulièrement protégés et leurs accès pour changement ou modification réservés aux seules personnes autorisées. En cas de fonctionnement anormal, un compte rendu immédiat doit être fait à l'autorité de sécurité et il faut effectuer un isolement de la partie du système en anomalie le plus rapidement possible.

Le SAE doit reposer sur des règles de sécurité spécifiques mais qui viennent s'ajouter à celles définies à titre général dans la politique de sécurité des systèmes d'information.
A ce titre, le SAE qui est un système d'information doté d'une finalité particulière doit intégrer une analyse des risques tout au long du processus d'archivage. Les règles énoncées ci-dessus contribuent à dégager le noyau de la sécurité du SAE.

4 Les offres d'archivage électronique

Pour la partie records management, le marché propose aujourd'hui un panel assez large et diversifié de solutions d'archivage qui se précise et se complète d'année en année. La typologie des produits va du coffre-fort à la solution générale qui englobe l'archivage dans la gestion du cycle de vie complet des données (ILM). Les produits du marché mettent tantôt l'accent sur la gestion de contenu, tantôt sur l'archivage légal (l'expression est répandue mais il serait plus exact de dire « archivage à des fins de preuve »). Ils visent tantôt l'ensemble des données d'une organisation (incluant parfois les données sur les archives papier), tantôt un type d'information ou un format de document bien spécifique, tel que les messages électroniques.

Dans le secteur technique et scientifique, existent également des offres notamment en terme d'infrastructures de stockage (très grandes volumétries) et d'outils performants d'accès et de consultation des données archivées.

En revanche, existent encore très peu de briques logicielles prenant notamment en compte la partie gestion des versements sur la plate-forme d'archivage suivant un format donné, le contrôle des formats, leur conversion éventuelle…" , ainsi que l'alimentation automatique d'une base de données descriptive à partir notamment des métadonnées des objets archivés accompagnant le versement.

4.1 Les offres logiciels

Même si la recherche d'un logiciel correspond à la meilleure relation entre son besoin et l'offre du marché, tous les besoins identifiés n'ont pas encore trouvé leur solution d'archivage idéale. Par exemple, l'extraction de données des ERP pour les archiver en fonction de leurs durées de conservation respectives reste un problème non résolu.

Avant d'entrer dans le détail des critères de choix des différents logiciels, nous abordons la question importante à se poser : que choisir entre solution du marché, logiciel libre ou développement spécifique ? En dehors du fait que chacune de ces approches a ses partisans, l'essentiel est de bien prendre la mesure de ses choix, étant entendu que les changements de politique auront un coût qu'il vaut mieux connaître et si possible éviter. On trouve dans la presse spécialisée un certain nombre de témoignages d'abandon du marché vers le libre et d'abandon du libre pour revenir au marché. Dans les deux cas, il est souhaitable de prendre en compte les questions techniques de récupération des données et de maintenance.

En tout état de cause nous recommandons de limiter le développement spécifique à des projets eux-mêmes très spécifiques pour lesquels, même après reconfiguration des processus, le marché ou le libre n'offre aucune solution satisfaisante.

4.1.1 Principaux critères à analyser et vérifier

4.1.1.1 Interopérabilité et partage de ressources

La question de l'interopérabilité est fondamentale sauf dans les cas particuliers où la communauté d'utilisateurs serait par définition limitée et fermée. Le plus souvent, l'outil devra pouvoir communiquer avec les autres composantes du système d'information ou partager des ressources telles qu'une base de données ou un thésaurus avec d'autres applications. L'interopérabilité avec l'extérieur, même pour un outil d'archivage, peut être un besoin fort et doit être étudiée. De même il est important de prévoir dès le départ une notion de réversibilité de l'information dans le cas d'un changement ultérieur du système.

4.1.1.2 Facilités d'indexation

Il est important de vérifier les facilités d'indexation classique, d'indexation par mots-clés et surtout la complémentarité ou la co-existence des deux systèmes, en fonction des besoins exprimés sans tomber pour autant dans l'excès. En matière de présentation des résultats il pourra être intéressant de vérifier que l'outil permet de les hiérarchiser et de faire des recherches en cascade.

4.1.1.3 Accès (temps)

Le temps d'accès à l'information est un critère de choix mais qui dépend largement du besoin de chaque entreprise : soit l'accès à l'information archivée est toujours urgent (besoins de chercheurs ou de juristes par exemple), soit il peut attendre plusieurs minutes voire davantage. Il est donc préférable d'avoir défini ses besoins avant la recherche de la solution satisfaisante. On aura également soin de vérifier que les performances annoncées ne se dégradent pas avec la montée en charge et l'augmentation des volumes.

4.1.1.4 Accès (sécurité)

De la même façon, les données archivées peuvent être hautement confidentielles (données commerciales) ou en partie publiques (certaines données administratives ou documentaires). Cet aspect devra être évalué en fonction du besoin identifié par rapport aux possibilités offertes.

4.1.1.5 Montée en charge et volumétrie

Ce point a déjà été évoqué pour les problèmes de temps d'accès et ne peut être évalué lors d'une simple démonstration. Dans la mesure où la question de la volumétrie est importante, il faut obtenir des garanties de l'éditeur et une démonstration grandeur réelle, sur le site de l'éditeur ou chez un de ses clients.

4.1.1.6 Format

À partir du moment où le choix d'un format aura été fait, le système devra d'une part être capable d'effectuer toutes les vérifications d'usage concernant ce dernier au moment des versements et d'autre part permettre ultérieurement des migrations de formats rendues nécessaires pour le moyen et surtout le long terme.

4.1.1.7 Stockage

La problématique consistera à vérifier si les modalités de stockage correspondent bien aux besoins et aux souhaits de l'organisation : en ligne (on line), en différé (off line), en léger différé (near line) voire en un panachage de ces différentes options. Dans la mesure où plusieurs technologies de stockage sont possibles il y aura lieu de vérifier selon quels critères le système les attribue et s'il a recours à un module spécifique de gestion de type HSM (hierarchical storage management). Par ailleurs il est important d'analyser quels types de migrations sont possibles, plus spécialement pour les changements de supports et de format ainsi que les critères associés de déclenchement de telles migrations. Sur ce dernier point on s'attardera également sur le type de contrôles destinés aux supports afin de lancer au besoin une migration. Il ne faudra pas oublier également de vérifier la possibilité de travailler sur plusieurs sites géographiquement distincts, pour des raisons évidentes de sécurité des données.

