GA Z42-019

2010-06

www.afnor.org

Contacter :
AFNOR – Norm'Info
11, rue Francis de Pressensé
93571 La Plaine Saint-Denis Cedex
Tél : 01 41 62 76 44
Fax : 01 49 17 92 02
E-mail : norminfo@afnor.org

http://www.afnor.org

Guide d'application

Guide d'application de la NF Z 42-013

(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)

Guidelines for NF Z 42-013 (Electronic archival storage — Specifications relative to the design and operation of information processing systems in view of ensuring the storage and integrity of the recordings stored in these systems)

Liens avec des documents existants

À la date de publication du présent document, il n'existe pas de travaux de normalisation internationaux ou européens traitant du même sujet.

Avant-propos

Membres du groupe de travail «Applications pour l'archivage et la gestion du cycle de vie du document»

Chef de projet : M WEISZ

Secrétariat : M CHEVAUCHÉ - AFNOR

MME	FRANCOISE BANAT-BERGER	DIRECTION DES ARCHIVES DE FRANCE
M	ALAIN BOBANT	CHAMBRE NATIONALE DES HUISSIERS DE JUSTICE
M	ALAIN BORGHESI	CECURITY.COM
M	MARC CHEDRU	FEDERATION NATIONALE TIERS CONFIANCE
MME	MARIE-CHANTAL DEBIZE	BNP PARIBAS
M	DIDIER DESMONS	SOCOTEC
M	BRUNO DILLET	CDC ARKHINEO
M	CHRISTIAN DUBOURG	EVER TEAM
M	JEAN-MARC FONTAINE	LABORATOIRE ACOUSTIQUE MUSICALE
M	PIERRE FORT	STS GROUP
M	GERARD GODART	SAFRAN
M	PHILIPPE HOUDEBINE	BNP PARIBAS
M	PHILIPPE L'HEUREUX BOURON	BNP PARIBAS
M	OLIVIER LUBLINER	FRANCE TELECOM
MME	TIPHAINE MARIE	FRANCE TELECOM
M	PHILIPPE MARTIN	BUREAU VAN DIJK
M	JACQUES PERDEREAU	LABORATOIRE NATIONAL D'ESSAIS ET DE METROLOGIE
M	LAURENT PREVEL	LP CONSULTANTS
M	GÉRARD WEISZ	SIRIUS SYSTEMS

Table des matières

Page

1 Introduction

Pourquoi cette norme, les éléments qui sont à l'origine de sa création et de ses révisions successives

- S'assurer que le document archivé garde la même valeur que le document d'origine et garantir son intégrité et sa pérennité. Répondre à l'évolution et à la modernisation de l'État (utilisation de l'internet par les administrations et dématérialisation des processus) ;
- prendre en compte les travaux et les études effectués sur le sujet et en particulier par le Forum des Droits sur l'Internet sur l'Archivage Électronique (recommandation du 1er décembre 2005).

Les objectifs de la norme et leur portée

- Dans le prolongement des dispositions légales et/ou réglementaires du droit français fournir un cadre technique permettant de mettre en place des systèmes d'archivage électronique (SAE) à vocation probatoire destinés à conserver des documents numériques d'origine ou obtenus par numérisation ;
- proposer un texte décrivant les aspects techniques et organisationnels nécessaires et suffisants pour garantir l'intégrité, la pérennité, la sécurité et la traçabilité des documents conservés dans un SAE ;
- fournir un référentiel d'audit permettant de déterminer la conformité d'un SAE au regard des spécifications de la norme ;
- fournir aux éditeurs de progiciels un ensemble de points techniques à mettre en œuvre ;
- fournir aux archivistes et aux tiers-archiveurs (voir § 2.2.10 de ce guide) un ensemble d'indications leur permettant de mettre en conformité leurs offres de services.

Les objectifs du guide d'application NF Z 42-013

- Positionner la norme dans le projet d'archivage et fournir les éléments de compréhension des principaux points clés ;
- proposer une démarche projet ;
- répondre aux différentes interrogations au travers d'une FAQ.

Un système d'archivage électronique doit, pour le moins, garantir aux documents conservés leur fidélité, intégrité, pérennité et traçabilité pour que ceux-ci puissent conserver leur valeur d'origine.

L'intégrité suppose que le document ne pourra subir aucune destruction ni modification volontaire ou malveillante durant sa période de conservation.

La fidélité d'un document électronique est interprétée comme la faculté pour celui-ci de reconstituer toute l'information auquel le document d'origine était destiné. Il peut donc être fait une analyse du contenu informationnel qui doit être restitué indépendamment de la forme qu'il doit avoir (voir norme NF Z 42-013 § 3.14).

La pérennité réside dans la garantie que le système peut restituer de façon intelligible un document électronique tout au long de sa période de conservation. Cette fonction est largement basée sur des aspects techniques qui ont trait notamment à l'exploitabilité des supports de stockage dans le temps (processus de migration des supports — voir norme NF Z 42-013 § 5.4.6), aux systèmes de gestion de fichiers utilisés avec ces supports et aux outils informatiques qui interprètent les formats d'encodage et de présentation.

La traçabilité (voir norme NF Z 42-013 § 3.34) est assurée par les dispositifs décrits tels que l'historisation des évènements. Celle-ci a pour but d'apporter les moyens de preuves concernant les opérations ayant trait au cycle de vie des documents ainsi qu'aux évènements relatifs au fonctionnement du système d'archivage.

Pour atteindre ces objectifs lors de la mise en place d'un système d'archivage électronique, il convient d'utiliser un éventail de dispositifs techniques dont les caractéristiques et l'organisation sont spécifiées par la norme AFNOR homologuée NF Z 42-013 [1)].

Le schéma ci-dessous donne une illustration de la correspondance entre les principaux objectifs à garantir pour les documents à conserver et les dispositifs techniques susceptibles d'être mis en œuvre.

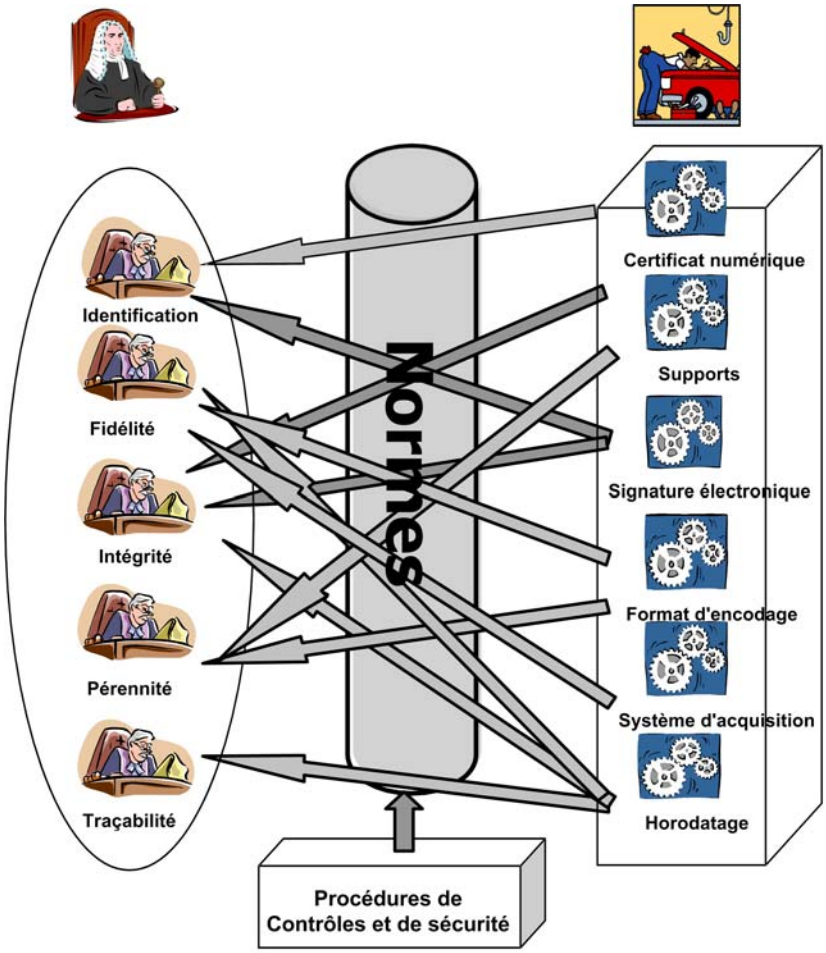


Figure 1

1) *Une norme technique se définit comme une «spécification technique approuvée par un organisme reconnu à activité normative pour application répétée ou continue, dont l'observation n'est pas obligatoire» (Directive 83/189/CEE mod. du Conseil du 28 mars 1983). En l'occurrence, certaines normes telles que la norme NF Z 42-013 se voient reconnaître le caractère d'une codification écrite regroupant «les règles de l'art» ou des «usages loyaux et constants». La Cour de Cassation a d'ailleurs confirmé cette conception en considérant que l'existence d'une norme permet de représenter l'état de l'art dans le domaine auquel elle se rapporte (Cass. civ. 3e ch., 4 février 1976, Bull. civ. III, n°49.).*

Les niveaux d'exigence

Les organisations n'ayant pas les mêmes besoins en matière d'archivage et les risques qu'elles sont susceptibles d'assumer étant différents, la norme NF Z 42-013 a introduit le principe de deux niveaux d'exigences (voir Norme NF Z 42-013 § 4.2).

Les exigences minimales décrites dans le Tableau n°1 constituent le socle de base auquel les systèmes doivent répondre pour être conforme à la norme.

Au-delà de ces exigences minimales, les organisations sont amenées à considérer certaines des exigences complémentaires listées également dans le Tableau n°1 (voir norme NF Z 42-013 § 4.2).

NOTE Concernant les aspects sécurité, on pourra utilement se référer aux principes de sécurité du SI détaillés dans la recommandation publiée par la CNIL le 12 octobre 2009.

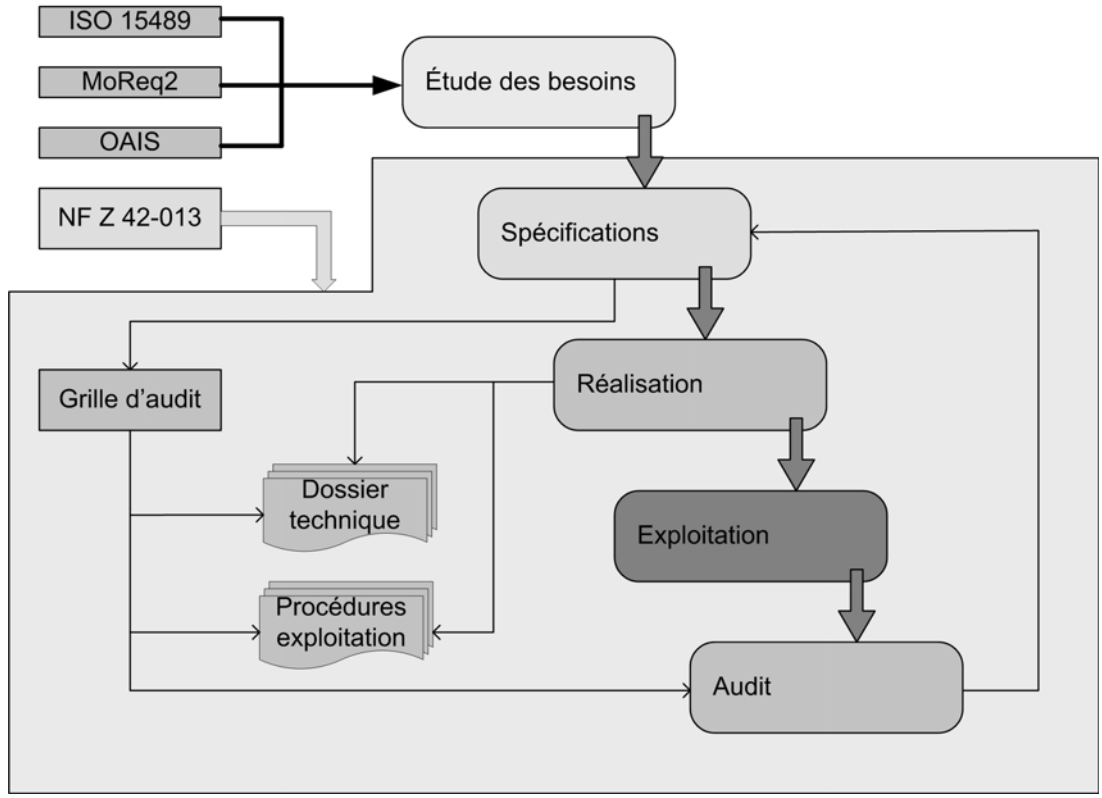
2 Comment appliquer la norme NF Z 42-013

La version actuelle a été publiée officiellement le 3 mars 2009 après une première édition datant de juillet 1999 et une révision publiée en décembre 2001. Dans la version 2009, la norme apporte des réponses importantes concernant notamment l'élargissement du périmètre des objets numériques pouvant être pris en considération et la nature des supports susceptibles d'être mis en œuvre par les systèmes d'archivage électronique.

Désormais les séquences sonores et vidéo, les dessins ou les plans 2D ou 3D ainsi que les images médicales entrent également dans le champ d'application de la norme révisée. Ces objets pouvant être créés directement sous forme numérique ou provenir de processus de numérisation à partir de supports analogiques (film, bandes, etc.).

L'autre apport décisif vise à étendre la version précédente en prenant en compte toutes les natures de supports informatiques susceptibles d'être utilisés pour archiver les documents : supports fixes ou amovibles, de type WORM physique ou logique, ou simplement réinscriptibles.

2.1 Positionnement de la norme dans le projet du système



(Référence des normes valides en novembre 2009)

Figure 2

2.2 Fondamentaux et points clés de la norme

2.2.1 Politique d'archivage

L'information est l'un des actifs essentiels que les organisations ont à leur disposition.

L'information, comme n'importe quel autre élément d'actif, doit être classée, structurée, validée, sécurisée et contrôlée, en conformité avec la réglementation applicable et les règles définies par l'organisation.

La conception et l'exploitation d'un SAE s'appuie en amont sur l'existence d'une politique d'archivage de l'organisation.

La politique d'archivage (PA) décrit les règles de fonctionnement concernant la gestion des documents et leur archivage au sein du SAE.

Une politique d'archivage doit prendre en compte en particulier la définition des objectifs poursuivis, l'environnement légal, réglementaire et normatif, les exigences opérationnelles, ainsi que le fonctionnement et les processus métiers de l'organisation.

La politique d'archivage inclut un tableau de gestion des documents, encore appelé charte d'archivage, qui établit notamment pour chaque catégorie d'archives les raisons de conservation, les niveaux de sécurité et de confidentialité, et qui détermine les durées de conservation et leur point de départ.

La politique d'archivage doit être approuvée par la direction générale de l'organisation et doit être soumise à des revues régulières pour mise à jour.

Concernant les méthodologies d'élaboration d'une politique d'archivage, on pourra se reporter aux normes et documents de référence du domaine «Records Management» ou Management de l'information et des documents. Pour le secteur public, une politique d'archivage type a été élaborée : Archivage électronique sécurisé. La politique et les pratiques d'archivage». Elle est disponible sur le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) à l'adresse suivante : http://www.ssi.gouv.fr/site_article48.html.

Les préconisations et choix effectués dans la politique d'archivage, notamment en termes de valeur de l'information et d'exigences de conservation, peuvent permettre aux entreprises et organismes de déterminer :

- Quels types de documents nécessitent la conformité aux exigences du présent document (exigences de base ou exigences complémentaires) ?
- Quels types de documents ne nécessitent pas la conformité à ces exigences ?
- Quels types d'originaux peuvent être détruits après numérisation ?

De manière générale, la politique d'archivage définit et décrit les caractéristiques et niveaux d'archivage pour chaque type de document.

La documentation de la politique d'archivage contribue à établir que l'information et son archivage par le SAE répond aux critères d'intégrité, de fidélité, de pérennité et de traçabilité. Cette documentation actualisée régulièrement peut également être utilisée pour démontrer que le SAE fait partie intégrante des procédures mises en place dans le cadre des activités de l'organisation.

En substance, une PA peut contenir les sections suivantes :

- Spécifier quelles sont les informations concernées par la PA (périmètre informationnel de la PA) ;
- Établir quelles sont la ou les solutions retenues pour les aspects stockage : types de supports choisis, solutions de sauvegarde mises en œuvre, solutions de duplication/réplication sur des sites distants, surveillance des supports et politique de migration de ces supports ;
- Établir la politique concernant les formats des documents numériques versés dans le SAE et les moyens mis en œuvre pour identifier, contrôler ces formats ;
- Établir les politiques et processus de conversion — migration des archives numériques (conversion : changement de format des archives, migration : changement de supports ou de systèmes) ;
- Établir la politique concernant les normes applicables en matière de gestion des archives ;
- Définir les politiques de conservation des archives, des métadonnées et des journaux, garantissant notamment leur sécurité et leur intégrité ;
- Définir les politiques de destruction des archives, des métadonnées et des journaux ;
- Définir l'ensemble des éléments de traçabilité visant à sécuriser l'archivage ;
- Définir les responsabilités pour les fonctions de gestion des archives, ainsi que pour les fonctions en charge de l'application de la PA.

Dans le but de définir la PA, il est fortement recommandé que les documents soient regroupés par catégories cohérentes.

À titre d'exemple, il pourra être possible de définir ces catégories en référence à leur application (prévisions financières, facturation, listes de clients) ou en association avec des procédures métiers (traitement des réclamations, renouvellement de contrats, etc.) ou en référence à des groupes d'informations génériques (documents comptables, documents clients, documents de fabrication, etc.).

2.2.2 **Profils d'archivage** (définition et utilisation)

Afin de faciliter la mise en œuvre de la politique d'archivage, la norme NF Z 42-013 a prévu de pouvoir mettre en place des profils d'archivage (voir paragraphe 5.2). La mise en place des profils d'archivage mais peut être considérée, dans certains projets de système d'archivage électronique, comme structurante. Un «profil» peut ne pas être simplement lié à la sécurité ou aux droits d'accès. Les profils doivent permettre notamment de factoriser, lorsqu'il y a lieu, des règles communes applicables à des catégories de documents qui partagent les mêmes critères de valeur de l'information, de description, de sécurité, de confidentialité, de point de départ et durée de conservation.

Les profils d'archivage facilitent également la mise en œuvre de processus communs aux documents pour leur dépôt, y compris par lots, pour la communication, et pour la gestion de la destruction et de la restitution.

Quelques exemples (non exhaustifs) peuvent illustrer l'intérêt de mettre en œuvre des profils d'archivage pour factoriser les règles applicables lors d'un dépôt :

a) Lors d'un dépôt d'objets qui mentionne un profil d'archivage, le profil peut être utilisé afin de vérifier que le format des fichiers acceptés est compatible avec le ou les formats déclarés par rapport au profil et par rapport à la table des formats que le SAE accepte de prendre en charge (section 10.5).

b) Lors d'un dépôt d'objets, les métadonnées qui décrivent les objets versés (section 5.2) peuvent être vérifiées par rapport à un schéma XML associé au profil (section 10.1.6) ou peuvent être extraites des objets versés (section 10.1.7). Par exemple, dans le secteur public, les versements ou éliminations d'archives sont conformes à un format d'échange (le standard d'échange de données pour l'archivage ou SEDA) et à un modèle de description appelé profil, lui-même dérivé du SEDA, ce qui permet d'automatiser les contrôles lors de la prise en charge dans le SAE.

2.2.3 Positionnement du SAE dans le système d'information

2.2.3.1 *Analyse de la situation*

Le positionnement d'un SAE dans le système d'information est un élément important, notamment parce que fréquemment les organisations et les entreprises, confrontées à l'accroissement important des documents numériques reçus et émis ont mis en place des solutions visant à en permettre la gestion.

L'état actuel de ces systèmes d'informations présente une architecture orientée en général sur :

— un axe fonctionnel recouvrant les fonctions de l'organisation ou de l'entreprise : ressources humaines (RH), comptabilité, achats, ventes, production, etc.

— un axe services couvrant les moyens standards de communication, édition : messagerie électronique, bureautique et éditique.

En matière de gestion des documents numériques (ou des objets numériques : données et documents) de nombreux composants peuvent être présents :

— solution de GED, interfacée ou non avec les applications informatiques ;

— applications métiers ;

— serveur de messagerie ;

— répertoires partagés ;

— «pseudo-solutions» d'archivage dans le cadre d'ERP, qui sont en réalité des solutions de déplacement d'informations ;

— etc.

La notion de cycle de vie de l'information et d'archivage est rarement présente dans ces architectures alors qu'un des enjeux majeurs des organisations est la conservation couvrant notamment le respect de la réglementation (fiscale : contrôle des comptabilités informatisées, sociale, commerciale, etc.), les besoins opérationnels et les obligations patrimoniales.

Schématiquement deux orientations sont envisageables :

— mise en œuvre d'un SAE (ou de plusieurs SAE) répondant aux principes structurels et fonctionnels fondamentaux :

1) autonomie de l'archive par rapport au système versant ;
2) formalisation des opérations de versement (enregistrement) ;
3) gestion des archives (durée de conservation, migrations, etc.), formalisation des opérations de communication et de restitution/destruction.

— aménagement et adaptation des SI (applications métier, GED, gestion de contenus) actuels pour leur conférer les caractéristiques de base en matière de gestion du cycle de vie et d'archivage (détermination des durées de conservation à partir desquelles on pourra mettre en place des fonctionnalités de destructions par lots qui seront tracées voire de transferts pour archivage dans une autre organisation en cas de durées de conservation élevées). Cette orientation peut être retenue à titre de transition avant la mise en place d'un SAE.

L'objectif de la mise en place d'un SAE est de définir, de spécifier et de mettre en œuvre les adaptations des SI (spécifiques ou mutualisées) qui répondront aux étapes successives de l'archivage :

— gestion du cycle de vie de l'information ;

— préparation des versements : structuration, formatage des objets et attribution des métadonnées (explicites ou incluses dans les objets), sécurisation ;

— enregistrement : choix des supports ;

— gestion des destructions et des restitutions ;

— communication : gestion des sécurités et des droits d'accès ;

— gestion des archives (migrations, réplications, traçabilité, etc.).

Trois étapes sont nécessaires pour déterminer et mettre en œuvre les dispositions d'archivage conformes dans un environnement existant :

a) Étude de l'existant — État des lieux :
   - pour chaque composant du SI : relevé des dispositions actuelles de gestion/sauvegarde/archivage des «objets numériques» ;
   - évaluation des dispositions prises au regard de ce qui devrait être fait ;
   - diagnostic global.

b) Plan d'actions : mise en conformité avec la norme :
   - scénarios d'évolution ou d'adaptation de l'architecture ;
   - définition des adaptations permettant la formalisation des étapes amont de l'archivage : gestion du cycle de vie de l'information, préparation des versements (structuration des objets numériques, formats, métadonnées, sécurisation), versement (écriture sur les supports retenus, mise à jour des référentiels) ;
   - gestion des restitutions et des destructions ;
   - définition des adaptations pour la mise en œuvre des phases aval : communication (gestion des droits d'accès, etc.) ;
   - définition des adaptations nécessaires à la gestion des archives ;
   - évaluation du plan d'actions ;
   - planification.

c) Réalisation des actions.

2.2.3.2 *Intégration du SAE dans une démarche d'urbanisation*

La démarche détaillée ci-dessus peut conduire, après l'étude de l'existant, à un constat remettant en cause le système d'information en raison de son inadaptation plus ou moins profonde à une application transversale telle qu'un SAE. L'urbanisation vise à assurer l'interopérabilité du SAE avec l'ensemble des autres composants.

Il est probable que l'état des lieux montrera un empilement d'applications non interopérables ayant, par exemple, chacune un annuaire particulier non partagé, une authentification locale, un workflow local, un IHM dédié non intégré dans un portail ou un archivage spécifique dans un «coffre fort électronique». Ces applications pourront s'appuyer sur des modèles de données différents, ciblés pour le domaine de l'application, avec de fortes chances d'incompatibilité entre ces modèles.

Dans ce type relativement fréquent de SI monolithique, toutes les applications créent leurs documents et les gèrent avec une multiplication de formats et de procédures.

La mise en place d'un SAE va alors poser plusieurs problèmes :

a) définition de multiples interfaces pour les versements en raison de la dispersion des documents ;

b) conversions des formats non conformes avec le risque de rejet par le contrôle du SAE ;

c) renseignement manuel des métadonnées (MCD différents) ;

d) définition de multiples interfaces pour les communications ; etc.

Les actions à réaliser peuvent conduire dans ce cas à l'accroissement de la complexité du SI, à des coûts de développement et de déploiement très significatifs et une maintenabilité difficile du système.

Devant cette situation, une solution non optimum et coûteuse peut être la mise en place de plusieurs SAE, mais ce constat peut aussi conduire à une réflexion plus globale de remise en cause du système d'information en procédant à son urbanisation progressive.

Principe d'urbanisation d'un système d'information

La congestion croissante et l'inadaptation de plus en plus préoccupante des systèmes d'information monolithiques renforcent l'émergence de nouvelles approches s'appuyant sur des concepts différents et des choix plus orientés vers des standards où les logiciels libres prennent une plus grande place.

L'urbanisation d'un SI repose notamment sur la définition d'un MCD commun et une architecture ouverte permettant :

a) la mutualisation des ressources partageables : annuaire, authentification, SSO, signature électronique, horodatage, workflow, portail, moteurs de conversion, de hachage, etc.

b) la mise en place de bus d'échange construit sur des standards ;

c) la mise en place de sous-systèmes transversaux indépendants permettant des regroupements fonctionnels tels que gestion documentaire, archivage papier et électronique, ces sous-systèmes échangeant uniquement selon leurs interfaces.

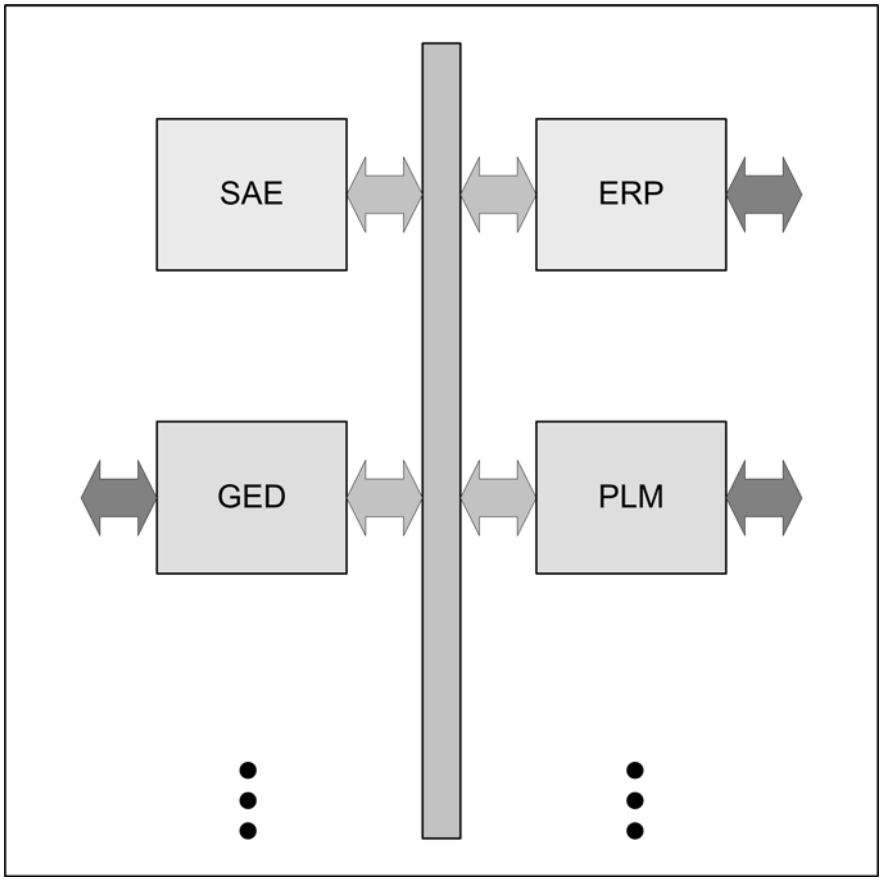


Figure 3

Dans ce type d'architecture, on peut envisager la refonte d'un sous-système que ce soit pour adopter de nouvelles technologies ou pour répondre à un besoin fonctionnel nouveau. Du moment que ses interfaces avec les autres sous-systèmes sont préservées, le périmètre de la refonte est maîtrisé. Les échanges se font par des protocoles normalisés ouverts dans lesquels les informations sont encapsulées.

Les objectifs de l'urbanisation, au-delà du déblocage des situations créées par les systèmes monolithiques, sont :

a) une économie de moyens (matériels logiciels et humains) par une optimisation des ressources ;

b) une sécurisation du fonctionnement par une disponibilité transversale d'informations à jour ;

c) une indépendance technologique grâce à l'adoption de standards ;

d) une maintenance plus aisée et une évolution simplifiée en agissant au niveau des sous-systèmes, etc.