4.1.1.8 Évolutivité

Dans le cas, fort probable, où le système de base devra faire l'objet d'évolutions tant en matière d'accessibilité que de capacité de stockage, il faudra s'assurer que de telles évolutions sont d'une part possibles et de plus n'auront pas d'incidences majeures sur le système existant et sur sa disponibilité vis-à-vis des utilisateurs. Pour les évolutions il y aura également lieu de vérifier qu'elles sont possibles avec des systèmes différents de ceux proposés par le fournisseur d'origine et ce à des conditions raisonnables, tant techniques qu'en matière d'investissement.

4.1.1.9 Coût du logiciel

Il faut faire attention à ce niveau d'analyser l'ensemble des éléments de facturation : serveur, client, microprocesseur. Il est fortement recommandé de faire une simulation d'exploitation sur trois ans comme indiqué plus précisément dans un chapitre spécifique sur le sujet.

4.1.1.10 Coûts associés

La remarque est identique à celle réalisée pour le coût du logiciel. La meilleure façon de procéder est incontestablement de simuler l'exploitation pour laquelle il ne faudra pas oublier d'inclure les coûts associés de maintenance (évolutive ou corrective) voire d'autres types de coûts.

4.1.1.11 Pérennité du fournisseur/éditeur

La pérennité du fournisseur est également à prendre en compte même si rien ne peut la garantir à 100 %. Ainsi la reprise ou le transfert des données, la récupération des codes sources doivent être précisément envisagés (modalités et coût). La notion de réversibilité de la donnée trouve ici également tout son sens.

4.1.1.12 Réorganisations de l'entreprise

En complément au point précédent il est incontestable que les réorganisations (y compris les fusions et acquisitions) font partie des événements courants de la vie des entreprises. Il est donc préférable que les systèmes d'archivage soient compatibles ou du moins qu'on puisse mutualiser les outils de recherche. Ceci plaide aussi pour des solutions modérément sophistiquées et des procédures unifiées.

4.1.2 Présentation des offres logiciels

Nous donnons ci-après à titre indicatif une liste non exhaustive des principaux acteurs sur le marché du logiciel touchant à la gestion de l'archivage électronique dans sa partie essentiellement courante et intermédiaire.

Argus	http://www.argus-dms.com
Cecurity.com	http://www.cecurity.com
Ceyoniq	http://www.ceyoniq.com
Damaris	http://www.damaris.com
Docubase Systems	http://www.docubase.com
EADS, l'offre se compose actuellement de trois produits fondés sur une logique OAIS : - pour l'entrée, une brique générique GFE pour Generic Front End, à personnaliser en fonction des besoins métier, - pour le stockage, une brique Satstore qui correspond à tous types de données et aux gros volumes, - pour la dissémination des données (restitution), une brique générique PFD pour Product Formatting & Delivery.	
EMC Documentum	http://www.documentum.com
Ever et sa suite EverSuite	http://www.ever-team.com
FileNet, an IBM Company, et sa plate forme FileNet P8	http://www.filenet.com
IBM et sa suite logicielle Content Manager	http://www.ibm.com/software/info/ecatalog/fr_FR/db2/SWB40.html
Itesoft	http://www.itesoft.fr
Open Text Corporation et la suite de produits Livelink Enterprise Suite	http://www.opentext.com
Storagetek et son produit Arcsys	http://www.storagetek.com

4.2 Les offres de services

4.2.1 Le tiers archiveur

Dans la mesure où la mise en place d'un système d'archivage électronique est incontestablement complexe voire compliquée, il est clair que le recours à un tiers peut paraître séduisant au moins pour deux raisons :

- la mutualisation et donc le partage des coûts ;
- le professionnalisme de la solution, gage supplémentaire de la force probante des éléments archivés.

Attention toutefois au fait qu'un archivage interne est parfois obligatoire, par exemple, pour les collectivités territoriales.

Ainsi est née la notion de tiers archiveur qui est une personne physique ou morale en charge, pour le compte de tiers, de la réception, de la conservation et de la restitution de documents électroniques dont il doit garantir l'intégrité.

Ce dernier point fait ressortir un des intérêts de recourir à un tiers archiveur lequel utilise des moyens permettant d'offrir cette garantie d'intégrité du document archivé et ainsi sa force probante voire sa validité. A ce titre, le tiers archiveur a la possibilité de changer le support ou le format physique de l'archive sous condition bien évidemment de conserver son intégrité.

Le tiers archiveur fait évidemment partie de la famille des tiers de confiance avec lesquels il doit être capable de bâtir des partenariats du moins avec deux d'entre eux :

- le tiers certificateur pour les aspects liés à la signature électronique ;
- le tiers horodateur.

Ceci est indispensable afin de s'assurer que le système d'archivage proposé est fiable et conforme à la loi et aux différentes réglementations et adapté au client.

4.2.1.1 Obligations liées au service

En tant que tiers de confiance les obligations et les responsabilités qui pèsent sur le tiers archiveur sont nombreuses. A titre indicatif, nous citerons les obligations auxquelles est soumis le tiers archiveur par rapport à la prestation offerte. Il doit notamment :

- disposer d'une capacité de stockage suffisante et évolutive pour pouvoir assurer sans discontinuité la prise en charge des documents ;
- mettre en place un niveau de sécurité physique et logique suffisant. Les mesures de sécurité étant établies et documentées en fonction des besoins ;
- conserver l'intégralité des éléments qui lui ont été confiés de façon fiable. A ce titre le tiers archiveur devra assurer la sauvegarde des données sur au moins un autre site ;
- ne communiquer les documents archivés qu'aux destinataires désignés dans le contrat, et cela même après que le contrat ait pris fin ;
- permettre un accès direct et sécurisé (contrôle d'accès) au client pour consulter les archives ;
- permettre la restitution des documents archivés sur tout type de support, de format, etc. défini avec le client ;
- documenter et permettre l'audit des procédures d'archivage, de migration de support et de restitution ;
- prendre une assurance couvrant les risques liés à l'exécution du contrat ;
- détruire les éléments reçus à la demande du client et fournir à celui-ci une attestation de destruction ;
- proposer un processus de réversibilité ;
- disposer d'une interopérabilité effective avec d'autres prestataires identifiés ;
- informer le client à chaque modification du service d'archivage.