2.2.4 Dossier technique

Le SAE est un composant du Système d'Information de l'entreprise, dédié à la gestion des archives électroniques c'est-à-dire un ensemble organisé tel un système informatique : matériels, outils réseaux, système d'exploitation, progiciels, logiciels applicatifs, structure de données, procédures, qui ont pour but la gestion des archives électroniques.

Le dossier de description technique du système (DDTS) qui accompagne la mise en place d'un SAE est un document de référence qui doit décrire minutieusement l'intégralité de la solution mise en place conformément aux recommandations de la norme. Ce dossier technique est un document vivant. Il est amené à évoluer régulièrement dans le temps. Il est donc nécessaire, comme tout document, de tracer et versionner ses évolutions et d'indicer chaque changement via un numéro de version permettant de synthétiser la date des changements, le numéro de version du nouveau document et la liste des changements survenus. Ce document est un support indispensable pour les phases d'audits d'un SAE durant lesquelles il doit être utilisé et vérifié.

Par exemple pour formaliser ces éléments de réponse, sur la base des recommandations de la norme NF Z 42-013:2009, le DDTS doit ainsi comporter obligatoirement les points suivants :

a) Un dossier d'architecture technique comportant (norme NF Z 42-013 § 5.1) :
   - l'ensemble des informations liées aux matériels utilisés par le SAE ;
   - l'ensemble des informations liées aux progiciels utilisés avec le SAE ;
   - l'ensemble des informations liées aux logiciels spécifiques éventuellement utilisés avec le SAE ;
   - l'architecture réseau dans laquelle le SAE est positionné ;
   - les éléments de sécurité du réseau autour du SAE et vers les tiers éventuels ;
   - le MCD ;
   - le principe de récupération et de synchronisation de l'heure pour tous les éléments du SAE qui produisent des traces horodatées (norme NF Z 42-013 § 5.5).

b) Un dossier des conditions d'exploitation et de maintenance du SAE (norme NF Z 42-013 § 5.1) :
   - conditions physiques ;
   - liste des opérations de maintenances et leur type (norme NF Z 42-013 § 5.4.5) ;
   - moyens techniques et physiques assurant le bon fonctionnement du SAE et la continuité d'accès aux objets archivés (norme NF Z 42-013 § 5.8) ;
   - mécanisme d'horodatage retenu (norme NF Z 42-013 § 5.5) ;
   - exploitation des journaux (norme NF Z 42-013 § 5.6).

c) Un dossier des conditions liées à la sécurité du SAE (norme NF Z 42-013 § 5.1) :
   - moyens de protection physique du matériel et des supports éventuels ;
   - description des mécanismes de détection des fraudes liées à la manipulation volontaire des fichiers en vue de leurs substitutions par d'autres objets (norme NF Z 42-013 § 8) ;
   - description de la gestion des habilitations, description de la gestion des droits.

d) Un dossier lié aux supports d'archivages :
   - description associée à la surveillance et à la migration des supports (voir norme NF Z 42-013 § 5.4.6) ;
   - description associée aux mécanismes de duplication/réplication (voir norme NF Z 42-013 § 5.6.3) ;
   - description associée au marquage des supports (norme NF Z 42-013 § 7.3).

e) Un dossier des procédures (norme NF Z 42-013 § 5.3) mises en place pour l'enregistrement, le stockage, la communication, la restitution, la destruction des documents comportant :
   - la description des procédures d'exploitation (norme NF Z 42-013 § 5.3) :
     i) Pour tous les types de documents (norme NF Z 42-013 § 5.3.3) ;
     ii) Pour les documents numérisés (norme NF Z 42-013 § 5.3.1) ;
     iii) Pour les documents nativement numériques (norme NF Z 42-013 § 5.3.2).
   - la description des processus de conversion vers les formats d'archivage et du traitement des erreurs de conversion (norme NF Z 42-013 § 10.5) ;

- la description des procédures de constitution et de contrôles des métadonnées (norme NF Z 42-013 § 10.1.7) ;
- la description des procédures de traitement des images dans le cadre du processus de capture des archives (norme NF Z 42-013 § 10.2.2) ;
- la description des procédures de traitement des fichiers sonores et audiovisuelles (norme NF Z 42-013 § 10.3.3) ;
- la description des algorithmes de compressions utilisés et du référentiel normatif associé (norme NF Z 42-013 § 10.4.1) ;
- la description des procédures de communication des objets archivés (norme NF Z 42-013 § 11.1) ;
- la description des procédures de restitution d'objets archivés (norme NF Z 42-013 § 11.2).

2.2.5 Choix des supports

Dans la typologie présentée dans la norme (voir Article 6), il convient d'ajouter les précisions suivantes sur les caractéristiques des différents supports :

a) Supports amovibles

Le support physique est extractible du lecteur-enregistreur et portable sur un autre lecteur-enregistreur compatible. Sont concernés notamment les disques optiques, les cartouches de bandes magnétiques, les mémoires à semi-conducteurs (carte mémoire flash). Les disques durs externes, certes toujours intégrés dans un lecteur-enregistreur, peuvent être rangés dans cette catégorie. Les disques magnétiques composant une baie de stockage n'entrent pas dans cette catégorie.

b) Supports fixes

Le support physique est entièrement solidaire de son lecteur-enregistreur et **ne peut en être extrait** : cas des disques durs internes et mémoires à semi-conducteurs (carte mémoire flash) qui équipent divers systèmes d'enregistrements audiovisuels et des ordinateurs portables.

c) WORM physique

L'information est écrite une fois par un processus de modification physique et irréversible du support et, à l'issue de cette opération, ne peut pas être modifiée ou effacée. Les disques CD-R, DVD+/- R, BD-R et UDO enregistrables une fois sont des WORM physiques.

d) WORM logique

Le support est réinscriptible, mais un dispositif logiciel et/ou matériel interdit la modification ou l'effacement de l'information. Les procédés de blocage de l'écriture concernent les supports magnétiques ou optiques effaçables. Il est important de noter que les supports WORM logiques, fixes ou amovibles, sont soumis aux mêmes exigences que celles applicables aux systèmes basés sur des supports réinscriptibles.

e) Supports réinscriptibles

Les informations peuvent être enregistrées, modifiées ou supprimées sans restriction. Cette catégorie comporte : les supports magnétiques (disques durs et bande), les disques optiques (CD-RW, DVD+RW, BD-RE, UDO enregistrable) ainsi que les mémoires à semi-conducteurs.

2.2.5.1 *Procédures à suivre pour le contrôle des WORM physiques*

Il s'agit de s'assurer de la qualité des medias après enregistrement et du suivi des performances dans le temps.

Les systèmes de contrôle, de test, d'analyse.

Sous réserve de disposer d'un système de test, les disques optiques se prêtent particulièrement bien aux procédures de contrôle de qualité.

Un testeur est constitué d'un lecteur doté des dispositifs permettant d'extraire un certain nombre de paramètres, au premier rang desquels les taux d'erreurs.

Différents systèmes de contrôle sont proposés, depuis le simple logiciel téléchargé qui dressera un bilan des conditions ordinaires de lecture du disque jusqu'au système d'analyse dit de référence disposant d'un driver de très haute qualité.

La fiabilité des dispositifs peut être mise en cause, aussi est-il nécessaire d'avoir périodiquement recours à un système d'analyse de référence pour valider les mesures : une fois par an et à tout changement de graveur.

Pour chaque type de disque, des limites de taux admissibles d'erreurs avant correction sont définies : BLER pour la famille CD, PISum8 pour les DVD, RSER10k pour les BD. D'autres paramètres permettent de poser un diagnostic de l'état du disque plus précis. Les contrôles ont pour but de prévenir le moment où un taux d'erreurs incorrigibles peut se manifester : les indicateurs E32 (CD), POF (DVD), UnCorr (BD) doivent rester nuls.

La fréquence des contrôles est typiquement annuelle, mais elle peut être modulée en fonction du degré de stabilité constaté. Les disques contrôlés sont repérés pour servir de témoin d'éventuelle évolution ultérieure. Outre ces disques témoins, d'autres exemplaires pourront être prélevés et faire l'objet de tests.

Étant donnée la disparité des marques, des millésimes, des conditions de gravure, des conditions de stockage antérieures, il convient d'examiner soigneusement l'homogénéité des disques. La constitution de lots homogènes constitue la première et essentielle phase des procédures d'échantillonnage. Chaque lot représenté doit en effet faire l'objet de contrôles spécifiques.

Pour les règles d'échantillonnage et les procédures de contrôles par attribut, on se reportera à la norme NF ISO 2859-1:2000, précisant que, s'agissant de se prémunir de risques de perte d'information, les niveaux d'exigences choisis seront les plus élevés.

On peut également se reporter avec profit à la circulaire de la direction des Archives de France : Recommandations relatives à la gravure, à la conservation et à l'évaluation des CD-R : Instruction DITN/RES/2005/004 du 29 mars 2005, accessible sur le site de la DAF à l'adresse suivante : http://www.archivesdefrance.culture.gouv.fr/static/1056.

2.2.5.2 *Procédures à suivre pour le contrôle des WORM logiques et des supports réinscriptibles*

La garantie d'intégrité n'étant plus conférée uniquement par le support matériel lui-même mais par les logiciels de scellement cryptographique qui les utilisent, les procédures de contrôle de ces familles de supports doivent s'appuyer sur des principes différents de ceux des Worm physiques. C'est donc notamment au niveau des logiciels constituant le SAE que devront s'effectuer les contrôles. Le SAE doit disposer des procédures de contrôle devant permettre d'assurer et de vérifier l'intégrité des archives et leur complétude.

Ces procédures doivent en outre être décrites dans le dossier technique du SAE.

Le contrôle de l'intégrité des archives pourra s'effectuer par comparaison de leurs empreintes avec celles qui sont conservées dans les journaux de leurs cycles de vie. Les modalités de ces contrôles devront être définies après appréciation des risques encourus ; ils pourront par exemple être assurés sur la base d'échantillonnage (voir la norme NF ISO 2859-1:2000) et selon une fréquence définie, typiquement mensuelle ou trimestrielle.

Une procédure devra être établie pour contrôler la complétude des archives, par exemple par vérification de la cohérence entre les archives elles-mêmes et leurs métadonnées associées, notamment celles servant à leur recherche (bases de données d'index).

Les contrôles d'intégrité et de complétude devront être effectués sur le site primaire de conservation des archives et, *a minima*, sur un site secondaire de réplication. Des contrôles additionnels devront permettre d'assurer la cohérence des contenus archivés sur les différents sites.

2.2.6 Choisir un format de fichier pour l'archivage

2.2.6.1 *Critères clés pour le choix*

Plusieurs points fondamentaux doivent être étudiés lors de la conception d'une solution d'archivage et, en particulier, pour le choix de formats d'archivage.

À l'entrée dans le SAE, le format des documents peut être identifié et contrôlé (conformité aux spécifications d'un format donné). Dans ce cas, le résultat des contrôles doit être conservé et exploité si nécessaire, au titre des métadonnées techniques du document.

La nature de l'information à archiver (le contenu) est le premier point à analyser. Il peut s'agir : de texte, de graphiques statiques (illustrations, dessins industriels) ou de graphiques animés en 2D ou en 3D, d'images (photos à tons continus), de son (musique, discours, messages vocaux), de vidéo (analogique ou numérique) et de contenus mixtes. Pour chaque type d'information, un ou plusieurs formats numériques sont utilisables pour l'archivage.

Ces données peuvent provenir de différentes sources qui déterminent le format des données disponibles pour l'archivage.

Actuellement, les outils bureautiques sont une source majeure de données susceptibles d'être archivées. La multiplicité des logiciels et des conditions d'utilisation créent une situation complexe dans la perspective d'un projet d'archivage organisé à partir des données produites.

L'archivage numérique des documents disponibles uniquement sur support physique (papier, film, etc.) implique la numérisation des documents avec un numériseur adapté aux caractéristiques physiques du support disponible. Des traitements complémentaires des images obtenues peuvent être nécessaires pour en réduire le volume (compression) et en extraire le contenu textuel (OCR / LAD).

Certains outils spécialisés produisent des données qui vont appeler des solutions spécifiques et des formats d'archivage adaptés : messagerie électronique, logiciels de CAO et DAO, appareils photos numériques, appareils de prise de sons et caméras vidéo.

Enfin l'archivage des bases de données pose un problème majeur. Il ne faut pas confondre l'image d'une base de données (copie de sauvegarde) avec son archivage. Pour archiver une base de données, il est nécessaire de figer son état, d'extraire son contenu d'une manière intelligible dans des fichiers (par exemple, extraction à plat au format csv.) ainsi que les métadonnées associées et la description complète (dictionnaire des données, modèle conceptuel des données, dessins des fichiers, etc.) permettant de comprendre le fonctionnement de la base.

Par ailleurs, dans certains cas, il faudra choisir entre conserver le contenu (un flux de données représentant toute l'information utile) ou conserver le document présentant l'information sous une forme plus habituelle (mise en page, logo, etc.). Par exemple, faut-il archiver le flux de données permettant d'imprimer un ensemble de factures ou les factures elles-mêmes avec toutes données redondantes (mentions légales, fonds de page, etc.) ? Le volume archivé peut varier d'un facteur 10 selon l'option choisie.

La portée des services à rendre en matière d'accessibilité est également un point structurant. S'agit-il simplement de permettre la lecture des documents à l'écran ou en sortie d'imprimante ou faut-il répondre à d'autres besoins tels que la recherche sur le contenu textuel ? Dans le premier cas, une simple numérisation en mode image sera satisfaisante, dans le second cas, il faudra faire un traitement OCR, applicable aux documents imprimés et avec plus de difficultés aux documents manuscrits. Des progrès sont prévisibles dans ces techniques.

La gestion des métadonnées dans le processus d'archivage est une question clé. Certains formats permettent l'intégration des métadonnées directement dans le fichier des documents. C'est le cas des formats reposant sur le codage en XML ou d'un grand nombre de formats image. Si cette intégration n'est pas possible, l'accès aux documents passera par la consultation d'une base de données externe.

Le Tableau 1 ci-dessous résume les combinaisons possibles.

Tableau 1 — Combinaisons possibles

<table>
<tr><th>Contenu
Source</th><th>Texte</th><th>Graphique</th><th>Image</th><th>Son</th><th>Vidéo</th><th>Mixte</th></tr>
<tr><td>Bureautique</td><td colspan="3">Documents bureautiques</td><td colspan="3">Insertion de contenus audiovisuels dans les documents bureautiques</td></tr>
<tr><td>Numérisation</td><td colspan="3">Numérisation en mode image de tout support physique</td><td colspan="3">Conversion de sources analogiques</td></tr>
<tr><td>Outils spécialisés</td><td>Messagerie électronique</td><td>Plans CAO 2D et 3D</td><td>Appareils photos</td><td colspan="3">Appareils de prise de sons et caméras vidéo</td></tr>
<tr><td>Documentation technique</td><td colspan="6">Contenu mixte</td></tr>
<tr><td>Contenu de base de données</td><td>Fichiers de texte</td><td>Données CAO</td><td colspan="4">Contenus binaires</td></tr>
</table>

Devant la diversité des situations possibles, il est recommandé de s'appuyer sur le Référentiel Général d'Interopératibilité (RGI) version 1.0, qui a été approuvé par un arrêté en date du 9 novembre 2009, publié par la Direction générale de la modernisation de l'État (DGME). Les préconisations qui suivent sont basées sur cette version, sections 3.1 et 3.2.

2.2.6.2 *Formats d'images fixes*

Choix possibles :

- GIF (*Graphic Interchange Format*) : particulièrement adapté pour les images de 256 couleurs ou moins ;
- PNG (*Portable Network Graphics*) : défini par la norme ISO 15948, il supporte 16 millions de couleurs ;
- JPEG (*Joint Photographic Experts Group*) : défini par la norme ISO 10918, il est très utilisé pour la photographie numérique ;
- JPEG 2000 (ISO/IEC 15444-1 et 15444-2) est une norme de réduction de débit à taux variable avec ou sans perte pour les images fixes. Elle met en œuvre de nouveaux traitements qui fournissent une qualité d'image élevée y compris aux faibles débits ;
- TIFF (*Tagged Image File Format*) : format de fichier graphique bitmap, adapté pour les images de tailles importantes et de haute qualité ;
- DNG (*Digital Negative*) : format dérivé de TIFF qui enregistre les signaux bruts des appareils photographiques ;
- BMP (Bitmap) est un format propriétaire très largement répandu. Adapté aux images de grande taille, ce format n'est généralement pas compressé. Il supporte toutefois une compression sans perte.

Il convient de souligner le fait que les normes en matière de compression-décompression sont établies pour permettre le décodage des informations, et seulement cette phase. Les spécifications ne concernent pas l'encodage (modalités non communiquées), elles fournissent les éléments permettant de décoder le fichier compressé. Aussi faut-il s'attendre à des différences de qualité qui peuvent être significatives selon le système de décodage utilisé.

2.2.6.3 *Graphiques 2D*

Choix possibles :

- SVG (Scalable Vector Graphic) est une recommandation du consortium W3C. Il est basé sur le langage XML et permet la description d'objets graphiques vectoriels en deux dimensions ;
- CGM (Computer Graphic Metafile) est une norme pour l'échange et la conservation de données graphiques à deux dimensions ; CGM (ISO 8632).

2.2.6.4 *Graphiques 3D*

Choix recommandé :

- X3D (Extensible 3D) est un format de fichier graphique et multimédia orienté 3D. Il a été créé par le consortium Web3D dans le but de succéder à VRML 2.0. Ce format a été normalisé par l'ISO.

2.2.6.5 *Formats de dessin technique*

Choix recommandés :

- DWGdirect, ou à défaut le format DWG, pour les échanges de dessins techniques en mode révisable ;
- PDF 1.7, ou à défaut le format DWF, pour les échanges de dessins techniques (par exemple des plans) en mode non révisable.

2.2.6.6 *Échanges de documents bureautiques*

Choix possibles :

Pour les documents révisables :

- ODF est un format bureautique basé sur le langage XML. La version 1.0 du format de document ouvert a été approuvée par l'organisation OASIS en mai 2005, puis par l'ISO en mai 2006.
- Office Open XML a été validé comme standard ECMA en décembre 2006. Depuis, les spécifications du format ont été amendées et sa normalisation par l'ISO est intervenue en novembre 2008 (ISO 29500).

Pour les documents non révisables :

- PDF 1.7 a été normalisé par l'ISO en juillet 2008 et ses spécifications rendues publiques. Avant cette normalisation, le format PDF était devenu un standard de fait de par son adoption par la très grande majorité des utilisateurs.

2.2.6.7 *Archivage des documents bureautiques*

Choix possibles pour les documents non révisables :

- PDF/A-1 décrit dans la norme ISO 19005-1, répond aux problématiques d'archivage à long terme. Il est important de noter qu'il y a deux variantes de PDF/A-1 :
  - PDF/A-1a implique le respect de la norme complète, y compris de la structure logique et des métadonnées. Ce niveau est utilisable pour l'archivage des documents de source bureautique ;
  - PDF/A-1b est une forme allégée qui garantit la préservation de la lisibilité et la restitution à l'affichage et à l'impression. Ce niveau est utilisable avec les documents numérisés en mode image.

2.2.6.8 *Les formats de fichiers audio et audiovisuels*

a) Les formats audio

Ces formats sont très nombreux et il n'existe pratiquement pas de format libre, mais plutôt un consensus général se portant sur certains codages et procédés de compression. Dans ces conditions, seuls les principaux formats peuvent être cités.

1) Formats linéaires

PCM (Pulse Code Modulation), terme générique désignant un procédé de numérisation des données audio sans compression. La résolution est définie par la fréquence d'échantillonnage (kHz) et la longueur du mot numérique décrivant l'échantillon (nombre de bits). On admet généralement que la qualité minimale de la restitution de la musique correspond au format du disque compact audionumérique (CD Audio mentionné ci-dessous)

Le format PCML (PCM Linéaire) propose un type d'encodage multicanaux (jusqu'à 6 voies).

Le format CDA (CD Audio), seul exemple définissant les caractéristiques de conversion numériques dédié strictement à un support physique (disque compact). La qualité CDA (44,1 kHz sur 16 bits) constitue un point de référence.

2) Un format de compression sans perte

FLAC (Free Lossless Audio Codec). Il s'agit d'un des rares formats libres disponibles en open source.

Format libre de compression-décompression (CODEC) sans perte, spécifique pour l'audio.

Réduction de taille de 30 % à 70 % selon les caractéristiques de la source.

Peut traiter toutes données audio PCM : toute profondeur et fréquence d'échantillonnage, 1 à 8 canaux.

3) Formats de compression avec perte

Les traitements visant à réduire la qualité d'information prennent en compte les redondances de l'information sonore et la tolérance de l'auditeur vis-à-vis de la qualité de restitution de celle-ci.

Lorsque les applications d'archivage sont envisagées, les opérations de numérisation (transferts d'enregistrement analogiques) et d'enregistrement direct devront éviter systématiquement tout procédé de compression avec perte. De très nombreux dispositifs de compression sont proposés, nous ne citerons que quelques exemples. Il est important de mentionner que la désignation d'un format recouvre en fait une gamme de formats avec différents taux de compression.

MP3 : procédé de codage avec compression élaboré par le groupe MPEG (Moving Picture Expert Group), abréviation de MPEG-1 (repris par MPEG-2 qui en constitue une extention)-Layer 3. Les taux de compression MP3 varient de 1/4,4 à 1/44 (320 kb/s à 32 kb/s).

AAC (Advanced Audio Coding) : extension du codage MPEG-2 issu de plusieurs firmes, choisi par Apple qui a développé son propre système de gestion des droits (FairPlay).

Vorbis : procédé de compression libre. Il propose 10 niveaux de compression. Encore peu répandu.

4) Formats conteneurs

Il s'agit de formats pouvant contenir différents types de données audio (avec ou sans compression).

Wave (WAV) : format propriétaire, extrêmement répandu, il peut accueillir de très nombreux formats compressés ou non.

BWF (Broadcast Wave Format File) : format conteneur audio défini par l'Union européenne de radiodiffusion (UER) ou European Broadcast Union (EBU). Intègre seulement des formats Wave codés en PCM ou MPEG. A pour particularité de permettre l'insertion d'un certain nombre de données documentaires.

Ogg : format libre, encapsule généralement le format ouvert Vorbis.

AIFF (Audio Interchange File Format) est un format propriétaire. Ne concerne que des données non compressées.

Le RGI (Référentiel général d'interopérabilité — Direction générale de la modernisation de l'état) recommande les formats MP3 et WAV pour l'échange, la présentation et la conservation de séquences sonores.

NOTE Tout traitement de compression doit être évité lors de la conversion numérique de documents audio destinés à la conservation : les dispositions de préservation de la qualité de l'information, de réduction des risques liés aux incompatibilités et à l'obsolescence des formats de compression doivent être mises en œuvre. **Les formats audio acceptables pour l'archivage sont WAV ou BWF encapsulant un format linéaire (PCM) de plus haute résolution possible**

b) Les formats vidéo

Toutes les étapes, depuis la saisie du flux d'images jusqu'à l'écran de l'utilisateur final font l'objet de nombreux traitements qui prennent en compte les contraintes d'acquisition, d'enregistrement, de transport, d'usage, de stockage des informations. Deux objectifs sont visés : obtenir un débit le plus bas possible, obtenir une image de la meilleure qualité possible, ceci dans des conditions économiques acceptables. Des objectifs contradictoires qui exigent des consensus qui se traduisent par une multiplicité de formats sans cesse en évolution, etc.

Très schématiquement on distingue trois étapes de traitement :

- le codage des composantes primaires (composantes — composite PAL/SECAM/NTSC) ;
- la numérisation (4 :2 :2 Betacam numérique — 4 :1 :1 DV et DVCPRO) ;
- la compression.

1) Le codage analogique des signaux primaires

Ce codage peut être réalisé de deux manières :

- système de codage en composantes : RVB, YUV, YC ;
- système de codage en composites : assemblage des composantes en un seul signal sous la forme des standards concurrents : PAL, SECAM et NTSC.

2) Numérisation

Les signaux analogiques codés font l'objet d'une numérisation avec des résolutions variables.

- Dans le cas de la conversion des signaux composantes, la sélection et la répartition des échantillons de luminance et de chrominance (différence couleur) sur une ligne (une ligne sur deux peut-être ignorée) définit une structure dite référentielle, par exemple 4:2:2 (Bétacam numérique, etc.), 4:1:1 (DV et DVCPRO, etc.).
- Dans le cas des signaux composites, l'échantillonnage porte directement sur le signal porteur de luminance et de chrominance.

3) Compression

Les quantités d'informations recueillies et les contraintes liées à la transmission des programmes rendent la compression incontournable. Les techniques de compression reposent sur les redondances d'une image (degré d'uniformité), sur les redondances d'une image à l'autre (degré de changement), sur la qualité souhaitée (tolérance aux imperfections), et enfin sur les possibilités d'économie relatives à la description numérique de l'information.

Les normes relatives au codage, à la conversion, à la compression et à la gestion des contenus constituent des «boîtes à outils» correspondant aux applications envisagées, ainsi de produire des documents destinés à différents types d'usage : exploitation dans un contexte donné, visionnage, sauvegarde, conservation de l'information.

La norme MPEG (Motion Picture Expert Group) :

- **MPEG-1** : réduction des débits : 1,5 Mbits/s
- **MPEG-2** : réduction appliquée aux signaux composantes atteint 10 Mbits/s
- **MPEG-3** : vise des débits de 18 à 25 Mbits/s (HD)
- **MPEG4** : élaborée à l'aide de traitements du signal particulièrement élaborés, cette norme (ISO/IEC 14496) a vocation de prendre en charge tout type de programmes multimédia, depuis les plus bas débits (64 kb/s) aux plus élevés (1,2 Gb/s). Ceci pour toutes les applications possibles : création, imagerie scientifique, synthèse sonore, jeux, TV numérique (TNT,…) avec degré d'interactivité élevé.

  La norme MPEG-4 partie 10 (ISO/IEC 14496-10, H264 ou encore AVC : Advanced Video Coding) propose une très large gamme de débits répondant de manière flexible à tous types d'applications de transmission et d'enregistrement jusqu'à la haute définition (HD).

  À propos de HD, le format Blu-ray autorise un débit maximum utile de 48 Mb/s. Ce format supporte plusieurs définitions moyenne et élevée) et les principaux codecs (MPEG-2, MPEG-4,…).

  Le son accompagnant la HD fait l'objet de codages spécifiques compte-tenu de la qualité requise et de la multidiffusion par 6 (5.1) ou 8 (7.1) canaux.
- **MPEG7** (Interface de description des contenus multimedia) : n'est pas une norme liée aux précédentes. Elle concerne la représentation des contenus multimédias (numériques ou analogiques). Tous les éléments du document peuvent être pris en compte : création (auteurs, interprètes, producteurs,…), utilisation (droits d'accès, de diffusion,…), le média physique et le format numérique (compression,…), la description du contenu, les aspects conceptuels (présentation, critique des contenus).

Le RGI recommande les formats MPEG pour l'échange, la présentation et la conservation de séquences vidéo en basse définition (MPEG-2) et en haute définition (MPEG-4).

c) Les formats conteneurs vidéo

Les formats conteneur vidéo associent, de manière simultanée, les données vidéo, audio, et, pour les formats les plus élaborés, des éléments descriptifs du programme.

Les formats conteneurs de données vidéo en concurrence sont très nombreux, toujours en développement pour la plupart d'entre eux. Les plus répandus sont :

- AVI (Audio video interleave), développé par Microsoft, accueille tous types de fichiers compressés vidéo ou audio.
- OGG (Ogg media video), pratiquement, le seul format libre. Il supporte les formats libres de compression vidéo Théora, ainsi que les formats libres audio cités en première partie.
- MOV Quick Time, développé par Apple, gère de nombreux formats vidéo jusqu'au standard HD.
- RM (Real media), développé par RealNetwork, associe les formats de compression vidéo (RealVideo) et audio (RealAudio) pour permettre la diffusion de programmes en continu (streaming).
- MPEG. Certaines normes MPEG (MPEG 2/4, MPEG-21) proposent l'interopérabilité de différents contenus multimédia.
- WMV (Windows Media Video), format propriétaire fréquemment utilisé pour la communication de fichiers audio-vidéo.
- TS (Transport Stream), format de communication de programmes audio, vidéo avec données de service spécifié dans la norme MPEG-2 partie 1.
- Vob (Video Object File) est un format basé sur la norme MPEG-2 élaboré pour les disques DVD Vidéo.

2.2.6.9 *Repères méthodologiques*

Pour terminer, il convient de souligner que le choix des formats doit s'insérer dans une réflexion plus large de conception d'un projet d'archivage électronique qui devra répondre aux exigences d'une politique d'archivage définie au niveau de l'entreprise ou de l'institution.