4.2.1.2 Obligations liées au contenu

À ces obligations s'ajoutent des obligations de nature légale directement liées au contenu des documents que le tiers archiveur sera amené à conserver. Ces obligations dépendent directement du type des données gérées. Ainsi, le tiers archiveur est notamment tenu de respecter:

- les formalités préalables nécessaires à la mise en place de traitements automatisés d'informations nominatives ;
- l'obligation de confidentialité et de protection des données à caractère personnel qu'il traite.

En revanche, le tiers archiveur n'est soumis à aucune obligation générale de surveiller les informations qu'il héberge quant à leur contenu.

S'agissant spécifiquement du processus d'indexation, celui-ci peut avoir lieu, en amont, chez le client (idéalement) ou être effectué par le tiers archiveur. Dans ce dernier cas le processus

d'indexation ne devra pas être interprété ni être interprétable comme un traitement du contenu de l'information afin de rester hors des obligations de contrôle du contenu comme indiqué ci-dessus.

Précisons que ce processus d'indexation comprend deux étapes distinctes après avoir défini le détail du contenu des index. La première étape à laquelle il faut faire référence pour ce qui précède, consiste à rechercher à l'intérieur du document les informations nécessaires à l'indexation, il s'agit d'une forme d'analyse syntaxique de chaque document. La deuxième étape revient à mettre à jour les bases de données ou systèmes équivalents à partir de ces informations qui permettront ultérieurement de retrouver le document ainsi archivé.

4.2.2 Importance du contrat

Compte tenu de ces obligations, l'on perçoit immédiatement l'importance que peut revêtir le contrat que le tiers archiveur propose à ses clients. Sans vouloir être exhaustif nous donnons ci-dessous les rubriques essentielles qui doivent y figurer :

- Description fonctionnelle du service et des procédures associées, y seront entre autres précisés les mécanismes de :
  - Versement (prévoir le contrôle les documents et de leurs métadonnées selon un format prédéfini) ;
  - Conservation ;
  - Interrogation.
- Modalités d'accès, infrastructure de télécommunication à mettre en place ;
- Conditions d'accès, définition des droits des utilisateurs destinée à garantir l'identification unique et fiable des clients ;
- Modalités de modification du service ;
- Conditions de destruction ;
- Sécurité, dispositifs et procédures destinés à garantir la confidentialité, l'intégrité des documents électroniques et l'authentification du client ;
- Définition de la qualité du service, référence à une SLA éventuelle, voire ci-dessous ;
- Maintenance, définition des opérations de maintenance éventuelles ;
- Conditions particulières, par exemple, mise en place d'un journal des accusés de réception ou encore dans le cas où les documents sont chiffrés, préciser comment la gestion des clés de chiffrement est assurée et notamment son incidence dans le processus de restitution.

Définition d'une SLA (Service Level Agreement)

Comme indiqué précédemment et afin d'être aussi précis que possible dans la définition de la prestation et de son niveau de service, le contrat pourra faire référence à une SLA ou mieux à une véritable politique d'archivage (objet de la deuxième partie).

Les besoins auxquels doit répondre une SLA sont essentiellement destinés à permettre au client d'avoir une parfaite compréhension du service offert tant au niveau de ses fonctionnalités que de la façon dont elles seront délivrées. Il s'agit donc de :

- définir un niveau de service en fonction des besoins;
- indiquer comment établir, suivre et mesurer la performance du service ;
- permettre une évolution du niveau de service dans le temps.

Nous donnons à titre indicatif quelques uns des éléments principaux que l'on retrouve dans une SLA afin de répondre à ces besoins, à savoir :

- détail de l'architecture technique ;
- support et assistance, classification et définition des niveaux des incidents, délais de réponses, principe d'escalade ;
- surveillance des évènements ;
- qualité de service, performances, disponibilité ;
- pénalités, critères retenus, précision du type de dédommagement ;
- analyse des données de performances, périodicité, alertes, quantification.

Comme on peut le constater, les obligations encadrant le contrat de tiers archivage sont nombreuses et il faudra prendre un soin particulier à la rédaction des clauses. En effet, cette rédaction aura, dans l'hypothèse de la survenance d'un litige, une influence déterminante sur les moyens probatoires

(Exemple : charge de la preuve, contenu de l'obligation, etc.) qui selon les cas reposeront sur le client (obligation de moyens) ou sur le tiers archiveur (obligation de résultat). D'où l'importance d'une politique d'archivage destinée à détailler et à préciser au mieux les obligations et conditions d'exécution de la prestation en fonction du niveau de service attendu, par exemple en matière de sécurité.

4.2.3 Détail des offres

Au niveau des prestataires potentiels, le métier de tiers archiveur trouve ses origines dans plusieurs sources :

- une déclinaison du modèle ASP qui de façon générique consiste à mettre à disposition d'un client des traitements informatiques et des services auxquels il peut accéder à distance via un lien de télécommunication plus ou moins sécurisé ;
- une évolution du métier d'archiveur papier traditionnel, vu plus comme un dépositaire ;
- une diversification des spécialistes de l'éditique qui sont amenés naturellement à répondre aux demandes de leurs clients ;
- une opportunité de marché.

Ainsi depuis quelques années plusieurs sociétés se sont positionnées en tant que tiers archiveur soit à titre d'activité unique, soit plus généralement en tant qu'extension de leur offre.

Historiquement la société CDC Zantaz, aujourd'hui CDC Arkhineo, a été le premier tiers archiveur en France. Créée conjointement par la Caisse des Dépôts et Consignations et l'Américain Zantaz, cette société a proposé, dès la fin 2001, un service d'archivage électronique avec une spécialisation pour les e-mails.

D'autres sociétés ont suivi dont nous donnons ici un bref aperçu :

- Orsid, spécialiste de l'éditique ;
- Asterion, filiale de la poste belge et regroupement de plusieurs sociétés venant notamment du monde de l'éditique, propose une solution de tiers archivage électronique sécurisé des documents, sur support numérique de type WORM, baptisée e-STAR® (électronique - Système de Tiers ARchivage) ;
- Aspheria, filiale du groupe La Poste propose une gamme de solutions d'archivage répondant à des besoins et contraintes différentes en fonction du type de document archivé : archivage sur serveurs et consultation en ligne, archivage sur microfiches ou CD-Rom / DVD-Rom ;
- Steria, gros intégrateur informatique français propose Stromboli, service d'archivage électronique basé sur la technologie Centera de chez EMC associée à un frontal logiciel développé par la société STS (Security Tracking Solutions) ;
- Thales Security Systems, vient d'intégrer à son offre le Coffre-Fort Electronique Communicant (CFEC), solution d'archivage électronique légal, de l'éditeur français Cecurity.com ;
- Atos, propose une offre complète de tiers archivage associée aux autres métiers de la confiance que sont la certification et l'horodatage ;
- La banque du document, SGA (société générale d'archives)…

5 Partie coûts

5.1 Processus de décision

Tout processus de décision est relativement complexe. En ce qui nous concerne, il s'agit de la décision d'investir dans une technologie ou un service, sans rentabilité apparente. En effet, un système d'archivage n'est malheureusement pas source de revenus directs.