Cette réflexion sur les formats doit passer par les étapes suivantes :

- recenser et caractériser les contenus à archiver : typologie des documents et des flux à conserver, sources des données et mode d'obtention de ces données ;
- définir les fonctionnalités attendues en termes de services à rendre : simple consultation sur écran avec quelles fonctions, impression, indexation des contenus textuels, gestion des métadonnées intégrées dans les documents, extraction de contenu pour récupération, possibilité de charger les données archivées pour créer de nouveaux documents ;
- choisir et spécifier les formats retenus pour l'archivage : versions à utiliser, paramétrage des options, contrôles à prévoir ;
- rechercher et qualifier les outils d'identification, de contrôle et éventuellement de conversion parmi les produits offerts sur le marché ;
- organiser la migration : choix des acteurs, planification des opérations, pilotage du chantier ;
- vérifier les droits pour le traitement des documents audiovisuels.

2.2.7 Destruction des archives

2.2.7.1 *Définir le point de départ et la durée de conservation*

La conservation des archives (documents ou lots de documents) est, à durée limitée, à l'exception des documents qui, en raison de leur valeur patrimoniale, doivent être conservés à titre définitif.

Cette durée est fixée de manière légale, réglementaire ou contractuelle en fonction de la typologie des documents. Elle peut aussi dépendre de la survenance d'un évènement prédéfini et lié à l'archive.

Lors du versement d'une archive (document ou lot de documents) dans le SAE, l'utilisation de profil d'archivage peut apporter une aide à la gestion de la durée de conservation.

La date de destruction peut être indiquée précisément ou calculée, au moment du versement, à partir de la date de versement additionnée de la durée de conservation. La date de destruction ou la durée de conservation sera inscrite dans les métadonnées de l'archive.

La destruction peut être conditionnée à la survenance d'un évènement prédéfini lors du versement et différent d'une date. La condition de destruction sera clairement inscrite dans les métadonnées de l'archive.

NOTE L'introduction d'une date ou d'une durée de conservation a priori, même révisable, présente des risques. Ce risque peut être par exemple la destruction d'un dossier de patient encore vivant, d'un salarié encore en poste, d'un dossier de maintenance d'un équipement encore utilisé ou d'un document concerné par une décision de justice. À l'opposé, ce risque peut être la conservation abusive de données à caractère personnel, devant être légalement détruites.

Pendant toute la phase de conservation, il doit être possible de bloquer la destruction dans le SAE d'une archive, à condition de tracer dans les journaux cette modification et d'inscrire les nouvelles conditions de destruction dans les métadonnées de l'archive.

Pour les destructions conditionnées à la survenance d'un évènement pré défini, la difficulté principale se situe dans la définition et la pertinence de cet évènement qui peut arriver de nombreuses années après la date de versement, dans un environnement profondément modifié en termes de personnels, de responsabilité, d'organisation, de processus, de système d'information, d'applicatifs, de moyens techniques du SAE.

Cette organisation repose sur une identification (type, cible, secteur responsable) des événements à suivre et sur des agents qui régulièrement lancent des requêtes auprès des secteurs responsables afin de vérifier l'occurrence de l'événement ou de procéder à la mise à jour des métadonnées utilisées par ce système de capture. L'identification est faite au moment du versement.

La solution idéale est un système d'information entièrement urbanisé. Si un tel système n'est pas opérationnel, il appartient aux concepteurs du SAE de mettre en place une organisation pérenne qui aura pour tâche de capturer ou de gérer ces événements.

La destruction peut enfin être manuelle. Le lancement d'une destruction manuelle doit être contrôlé par le SAE, notamment quant à l'identité du requérant, et dûment tracé dans les journaux.

Il doit être possible dans les mêmes conditions de contrôle et de traçabilité de prolonger la durée de conservation d'une archive.

2.2.7.2 *Motivation de la destruction*

Maîtriser les destructions permet d'une part, de faire face à la dilution des responsabilités et obligations dans le temps des services détenant à l'origine les documents et permet d'autre part, de réaliser des gains économiques grâce à l'allègement de la volumétrie, la simplification de la gestion et l'accroissement des performances (temps de recherche, temps d'accès, temps de chargement).

Les obligations légales en matière de gestion fiscale, comptable ou sociale imposent souvent aux entreprises de conserver sur de longues périodes des documents contenant des données à caractère personnel.

L'archivage électronique de ces documents doit se faire dans le respect des principes de la loi informatique et libertés, notamment le droit à l'oubli et la finalité.

La CNIL recommande dans sa délibération (Délibération n° 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel) :

a) de respecter le principe du «droit à l'oubli» : Les archives courantes et intermédiaires doivent répondre à des durées de conservation spécifiques, proportionnées à la finalité poursuivie (en particulier au regard des durées de prescription définies par la réglementation commerciale, civile ou fiscale) ;

b) de protéger les données archivées notamment contre la diffusion ou l'accès non autorisés ainsi que contre toute autre forme de traitement illicite ;

c) d'éviter la «dilution» des données archivées dans le système informatique de l'entreprise : la CNIL recommande que l'accès aux archives intermédiaires soit limité à un service spécifique (par exemple un service du contentieux) et qu'il soit procédé, a minima, à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations) ;

d) de mettre en œuvre des dispositifs de traçabilité des consultations des données archivées ;

e) d'utiliser des procédés d'anonymisation en cas de conservation à long terme en particulier pour les données sensibles au sens de l'Article 8 de la loi «Informatique et Libertés» (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale, données relatives à la santé ou à la vie sexuelle) ;

f) de développer, dans les entreprises, des procédures formalisées et qu'une information puisse être fournie sur ces règles, en cas de demande exprimée de leur part, aux individus faisant l'objet des traitements archivés.

La recommandation a vocation à s'appliquer aux archives dites courantes, intermédiaires et définitives.

Dans le secteur public, la prise en charge de données à caractère personnel pour archivage par un service public d'archives, repose également sur la loi de 1978 et sur des principes identiques à ceux développés ci-dessus, mais il convient également de prendre en compte spécifiquement l'Article 36 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, selon lequel : «Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'Article 6 qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques ; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine.

Les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives dans le cadre du livre II du même code sont dispensés des formalités préalables à la mise en œuvre des traitements prévues au chapitre IV de la présente loi».

La justification de cet archivage est que sa finalité n'est plus celle qui a prévalu lors de la mise en œuvre du traitement (finalité patrimoniale). Il s'ensuit que les producteurs de cette information n'y ont plus accès, une fois l'archivage effectué.

2.2.7.3 *Caractéristique de la destruction*

Si des documents ont fait l'objet d'une migration de support ou de format, on s'assurera de la destruction des documents dans leur format d'origine ou sur leurs anciens supports. La destruction doit être complète **et irréversible** et ce caractère définitif doit être contrôlable.

La destruction d'un document peut être accompagnée ou non par la destruction des métadonnées associées, ainsi que celle des éléments de traçabilité (à l'exception des journaux). Ce choix peut être fait au niveau de chaque typologie de document ou de chaque profil. Ce choix doit être défini dans la politique d'archivage.

La destruction de documents peut être liée à des opérations de migration de formats ou de supports. Dans ce cas il peut être nécessaire de s'assurer que les anciens fichiers ou les anciens supports soient détruits.

La possibilité d'utiliser des supports variés comme moyen de stockage dans un SAE conduit à définir, pour chacun d'entre eux, les exigences relatives à la destruction des documents.

2.2.7.4 *Réalisation des destructions*

Au sein, d'un SAE, la destruction doit pouvoir être effectuée au niveau unitaire, archive par archive.

La destruction d'une archive (document ou lot de documents) dans un SAE suppose l'effacement ou la disparition des fichiers de ce document. Lorsque l'effacement n'est pas possible car la fonction écriture n'est pas accessible, la seule solution est la destruction physique des médias.

2.2.7.5 *Destruction physique (Worm physique)*

La destruction d'un document implique donc la destruction physique du support.

Même si au départ il avait été choisi d'inscrire des documents ayant la même date de destruction sur le même support, il est possible qu'à terme, il soit nécessaire de gérer pour un même média, plusieurs durées de destruction différentes.

Plusieurs solutions sont envisageables suivant la nature des documents contenus sur le média et les choix de la politique d'archivage :

a) une destruction réelle lorsqu'il est impératif de faire disparaître les documents. Cette destruction doit être précédée d'une migration de supports pour les documents ne devant pas être détruits ;

b) une destruction virtuelle (ou système) rendant inaccessible un document en attendant la destruction réelle qui arrivera avec la fin de vie du support programmée et contrôlable.

2.2.7.6 *Destruction par effacement (Supports réinscriptibles, certains Worm logiques)*

Les supports réinscriptibles et les Worm logiques doivent permettre l'effacement définitif et contrôlable des fichiers.

Dans le cas des supports magnétiques il est nécessaire d'appliquer plusieurs séquences d'écritures. Plusieurs algorithmes existent. Ce choix doit être consigné dans le dossier technique du SAE.

Tableau 2 — Exemples d'algorithmes d'effacement

N°	Algorithme	Nbre passes	Actions
1	USA : DoD 5220.22-M	4	P1 — symboles choisis aléatoirement écrits dans chaque octet de chaque secteur P2 — complémentaire à l'écriture de la 1re passe P3 — symboles aléatoires à nouveau P4 — vérification
2	USA : NAVSO P-5239-26 (RLL)	4	P1 — 0x01 dans tous les secteurs P2 — 0x27FFFFFF P3 — séquences de symboles aléatoires P4 — vérification
3	USA : NAVSO P-5239-26 (MFM)	4	P1 — 0x01 dans tous les secteurs P2 — 0x7FFFFFFF P3 — séquences de symboles aléatoires P4 — vérification
4	Allemagne : VSITR	7	P1 à 6 — séquences alternatives de 0x00 et OxFF P7 — OxAA ; resp. 0x00, OxFF, 0x00, OxFF, 0x00, OxFF, OxAA
5	Russie : GOST P50739-95	1	Zéros logiques (nombres 0x00) dans chaque octet de chaque secteur pour les niveaux de sécurité système du 6e au 4e. Symboles aléatoires (nombres) dans chaque octet de chaque secteur pour les niveaux de sécurité système du 3e au 1er.
6	Algorithme de P. Gutmann	35	Basé sur la théorie de la destruction des données de Gutmann
7	Algorithme de B. Schneier	7	Bruce Schneier propose un algorithme avec 7 passes de réécriture dans son livre «Applied Cryptography». P1 — OxFF P2 — 0x00, puis cinq fois de suite avec une séquence pseudo-aléatoire sécurisée de manière cryptographique.

2.2.8 Journalisation [2)]

La norme distingue deux types de journaux : le journal de cycle de vie des archives et le journal des évènements. Cependant, la norme définit le journal des évènements comme un **«journal assurant la traçabilité des opérations (…) autres que celles consignées dans le journal de cycle de vie des archives»** (voir la norme page 10 — Chapitre 3.19 : Journal des évènements).

Dans ces conditions, le journal des évènements vient donc compléter le journal de cycle de vie des archives comme cela est synthétisé avec le schéma ci-dessous :

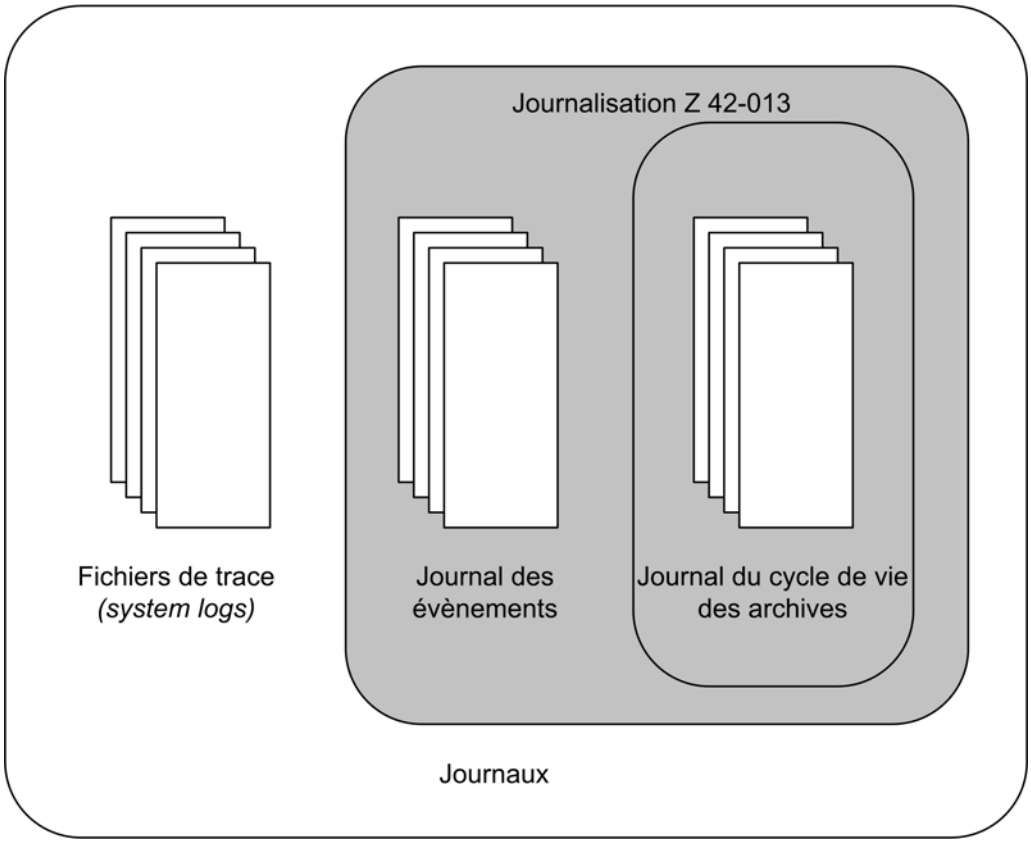


Figure 4

Tous les évènements qui concernent le système (**«Journal des évènements»** au sens de la norme) ou les archives (**«Journal du cycle de vie des archives»** au sens de la norme) sont enregistrés de façon séquentielle dans le ou les journaux correspondants.

Le ou les journaux sont créés automatiquement par le système.

«Il doit être possible de lire les journaux de façon simple et leur exploitation doit être détaillée dans le dossier de description technique du système.» voir la norme page 19 — Chapitre 5.6 : Journalisation

Les journaux doivent être archivés selon une périodicité et des conditions définies par la politique d'archivage en assurant au moins la même pérennité et intégrité que les documents numériques auxquels ils se rapportent.

Les journaux ne doivent être accessibles qu'aux seules personnes dûment habilitées.

---

2) *Ce chapitre emprunte de larges extraits au document « Niveau de services d'archivage électronique — Année 2009 » réalisé par le CFONB.*

La journalisation permet la production d'attestations. Celles-ci doivent être archivées dans les mêmes conditions de conservation que les documents qu'elles concernent.