5.1.1 Décision d'investir

La première étape revient à **décider ou non d'investir**. Pour cela il faudra disposer d'une première évaluation du montant de l'investissement envisagé et surtout bien avoir analysé l'ensemble des risques encourus si l'investissement n'était pas réalisé. Ces risques se retrouvent à plusieurs niveaux : financier bien sûr, juridique (non respect des lois et des réglementations), qualité du service offert, etc. Certains de ces risques son tangibles et mesurables tandis que d'autres sont au contraire intangible et difficilement mesurables.

Le raisonnement que nous proposons ici est sensiblement équivalent à celui utilisé en matière de sécurité. La prise de décision est en générale déterminée en opposant le coût de l'investissement envisagé à celui des conséquences d'un sinistre si rien n'était fait. Nous nous rapprochons ainsi de la notion de ROSI (*return on security investment*) issue du ROI (*return on investment*), soit en clair : qu'est ce que me rapporte mon investissement par rapport à son coût ?

5.1.2 Choix de la solution

Au-delà de la décision d'investir l'analyse économique doit également permettre de **choisir une solution** spécifique parmi un ensemble de solutions proposées. Contrairement à la première étape où les critères de décision étaient pour certains difficiles à quantifier, le principe du choix est plus facile dans la mesure où les critères sont, a priori, tous quantifiables. Néanmoins la difficulté subsiste car il faut s'efforcer de comparer des choses qui sont effectivement comparables et ne rien oublier dans la liste des éléments à prendre en considération.

5.1.3 Hypothèses

Pour la suite de notre exposé, nous nous placerons dans une logique de choix et nous supposerons que ces solutions satisfont à la majorité des exigences liées aux besoins et dans le cas d'un système à installer en interne, correspondent à une même infrastructure technique, notamment quant au choix d'un site de réplication.

Enfin, traitant du cas particulier d'un service d'archivage de documents électroniques, nous nous placerons également dans l'hypothèse où ce service pourrait être réalisé par un tiers ce qui renvoie à la question : « faire » ou au contraire « faire faire » ?

5.2 Détail des coûts et de la volumétrie

5.2.1 Coûts

Comme indiqué précédemment, l'une des difficultés rencontrées est de répertorier l'ensemble des coûts de façon exhaustive. Nous listons ci-dessous, **à titre indicatif et non limitatif**, un certain nombre d'ente eux :

Investissements :

- Matériel informatique : serveur, baies de disque… ;
- Matériel réseau ;
- Matériel de télécommunication ;
- Matériels liés à la sécurité : (firewall, cartes de contrôle d'accès…) ;
- Logiciels : archivage, backup, redondance… ;
- Prestations de mise en place : installation, recette ;

- Formation.

Exploitation :

- Télécommunications : coût mensuel des communications ;
- Locaux sécurisés : si possible à évaluer en coût de location mensuel ;
- Personnel : détail du temps nécessaire pour chaque processus (par exemple pour les sauvegardes, opérations de maintenance), des personnes et des salaires correspondants chargés ou équivalents en sous-traitance ;
- Maintenance : matériel et logiciel, en tenant compte de la période de garantie et des extensions possibles ;
- Support : coûts et conditions (délais d'intervention et de remise en marche : 2h, 4h, 8h).

Autres coûts :

- Consommables : bandes, disques,… ;
- Augmentation de la capacité (matériel, logiciel, installation), cas d'une évolutivité par palier ;
- Migration (achat de matériel, temps nécessaires…).

Prestataires de TA :

Concernant des prestataires de tiers archivage il faudra recenser les coûts des différents services offerts en fonction de leurs propres critères, généralement directement liés à la volumétrie à traiter. Les différents modes de facturation sont habituellement basés sur les trois éléments suivants :

- Versement : montant facturé au moment où l'information arrive chez le tiers archiveur, peut être fonction du volume ou non ;
- Conservation : montant facturé pour le stockage de l'information dans le temps, directement fonction du volume (linéaire, par palier, avec ou non un minimum);
- Interrogation : facturé à chaque fois qu'un utilisateur désire accéder à l'information archivée.

5.2.2 Hypothèses de volumétrie

Après avoir déterminer les coûts, il nous reste à faire des hypothèses quant à la montée en charge de notre système d'archivage dans le temps, en matière de volumétrie, voire d'interrogations effectuées par les utilisateurs en nombre et en fréquence.

5.3 Simulation d'exploitation

Dès l'instant où l'ensemble des informations précédemment mentionnées aura été collecté, l'on pourra mettre en place une véritable simulation du fonctionnement du système d'archivage, en terme de coûts et pour une période donnée. Les résultats seront alors présenté dans un ou plusieurs tableaux de synthèse qui devront permettre de guider le choix final.

L'avantage de disposer d'un système de simulation est avant tout de permettre la prise en compte à la fois des coûts ponctuels et des coûts récurrents. Accessoirement, un tel système permet également d'analyser la sensibilité de l'évolution de ces différents coûts au changement de tel ou tel paramètre comme par exemple celui de la montée en charge.

Annexe : Détail des supports destinés à l'archivage

Les supports magnétiques

Les bandes magnétiques

Il faut bien garder en mémoire que la capacité de stockage des lecteurs de bandes magnétiques comporte deux données distinctes : la capacité sans compression dite en mode natif et la capacité avec compression matérielle intégrée, en général le double de la précédente.
Nous donnons ci-après les formats les plus connus et utilisés de nos jours.

SLR (Scalable Linear Recording)

La technologie SLR a été développée par Tandberg et accepte de 2 à 70 Go de données non compressées et un taux de transfert de 380 Ko/s à 6 Mo/s. La base des cassettes est composée d'une plaque de métal. D'ailleurs, les lecteurs SLR ont beaucoup hérité de cette technologie. Quatre pistes sont écrites simultanément et la densité des données est calculée suivant la technologie PRML (Partial Response Maximum Likelihood). Cette technologie réduit l'interférence signal-bruit (S/B), ce qui permet des densités surfaciques et des taux de transfert élevés, sans sacrifier la fiabilité de l'unité. L'utilisation du codage PRML, le servo-tracking et le test de la qualité de la bande avant chaque écriture contribuent à l'intégrité des données.

ADR (Advanced Digital Recording)

L' ADR a été développée par Philips et se caractérise par des vitesses variables. L'ADR travaille sur 192 pistes, alors que la récente ADR-2 lit et écrit un total de 384 pistes. La tête de lecture peut lire et écrire simultanément 8 canaux de données et permet d'avoir des taux de transfert impressionnants avec des vitesses de bande relativement faibles. Les lecteurs ADR utilisent en permanence une vitesse variable leur permettant d'adapter cette dernière au débit des données du système qui lui-même change en permanence. Ceci les empêche donc de devoir s'arrêter pendant un enregistrement, reprendre ensuite et devoir se repositionner, ce qui fragiliserait les bandes. Les cassettes ADR offrent de 15 à 60 Go de capacité et de 2 à 2,5 Mo/s de taux de transfert.

DAT (Digital Audio Tape) DDS (Digital Data Storage)

Le standard DAT, créé en 1987, est à la base un format d'enregistrement numérique qui offre 3 heures de son 100 % numérique sur une cartouche de 4 mm deux fois plus petite qu'une cassette classique, au même format que le CD. Le format « informatique » DAT, dérivé du format d'enregistrement du son DAT de SONY, a été développé conjointement par HP et SONY à l'époque. Il est rapidement devenu le support de sauvegarde sur bande le plus répandu, avant l'archivage. Les bandes DAT ont un débit de 1,5 Mo/s et une capacité de quelques Go.

Le DDS, actuellement dans sa version 4, est une évolution du format DAT aux applications informatiques qui permet de stocker 20 Go de données en natif (non compressé). Cette technologie qui offre un débit moyen de 3 Mo/s, est d'une fiabilité plus élevée que le DAT. La cinquième génération DAT 72 vient d'être annoncée, portant la capacité à 36 Go en natif.

DLT (Digital Linear Tape) S-DLT (Super Data Linear Tape)

Quantum est à l'origine de cette technologie qui offre un débit de 3 à 8 Mo/s et une capacité de stockage de 40 à 80 Go. Les données sont enregistrées sur des pistes parallèles à la direction de défilement.

Evolution de la technologie précédente DLT, la S-DLT permet de stocker de grandes capacités de données jusqu'a 300 Go avec un débit élevé qui peut atteindre les 36 Mo/s en mode natif non compressé.

Afin de satisfaire aux exigences directement liées à l'archivage et afin de contenter les utilisateurs sensibles aux coûts d'exploitation de la bande, Quantum propose pour ses lecteurs DLT la fonction WORM DLTice qui n'impose pas l'usage de médias spécifiques et interdit toute réécriture ou suppression intempestive avant la fin de la durée de conservation.

LTO (Linear Tape-Open)

La spécification LTO a été développée et lancée conjointement en 1999 par trois des meilleurs fabricants de solutions de stockage au monde : IBM, Hewlett-Packard et Seagate. Présenté comme une solution alternative au SuperDLTtape, ce format, appelé Ultrium, est implémenté dans

des produits capables de stocker 100 Go par cartouche et de transférer les données au taux de 15 Mo/s en mode natif pour l'Ultrium-1, 200 Go et 30 Mo/s pour l'Ultrium-2, 400 Go et 80 Mo/s pour l'Ultrium-3.

Cette technologie est similaire à celle des lecteurs DLT. Chaque média intègre en outre une puce mémoire de 4 Ko sur laquelle sont inscrits le numéro de série, une indication permettant de savoir si la cassette est utilisée pour la première fois ou encore la « *table des matières* » des données. Plusieurs nouvelles générations sont déjà planifiées, dont la quatrième devrait atteindre 800 Go en 2006.

Imation, fournisseur des LTO, propose également des cartouches LTO 3 transformées en supports non réinscriptibles. Elles ne peuvent être effacées que par une opération de démagnétisation et sont donc considérées comme des WORM logiques. Quoique non conformes à la norme NF Z42-013, elles répondent néanmoins aux obligations telles que celles imposées par le Sarbannes Oxley act, les accords Bâle II ou encore la rule SEC 17a-4.

AIT (Advanced Intelligent Tape) S-AIT

La technologie AIT, développée par Sony est une technologie 8mm. L'AIT met en œuvre l'efficace compression de données ALDC (Advanced Loss Data Compression) et l'utilisation exclusive de supports AME (Advanced Metal Evaporated). Une des particularités de ces cassettes est la présence d'une puce mémoire de 64 Ko (MIC, Memory-in-Cassette) qui accélère l'accès aux données. L'AIT-1 offre une capacité maximale de 35 Go, l'AIT-2 50 Go et l'AIT-3 100 Go et un débit de12 Mo/s. Tout dernier concept d'enregistrement haute capacité et hautes performances, la technologie S-AIT présente une volumétrie par cassette de 500 Go et un débit de 30 Mo/s.

Tout comme pour les LTO, la présence d'une puce mémoire permet de disposer d'un dispositif WORM logique en conformité avec les réglementations évoquées ci-dessus dont la première a été la SEC Regulation 17 CFR § 240.17a-4.

Bande ½ pouce haute performance

Nous ne citerons ici que le dernier format proposé par StorageTek dans cette catégorie des bandes ½ pouce, le 9840 et ses évolutions. Ce format, présenté sous forme de cartouches, allie vitesse, capacité et temps d'accès réduit. Nous trouvons dans ce format des capacités allant de 20 Go et 10 Mo/s pour le 9840A à 200 Go et 30 Mo/s pour le 9940B. Cette technologie est plutôt destinée aux librairies de bandes.

Storagetek propose en option la fonction Volsafe correspondant à du WORM logique pour les formats 9840 et 9940.

Cartouches 3592 IBM

Offrant une capacité en mode natif de 300 Go pour un débit de 40 Mo/s, ces cartouches sont également disponibles avec l'option WORM logique. IBM propose ainsi des cartouches spécifiques identifiées par un numéro unique et qui incorporent un contrôleur chargé du pilotage des secteurs enregistrés.