Il conviendra de distinguer les fichiers de traces (system *logs*) des journaux qui, au sens de la norme, sont des vues fonctionnelles : «Journal du cycle de vie des archives» et «Journal des évènements» du système d'archivage.

2.2.8.1 *Journal du cycle de vie des archives*

«Le journal du cycle de vie des archives comprend les attestations électroniques suivantes :

— attestation de prise en compte initiale d'un dépôt ;

— attestation de prise en compte d'une modification de la durée d'un dépôt, le cas échéant ;

— attestation de destruction anticipée ou à terme d'un dépôt, le cas échéant ;

— attestation de restitution d'un dépôt, le cas échéant ;

— attestation pour toute création, modification ou suppression d'un profil d'archivage.»

(voir la norme NF Z 42-013 § 5.6.2 : Journalisation du cycle de vie des archives)

La journalisation du cycle de vie devra enregistrer les traces applicatives.

Celui-ci doit permettre l'enregistrement des évènements significatifs affectant la «vie» d'une archive. À partir de ces enregistrements, on doit pouvoir reconstituer ces évènements, depuis la prise en compte initiale du dépôt, les dates, types et résultats des contrôles effectuées sur cette archive, éventuellement des modifications de ses durées de conservation, des migrations subies par cette archive, jusqu'à son élimination ou sa restitution. Un identifiant pérenne et signifiant pour l'utilisateur doit pouvoir permettre de faire un lien entre ces différents enregistrements et ainsi de reconstituer la «vie» de cette archive dans le système.

a) Contenu :

Le journal du cycle de vie rend compte au minimum des opérations de :

— création d'archive/dépôt ;

— suppression d'archives ;

— changement de durée (prolongement) de l'archive ;

— restitution d'une archive ;

— contrôles correspondant à ceux du niveau de services.

De plus, en fonction des modalités définies dans la Politique d'archivage, il pourra être décidé de conserver une trace systématique des consultations pour certaines familles d'archives.

Un évènement sur le cycle de vie, doit faire l'objet d'une ligne dans le journal.

Chaque ligne doit comporter au minimum :

— une date fiable ;

— l'identifiant unique de l'archive ;

— le type d'événement ;

— l'empreinte du document numérique.

Lors de l'opération de dépôt, l'empreinte de l'objet archivé doit être consignée dans le journal si le support de stockage n'est pas de type WORM physique, elle servira notamment à vérifier l'intégrité de l'objet lors de sa consultation, ou de sa restitution.

En cas de stockage sur un support WORM physique, l'intégrité est assurée par le support : pas de dispositif particulier au niveau du journal.

b) Sécurisation

Le journal du cycle de vie des archives doit faire l'objet d'un horodatage (voir la norme paragraphe 5.5 page 18 : Horodatage) par vingt quatre heures.

La continuité des journaux sera assurée par leur chaînage.

À titre d'exemple :

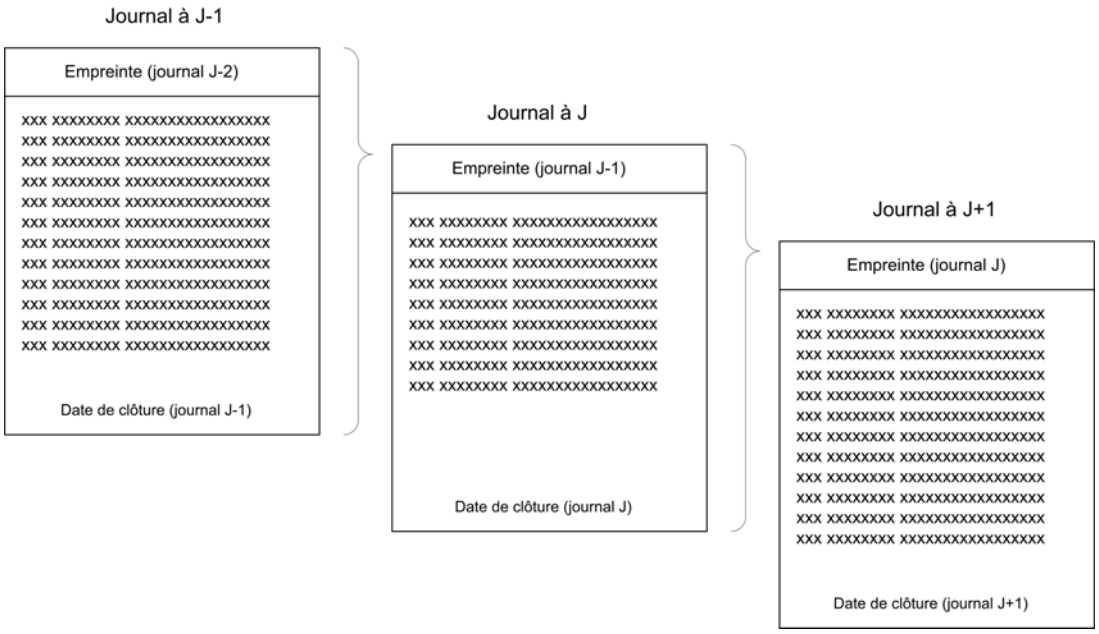


Figure 5 — Principe de chaînage des journaux

c) Conditions de conservation

Chaque journal ainsi constitué sera archivé dans les mêmes conditions que les archives auxquelles il se rapporte.

Sa durée de conservation est égale au minimum à la durée maximale de la durée de conservation la plus longue de l'archive.

La conservation de ces journaux pourra aller au delà de la durée fixée, à des fins de traçabilité. Si ces journaux permettent l'identification, la récupération ou la reconstitution de données à caractère personnel définitivement effacées, alors le responsable du traitement de la conservation devra effectuer les formalités obligatoires auprès de la CNIL.

2.2.8.2 *Journal des évènements*

Ce journal se décompose en trois parties :

— une partie pour les évènements relatifs à l'application d'archivage ;

— une partie pour les évènements relatifs à la sécurité ;

— une partie pour les évènements relatifs au système.

(voir norme NF Z 42-013 — § 5.6.3 : Journal des évènements)

2.2.8.3 *Détails de la journalisation par niveaux d'exigences*

RAPPEL Les niveaux d'exigences de la norme ne s'imposent que pour les Worm logiques et les supports réinscriptibles.

La journalisation doit permettre notamment de tracer les éléments suivants :

— authentification ;

— journal du cycle de vie ;

— attestations ;

— journal des évènements ;

— horodatage.

Pour les Worm logiques, et les supports réinscriptibles, les détails de la journalisation évolueront en fonction des niveaux d'exigences.

2.2.9 Audits

La procédure d'audit est destinée à mesurer le niveau de conformité à la norme AFNOR NF Z 42-013 d'un système d'archivage électronique incluant ou non les processus de capture et de conversion des documents.

Le rapport d'audit permet à l'ensemble des services concernés par le projet d'avoir une visibilité précise des fonctionnalités, des procédures et du suivi d'exploitation prévu dans le projet en comparaison avec les recommandations contenues dans les normes citées et de fournir une évaluation objective de la qualité et de la fiabilité de la chaîne de la confiance inhérente au projet.

Le niveau d'application de la norme NF Z 42-013 dans le cadre d'un système de capture et d'archivage correspond aux exigences minimales précisées dans le texte de celle-ci tandis que les exigences complémentaires résultant des choix technologiques ou organisationnels sont prises en compte dans un référentiel annexe.

Un audit de sécurité doit être considéré comme une démarche complémentaire aux procédures de sécurité des systèmes d'information déjà en place dans l'entreprise.

En particulier, s'agissant des aspects «sécurité» ce document concerne les méthodes et l'organisation utilisées pour la gestion de la sécurité en rapport avec le système de numérisation et d'archivage :

— sécurité physique des locaux ;

— contrôle d'accès des personnels aux matériels ;

— contrôle d'accès des personnels aux informations ;

— sécurité des supports optiques ;

— sécurité des matériels ;

— sécurité des logiciels et progiciels.

a) Principes généraux

1) Définitions

L'audit de conformité présente plusieurs niveaux d'investigation associés à des objectifs de résultats gradués :

i) **l'observation** : recensement des fonctionnalités et procédures du système en vue d'obtenir un inventaire des principes et des outils mis en œuvre.

ii) **l'analyse** : évaluation, dans les différents compartiments du système, du niveau de conformité à la norme atteint en fonction des objectifs visés permettant l'identification des risques dus aux non-conformités résiduelles.

iii) **la confirmation** : contrôle de l'efficacité des dispositifs mis en œuvre pour le traitement, l'archivage et la conservation des documents au moyen de sondages et de tests permettant de vérifier l'intégrité des documents et la pérennité de leur conservation.

2) Objectifs

L'audit de conformité répond à un triple objectif :

- s'assurer de l'identification des écarts de conformité en fonction des options techniques et organisationnelles retenues ;
- valider l'adéquation des moyens et procédures mis en œuvre et identifier les risques résiduels ;
- maintenir et faire progresser le niveau de conformité au travers de recommandations pratiques.

b) Domaines d'investigation

1) Le périmètre de l'audit

La démarche d'audit, quels que soient les niveaux d'investigation retenus (observation, analyse, confirmation) peut s'appliquer à des domaines plus ou moins ciblés.

À ce titre certains domaines relèvent d'une «**approche référentielle»** de la norme, reposant sur la vérification des directives édictées, ainsi :

i) **l'audit global** s'attache à l'examen de l'ensemble des principes et moyens contribuant au fonctionnement du système d'archivage électronique, tels que décrits dans les différents documents techniques (Document de spécifications fonctionnelles, Document de conception technique, etc.).

ii) **l'audit de service** prend en compte chaque fonction spécifique parmi celles définies au sein des différents documents de spécification (ex : la numérisation, le stockage des documents, le contrôle d'accès logique, la sécurité et la gestion des média, etc.). Il sera par la suite associé à un planning d'audit annuel dont le contenu pourra être défini en fonction de l'évolution des fonctionnalités et sera réalisé sous la responsabilité du responsable du SAE.

D'autres audits s'apparentent à une «**approche opérationnelle»** du fonctionnement du SAE :

i) **l'audit «suivi» des procédures** se focalise sur chaque aspect fonctionnel du système et analyse les dispositions et les enregistrements de suivi.

ii) **l'audit «sécurité»** s'applique aux différents composants du système, qu'ils traitent spécifiquement de la sécurité de l'information (ex : élaboration d'un plan de continuité), de la mise en œuvre d'une ressource informatique (ex : juke-box de D.O.N, ouverture d'un Intranet, etc.) ou du développement d'une nouvelle activité de l'entreprise interne ou externe. Ce type d'audit peut être mené spécifiquement pour le SAE ou faire partie intégrante des audits «Sécurité» menés par ailleurs. Il est déclenché par le Responsable concerné au niveau système de numérisation et d'archivage ou Sécurité.

iii) **l'audit «pérennité» du SAE** se focalise sur la vérification de la pérennité du système utilisé et la vérification de la possibilité de migration des documents archivés.

2) Les axes d'audit

Les axes d'audit seront choisis en fonction du périmètre retenu pour l'audit régulier parmi les aspects suivants :

i) **le cadre réglementaire du maître d'ouvrage** formalisant les principes édictés au sein de sa Politique d'archivage des documents (cadre législatif, bonnes pratiques, guide de management) et déclinés au niveau opérationnel au sein des projets et des activités du client.

ii) **l'organisation** supportant l'application et le contrôle des moyens mis en œuvre pour l'archivage des documents et définie en termes de rôles et responsabilités des acteurs impliqués (au niveau décisionnel et opérationnel) et principes de délégation.

iii) **les dispositifs** composant l'architecture technique qui supporte la mise en œuvre des systèmes d'archivage.

iv) **les aspects contractuels** qui régissent les relations du maître d'ouvrage et les exigences de conservation de documents avec ses clients, fournisseurs, partenaires et assureurs en termes d'engagement de moyens et/ou de résultats.

c) Démarche d'audit

1) Interviews

La collecte d'informations peut être réalisée au moyen d'entretiens menés avec les principaux acteurs concernés par le domaine d'investigation retenu.

Ces intervenants peuvent être positionnés à un niveau décisionnel (Direction Générale, Responsable Projet SAE) ou opérationnel (Maître d'œuvre, Administrateur) et rattachés à une entité utilisatrice (Propriétaire de l'information, Collaborateur) ou une direction informatique (Développeur, Exploitant).

Il peut également s'agir de collaborateurs du maître d'ouvrage, mais aussi de prestataires, de partenaires voire de clients.

2) Études documentaires

L'analyse de la documentation existante vise plusieurs objectifs distincts : l'identification du formalisme existant sur le domaine audité, l'appréciation de la gestion documentaire proprement dite (référencement, typologie, émetteur, liste de diffusion, attribut de confidentialité), l'évaluation de l'exhaustivité, de la pertinence et de l'actualisation des documents.

Les documents entrant dans le champ de l'étude peuvent être des spécifications fonctionnelles détaillées, des descriptions d'architecture technique, des règles et procédures d'exploitation ou d'installation, des descriptifs détaillés de paramétrage, des textes réglementaires, des résultats de contrôles permanents, d'audits antérieurs, etc.

3) Visites de sites

La visite des sites et locaux entrant dans le champ de l'audit permet un contrôle visuel de l'organisation et de la mise en œuvre des procédures ainsi que des vulnérabilités et des moyens existants pour le domaine particulier de la sécurité.

Ces visites peuvent notamment concerner les salles informatiques et télécoms, les locaux techniques et unités logistiques, qu'ils soient situés sur des sites appartenant au maître d'ouvrage ou chez des prestataires, partenaires ou fournisseurs externes, par exemple pour le stockage des média de sauvegarde.

4) Tests techniques

Les investigations techniques sont nécessaires au contrôle de l'efficacité des fonctionnalités mises en place.

Elles peuvent reposer sur l'utilisation d'outils spécifiques permettant la détection des non-conformités par rapport au référentiel normatif liées à la conception, à l'implémentation ou aux procédures d'exploitation ou de sécurité.

d) Résultats de l'audit

1) Diagnostic

L'audit de conformité permet de dresser un diagnostic précis sur la conformité du SAE par rapport aux recommandations des normes citées et au niveau d'application souhaité par le maître d'ouvrage.

Ce constat aboutit à l'identification des sous-ensembles ou procédures non conformes et des risques éventuels qui en résultent.

2) Recommandations

Les recommandations sont de plusieurs niveaux : niveau politique/management, contractuel, fonctionnel et technique.

Elles sont classées par degré de priorité en fonction des domaines à couvrir, du contexte, des contraintes organisationnelles et techniques.