Synthèse des différents formats de bandes magnétiques

Format	Fonction WORM	Capacité Go	Débit Mo/s
SLR		**2 à 70**	380 Ko/s à 6 Mo/s
ADR		**15 à 60**	2 à 2,5
DDS		**2 à 36**	0,5 à 3
DLT	**X**	**40 à 80**	3 à 8
S-DLT	**X**	**110 à 300**	11 à 36
LTO	**X**	**100 à 400**	15 à 80
AIT	**X**	**35 à 100**	12
S-AIT	**X**	**500**	30
Bandes ½ pouce	**X**	**20 à 200**	10 à 30
Cartouche 3592	X	300	40

Les nouvelles technologies « disque dur »

Par rapport à ce que l'on pourrait qualifier de « *phénomène disque dur* » résultant de l'effet conjugué des différents éléments suivants : moins cher, toujours plus de capacité, accès rapide, nouvelle fonction WORM logique ; différents constructeurs se sont orientés vers ce type de support

afin de proposer des solutions innovantes pouvant répondre aux besoins d'archivage. On voit aujourd'hui apparaître sur le marché de nouvelles technologies combinant un ensemble d'éléments permettant d'assurer une conservation fiable et pérenne de l'information sur du disque magnétique.

IBM

Ce constructeur bien connu, disposant toujours de jukeboxes de disques optiques à son catalogue pour l'environnement iServer (AS/400) propose également depuis quelques années une solution d'archivage WORM à base de disques magnétiques, le Totalstorage DR550 (pour Data Retention). Il s'agit d'un système à haute disponibilité, basé sur un cluster à deux serveurs sous AIX, équipé de commutateurs Fibre Channel redondants et de tiroirs de disques S-ATA organisés en RAID 5. Ce système repose sur le module SSAM (System Storage Archive Manager), une extension du logiciel TSM (Tivoli Storage Manager), connu pour la gestion du stockage. Outre la garantie de protection WORM des données sur disque et leur cryptage, le DR550 offre des fonctions sophistiquées et auditables de conservation des informations répondant aux exigences multiples et évolutives des législations et des outils de gestion de contenu. Pour les conservations de longue durée, et dans le but d'assurer un véritable ILM, le DR550 prend à son compte les évolutions technologiques et assurera au moment opportun la migration des données vers une unité de conservation WORM plus récente. Sa capacité brute peut atteindre jusqu'à 112To.

Network Appliance

De son côté NetApp défend une approche orientée **serveur d'archivage** sécurisé. Par rapport à son offre de stockage de base NetApp a développé le module SnapLock dans ses versions Compliance et Enterprise (un peu moins restrictif). Ces produits logiciels permettent de doter les systèmes NetApp de stockage sur disque de fonctions de permanence sécurisées des données équivalentes à du WORM logique.

Hitachi

En tant que fournisseur de baies de stockage Hitachi a développé un **gestionnaire d'archivage** avec son logiciel Data Retention Utility. Ce logiciel utilitaire de rétention des données offre ainsi la fonction WORM sur les systèmes de stockage sur disque Hitachi dans les environnements de systèmes ouverts ou de type mainframe

EMC

Également fournisseur de baies de stockage, EMC suit le même raisonnement concernant la notion de gestionnaire d'archivage et a ainsi conçu des baies d'archivage dédiées, proposées au travers des systèmes Centera.

La solution Centera est basée sur une technologie de pointe, le stockage CAS (Content Access System). Ainsi, à la place de stocker, d'extraire et de gérer les informations au travers d'un système traditionnel de fichiers ou de volumes logiques, on accède à l'information par une empreinte numérique unique créée pour chaque nouvel objet entrant. Toute modification du contenu déclenche automatiquement la création d'une nouvelle adresse de contenu. Les principaux avantages sont représentés par un accès rapide aux ressources, une gestion et une administration simplifiée même pour de gros volumes et une garantie d'intégrité du contenu à long terme. Vu de l'extérieur le système peut être assimilé au fonctionnement d'une consigne. Le principe consiste, en effet, à y déposer un objet en échange duquel on vous remet un ticket (adresse de contenu). Afin de pouvoir récupérer cet objet il vous faudra absolument disposer de ce ticket. La façon dont est conservé l'objet est garantie par le système.

Hewlett Packard (HP)

Tout comme Centera, RISS (Reference Information Storage System) est avant tout une solution intégrée d'archivage, indépendante des applications avec une méthode d'accès aux enregistrements normalisée. Cette solution utilise une nouvelle approche du stockage, le stockage dit en grille, constitué de plusieurs cellules (smartCell) interconnectées via un réseau Ethernet. Chaque cellule participe à la solution et une demande d'archivage est ainsi répartie sur l'ensemble des cellules. Cette technologie permet la réalisation de solutions performantes indépendantes du nombre d'enregistrements gérés.

Une cellule possède un processeur, un espace de stockage pour l'indexation des « contenus » et les « méta données » et un espace de stockage pour les données.

Cette solution est une première intégration du « stockage en grille » que Hewlett-Packard appliquera dans les prochains développements de systèmes de stockage. Elle permet la réalisation facile de systèmes de stockage complexes à partir d'éléments standard.

Les supports optiques

Les formats amovibles optiques

Les lecteurs de médias de stockage amovibles optiques utilisent une source de lumière laser pour lire et/ou écrire des données sur le disque. Les CD (Compact Disc) et les DVD (Digital Versatile Disc) sont les deux principaux formats optiques. Les CD et les DVD ont des compositions similaires consistant en une couche protectrice, une couche réfléchissante (aluminium, argent, ou or), une couche d'enregistrement des données moulée en polycarbonate, et une couche inférieure épaisse en polycarbonate pour assurer la rigidité du disque (le substrat).

Les formats de CD comprennent:

- les CD-ROM, en lecture seule ;
- les CD-R, enregistrables ;
- les CD-RW, réinscriptibles.

De même les formats de DVD comprennent:

- les DVD-ROM, en lecture seule ;
- les DVD-R enregistrables ;
- les DVD-RAM, DVD-RW et DVD+RW, réinscriptibles.

Les différences entres ces formats de DVD réinscriptibles sont assez importantes, comme nous allons le voir par la suite.