Chaque recommandation est qualifiée en termes d'enjeux et de résultats attendus.

Elles sont intégrées dans une démarche de mise en œuvre structurée au sein d'un plan d'action spécifiant le calendrier et les préalables éventuels à chaque action, les acteurs concernés et les charges internes, les investissements matériels et logiciels, la nécessité d'assistance externe ou d'intervention d'experts.

3) Le rapport d'audit

L'ensemble des travaux accomplis est rassemblé, consigné et structuré au sein d'un rapport d'audit qui vient à l'appui des conclusions formulées et des recommandations effectuées, également formalisées dans ce document de référence.

La diffusion des documents ayant trait à l'audit de conformité (comptes-rendus, rapport, ...) est limitée à une liste de destinataires définie par le responsable commanditaire de la mission.

Les différentes recommandations peuvent être communiquées indépendamment les unes des autres en fonctions des acteurs concernés.

2.2.10 Les acteurs du projet

LES ACTEURS DU SYSTÈME D'ARCHIVAGE ÉLECTRONIQUE

Un système d'archivage électronique (SAE) est une application complexe, liée à l'ensemble du cycle de vie des documents et faisant intervenir de nombreux acteurs depuis la phase projet jusqu'au MCO. Le SAE adresse donc des aspects organisationnels et techniques de plusieurs composantes d'une société :

— les directions opérationnelles et fonctionnelles ;

— l'architecture du Système d'Information ;

— les processus ;

— les matériels et les applications.

La conception, la mise en place et l'exploitation du SAE doivent donc réunir plusieurs compétences complémentaires.

a) Définition de la politique

La **direction générale** doit approuver le document définissant la politique d'archivage.

Le **responsable gestion documentaire et archivage** doit définir cette politique en coopération avec les différentes directions de l'entreprise. Il assure la maîtrise d'ouvrage du SAE. Ce nouveau rôle apparaît dans les entreprises en raison de la complexité des problématiques documentaires liées aux documents numériques.

b) La conception et mise en place du SAE

Cette phase projet fait appel aux compétences suivantes :

1) Le **chef projet SAE** est en général le responsable de la gestion documentaire et archivage. Lui-même ou un de ses collaborateurs est responsable de la finalisation du cahier des charges SAE. Il doit plus particulièrement définir les fonctionnalités en termes de services à offrir et les conditions d'intégration dans le système d'information existant et son éventuelle urbanisation. Il lui revient en particulier de spécifier la ou les interfaces nécessaires avec les applications sources produisant des documents à archiver. Par ailleurs, il précise les métadonnées à fournir, les formats à utiliser, les modalités d'intégration dans les processus métier et la définition des profils nécessaires dans le cadre de la politique d'archivage.

2) La **direction informatique** doit compléter le cahier des charges du SAE par rapport à l'existant du système d'information et son plan de développement. Elle devra assurer la maîtrise d'œuvre des moyens informatiques nécessaires au SAE.

3) Les **directions supports** et les **directions opérationnelles**, en collaboration avec le responsable de la gestion documentaire et archivage, ont la responsabilité de la définition des contraintes (sécurité, confidentialité, etc.) et de la définition des tableaux de conservation par une analyse des textes légaux, réglementaires et contractuels concernant leurs métiers (risque, juridique, qualité et développement durable, RH, R&D, RPI, RSSI, Production, etc.).

4) Les **prestataires de services** ou les tiers archiveurs fournissent des propositions d'éventuelles prestations qui seront intégrées dans la conception et dans la rédaction du cahier des charges du SAE.

5) L'**éditeur de progiciel** SAE offre une solution paramétrable permettant de définir les typologies de documents à archiver ainsi que les éventuels profils d'archivage associés, la gestion du référentiel des archives et versements, la gestion des dépôts, la conservation, la communication, destruction ou restitution. Le progiciel peut également gérer le versement des objets archivés vers le tiers-archiveur.

c) Exploitation du SAE

Les **responsables des documents,** en collaboration avec les archivistes**,** engagent le sous-processus de versement suivant les règles définies par la politique d'archivage.

Les **archivistes** assurent le contrôle de la bonne exécution des sous-processus :

- de versement ;
- de conservation ;
- de recherche/communication ;
- de surveillance et de migration des supports ;
- de duplication ou réplication des archives sur des sites distants ;
- de migration des formats de fichiers ;
- de destruction ;
- la bonne tenue des journaux.

Ils assurent le «reporting» de l'activité et fournissent les indicateurs qualité.

Ils peuvent être aidés par une automatisation d'une partie des tâches :

- automatisation de la production des métadonnées sur la base des profils d'archivage définis ;
- identification et contrôle des formats ;
- contrôle des conversions et des formats ;
- contrôle de la complétude des éléments du dossier d'archive ;
- gestion des empreintes ou des signatures.

La **direction informatique** apporte son support technique pour toutes les opérations impliquant le système d'information.

Les **prestataires de services** sont des acteurs externes pouvant être impliqués selon l'architecture et la composition du SAE. La qualité des services rendus, leur conformité aux règles de fonctionnement et leur respect de la charte d'archivage devront être supervisés par les responsables de chaque domaine concerné.

Le **tiers-archiveur** offre *a minima* les fonctionnalités du service d'archivage, à savoir : réception des dépôts, conservation, communication, destruction ou restitution. Les conditions de réalisation de ces services doivent être définies dans un contrat de services conforme aux recommandations de la norme.

D'autres prestataires peuvent intervenir. Les fournisseurs de marques de temps (tiers horodateur) doivent respecter les clauses de leur contrat de services dans la conformité aux recommandations de la norme.

d) Maintien en Condition Opérationnelle du SAE

La **direction informatique** ou le **tiers-archiveur** assure la maintenance du SAE et est en charge de la veille technologique sur ses composants et les supports.

La **direction qualité** surveille la bonne exécution des processus et organise les audits et les certifications.

Les interventions des **auditeurs** permettent de vérifier la conformité du SAE aux spécifications initiales et le respect des procédures dans le fonctionnement permanent du système. Rappelons que la norme préconise un audit régulier avec une périodicité minimale d'un an. Les auditeurs doivent appartenir à une entité indépendante des services utilisateurs et des exploitants. L'audit sera réalisé sur la base d'un référentiel défini sous le contrôle du **responsable gestion documentaire et archivage** ou d'après une procédure de certification choisie par le responsable du SAE.

Les **directions supports** et les **directions opérationnelles** en collaboration avec le responsable gestion documentaire et archivage assurent la veille sur les textes permettant la définition des contraintes et des tableaux de conservation.

3 FAQ

Tableau 3

N°	Questions	Réponses
1	Suffit-il de donner la documentation technique fournisseur du système de stockage pour répondre aux exigences de la norme ?	Non, car le périmètre de la norme ne se réduit pas au seul choix du système de stockage.
2	Les exigences de la norme sont-elles identiques pour les Worm physiques et les Worm logiques ?	Non.
3	Les exigences de la norme sont-elles identiques pour les Worm logiques et les supports réinscriptibles ?	Oui.

Tableau 3 (suite)

N°	Questions	Réponses
4	À quoi servent les conventions de preuve en matière de documents électroniques ?	En l'absence de dispositions légales expressément applicables à la conservation électronique de documents ou de jurisprudence sur l'applicabilité du régime juridique des copies de document à la conservation électronique, il est possible de recourir à des conventions de preuve pour faciliter la preuve et les échanges. Une convention de preuve permet aux parties de décider contractuellement d'accepter certains modes de preuve et de reconnaître la valeur probatoire des écrits électroniques qu'elles échangent et par là même les modalités de conservation de ces actes pour leur attribuer une force probante. NOTE La valeur de ces conventions peut être cependant soumise à l'appréciation du Juge qui est chargé par la Loi de régler les conflits de preuve littérale.
5	Qu'est-ce qu'un original ?	D'un point de vue juridique un document original est celui qui émane directement de son auteur, et qui peut lui être attribué de façon certaine.
6	Comment un document qui n'est pas un acte authentique au sens juridique peut néanmoins présenter un caractère d'authenticité ? Définition de l'authenticité — hors «qualité de l'acte reçu par un OPM» : qualité d'un écrit qui émane réellement de l'auteur auquel on l'attribue	L'authenticité est définie par la norme ISO 15489 comme le caractère d'un document dont on peut prouver : — qu'il est bien ce qu'il prétend être : mauvaise formulation : un document ne peut prétendre être quelque chose. Remplacer par «… dont on peut prouver qu'il est bien ce qu'il est réputé être» ; — qu'il a été effectivement produit ou reçu, par la personne qui prétend l'avoir produit ou reçu, et — qu'il a bien été produit ou reçu au moment où il est déclaré l'avoir été. Ainsi, du point de vue archivistique, un écrit (acte sous seing privé, simple courrier voire copie) peut présenter un caractère d'authenticité. Pour éviter toute confusion, il est préférable de parler de l'authenticité des documents archivés que de documents ou d'archives authentiques. La notion «*d'acte authentique*» est réservée aux documents établis et signés par un officier public et ministériel.
7	Peut-on stocker les informations de traçabilité dans un même journal qu'il s'agisse des évènements systèmes ou du cycle de vie des archives ?	Oui, à condition de respecter le contenu requis pour chacun des journaux et de disposer d'un outil présentant une vue propre à chacun.
8	Que faire lorsque les sous-systèmes produisent leurs propres journaux (ex : systèmes de capture) ?	Oui, à condition de respecter le contenu requis pour chacun des journaux et de disposer d'un outil de réconciliation permettant d'avoir une vue par type de journal.

Tableau 3 (suite)

N°	Questions	Réponses
9	Quel intérêt présente l'archivage des empreintes ?	L'empreinte d'un document permet de garantir l'intégrité de celui-ci. La taille d'une empreinte étant d'un volume de quelques dizaines d'octets, sa conservation est donc très économique.
10	Est-il suffisant de conserver uniquement les empreintes ?	Non. Il faut aussi conserver les documents pour pouvoir exploiter leur contenu.
11	Quelles sont les particularités des droits d'accès pour l'archivage ?	Les droits d'accès d'un document peuvent varier dans le temps. Ainsi un document peut être considéré comme confidentiel lors de sa création, et perdre ce caractère au bout de quelques années (exemple : projet de fusion d'entreprises). Les droits d'accès sont personnels (nominatifs) ou attribués par fonction, activité, etc. Deux aspects sont à considérer : — l'historique des droits d'accès (qui a eu le droit d'accéder à l'information tout au long de son cycle de vie) ; — l'historique des accès. Cette «traçabilité» peut constituer un élément de preuve (qui a eu accès à l'information et quand). Les modalités de définition et de gestion des droits peuvent aussi varier au court du temps. Ainsi pour les archives patrimoniales, les droits sont d'abord donnés à des personnes ou des groupes à travers des profils, bases de connaissances, puis par les règles de communicabilité définies dans la loi et le code du patrimoine pour la conservation au titre des archives historiques.
12	Que faut-il entendre par traçabilité du cycle de vie de l'archive ?	C'est une qualité du système ou de l'application permettant de suivre les évolutions fonctionnelles ou techniques au cours du cycle de vie du document et montrant le respect des caractéristiques exigées pour le SAE. Elle repose sur la possibilité de suivre les évènements intervenus sur une archive depuis sa création jusqu'à la fin de son cycle de vie. L'identifiant unique de l'archive en est un élément clé dont la maîtrise doit être assurée sur tout le cycle de vie.
13	Quelle relation entre traçabilité et horodatage ?	L'horodatage contribue à la traçabilité en permettant d'établir la chronologie précise des évènements tracés.

Tableau 3 (suite)

N°	Questions	Réponses
14	Peut-on archiver des documents signés électroniquement ?	Oui. Selon les clauses de services ou de la PA, il peut être nécessaire de vérifier la validité de la signature et d'assurer la traçabilité de ce contrôle.
15	Le certificat de signature utilisé pour un original numérique arrive à expiration dans 2 mois, alors que mon document doit être archivé pendant 10 ans. Comment démontrer la valider du document dans 9 ans par exemple.	D'une manière générale, pour démontrer qu'une signature électronique est valide, il est nécessaire de pouvoir établir que cette signature électronique a été effectuée à la fois : — avant la date de fin de validité du certificat du signataire ; — avant la révocation du certificat du signataire ou de tout autre certificat du chemin de certification. Pour pouvoir vérifier la validité de la signature dans 9 ans, il faudrait conserver le contexte complet de la signature au moment de la signature (chaînes de certificats, listes de révocations etc.). Ce qui peut rapidement être très couteux. En pratique il est recommandé de vérifier la validité de la signature au moment du versement et d'archiver l'attestation de cette vérification.
16	Peut-on archiver des documents chiffrés ?	Oui, mais la gestion à long terme des codes de déchiffrement présente un risque majeur.
17	Que doit-on faire en cas de non-conformité d'un versement à l'entrée du SAE ?	La réponse doit être contenue dans la PA.
18	Les attestations électroniques de prise en compte initiale d'un dépôt qui doivent être produites et enregistrées dans le journal de cycle de vie des archives sont-elles nécessairement liées à un acte signé électroniquement ?	Non. Il peut tout simplement s'agir d'une trace mise en œuvre par le SAE mentionnant obligatoirement l'empreinte du document déposé et son adresse logique de stockage indépendante du ou des lieux de stockage (voir norme NF Z 42-013 § 9)
19	Comment procéder à l'archivage des données applicatives issues de bases de données ?	Afin d'assurer leur intelligibilité dans le temps, il est recommandé de produire des documents contenant les données au moment de leur extraction ainsi que toutes les informations permettant de les interpréter (description, nature, type, etc.). Ce sont ces documents qu'il conviendra alors d'archiver en respectant les principes de la norme.
20	Distinction entre archivage et sauvegarde.	L'archivage et la sauvegarde ont des finalités différentes. L'archivage est défini au § 3.1 de la norme. La sauvegarde est une procédure d'exploitation qui permet une reconstruction du système ou des données en cas d'incident ou d'erreur. Par essence la sauvegarde ne peut porter que sur une période limitée.

Tableau 3 (suite)

N°	Questions	Réponses
21	Peut-on détruire des originaux après numérisation ?	Remarque préalable sur la terminologie : le texte de la norme utilise deux termes : — original à qui peut être associé un sens juridique; mais en fait la norme emploie ce terme d'une part pour fixer la référence de fidélité du document numérique et d'autre part pour exprimer le fait qu'il s'agit des documents qui sont initialement sur support analogique ; — document d'origine qui amène à situer un document dans un processus, dans son contexte de création avant qu'il fasse l'objet d'une numérisation (sans préjuger à ce stade de sa qualification et de sa valeur). Ces deux termes, au sens de la mise en œuvre de la norme, doivent être considérés avec la même signification. On parle naturellement de documents d'origine dont la forme est matérielle (papier et autre formes). Ne sont pas concernés les documents nativement numériques. **1. Problématique de la destruction des documents originaux après leur numérisation** La problématique de la destruction de documents après leur numérisation, au-delà des considérations d'ordre réglementaire, contractuel, légal, donc juridique au sens large, renvoie essentiellement à des questions d'ordre économique pour éviter le «double archivage» et donc réduire les coûts associés. La réponse à cette problématique doit être élaborée dans un contexte d'appréciation des risques. Plusieurs pays ont adapté leurs réglementations pour autoriser et encadrer la destruction : notamment la Belgique, le Luxembourg et le Canada. En France, il est clair qu'une copie numérique d'un document créé sous forme analogique n'a qu'une valeur de copie et n'acquiert de ce fait pas la valeur de preuve que possède le document original. Par conséquent, si on souhaite détruire des documents et dossiers après leur numérisation, il convient de mener une étude juridique afin de déterminer lesquels de ces documents ont une valeur de preuve.

Tableau 3 (suite)

N°	Questions	Réponses
		À titre d'exemple on peut noter que dans le cas des dossiers de titres de séjour numérisés dans les préfectures, le seul document à forte valeur de preuve qui emporte la responsabilité de l'administration est le formulaire CERFA sur lequel se trouve la décision de l'administration. À l'inverse les autres pièces du dossier qui, à l'origine, n'étaient que des copies (justificatifs divers fournis par l'intéressé) peuvent faire l'objet d'une destruction, une fois la numérisation effectuée et la preuve que l'opération de numérisation a été bien conduite. À ce sujet, il est intéressant de consulter l'instruction de la direction des Archives de France DITN/DPACI/RES/2005/001 en date du 14 janvier 2005, relative aux modalités de délivrance du visa d'élimination des documents papier transférés sur support numérique ou micrographique (http://www.archivesdefrance.culture.gouv.fr/static/1049). En France, plusieurs actions ont été faites pour faire évoluer la réglementation, sans succès jusqu'à ce jour (on notera le rapport établi par le Forum des Droits sur l'Internet en décembre 2005 sur l'archivage électronique). Le point de départ de l'analyse des possibilités de destruction de documents après leur numérisation est de considérer que la numérisation est une opération qui consiste à créer une copie sous forme numérique. À partir de là, deux orientations peuvent être envisagées : — la création par numérisation d'une copie numérique dont les caractéristiques de création lui confèrent la valeur légale de copie ; — la création d'un document pouvant être qualifié de nouvel original sous forme numérique (procédé qui nécessite l'intervention de tiers habilités).

Tableau 3 (suite)

N°	Questions	Réponses
		Cas N°1 : Création d'une copie numérique dotée d'une «valeur légale» La possibilité de créer des copies numériques à «valeur légale» et donc de pouvoir, à risques limités détruire les originaux doit être traitée en trois étapes : **1re étape :** détermination de la valeur des documents qui seront numérisés et que l'on envisage ensuite de détruire ; de cette détermination de la valeur des documents (en pratique par l'identification des textes auxquels se rattachent les documents (Code Civil, Code Général des Impôts, Code de Commerce, Code des Assurances, etc.) on en déduit la valeur des copies ; à titre d'illustration : — la copie numérique d'une facture (fournisseur) reçue sous forme papier n'a, du point de vue fiscal, aucune valeur ; — la copie numérique d'un contrat a une valeur de copie mais les conditions dans lesquelles sa numérisation a été effectuée peut lui donner les caractéristiques de copie fidèle et durable ; — la copie numérique d'un courrier reçu d'un client peut avoir la même valeur que le document d'origine si le document reçu est lui-même une copie. En revanche, la copie n'a qu'une valeur de copie si le document reçu était un original. Cette étape est habituellement réalisée par des services juridiques. **2e étape :** appréciation du risque de destruction, c'est-à-dire la qualification du risque (financier, fiscal, social, etc.) et son évaluation (valeur financière, valeur commerciale, image, etc.). Dans de nombreux cas, le risque est nul, soit parce que le document n'a pas de valeur réglementaire soit qu'il est déjà une copie ; dans la plupart des situations, le risque est faible étant entendu que la majorité des situations rencontrées relèvent, en cas de contentieux, de réglementations dans lesquelles la preuve est libre. Cette étape, rarement effectuée, doit être réalisée par des professionnels compétents : direction des risques (si elle existe), audit, contrôle de gestion, organisation.

Tableau 3 (suite)

N°	Questions	Réponses
		3e étape : mise en œuvre des méthodes, organisation, procédures et solutions techniques visant à garantir la qualité des copies numériques : — fidélité par rapport au document d'origine ; — durabilité de la conservation, de la lisibilité et de l'intelligibilité ; — justification de l'ensemble des opérations de toutes natures depuis la numérisation jusqu'à la destruction de la copie numérique. Cette étape est réalisée par les entités qui sont chargées de concevoir et de mettre en œuvre les solutions de numérisation et de décrire les processus de numérisation que ce soit pour le stock ou pour le flux. La norme NF Z 42-013 comprend les spécifications qui, si elles sont mises en œuvre, vont apporter les garanties ci-dessus sur les différentes étapes des processus de numérisation, d'enregistrement des documents numériques, de gestion des systèmes d'archivage électronique : — préparation des documents ; — contrôle des dispositifs de numérisation ; — organisation et réalisation de la numérisation : procédures, contrôles ; — choix des formats et des supports ; — traçabilité des opérations. **Cas N°2 : Création d'un nouvel «original électronique»** **a) Cas des originaux sous forme papier** L'un des objectifs de la norme a pour objet de garantir qu'un fichier archivé sur un support numérique, et résultant de la conversion par numérisation d'un document sur support papier, aura la même valeur que le document papier d'origine lors de sa restitution sur un support papier depuis son support électronique. Pour aboutir à cette finalité, il est indispensable d'être certain, et de le certifier, qu'après numérisation du document original «papier», le fichier numérique produit, est totalement fidèle au document original papier et qu'il en est l'exacte réplique sur support électronique. Mais quelle est la nature de ce fichier sur support électronique ?

Tableau 3 (suite)

N°	Questions	Réponses
		La première fonction d'un original étant d'être un document unique, si l'original sur support papier n'est pas détruit, après sa conversion sur support électronique, le fichier produit et archivé sur support électronique, devenu une «archive sur support électronique», est désormais une «copie conforme de l'original sur support papier». L'original est devenu la source de cette copie conforme. Dans ce cas, si l'original papier a été perdu, la preuve de son existence sera rapportée par la présentation de cette copie conforme, reproduction fidèle et durable (Art.1316/1334/1348 du Code Civil). Si une destruction de l'original sur support papier a été effectuée, après sa conversion sur support électronique, le fichier produit, et qui va être conservé sur support électronique, est considéré comme «établi» pour la première fois sur support électronique : il devient un original électronique conformément aux dispositions de l'article 1316 du Code Civil. Mais se pose la question de l'origine du nouveau document, c'est-à-dire de l'identification de son auteur. Selon l'article 1316-4 alinéa 1 du Code Civil, l'auteur qui a apposé sa signature manuscrite sur l'original sur support papier, est dûment identifié. Il résulte des dispositions de la Loi du 13 mars 2000, que le document produit sur support électronique soit signé numériquement par son auteur, puis qu'il soit conservé pour préserver l'intégrité de son contenu informationnel. Est-ce que cela sous-entend que l'auteur du document en garde la «maîtrise» jusqu'à son versement en archivage, et qu'il doive produire une copie sous sa signature numérique, copie destinée à devenir le nouvel original après destruction du document papier ? Probablement, si l'on raisonne par analogie avec la prescription normative relative au «document nativement électronique». L'original papier ayant été détruit, la partie qui devra prouver l'existence d'un document original, présentera un document dont la nature ne sera pas une copie/reproduction fidèle mais durable, au sens de l'article 1348 du Code Civil mais un «nouvel» original : un original sur support électronique. Dans ce cas, il est indispensable de prendre acte de la destruction de l'original et de la certifier.

Tableau 3 (suite)

N°	Questions	Réponses
		Il faut ajouter au fichier numérique produit lors de la conversion, des métadonnées au format XML exprimant cette certification de destruction du «document papier mère». L'ensemble, encapsulé, doit être horodaté et signé numériquement par un tiers de confiance (entité légitime, pérenne et neutre), pour pouvoir être admis à fin probante devant un Juge, dans le cadre d'un procès. Cette entité pourrait être notamment un officier public et ministériel. L'écrit électronique ne valant preuve qu'à condition que son auteur puisse être dûment identifié, il faudra également que le tiers de confiance certifie l'identité de l'auteur du «document papier mère» en attestant avoir vérifié la validité du certificat du signataire de l'original électronique. Ce processus peut paraître lourd, mais il n'est pas envisageable de laisser «traîner» plusieurs documents susceptibles d'être présentés comme un original, quel que soit son support. On peut rétorquer, qu'en cas de confrontation entre deux documents, l'un sur support électronique, l'autre sur support papier, il suffira de lancer une comparaison entre eux. Dans ce cas, et si la comparaison est «matchée», il n'y aura certes pas de difficulté(s). Mais que se passera-t-il en cas de dissemblance(s) entre les deux documents ? Faudrait-il — logiquement — donner foi au document «papier» ayant fondé le document sur support électronique, et aller à l'encontre du principe de non-discrimination entre les différents supports ? La logique ne suffira pas au Juge. C'est pourquoi il faut préconiser ce qui suit : Après conversion du document original sur support papier, il faut ajouter au fichier numérique produit lors de la conversion, des métadonnées au format XML exprimant qu'il est une simple réplique du «document papier mère». L'ensemble, encapsulé, doit être signé numériquement par un tiers de confiance habilité.

Tableau 3 (suite)

N°	Questions	Réponses
		S'il est restitué pour pouvoir être produit devant un Juge, dans le cadre d'un procès, il sera identifié comme «réplique numérique» : Dans ce cas, le Juge, informé, aura le choix de le prendre en compte, ou d'exiger la présentation de l'original sur support papier. **b) Cas des documents nativement électroniques :** La norme a pour objet de permettre qu'un fichier archivé sur un support numérique, et provenant de la transmission chez l'archiveur d'un document produit nativement sur un support électronique, ait la même valeur que le document numérique d'origine lors de sa restitution sur un support papier depuis son support électronique d'archivage ou sur un support électronique depuis son support électronique d'archivage. Quelle est la nature de ce fichier archivé sur support électronique ? Si une destruction de l'original sur support électronique a été effectuée, après sa transmission pour archivage externalisé sur support électronique, le fichier archivé sur support électronique devient l'unique original. Il est indispensable de prendre acte de la destruction de l'original et de la certifier. Le «propriétaire» de l'original conçu nativement sur support électronique, ne doit plus être en mesure — dans l'avenir — d'exhiber et de présenter ce document — auquel il aurait pu apporter des modifications après sa transmission pour archivage — comme l'original. Il faut ajouter au fichier numérique produit lors de l'entrée en archivage, des métadonnées au format XML exprimant la certification de destruction du «document électronique mère». L'ensemble, encapsulé, doit être signé numériquement par une autorité habilitée pour pouvoir être admis à fin probante devant un Juge, dans le cadre d'un procès. S'il est restitué sur support papier pour pouvoir être produit devant un Juge, dans le cadre d'un procès, il sera identifié comme «réplique papier» : Dans ce cas, le Juge, informé, aura le choix de le prendre en compte, ou d'exiger la transmission de l'original archivé sur support électronique.

4 Acronymes

DDTS : Dossier de Description Technique du Système

MCO : Maintien en Condition Opérationnelle

MCD : Modèle Conceptuelle des Données

PA : Politique d'Archivage

RAID : Redondant Array of Independant Disc

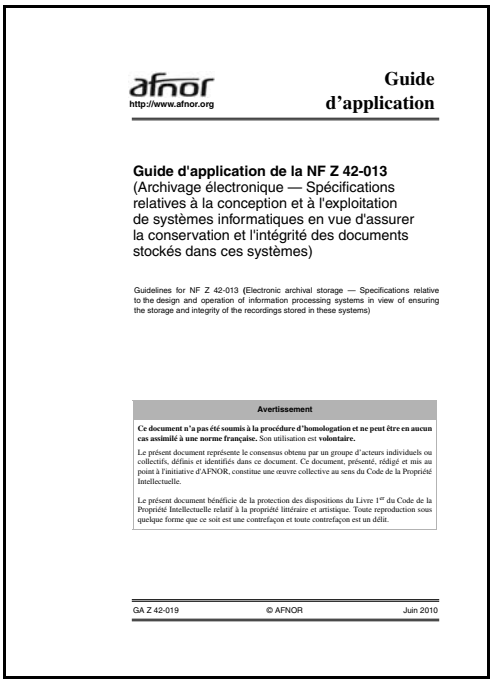
UDO : Ultra Density Optical

RH : Service des Ressources Humaines

R&D : Recherche et Développement

RPI : Responsable de la Propriété Industrielle

RSSI : Responsable de la Sécurité des Systèmes d'Information



afnor
http://www.afnor.org

Guide
d'application

Guide d'application de la NF Z 42-013
(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)

Guidelines for NF Z 42-013 (Electronic archival storage — Specifications relative to the design and operation of information processing systems in view of ensuring the storage and integrity of the recordings stored in these systems)

Avertissement

Ce document n'a pas été soumis à la procédure d'homologation et ne peut être en aucun cas assimilé à une norme française. Son utilisation est **volontaire.**

Le présent document représente le consensus obtenu par un groupe d'acteurs individuels ou collectifs, définis et identifiés dans ce document. Ce document, présenté, rédigé et mis au point à l'initiative d'AFNOR, constitue une œuvre collective au sens du Code de la Propriété Intellectuelle.

Le présent document bénéficie de la protection des dispositions du Livre 1er du Code de la Propriété Intellectuelle relatif à la propriété littéraire et artistique. Toute reproduction sous quelque forme que ce soit est une contrefaçon et toute contrefaçon est un délit.

GA Z 42-019 © AFNOR Juin 2010

Le présent document propose des méthodes de référence pour garantir que le document archivé garde la même valeur que le document d'origine, en conservant son intégrité et en assurant sa pérennité.

Mots-clés traitement de l'information, imagerie électronique, stockage de documents, archivage de données, enregistrement de données, support de données, disque optique, numérisation, image, fichier, format, choix, garantie, protection de l'information, contrôle de qualité, audit de qualité, droit de la preuve, cycle de vie.

FA167048 ISSN 0335-3931

ICS : 01.140.20 ; 35.240.30