CD-ROM (Compact Disc Read Only Memory)

Le Compact Disc a été inventé par Sony © et Philips © en 1981 afin de constituer un support audio de haute qualité. En 1984, les spécifications du Compact Disc ont été étendues (avec l'édition du *Yellow Book*) afin de lui permettre de stocker des données numériques. Les lecteurs de CD-ROM ainsi que les disques ont rapidement évolué vers une forme de stockage digital bon marché grâce à l'industrie déjà bien établie du CD audio.

Les bits sont stockés d'une façon permanente sur un CD sous la forme de creux moulés physiquement dans la surface d'une couche en plastique recouverte d'aluminium réfléchissant (ou d'or, ou d'argent). Les CD sont extrêmement pérennes, sous réserve de bonnes conditions de conservation, car aucun élément du lecteur optique ne touche la surface du disque. Comme les données sont lues à travers le disque, la plupart des rayures et des poussières sur la surface du disque sont hors du point focal du laser, et donc n'interfèrent pas avec le processus de lecture.
Avec une capacité de stockage de 650 Mo, un seul CD-ROM peut stocker l'équivalent de 450 disquettes. Et aujourd'hui, des CD-ROM de 700 Mo sont sur le marché. Le taux de transfert est approximativement de 5 Mo/s.

Les lecteurs de CD-ROM se distinguent par différentes vitesses de rotation mesurées relativement à la vitesse d'un lecteur de CD audio. Un CD-ROM 1X (simple vitesse) accède aux données au taux de 150 Ko/s environ, et ainsi de suite. Par exemple, un lecteur de CD-ROM 32X accède aux données 32 fois plus vite, soit en principe 4 800 Ko/s. Aujourd'hui, les lecteurs de CD-ROM les plus rapides atteignent les 56X, mais des vitesses plus élevées ne sont plus envisageables en raison de problèmes de vibrations et de bruits qui commencent à devenir préoccupants à cette vitesse.

CD-R (Compact Disk Recordable) :

Les graveurs de CD-R, qui sont apparus au début des années 90, contribuèrent pour une large part à faire des systèmes optiques de vraies solutions de stockage amovibles. Les graveurs de CD-R sont une évolution de la technologie de stockage WORM qui fit son apparition à la fin des années 80. Les CD-R utilisent une couche photosensible qui peut être brûlée avec un laser pour simuler les creux moulés d'un CD-ROM classique. La couche photosensible est relativement transparente jusqu'à ce qu'elle soit brûlée avec le laser pour la rendre plus sombre et moins réfléchissante.

Comme les CD-ROM, les CD-R ont une capacité de 650 Mo ou 700 Mo. La capacité réelle d'un CD-R de 650 Mo est d'environ 550 Mo quand il est formaté pour l'écriture par paquets. Les CD-R sont les médias de stockage amovibles les moins chers sachant qu'il est prudent de pondérer cette information en regard des volumes à conserver. Leur principal défaut est de ne pouvoir être écrits qu'une seule fois.

CD-RW (Compact Disk ReWritable)

Il a été inventé grâce à la collaboration de dix sociétés dont IBM, Philips, Sony, et Hewlett-Packard en 1995. Les graveurs de CD-RW, introduits en 1997, font appel à une technologie de changement de phase pour enregistrer les données sur le disque. Les CD-RW ont une couche photosensible plus complexe que celle des CD-R, constituée d'un alliage qui peut changer d'état en utilisant deux puissances de laser différentes. L'état cristallin de ce matériau reflète davantage de lumière que sa forme non-cristalline, simulant ainsi les surfaces non-creuses d'un CD-ROM classique. Ce processus d'écriture peut être répété environ 1 000 fois par CD-RW.

Les CD-ROM et les CD-R reflètent plus de lumière que les CD-RW. Par conséquent, les CD-RW ne peuvent être lus que par des lecteurs qui supportent le nouveau standard MultiRead.

DVD-ROM (Digital Versatile Disk Read Only Memory) VIDEO

Le standard DVD-ROM, introduit en 1995, est le fruit du travail d'un consortium composé de dix entreprises fondatrices : Hitachi, Matsushita Electronic, Mitsubishi Electric, Toshiba, Time Warner, Pioneer, Thomson Multimedia, Victor Company of Japan, Sony, et Philips.
Comme les lecteurs et les graveurs de CD, les lecteurs de DVD lisent les données à travers une couche protectrice, réduisant de la sorte les interférences dues aux poussières et aux rayures à la surface. Cependant, la technologie DVD-ROM offre au moins sept fois les capacités de stockage d'un CD-ROM classique, et arrive à ce résultat en améliorant la technologie utilisée par les lecteurs et graveurs de CD. La distance entre les pistes d'enregistrement est inférieure à la moitié de celle utilisée pour les CD et la taille des creux est également inférieure à la moitié de celle des CD, voir schéma ci-dessous. Cette seule différence donne aux DVD-ROM au moins sept fois la capacité de stockage des CD. Les DVD peuvent aussi avoir deux couches de données et les stocker sur les deux faces, ce qui multiplie la capacité du DVD de base par quatre. Ainsi les DVD-ROM offrent une capacité de stockage de 4,7 Go pour les disques simple face, simple couche. Les DVD simple face, double couche stockent 8,5 Go. Les DVD double face, simple couche stockent 9,4 Go, et les DVD double face, double couche peuvent stocker 17 Go.

Les lecteurs de DVD font tourner le disque plus lentement que les lecteurs de CD, mais le taux de transfert est considérablement plus élevé, car la densité de données est beaucoup plus grande que sur les CD. Ainsi, un lecteur de DVD 1X (simple vitesse) a un taux de transfert de 1 250 Ko/s, à comparer au taux de transfert de 150 Ko/s d'un lecteur de CD-ROM 1X. Les lecteurs de DVD actuels peuvent lire les DVD-ROM à des vitesses de 16X au maximum, et les CD à des vitesses de 48X.

DVD-R+R (Digital Versatile Disk Recordable)

Les graveurs de DVD enregistrables mais non réinscriptibles, ou DVD-R, ont fait leur apparition en 1997. Les DVD-R emploient une couche photosensible similaire à celle des CD-R. Avec une capacité de seulement 3,95 Go, les premiers DVD-R offraient un peu moins de capacité de stockage que les DVD-ROM. Maintenant, des DVD-R sont également disponibles avec une capacité de 4,7 Go. Le taux de transfert moyen des graveurs de DVD-R est de 1,4 Mo/s.

DVD-RW (Digital Versatile Disk ReWritable)

Le format DVD-RW retenu par le Forum DVD est similaire en de nombreux points au format DVD-R, mais permet la réécriture grâce à l'usage d'une couche enregistrable à changement de phase comparable à celle des CD-RW. Pioneer a introduit ce format en décembre 1999.
Les médias DVD-RW peuvent être réécrits environ 1 000 fois, comme les CD-RW.

DVD+RW

Cette technologie a été introduite en 1997, adossée à un groupe de grands noms de l'industrie regroupés au sein de l'Alliance DVD+RW composée de Sony, Hewlett-Packard, Dell, Thomson Multimedia, Mitsubishi Chemical (Verbatim), Yamaha, Ricoh et Philips. Le temps de gravage est deux fois plus rapide que pour le format –RW. Le nombre de réécriture est par ailleurs identique à ce dernier format soit environ 1 000 fois.

DVD-RAM (Digital Versatile Disk Random Access Memory)

Les DVD-RAM ont été introduits en 1998 par un consortium composé de Matsushita Electric, d'Hitachi et de Toshiba. Les graveurs de DVD-RAM utilisent la technologie magnéto optique à changement de phase. La capacité est de 2,6 Go par face, mais une version de 4,7 Go, obtenue en réduisant la taille des creux ainsi que la distance entre les pistes d'enregistrement, est également disponible sur le marché. L'on trouve également des versions de 5,2 Go et 9,4 Go grâce à l'utilisation des deux faces. Les fabricants travaillent à porter sa capacité à 8,5 Go par face soit 17 Go au maximum.

Les DVD-RAM Type 1 sont logés dans des cartouches qui protègent le disque mais nécessitent un lecteur spécifique.

Chaque DVD-RAM est donné pour pouvoir assurer plus de 100 000 réécritures. Enfin les DVD-RAM font appel à une structure de stockage basée sur des secteurs, au lieu du sillon en spirale utilisé par les CD. Ce stockage en secteurs est similaire à la structure de stockage utilisée par les disques durs, et il en découle un taux de transfert plus rapide, d'où son nom (Random Access Memory).

Récapitulatif des formats amovibles optiques

Format	**Capacité Go**	Débit Mo/s
CD-ROM	**650 Mo**	7 (48X)
CD-R	**650-700 Mo**	6,9
CD-RW	**650 Mo**	1.000 réécritures
DVD-ROM / VIDEO		
Simple face	**4,7**	21 (16X)
Simple face double couche	**8,5**	
Double face simple couche	**9,4**	
Double face double couche	**17**	
DVD-R+R	**4,7**	1,4
DVD-RW+RW	**4,7**	1.000 réécritures
DVD-RAM	2,6 à 17	100.000 réécritures

Ni optique, ni magnétique mais les deux à la fois, le magnéto-optique ou MO (magnéto-optical), déjà mentionné précédemment pour les DVD-RAM, va nous permettre de terminer notre descriptif des supports optiques. Cette technologie offre en fait des disques avec des densités très élevées et présente un potentiel encore plus important de progrès à ce niveau, d'où son emploi en matière d'archivage.

La technologie magnéto-optique (MO)

Cette technologie combine les points forts des technologies magnétiques et optiques en utilisant un faisceau laser pour lire les données et la combinaison du laser et d'un champ magnétique pour écrire les données. La face du dessus du disque est exposée à un champ magnétique pour écrire les données, et la source de lumière laser atteint la couche de données à travers le substrat du dessous pour lire les données.

A la différence des solutions purement optiques, les systèmes magnéto-optiques permettent de réécrire à l'infini sur le support. De plus, ce dernier est bien protégé dans sa cartouche plastique de telle sorte que sa surface n'est pratiquement jamais endommagée si on l'utilise correctement.

Les disques magnéto-optiques les plus récents ont des densités surfaciques de l'ordre de 20 à 40 Gbits/in^2 (Giga bit par puce carré), avec des temps d'accès comparables à ceux des disques durs actuels. On peut espérer accroître considérablement cette capacité jusqu'à des centaines de Gbits/in^2, en remplaçant les supports magnétiques actuels composés d'alliages à base de métaux de terre rare et de transition, par des films minces qui associent des métaux de la première et troisième série de transition.

Les disques MO au format 3,5" sont disponibles avec des capacités de 128 Mo, 230 Mo, 540 Mo, 640 Mo, 1,3 Go, et depuis peu 2,3 Go. Les disques MO au format de 5,25" existent en versions 640 Mo, 1,3 Go, 2,6 Go, et 5,2 Go. Avec des temps d'accès d'environ 19 ms, les technologies MO sont nettement plus rapides, sur ce point, que les technologies CD et DVD avec leurs temps d'environ 100 ms.

L'UDO (Ultra Density Optical) représente la nouvelle génération de technologie professionnelle de stockage optique de 5,25". Il s'agit d'une technologie convergente qui offre la performance de la technologie magnéto-optique de 5,25", la longévité des disques non réinscriptibles de 12" et la rentabilité du DVD. Elle utilise un laser bleu violet et la technologie d'enregistrement de changement de phase des produits de consommation de DVD pour fournir un progrès prodigieux dans les densités de stockage de données. On atteint, en effet, des capacités de 30, 60 voire 120 Go avec des taux de transfert de 8, 12 et 18 Mo/s.

Récapitulatif des formats magnéto optiques

Format	**Capacité Go**	Débit Mo/s
MO 3,5"	**de 128 à 640 Mo**	5

MO 5,25"	**de 640 Mo à 2,3 Go**	5
MO UDO 5,25" 30	**30**	8
MO UDO 5,25" 60 (2005)	**60**	12
MO UDO 5,25" 120 (2007)	120	18

Avantages et inconvénients des technologies présentées selon différents critères

Par rapport à cette grande diversité de supports tant magnétiques qu'optiques, il est clair que les critères de choix devront se porter essentiellement sur la **capacité** des supports, leur **fiabilité** par rapport aux différents mécanismes d'enregistrement et bien sûr leur **coût**. Le critère du taux de transfert (assimilable à la vitesse d'écriture sur le média) est quelque peu marginal dans la mesure où en règle générale les procédures d'archivage sont effectuées à des périodes non critiques. Comme autres critères, il ne faudra pas oublier l'**évolutivité** (problème des compatibilités ascendantes), les possibilités de **migrations**, la **sécurité** offerte.

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?
.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution