SAEM X

Politique de service d’archivage électronique

HISTORIQUE DES VERSIONS

Ver.	Description	Date	Rédacteur	Validation
1.0	Version initiale	23 avril 2013	Jean-Marc Rietsch	

REVUE DU DOCUMENT

Nom	Société	Chapitre(s)

APPROBATION DU DOCUMENT

Nom	Rôle	Signature

DOCUMENTS DE REFERENCE

Origine	Titre	Référence
ISO 14721	Système ouvert d'archivage d'information (OAIS)	
ANSSI	Politique et pratique d'archivage	

ction

PLAN

Cet avertissement semble inapproprié à une structure publique (?)

AVERTISSEMENT

La présente Politique est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive du SAEM X. La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par l'organisme X ou ses ayants droits, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'article L.122-5, d'une part, que « *les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collectiv*e » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « *toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite* » (article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

1. OBJET ET IDENTIFICATION DU DOCUMENT (à relire pour validation GP, peut passer en point 2)

1.1 Objet de la politique de service d'archivage

Ce document présente la Politique de Service d'Archivage destinée à décrire le service d'archivage électronique du SAEM* X mis à la disposition des entités utilisatrices afin de répondre à leur besoin en matière d'archivage de données/documents numériques.

**Système d'Archivage Électronique Mutualisé*

La présente politique de service d'archivage énonce les règles et pratiques sur lesquelles est fondée le service d'archivage. Elle précise l'ensemble des éléments participant à la mise en œuvre des processus d'archivage, permettant d'assurer qu'un document a été convenablement intégré, contrôlé, conservé, géré, consulté tout au long de son cycle de vie. Elle constitue le fondement du système d'archivage électronique et permettra d'apporter devant le juge, la preuve de la fiabilité et de la sécurité du procédé mis en œuvre au sein du SAE, conformément aux exigences légales issues notamment de la loi du 13 mars 2000 et de l'ordonnance n° 2005-1516 du 8 décembre 2005 .

Quel que soit le type de document archivé, la politique de service d'archivage permet également de définir :

1. les différents intervenants, leurs rôles respectifs et leurs obligations ;
2. les niveaux de sécurité identifiés en matière de : disponibilité, intégrité, confidentialité, traçabilité ;
3. les prestations attendues : niveaux de service.

Elle constitue le lien indispensable entre des bases purement techniques et organisationnelles caractérisant le SAE et les éléments juridiques et réglementaires voire les exigences propres, auxquels est soumise chaque collectivité utilisatrice du système -Il en résulte que la présente politique de service d'archivage, définie et validée par les instances de direction du SAEM X, doit être compatible avec les politiques d'archivage définies et validées par chaque CT utilisatrice .

2

2.1 Identification de la Politique de service d'archivage

La désignation du numéro d'identification d'objet (OID) pour la présente Politique est : 1.2.250.1.xxx.1.1.1.1.1

Le numéro d'OID de ce document répond aux principes de nommage suivants :

- ISO (1)
- member-body (2)
- fr (250)
- type-org (1)
- SAEM X
- service de confiance (1)
- département X (1)
- politique de service d'archivage (1)
- politique de service d'archivage du département X (1)
- version (1)

Dans l'hypothèse de modifications ultérieures sur ce document, le numéro d'OID sera modifié pour sa dernière valeur « Version »

2.2 Référentiel documentaire

Le service d'archivage repose sur un référentiel documentaire composé de :

- la Politique de Service d'Archivage (PSA), objet du présent document ;
- la Déclaration des Pratiques d'Archivage (DPA) qui vise à définir comment l'OA s'organise pour répondre aux objectifs et engagements de la PSA ainsi qu'à identifier les moyens mis en œuvre pour cela sous forme de spécifications techniques ;
- les Modalités de Mise en Œuvre Opérationnelles (MOO) qui complètent la DPA en ce qui concerne les procédures opérationnelles.
- le règlement de service d'utilisation du SAEM X applicable aux usagers

De façon générale, d'autres documents (voir schéma ci-dessous) sont également à prévoir afin de compléter le dispositif précisant les relations entre le SAEM X et ses clients, à savoir :

- La convention cadre de prestation de service précisant les conditions générales des relations entre le SAEM X et ses entités utilisatrices.
- Le cas échéant, le contrat de service où l'on retrouve en particulier :
  - les conditions de mise en œuvre de la PSA, plus précisément la définition des règles de versement et d'interrogation ;
  - les conditions de réversibilité ;
  - les niveaux de service proposés et tels qu'attendus par les entités utilisatrices du SAEM X.

•

2. CONTEXTE ET ~~,~~ ENJEUX (à relire pour validation GP, peut passer en point 1)

3.1 Contexte ~~global~~

L'actuelle « révolution numérique » depuis les dernières décennies du XXème siècle bouleverse les modes de pensée et de communication, les échanges ainsi que les méthodes de travail.
Désormais, les systèmes d'information (ou systèmes informatiques?) supportent la majorité du capital informationnel des entités publiques ou privées, sans que, dans le même temps, les utilisateurs disposent de règles et procédures adaptées leur permettant de bien gérer et hiérarchiser ce patrimoine essentiel.
Parallèlement, la généralisation des échanges dématérialisés génère une volumétrie exponentielle des données d'activité et implique un transfert de la preuve de l'écrit papier vers le numérique. Or, sans précautions spécifiques, sa valeur probatoire est fragile (falsifiable sans traces) et il est complexe d'assurer sa conservation durable avec des technologies elles-mêmes frappées d'obsolescence rapide.
L'administration est légalement tenue d'assurer la bonne conservation de tout écrit papier ou numérique lié à l'exécution des missions de service public, pour des durées conformes aux besoins :
opérationnels (assurer le service aux usagers)
juridiques (garantir les droits des personnes et de l'institution)
historiques (répondre à la finalité patrimoniale et démocratique légale pour l'utilité de l'histoire et de la science)

Elle doit donc disposer d'un « système d'archivage électronique » (SAE) sécurisé permettant de garantir la confidentialité, l'intégrité, l'accessibilité et la lisibilité des données / documents numériques.
L'archivage électronique consiste à conserver des données/documents numériques structurées, semi-structurés ou non structurés dans le but de pouvoir les interroger et les restituer à court, moyen ou long terme. Il doit garantir la valeur juridique des documents / données jusqu'au terme du délai durant lequel des droits y afférant peuvent exister et doit en outre assurer la conservation pérenne sans limitation dans le temps des documents/ données présentant un intérêt patrimonial.

La Région aquitaine, le Département de la Gironde, la Cub et la Ville de Bordeaux ont décidé d'unir leurs efforts dans un souci d'optimisation de l'ingénierie et de rationalisation des coûts, en mutualisant leur service d'opérateur d'archivage électronique, via le SAEM X qui pourra à terme accueillir les archives électroniques d'autres entités publiques.

~~Dans le cadre d'un futur déménagement des services et à l'initiative du Directeur général des services, le Conseil général de la Gironde a engagé en 2006 une opération qui avait pour premier objectif de traiter les archives papier et d'identifier les arriérés qui s'étaient accumulés depuis plus de vingt ans.~~

Conduite par la Direction des Archives départementales, cette opération, qui a abouti au traitement de quelques 4 kilomètres linéaires d'archives stagnantes, a aussi permis de mettre en place une organisation de l'archivage qui s'appuie sur :

- un groupe projet présidé par le Directeur général des services
- un réseau hiérarchisé de référents archives dans chacun des services du Conseil général
- des tableaux de gestion des documents élaborés conjointement par les Archives départementales et les services
- des procédures écrites
- des outils normalisés mis à disposition des référents archives et des agents
- des actions de sensibilisation et de formation
- une cellule Archives, antenne délocalisée des Archives départementales sur le site principal du Conseil général, qui fonde ses interventions sur les principes du *records management1* et plus particulièrement de l'ILM (*Information Lifecycle Management* ou gestion du cycle de vie de l'information).

Par ailleurs, l'année 2008 a vu le lancement de l'élaboration du schéma directeur du système d'information du Conseil général. Sa préparation a été découpée en 7 programmes, dont un portait sur le « Cycle de vie de l'information numérique ».
Ce programme, dont la direction avait été confiée à un conservateur des Archives départementales accompagné d'un chef de projet ingénieur Etudes de la Direction du système d'information, a été validé fin 2009. Le « cycle de vie de l'information numérique » constitue dorénavant un domaine socle du Schéma Directeur de l'Administration Electronique (SDAE) pour une période de cinq ans jusqu'en 2013 ; il est suivi par différentes instances dont le comité stratégique *ad hoc*.
C'est dans ce contexte que le Conseil général souhaite aujourd'hui déterminer sa politique d'archivage.

L'archivage électronique consiste à conserver des données/documents numériques dans le but de pouvoir les interroger et les restituer dans le temps. Ces données/documents peuvent être structurés, semi structurés ou non structurés. La conservation peut être à moyen ou long terme et doit être sécurisée.

3.2 Enjeux

Les principaux enjeux de l'archivage pour les administrations sont :

1/ Stratégique, organisationnel et financier : en s'appuyant sur des référentiels et bonnes pratiques, l'archivage permet l' optimisation des données de leur création à leur destruction ;
- du coût de gestion du patrimoine informationnel (tri et hiérarchisation des informations),
- du partage, de l'exploitation et de la réutilisation des données tant en interne que vis-à-vis des tiers (administrés, fournisseurs...)
- de la traçabilité preuve de la fiabilité et de l'intégrité des documents (conservation de la valeur probatoire pour la défense des droits des personnes et de l'administration).

2/ Légaux et réglementaires (compliance): les autorités administratives sont tenues de se conformer aux textes applicables à la production, la gestion, la communication, la conservation des archive publiques.
Notamment, les administrations ont le devoir démocratique de garantir une conservation fiable, pour l'éternité, des données d'utilité historique et scientifique.
Ceci implique
que chaque autorité administrative évalue, en amont de l'archivage, l'éventail des sensibilités/utilités (criticité) des données qu'elle aura à archiver et arbitre ensuite sur les moyens de conservation correspondants à mettre en œuvre qui devront être compatibles avec la politique de service d'archivage et intégrés dans sa propre politique d'archivage et sa politique de sécurité,

3/ Technique : la mise en place d'un SAE sécurisé est complexe puisqu'elle doit répondre au paradoxe de devoir conserver sur de longues périodes des données/documents en s'appuyant sur des technologies à l'obsolescence rapide ;

4/ Valorisation de l'image : organiser la bonne conservation du capital informationnel immatériel lié aux missions de service public permet de développer la communication de l'institution

~~Les principaux enjeux de l'archivage sont :~~

- ~~Stratégique : savoir ce qui est à archiver, les modalités d'archivage et créer de la valeur à partir de l'exploitation de la base d'archives pour les clients de l'organisme X. La politique d'archivage est définie et validée par les instances de direction de l'organisme X ;~~
- ~~Légaux et réglementaires : prendre en compte les obligations en matière de lois et de règlementation. La politique d'archivage s'accompagne d'une analyse de risques et d'arbitrages en fonction des différents types de données identifiés et leur sensibilité (criticité) ;~~
- ~~Technique : répondre au paradoxe de devoir conserver sur de longues périodes des données/documents en s'appuyant sur des technologies à l'obsolescence rapide ;~~
- ~~Organisationnel et financier : optimiser la gestion des données/documents de leur création à leur destruction. Le système d'archivage doit rendre l'information traçable, intègre et sécurisée en s'appuyant sur des référentiels et bonnes pratiques ;~~

~~Scientifique et historique : organiser la conservation du capital immatériel des clients de l'organisme X.~~

3. CHAMPS D'APPLICATION, PERIMETRE

Le périmètre des données/documents concernés par la présente Politique de service d'archivage correspond uniquement aux archives transmises par chaque entité utilisatrice du SAEM X.

Nous rappelons les définitions :

Selon l'article L. 211-1 du Livre II du Code du patrimoine : « Les archives sont l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale, et par tout service ou organisme public ou privé, dans l'exercice de leur activité ».

Archives courantes (Code du Patrimoine, R.212-10) :

  - « Sont considérés comme archives courantes les documents qui sont d'utilisation habituelle pour l'activité des services, établissements et organismes qui les ont produits ou reçus ».
- Archives intermédiaires (Code du Patrimoine, R.212-11) : « Sont considérés comme archives intermédiaires les documents qui :
  - Ont cessé d'être considérés comme archives courantes ;
  - Ne peuvent encore, en raison de leur intérêt administratif, faire l'objet de tri et d'élimination… ».
- Archives définitives (Code du Patrimoine, R.212-12) : « Sont considérés comme archives définitives les documents qui ont subi les tris et éliminations […] et qui sont à conserver sans limitation de durée ».

4. CADRE LEGISLATIF, REGLEMENTAIRE ET NORMATIF (annexes à relire pour validation GP)

L'archivage obéit à un cumul de réglementations qui se superposent. Elles sont reprises en annexe 1.

La norme technique permet de représenter un état de l'art dans le domaine auquel elle se rapporte (Cass. Civ. 3ème ch. du 4 février 1976, Bull. civ. III, n°49). Les principales normes ayant servi de base à la présente politique sont listées en annexe 2.

5. INTERVENANTS

Ce chapitre présente et précise les intervenants du système d'archivage électronique et leurs responsabilités dans l'application de la PSA, le cas échéant.

5.1 Définition des intervenants et obligations respectives

La production d'une archive, son versement et sa gestion s'organisent autour d'une chaîne d'intervenants dont les caractéristiques sont décrites ci-après.

5.1.1 Schéma de principe du fonctionnement d'un service d'archivage

Nous attendons le schéma dans une version modifiable pour le mettre à jour

proposition du GP le 31/05: ajouter dans le schéma, au centre, sous Système d'archivage électronique, une étiquette « Préparation au versement » au-dessus des autres (pour évoquer le rôle de la Ged sas)

5.1.2 **Autorités d'Archivages** (Entités utilisatrices)

5.1.2.1 Définition et responsabilités

L'Autorité d'Archivage (AA) est propriétaire des archives produites et détenues dans le cadre de ses activités et seule responsable de leur bonne gestion et conservation pour la durée de leur cycle de vie.
L'Autorité d'Archivage a également qualité d'Autorité Administrative au sens de l'ordonnance du 8 décembre 2005 relative à « l'e-administration ». A ce titre, elle est responsable du respect des obligations relatives aux décrets constitutifs des RGI RGS, RGAA.

5.1.2.2 Les intervenants

L'autorité d'archivage est constitué des acteurs suivants :

- Service versant : Désigne l'entité qui constitue et verse les objets d'archive ou paquets d'information à verser (PIV), au système d'archivage géré par l'Opérateur d'Archivage.
- Service producteur : Désigne l'entité qui produit ou reçoit les archives dans le cadre de ses activités. Il peut être distinct ou confondu au service versant ;
- Service d'Archive : Désigne l'entité qui prend en charge (enrichit, vérifie et collecte) les SIP, gère (enrichit, conserve ou élimine et administre) les AIP et communique les DIP ; Il est le garant du respect du cycle de vie des informations qui lui sont confiées ;
- Service informatique : Désigne l'entité en charge d'assister les métiers dans les opérations techniques. Il est garant du bon fonctionnement des interfaces entre le SAEM X et les SI de l'AA ;
- Contrôleur : Désigne l'entité mandatée par l'AA qui vérifie la manière dont l'Opérateur d'Archivage s'acquitte de sa mission d'exploitation du système d'archivage dans le respect des exigences de la PSA. A ces contrôles peuvent s'ajouter des missions d'audits spécifiques diligentées par l'AA.
- Utilisateur : Désigne toute entité autorisée par l'AA à consulter les archives (DIP) ou les données descriptives des AIP.

5.1.3 **Opérateur d'Archivage** (SAEM X)

5.1.3.1 Définition et responsabilités

L'Opérateur d'Archivage (OA) est l'entité qui fournit les services, liées au Service d'archivage, demandés et spécifiées par les AAs et à leur bénéfice, opérant dans un cadre contractuel.
Le SAEM X est l'OA prestataire des entités utilisatrices, autorités d'archivage (AA).

L'OA joue un rôle central dans la PSA dans la mesure où :

- Il définit les différents niveaux de sécurité et de service auxquels doit répondre le service d'archivage, ainsi que l'organisation fonctionnelle attendue ;

- Il est chargé de rédiger et de faire évoluer la présente Politique en fonction des évolutions législatives, réglementaires, technologiques ainsi que des besoins fonctionnels exprimés par les utilisateurs/ usagers voire l'évolution de son périmètre ;

L'OA est globalement responsable de la définition, de la gestion et de la bonne application de la PSA et en particulier :

- il est responsable de l'ensemble des prestations (précisées au travers des niveaux de services) rendues par le service d'archivage conformément à la présente PSA dont elle est à l'origine ;
- il s'engage à définir et à maintenir conformément à la PSA des procédures et mesures (précisées dans les niveaux de sécurité), propres à assurer le niveau de sécurité défini. Cette sécurité se décline au travers des différents aspects de la disponibilité, de l'intégrité, de la confidentialité, de la traçabilité et de la pérennité.

La responsabilité de l'opérateur consiste à mettre en œuvre un ensemble de processus autour d'une plate-forme dans le respect des exigences énoncées dans la Politique de service d'archivage et dont les modalités sont détaillées dans la déclaration des pratiques d'archivage (DPA) et la mise en œuvre opérationnelle (MOO).

L'Opérateur d'Archivage :

- est chargé d'appliquer techniquement les fonctionnalités décrites dans la politique de service d'archivage ;
- définit l'organisation opérationnelle et technique destinée à assurer les niveaux de sécurité et de service du système d'archivage tels que définis dans la PSA et les contrats de service ;
- est contrôlé régulièrement par les AAs, afin de vérifier la conformité des traitements et de la mise en œuvre du service d'archivage par rapport aux exigences de la PSA. Il fournit à cet effet toutes les informations nécessaires permettant d'assurer cette vérification.

L'OA est responsable du fonctionnement du service d'archivage conformément aux exigences définies dans la PSA. L'OA est responsable du SAE, de l'élaboration, de la mise à jour et de l'application de la DPA (Déclaration des pratiques d'archivage), des moyens techniques utilisés pour réaliser les fonctions définies dans la PSA ainsi que de la MOO (mise en œuvre opérationnelle), constituée de procédures destinées au Système d'Archivage Electronique.

5.1.3.2 Les intervenants

L'opérateur d'archivage est constitué des acteurs suivants :

- Opérateur : Désigne toute personne autorisée, habilitée à agir sur le système d'archivage pour des opérations d'administration, de maintenance, de sécurité ayant trait soit à une logique purement système.
- Contrôleurs :
- Direction et services supports :
- Comité de suivi PSA :

5.1.4 **Archives départementales**

5.1.4.1 Définition et responsabilités
Les archives départementales, exercent au nom de l'Etat le contrôle scientifique et technique sur les archives publiques courantes, intermédiaires et définitives (code du patrimoine articles L. 212-6 à L.212-14.). Dans ce cadre, elles peuvent procéder à des audits de la politique d'archivage des établissements et des systèmes mis en place et délivrent les visas d'élimination nécessaires avant toute destruction d'archives publiques (cf. code du patrimoine, article R212-14).

5.1.5 **Usagers (acteurs externes)**

5.1.5.1 Définition et responsabilités
Par usagers du SAEM X, on entend toute personne physique ou morale externe aux autorités d'archivage (grand public, chercheurs, utilisateurs d'un service public dématérialisé....).
Les usagers ont vocation à accéder, via une plate-forme de consultation, aux archives électroniques librement communicables, aux instruments de recherche, ou au suivi de dossiers administratifs particuliers les concernant.

5.2 Obligations communes des différents intervenants à relire pour validation GP)

5.2.1 Secret professionnel

L'article L. 211-3 du code du patrimoine, qui s'applique indistinctement aux archives publiques et privées, impose aux agents chargés de la conservation des archives (fonctionnaires, salariés ou autres) de respecter le secret professionnel pour « tout document qui ne peut être légalement mis à la disposition du public ».

Tout manquement est susceptible de donner lieu à des sanctions pénales en vertu des dispositions des articles L. 214-1 du Code du patrimoine, 226-13 et 226-31 du code pénal.

Toute entité intervenant dans le service d'archivage doit respecter ces obligations.

5.2.2 Protection des données personnelles

Chaque intervenant en sa qualité de responsable de traitement de données à caractère personnel au sens de la législation en vigueur s'engage à respecter la législation applicable en matière de traitement de données à caractère personnel.

Pour rappel, le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.

La responsabilité est encourue par le responsable du traitement y compris lorsqu'il recourt à un sous-traitant.

5.2.3 Obligation sur le caractère communicable des Archives

Chaque intervenant s'engage à respecter les règles législatives et réglementaires applicables en matière de communicabilité des documents administratifs et des Archives publiques.
Au sein du SAEM X X, les opérateurs doivent prendre leurs ordres des AAs en ce qui concerne la communication des archives, dès lors que celles-ci n'ont pas le statut « librement communicable », selon des procédures qui seront définies entre les parties dans le/la (quel document?).
Toute demande de consultation d'un usager à l'OA est aussitôt adressée au service versant concerné pour instruction et décision.
En effet le caractère communicable d'une archive se détermine par l'autorité fonctionnelle, conformément à la législation et à la réglementation applicables en la matière (notamment la loi du 17 juillet 1978 modifiée et le Code du patrimoine article L213-1 et L213-2).

~~Dans ce cadre, chaque intervenant s'engage notamment à déterminer et à vérifier, dès lors qu'il a connaissance du contenu de l'Archive, le caractère communicable de celle-ci conformément à la législation et à la réglementation applicables en la matière (notamment la loi du 17 juillet 1978 modifiée et le Code du patrimoine article L213-1 et L213-2).~~

Si une Archive a été à tort définie comme communicable, tout intervenant qui a connaissance de cette erreur, s'engage à en informer sans délai l'Autorité d'Archivage.

5.2.4 Droits sur la propriété intellectuelle et industrielle

Il peut arriver, de façon marginale, que des droits de propriétés intellectuelle et/ou industrielle portent sur des Archives. Dans ce cas, le Versement, le traitement et la gestion des Archives ou Objets d'archives dans le cadre du service d'archivage ne remettent pas en cause les droits de propriété intellectuelle et industrielle sur les Archives conformément aux dispositions législatives et réglementaires applicables en matière d'Archives.

Tous les droits de propriété intellectuelle protégés par la législation ou la réglementation en vigueur sur le territoire français sont respectés.

Dans ce cadre, la responsabilité civile et pénale de celui qui violerait ces droits est susceptible d'être engagée.

5.2.5 Force majeure

La responsabilité des intervenants ne saurait être engagée en cas de force majeure. Sont considérés comme des cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.

5.2.6 Régime juridique des moyens de cryptologie

La confidentialité des Archives et Objets d'archives peut nécessiter le recours à des moyens de cryptologie. Le cas échéant, le service concerné s'oblige au respect du régime juridique applicable en la matière conformément aux articles 29 à 32 de la loi pour la confiance dans l'économie numérique.

6. NIVEAUX DE SECURITE ET DE SERVICE (attente des avancées PSSI + à relire pour validation GP)

6.1 Généralités

La présente Politique concerne les données/documents versés a SAEM X par les entités utilisatricesà l'organisme X par ses clients. Ces données devront être classifiées au préalable en fonction des différents niveaux d'exigences, tels que décrit ci-après en matière de sécurité et de service.

Les niveaux de sécurité précisés devront être validés par la DSI du SAEM Xde l'organisme X afin d'être en parfaite conformité avec la politique de sécurité et aux les objectifs de sécurité poursuivis.

L'OA en charge de la mise en œuvre des fonctions de stockage et de consultation/communication propose des mesures de sécurité techniques ou non pour traiter les risques identifiés en fonction des objectifs de sécurité émis. Le SAEM X L'organisme X est également en charge de mettre en évidence les éventuels risques résiduels subsistant au traitement des risques.

Il revient à l'OA de valider les mesures de sécurité, éventuellement suite à plusieurs révisions, jusqu'à ce qu'elles soient satisfaites.

6.1 Définition des niveaux d'exigence

Pour chaque donnée/document destinés à être archivé, ont été identifiés les différents critères suivants, à renseigner obligatoirement par les services versants et regroupés en :

- Renseignements généraux ;
- Niveaux de service ;
- Niveaux de sécurité.

Une même typologie de données/documents correspondra donc à un ensemble constitué des trois éléments précédents.

6.2.1 Renseignements généraux (à adapter et à compléter)

Format pour les données/documents numériques :

*Afin de garantir la pérennité des données/documents et surtout leur intelligibilité dans le temps, l*e SAEM X accepte les formats de données conformes au RGI, les entités utilisatrices devront fournir les documents et données aux bons formats

~~Afin de garantir la pérennité des données/documents et surtout leur intelligibilité dans le temps, il convient de ne retenir qu'un nombre restreint de formats cibles pour l'archivage. Sont retenus ici les formats précisés par le RGI.~~

Volumétrie :

Le volume de documents versés par chaque collectivité utilisatrice devra être déterminé dans les contrats de prestation de service entre chaque AA et le SAEM X (choix d'une tranche de 1 à 4).

~~*La volumétrie peut être analysée de différentes façons sachant que l'élément essentiel reste l'espace réellement occupé. Il sera néanmoins important pour les AAs de préciser, en particulier des tranches telles que celles indiquées ci-après.*~~

Désignation tranche	***Numéro***
de 0 à 10 Go par mois ou jusqu'à 100.000 documents /mois	*1*
de 10 Go à 100 Go par mois ou jusqu'à 1 million de documents /mois	*2*
de 100 Go à 1 To par mois ou jusqu'à 10 million de documents /mois	*3*
au-delà de 1 To par mois ou au-delà de 10 million de documents /mois	*4*

Durée de conservation :

Les archives versées dans le SAEM X intermédiaire devront être accompagnées de mention de durée de conservation dans celui-ci, sachant que selon la durée souhaitée les opérations à mener sur les archives seront plus ou moins importantes (voir tranches 1 à 4 ci-dessous).

~~*Les délais de conservation exigés par les AAs seront de préférence indiqués sous forme d'intervalles fixant des bornes pour chaque catégorie de documents. Un exemple de bornes est fourni ci-après, plus particulièrement adapté aux données numériques.*~~

Désignation tranche	***Commentaires***	***Numéro***
inférieur à 5 ans	*Pas de problème particulier en termes d'exploitation*	*1*
de 5 à 10 ans	*Prévoir au moins une migration de support*	*2*
de 10 à 30 ans	*Plusieurs migrations sont à envisager ainsi qu'une éventuelle conversion de format sans omettre les contraintes liées à la signature électronique*	*3*
au-delà de 30 ans	*L'on doit anticiper l'ensemble des difficultés précédentes*	*4*

Début de la durée de conservation :

~~*Po*~~*Cette date devra être renseigné pour chaque versement par les Aas, par défaut elle pourra être la date de versement des archives* *Cette information est à renseigner par les entités utilisatrices du SAEM X* ~~*clients de l'organisme X*~~*. Elle vient en complément de la durée de conservation et correspond à l'élément déclencheur qui permettra de savoir à partir de quand l'on peut commencer à décompter le temps d'archivage, avant application du sort final (suppression ou conservation historique).* ~~*Dans la majorité des cas le décompte est immédiat. Pour certains contrats, il peut s'agir par exemple de la fin des relations commerciales.*~~

~~*Cela doit également permettre de gérer la déserrance qui concerne des données/documents pour lesquels rien n'a encore été défini quant à leur traitement final depuis leur versement !*~~

6.2.2 Niveaux de service (à adapter et à compléter)

Une convention de services devra établir et préciser les conditions de fonctionnement du service d'archivage. Cette convention (ou un contrat de prestation de service?) doit être passée entre le SAEM X et chaque collectivité utilisatrice ~~le client et l'organisme X~~. ~~La liste~~ Les précisera notamment les niveaux de service suivants, sachant que chacune des options retenues pourra s'appliquer soit à l'ensemble des documents archivés soit à une ou plusieurs typologies de document telle que définie préalablement: ~~présentée ci-après est indicative et non exhaustive~~.

~~*Chacune des options retenues pourra s'appliquer soit à l'ensemble des documents archivés soit à une ou plusieurs typologies de document telle que définie préalablement.*~~

Document signé électroniquement :
proposition : Le SAEM X fournira 4 niveau de service (cf tableau) ?
Ce critère est destiné à faire face à l'obsolescence cryptographique et à répondre potentiellement à deux préoccupations distinctes :

- *la vérification de la signature dans le temps : si possible, la signature doit être vérifiée en amont, le plus tôt possible mais le SAE peut également permettre cette vérification dans le temps sous réserve de conserver les informations nécessaires et en particulier les listes de révocation ;*
- *la protection de la signature en tant que telle : nécessite un traitement périodique destiné à re-signer les documents.*

Il n'y a aucune obligation pour l'organisme X de disposer ou non d'un tel service. Néanmoins il a une obligation de conseil vis-à-vis de ses clients afin d'attirer leur attention sur les risques potentiels de voir une signature inutilisable.

Le tableau présenté ici fournit à titre indicatif différents niveaux de service possibles en matière de conservation sécurisée d'une signature électronique.

Moyens de vérification de la signature électronique	***Besoin client***
Aucun traitement particulier	*Pas de signature*
Conservation de la trace de la vérification	*Signature vérifiée en amont par le client*
Capacité à vérifier ou faire vérifier la signature et à conserver la trace de la vérification	*Vérification lancée par l'OA avant archivage*
Dans la mesure où le format de signature le permet, mise en œuvre d'un archivage dit « cryptographique »	*Conservation de la signature sans vérification préalable mais dans un format adapté (..aDES)*

Plages d'ouverture du service (accessibilité) :? (choix GPSAE)
ouverture aux horaires de bureau des entités utilisatrices ?
Exemples de plages d'ouverture :

- *du lundi au vendredi de 8h à 18h, hors jours fériés*

- *7 jours/7 de 8h00 à 18h*
- *7 jours/7, 24h/24*

Taux de disponibilité du service pour les archives numériques : ***? (choix GPSAE)***

Ce critère complète celui de l'indisponibilité globale traité de façon sécuritaire. Il est mesuré dans la plage d'ouverture du service par la formule suivante :

Taux disponibilité = ((Durée_Ouverture – Durée_Arrêt)/ Durée_Ouverture) x 100

Ce taux peut prendre par exemple les valeurs suivantes :

- *99,000 %*
- *99,900 %*
- *99,990 %*
- *99,999 %*

Temps de réponse : ***? (choix GPSAE)***

Ce critère vient compléter le critère concernant les plages d'ouverture du service en matière d'accessibilité ainsi que le critère sécuritaire lié à la disponibilité, étudié plus loin.

Le temps de réponse tant en versement qu'en interrogation dépend à la fois de la façon dont est organisée l'information au sein du système avec à la base un bon plan de classement, et à la fois des performances dudit système, directement liées aux techniques utilisées tant en matière de support électronique qu'en matière de réseau.

En versement :
Il s'agit du temps d'attente pour obtenir un accusé de réception suite à l'intégration effective des données dans le système :

- *inférieur à la journée*
- *inférieur à la demi-journée*
- *inférieur à 2h*

Une autre façon de mesurer le temps de réponse consiste à raisonner en vitesse de versement. Ce critère permet d'appréhender la capacité du SAE à absorber des flux en entrée du système. A titre d'exemple nous donnons les valeurs suivantes :

- *10 Mo/h*
- *100 Mo/h*
- *1 Go/h*
- *10 Go/h*

Proposition : en versement le SAEM X devrait permettre d'absorber des flux en entrée du système jusqu'à 1 Go/h ce qui lui permettrait de transmettre à l'AA versante un accusé de réception suite à l'intégration effectiv des données dans le système en un temps inférieur à la journée (dans les jours ouvrés)

En consultation :
Le temps de réponse peut être traité de façon globale, auquel cas il s'agira du temps d'attente suite à une requête afin d'obtenir l'archive recherchée :

- *48h ou plus (cas de commandes différées)*

- *inférieur à 20 secondes*

De façon plus précise les temps de réponse permettent de connaître en combien de temps un utilisateur obtiendra une réponse suite à une interrogation, sans pour autant récupérer les archives correspondantes, objet du critère suivant :

- *moins de 5 minutes*
- *moins de 2 minutes*
- *moins de 30 secondes*
- *moins 2 secondes*

Proposition : en consultation le SAEM X devrait permettre d'afficher une réponse à une consultation en moins de 30 secondes

Temps de mise à disposition des données/documents conservés : ? (choix GPSAE)

Après une interrogation, le résultat est en général obtenu sous la forme d'une liste d'éléments correspondants à la sélection effectuée par l'utilisateur. Ce dernier peut alors sélectionner un ou plusieurs éléments afin de les recouvrer. Compte tenu du type d'archive ou de la taille des objets demandés, les temps de restitution peuvent être plus ou moins longs et l'on peut même envisager une restitution sur des supports amovibles, pour des gros volumes de données/documents numériques, plutôt qu'une restitution en ligne.

- *moins de 5 jours*
- *moins de 48 h*
- *moins de 12 heures*
- *moins de 2 h*
- *moins de 5 minutes*
- *quelques secondes*

Proposition : en temps de restitution le SAEM X devrait permettre d'afficher les résultats d'une recherche en ligne pour un volume de document inférieur à XX ? Go en moins de deux minutes. Pour des volumes de données supérieurs à XXX ? Go, le temps de restitution devra être de moins de 12 heures.

Accès simultanés, ou nombre d'accès simultanés que le SAE est capable d'absorber :
? (choix GPSAE)

- jusqu'à 10
- jusqu'à 100
- jusqu'à 1 000
- jusqu'à 10 000

Proposition : le SAEM X devra pouvoir absorber jusqu'à 100 accès simultanés

Type de suppression :? (choix GPSAE)

La suppression est une étape important dans la vie des documents et peut nécessiter plus ou moins de contraintes. Quoiqu'il en soit aucune suppression ne peut se faire de façon automatique et sans validation du bordereau d'élimination.

Dans tous les cas la suppression concerne l'ensemble des jeux de données gérés par l'OA, y compris les sauvegardes éventuelles sur tous les supports (fixes ou amovibles).

Nous donnons ici à titre indicatif différentes façons d'aborder la suppression :

- *suppression du lien (index)*
- *suppression des données conservées (on réutilise potentiellement les espaces libérés)*
- *suppression des données et des traces enregistrées*
- *suppression sans rémanence magnétique possible des données effacées*
- *destruction physique des supports, essentiellement pour les supports amovibles mais aussi tout ce qui concerne les archives physiques*

Proposition : Le SAEM X devra permettre une suppression sans rémanence magnétique possible des données effacées après obtention du visa d'élimination (mais conservation des traces du passage de ces archives dans le SAEM X sous forme de journaux et de fiches de métadonnées suite à des requêtes?)

Perte de données : *? (choix GPSAE)*
Acceptation ou non par le client de l'organisme X de perdre un pourcentage de ces données/documents, en particulier suite à la mise en œuvre d'un PCA/PRA.

6.2.3 Niveaux de sécurité *? (choix GPSAE et travail sur matrices)*

Nous proposons ici de définir une échelle à quatre niveaux de sécurité (1-4), de bas à très fort.

Bien évidemment, en tant qu'OA, l'organisme X se doit de répondre aux niveaux les plus hauts en matière de sécurité. Cette échelle est néanmoins nécessaire afin de répondre aux besoins des clients pour lesquels les exigences en matière de sécurité ne sont pas forcément les mêmes selon les typologies de données/documents identifiés. Ceci aura pour principale conséquence de permettre aux clients de trouver un service d'archivage parfaitement adapté en termes de coûts.

Nous reprenons ci-après les critères de sécurités traditionnels : Disponibilité, Intégrité, Confidentialité, Preuve / traçabilité / auditabilité. La métrique présentée est indicative et devra être validée par l'ensemble des parties en présence.

Disponibilité :
La disponibilité correspond au délai maximum d'indisponibilité d'un SAE. Même si le délai d'une semaine peut paraître élevé, précisons qu'il s'agit bien évidemment d'un maximum et que, malgré tout, les données/documents archivés sont protégés, même si ils sont inaccessibles temporairement.

Durée maximum d'indisponibilité	***Note***
Semaine	*1*
2 jours	*2*
4 heures	*3*
30 secondes	*4*

Intégrité :
L'intégrité consiste à garantir que les données/documents traités n'ont pas été corrompus dans le temps. En général les contrôles sont effectués grâce à l'emploi d'empreintes (hash)

calculées le plus tôt possible et vérifiées à différents moments du cycle de vie des données/documents.

Modalités des contrôles d'intégrité	***Note***	***Besoins client***
5.1.2.1 Contrôle interne du système de stockage	*1*	*Pas de besoin particuliers en matière d'intégrité*
Contrôle des données/documents en entrée et en sortie/empreinte	*2*	*Perte d'intégrité tolérée mais doit être détectée et signalée*
Contrôle périodique par échantillonnage et procédure de correction des erreurs indispensables	*3*	*Perte d'intégrité tolérée mais doit être détectée et corrigée automatiquement*
Contrôle continu des empreintes et procédures de correction indispensable	*4*	*Aucune perte d'intégrité tolérée*

<u>Remarque</u> : Le besoin réel en matière d'intégrité concerne l'intégrité au sens du contenu informationnel. De fait la traçabilité (voir infra) constitue un critère de sécurité supplémentaire qui peut venir compléter le seul critère d'intégrité au sens technique du terme. En effet, en cas de conversion de format, seule la trace dûment documentée permettra d'apporter au besoin la preuve que le contenu informationnel n'a pas été altéré.

Confidentialité :
La confidentialité est directement liée aux conséquences de la diffusion des données/documents à des personnes non autorisées, les conséquences de cette diffusion peuvent être plus ou moins importantes, allant de pertes financières ou d'image jusqu'à des poursuites judiciaires.

Type de confidentialité	***Note***	***Commentaire***
Données publiques	*1*	*Ces informations sont destinées à être largement diffusées Elles ne font l'objet d'aucune protection de confidentialité particulière.*
Données à diffusion restreintes	*2*	*La divulgation de telles informations est susceptible d'entraîner des préjudices pour l'organisme propriétaire des données, sans le mettre directement en péril.*
Données confidentielles	*3*	*La divulgation de ces informations peut entraîner des préjudices graves pour l'organisme propriétaire.* *Ces informations sont soumises à des règles de protection particulièrement rigoureuses.*
Données très confidentielles	*4*	*La divulgation de cette information pourrait causer un dommage exceptionnellement grave allant jusqu'à la disparition de l'organisme dont elle émane.*

Identification/authentification :
Même s'il ne s'agit pas directement du ressort exclusif du service d'archivage d'identifier/authentifier les personnes amenées à travailler sur le système, il est important

d'attirer l'attention sur ce point. En effet, ce sera en général aux clients de l'organisme X d'identifier/authentifier en premier lieu les usagers afin d'en déterminer les droits. Le SAE quant à lui aura à vérifier globalement l'identité de ses clients et récupérera de leur part les droits spécifiques correspondants à tel ou tel utilisateur/usager.

Par contre il est du ressort exclusif de l'OA d'identifier/authentifier les opérateurs, personnes amenées à administrer le SAE.

De ce fait nous proposons également une métrique en ce qui concerne l'authentification qui devra être choisie en cohérence avec le niveau de confidentialité recherché.

Critère authentification	***Dispositifs***	***Note***
Ce que sais la personne	*login mot de passe*	*1*
Ce que possède la personne, non remis en face à face et sans vérification d'identité	*token, certificat classe 1, ...)*	*2*
Ce que possède la personne, non remis en face à face mais avec vérification d'identité	*Téléphone portable, certificat classe 2, ...)*	*3*
Ce que possède la personne, remis en face à face après vérification d'identité	*certificat classe 3 et 3+)*	*4*

Preuve, traçabilité :
La traçabilité concerne ici les informations qui sont enregistrées au fur et à mesure de la vie des données/documents, à chaque fois que l'on va y accéder. Néanmoins, il est également nécessaire de prendre en compte les journaux relatifs à la vie du système qui sont traités de façon globale au niveau des éléments de la sécurité techniques.

<u>Remarque</u> : Les traces restituables correspondent à la notion primordiale de réversibilité. En effet dans le cas où il y a changement de SAE, non seulement il est nécessaire de récupérer les données/documents mais également les traces relatives à toutes les évolutions qui ont pu avoir lieu sur ces derniers. Ces traces constituent un élément indispensable destiné à assurer la valeur probante des données/documents conservés et contribuent à garantir la confidentialité (en fonction des accès) et l'intégrité (vis-à-vis du contenu informationnel).

Moyens mis en œuvre au niveau de la traçabilité	***Note***	***Besoins client/cycle de vie des données/documents***
Ne sont enregistrées que les opérations techniques nécessaires au suivi du bon fonctionnement du SAE et qui permettent ainsi de détecter d'éventuels dysfonctionnements, l'acquittement des traitements d'archivage et la suppression d'archives.	*1*	*Pas de besoin de journalisation spécifique concernant le cycle de vie des documents.* *La journalisation système permet de suivre le bon fonctionnement du système*
L'ensemble des opérations concernant le cycle de	*2*	*Journalisation complète de*

vie des documents est inscrit dans le journal. Pour chaque données/document, il y a un enregistrement dans le journal pour les évènements suivants : - *Versement* - *Suppression* - *Changement de durée de conservation* - *Restitution* - *Conversion (changement de format logique)* - *Migration (changement de support)*		*l'activité sur le système d'archivage. Conservation compatible avec les éléments journalisés.*
Aux éléments précédents, sont ajoutées les consultations qui sont donc également tracées dans le journal. *Les journaux possèdent des moyens de contrôle de leur intégrité et en cas de perte de leur intégrité disposent de solutions de reconstitution.* *Les journaux sont conservés dans les mêmes conditions de sécurités que les données/documents auxquels ils se rapportent et pour une durée compatible.*	*3*	*Journalisation complète avec conservation sécurisée au sens légal du terme*
Aux exigences précédentes s'ajoutent un mécanisme d'horodatage des journaux avec recours à une TSA externe au SAE.	*4*	*Journalisation complète, sécurisé et restituable pour chaque données/document traité (cf. réversibilité)*

Afin d'aider à choisir le niveau de sécurité, il sera possible de s'appuyer sur la notion d'impact, directement lié à la survenance d'un risque. Rappelons à ce sujet que les principales menaces consistent en matière d'archivage à ne plus pouvoir utiliser des documents/données suite à leur suppression intempestive, la perte de leur intégrité, leur non intelligibilité, ….ou encore à un accès non autorisé.

Evaluation du risque (vraisemblance et gravité) :

Vraisemblance :
Exemple d'échelle de vraisemblance :

Niveaux de l'échelle	**Description détaillée de l'échelle**
Minime	Cela ne devrait pas se (re)produire.
Significative	Cela pourrait se (re)produire.
Forte	Cela devrait se (re)produire un jour ou l'autre.

Maximale	Cela va certainement se (re)produire prochainement.

Il est également possible de raisonner en pourcentage correspondant à la survenance probable de la menace quel que soit le scénario d'origine. En ce qui concerne la vraisemblance, l'on pourra avantageusement s'appuyer sur l'historique de l'organisme X. Par exemple la perte d'une facture et sa non production sont déjà arrivés combien de fois et quelles en ont été les conséquences ?

Gravité (impact) :
Exemple d'échelle de gravité :

Niveaux de l'échelle	**Description détaillée de l'échelle**
Négligeable	l'organisme surmontera les impacts sans aucune difficulté.
Limitée	l'organisme surmontera les impacts malgré quelques difficultés.
Importante	l'organisme surmontera les impacts avec de sérieuses difficultés.
Critique	l'organisme ne surmontera pas les impacts (sa survie est menacée).

En matière de gravité, d'impact l'on peut également raisonner en montant destiné à mesurer les conséquences financières de la réalisation de la menace. Il sera alors possible de s'appuyer sur des fourchettes, comme indiquées ci-après :

- *<1 k€*
- *1 à 10 k€*
- *10 à 100 k€*
- *100 à 1 M€*
- *1 à 10 M€*

7. FONCTIONNALITES DU SERVICE D'ARCHIVAGE

7.1 Généralités

Le service d'archivage répond à quatre objectifs principaux :
- la réalisation des versements,
- la conservation pérenne et intègre des données
- la gestion du cycle de vie des archives
- la communication des archives en respectant les procédures contractuelles

Ces fonctionnalités doivent en outre permettre de répondre aux exigences définies pour les niveaux de sécurité et de service à atteindre tels que définis précédemment.

7.2 Prestations et fonctionnalités offertes par le service d'archivage, flux électronique

Le SAEM X a pour but d'offrir aux entités utilisatrices qui ont des besoins en terme d'archivage électronique, un système d'archivage complet incluant :
- préparation des versements (dépôts manuels ou automatiques, normalisation des paquets d'information, constitution des profils)
- recherche d'informations parmi les versements constitués et consultation des archives à partir de requêtes
- lancement d'opérations spécifiques sur des archives versées (éliminations, restitution).
- versements préalablement contrôlés et normalisés,
- conservation en archivage intermédiaire et/ou en archivage définitif (stockage et administration des données)
- communication des données archivées ,
gestion des données descriptives et du cycle de vie (conformément à leurs métadonnées, notamment versement en AD, élimination)
-restitution des archives et des journaux de traitement et d'événements en fin de contrat

7.2.1 Préparation des versements

La préparation des versements peut s'effectuer par dépôt manuel ou automatisé à partir de profils SEDA préalablement établis. Ce travail permet de normaliser les versements, en organisant les données brutes et en leur associant les métadonnées indispensables à la gestion de l'archive, de façon à constituer le SIP (paquet d'information à verser au sens de l'OAIS).
Cette préparation incombe aux Autorités d'Archivage, le cas échéant, assisté par le SAEM X.

7.2.2 Réalisation des versements

La réalisation d'un versement consiste à transformer les données versées (SIP) en AIP (paquet d'information archivée au sens de l'OAIS). Après contrôle et validation, le SAE accuse réception du versement à l'Autorité d'Archivage (*service versant*).

7.2.3 Stockage (suspension, suppression)

Le stockage consiste à assurer la conservation des AIP de façon intègre et pérenne pour les durées définies par la l'Autorité d'Archivage
Cette fonction permet également de gérer les suppressions des données (physique, logique, traçabilité garantie).

7.2.4 Gestion des données descriptives

Cette fonction consiste à assurer la gestion des données disponibles et conservées par la fonction Stockage. Elle permet l'enrichissement et/ou l'ajout de métadonnées destinées à décrire les archives : contexte, contenu, structure, évolution au cours du temps, gestion du cycle de vie (par exemple : gel d'un AIP pendant la durée d'un litige).
Ces informations servent de point d'entrée dans le SAE et permettent de retrouver les données recherchées en assurant le lien avec le système de stockage.

7.2.5 Restitution et élimination :

La fonction de restitution consiste, sur demande de l'Autorité d'Archivage, à rendre un ou plusieurs AIP ainsi que les métadonnées, et les journaux de traitement et d'événements qui lui/leur sont associés dans le SAE.
La fonction d'élimination consiste, sur demande de l'Autorité d'Archivage et après obtention du visa réglementaire auprès des Archives Départementales, à détruire un ou plusieurs AIP ou objets d'archive.
La traçabilité de ces deux fonctions sera assurée par le SAE.

7.2.6 Communication /Consultation des archives

La fonction regroupe l'ensemble des mécanismes permettant de rechercher, d'accéder, de consulter et de livrer les informations disponibles dans le SAE, qu'il s'agisse des données descriptives ou du contenu lui-même.
Elle permet à l'utilisateur et le cas échéant à l'usager de demander à recevoir le ou les contenus d'information, accompagnés d'informations complémentaires, sous la forme d'un DIP (paquet d'information diffusé au sens de l'OAIS).
La communication est assurée par le SAEM X sur instruction conforme de l'Autorité d'Archivage.

.

7.2.7 Administration du service d'archivage

La fonction consiste à assurer l'exploitation d'ensemble du SAE et sa pérennisation ainsi que la gestion des habilitations des différents intervenants propres au service d'archivage. Elle implique notamment une veille technologique et des choix adaptés (formats, supports, gestion des migrations, etc.)

7.2.8 Audit du système d'archivage

La fonction consiste à vérifier la conformité de l'ensemble du service par rapport aux spécifications attendues. Elle permet de garantir la fiabilité du SAE et son amélioration continue.

7.2.9 Reprise de l'existant (base d'archive des entités utilisatrices)

La fonction consiste à assurer la migration d'un SAE existant dans le SAE, après étude préalable.
Elle permet d'effectuer une reprise partielle ou totale des archives existantes d'une nouvelle collectivité intégrant le SAEM X. Si une telle reprise est décidée, il sera nécessaire d'indiquer les volumes d'archives à récupérer ainsi que le détail des caractéristiques techniques de ces archives.

7.2.10 Réversibilité

La fonction permet à chaque collectivité utilisatrice du SAEM X de récupérer la totalité de ses archives sous une forme exploitable par celle-ci. Ce choix implique un effacement irréversible de l'intégralité des AIP ainsi que des métadonnées, et des journaux de traitement et d'événements qui lui/leur sont associés dans le SAE.

7.4 Engagement de suivi des exigences (voir service qualité) (à relire pour validation GP)

Il est d'ores et déjà envisagé qu'une certification ISO/CEI 20000 (norme de certification des services informatiques des organisations prouvant le respect de normes de qualité éditées au travers de phases, de contrôles et de procédures mis en place) soit entreprise afin de vérifier l'adéquation entre les services attendus et ceux réellement rendus par le SAE.
Le suivi du respect des engagements et des niveaux de service est effectué par :

- *Le Comité de Direction Qualité du SAEM X*
- *xxx*

7.4.1 Processus de fourniture des services

- *Gestion des niveaux de services*
- *Rapport de services*
- *Gestion de la continuité et de la disponibilité des services*
- *Budgétisation et comptabilisation des services*
- *Gestion de la capacité*
- *Gestion de la sécurité de l'information*

7.4.2 Processus de gestion des relations entre clients et fournisseurs (Service Desk)

- *Les généralités*
- *Gérer les relations commerciales*
- *Gérer les fournisseurs*

7.4.3 Processus de résolution de problèmes

- *Le contexte*
- *La gestion des incidents*
- *La gestion des problèmes*

7.4.4. Processus de maintien pour le contrôle des systèmes d'informations

- *La gestion des configurations*
- *La gestion des changements*

7.4.5 Processus de mise en production

Normes liées à la gestion des services et à l'ISO 20000

8. ADMINISTRATION DE LA POLITIQUE DE SERVICE D'ARCHIVAGE, COMITE DE SUIVI (à relire pour validation GP)

8.1 Diffusion de la PSA

La PSA est diffusée à l'ensemble des parties concernées par le service d'archivage électronique du SAEM X et en particulier aux entités utilisatrices afin de permettre à chaque partie de prendre connaissance des principes que l'Opérateur d'Archivage s'engage à respecter dans le cadre de la délivrance du service d'archivage et des obligations en retour des parties concernées.

8.2 Évolution de la PSA

En tant que document de référence du service d'archivage, la PSA est tenue à jour aussi bien vis-à-vis des évolutions tant internes qu'externes au service d'archivage. Les principes mis en œuvre au sein du service d'archivage sont ainsi en permanence conformes à ceux présentés dans la PSA. En cas d'écart constaté, soit la mise en œuvre des principes est corrigée pour être conforme à la PSA, soit la PSA est corrigée pour être conforme aux principes effectivement mis en œuvre.

L'évolution de la PSA peut également être rendue nécessaire suite à des demandes des utilisateurs ~~usagers~~, voire suite à un changement de périmètre des données/documents traités.

L'évolution de la Politique de service d'archivage est placée sous la responsabilité de des Aas (entités utilisatrices) ~~l'Autorité d'Archivage~~ au travers d'un Comité de suivi.

8.3 Comité de Suivi, composition et fréquence de réunion

Ce Comité est constitué de :

- 1ou plusieurs (?)~~Le~~ représentant des métiers, services producteurs de chaque AA ?;
- Le responsable du service informatique de chaque AA ?;
- Le responsable de la sécurité et des risques de chaque AA ? ;
- Le responsable du service juridique de chaque AA ? ;
- Le représentant du service qualité de chaque AA ? ;
- Le représentant des services d'archives de chaque AA ? et/ou des archives départementales ;
- Les représentants équivalents du SAEM X (?)~~...~~

Il se réunit au moins une fois par an.

8.4 Procédures de suivi des modifications à appliquer en cas d'évolution

Les demandes de modifications intervenant autour de la Politique de service d'archivage peuvent être de natures différentes :

- Modification des objectifs de sécurité ou d'archivage du SAEM X , évolution de sa structure, de son organisation ou de ses activités ;
- Demandes des entités utilisatrices ;
- Changement de la législation et/ou de la réglementation, nouvelles normes ;
- Evolution des menaces et des enjeux liés au système d'information ;
- Adaptation ou évolution du périmètre fonctionnel, technologique ou organisationnel ;
- Correction suite à une non-conformité ;
- …

8.4.1. Procédures en cas de veille réglementaire et juridique

La veille réglementaire vise à contrôler la prise en compte des impacts des évolutions législatives et réglementaires en matière d'archivage sur le système d'information du SAEM X.

Le SAEM X assure cette veille de façon globale. Néanmoins chaque collectivité utilisatrice du SAEM X conserve son expertise au travers de son métier et s'engage à avertir l'OA de toute modification en la matière.

L'OA assurera la mise en œuvre des modifications induites sur le système d'information suite à la réunion du Comité de suivi.

8.4.2 Procédure en cas d'évolution fonctionnelle/ technique / technologique

Les demandes d'évolutions fonctionnelles sont envoyées à l'OA par les utilisateurs/usagers ou toute autre entité ou partie du service d'archivage.

Toute demande est transmise au Comité de suivi afin d'analyser la nécessité d'actualiser la Politique de service d'archivage.

Le Comité identifie si la demande présente un intérêt et décide du lancement de l'instruction de la demande ou de son rejet.

8.5 Modalités de contrôle d'application de la PSA par le contrôle interne du SAEM X

L'OA met en œuvre des procédures et moyens de contrôle interne de l'application et du respect, par les différentes entités intervenant dans le service d'archivage électronique, des principes définis dans la PSA et déclinés dans la DPA.

Il existe ainsi deux types de contrôles destinés à vérifier l'application de la PSA:

1 Contrôles permanents assurés par la Direction des Risques du SAEM X : ces contrôles sont permanents et s'inscrivent dans la gouvernance du SAEM X et s'appliquent à la Politique de service d'archivage au même titre qu'à toutes les autres activités,

2 Contrôles périodiques assurés par l'audit interne du SAEM X qui assurera au moins une fois tous les 3 ans la revue des processus liés à la Politique de service d'archivage (définition, révision, mise en œuvre,...)

Dans le cadre de la présente Politique, il sera effectué au moins un contrôle périodique par an.

Les Archives Départementales contrôlent également la pertinence et l'application de la politique de service d'archivage de l'OA.

Des missions d'audits externes spécifiques diligentées par les AAs ou l'Opérateur d'Archivage lui-même peuvent s'ajouter à ces contrôles.

9. Glossaire (à relire pour validation GP)

Terme	Définition
Archives	Ensemble des documents quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale ou par tout service ou organisme public ou privé, dans l'exercice de leur activité (loi du 3 janvier 1979 – code du patrimoine, livre II)
Archives courantes	Période pendant laquelle les données / documents temps seront nécessaire à la gestion des dossiers actifs (définition DISIC).
Archives intermédiaires	Conservation de données/ documents pour des besoins juridiques même si les données/documents ne sont plus utilisés dans le quotidien (Définition DISIC).
Archives définitives	Au-delà du la Durée d'utilité Administrative, conservation des données / documents en raison de leur valeur patrimoniale (historique, statistique, scientifique). Les archives dites définitives sont alors prises en charge en responsabilité par une institution publique d'archives (Archives nationales, Archives départementales…), (Définition DISIC).
Document	Tout écrit ou enregistrement considéré comme une unité, le document (Extrait norme ISO 15489) Information portée sur un support quel que soit sa forme ou ses caractéristiques.
Données	Dans les technologies de l'information, description élémentaire d'une chose, d'une transaction, d'un événement, etc. Une donnée peut être non-structurée, semi-structurée ou structurée.
Donnée non structurée	Absence de structure propre de la donnée la rendant non exploitable par un système informatique
Donnée semi-structurée	Interprétation partielle possible par un traitement logiciel. Une partie du contenu s'adresse à l'humain (texte, image, son, etc), alors qu'une autre partie est destinée au traitement du logiciel
Donnée structurée	Interprétation possible par un traitement logiciel. Les informations sont agencées de façon structurée : balises, base de données, champs des bases de données relationnelles, codes et requêtes des langages informatiques.
Empreinte	Résultat d'une fonction de hachage appliquée sur une suite de caractères numériques de longueur quelconque visant à réduire celle-ci en une donnée de longueur fixe représentative de cette suite de caractères. L'empreinte est l'un des éléments permettant de vérifier l'intégrité physique d'un document, d'un flux, d'un lot, d'une transmission,… cette empreinte étant unique pour chaque suite de caractères numériques traitée.
Intelligibilité	Qui est intelligible, compris, saisi aisément. L'intelligibilité ne doit pas être confondue avec la lisibilité qui concerne la capacité

	à relire sans garantie de bonne compréhension.
Métadonnée	Description de données / documents et éventuellement des parties de cet objet. Les métadonnées portent à la fois sur le contenu, la gestion et le format.
SAE	Système d'Archivage Electronique : système consistant à recevoir, conserver, traiter, restituer des archives, des paquets d'informations, des objets d'archives, et qui s'appuie sur une plate-forme informatique
SEDA	Modélisation des différentes transactions qui peuvent avoir lieu entre des acteurs dans le cadre de l'archivage de documents ou données, s'accompagnant d'une modélisation de la description des données qui seront échangées lors de ces transactions. Le standard propose des schémas XML pour la mise en œuvre de ces transactions fixant la forme des messages échangés ainsi que la forme de la description des données échangées (définition DISIC).
Service des archives	Concerne les personnes affectées au service des archives
Tiers-Archiveur	Personne physique ou morale qui se charge pour le compte de tiers d'assurer et de garantir la conservation et l'intégrité de documents électroniques (définition DISIC)

Rajouts possible (cf glossaire Sictiam)

« Archive : Paquet d'information reçu, conservé et communiqué par un Servie d'archives (def issu du SEDA)
Autorité d'archivage : entité responsable de la gestion du servie d'archive et du système d'archivage
Communication : fait de porter l'Archive ou toute information relative à l'Archive à la connaissance d'une personne déterminée ou d'un groupe d'intéressés ou des Usagers
Consultation : interrogation du système d'archivage électronique destinées à vérifier l'existence ou non d'un Objet d'archives »
Elimination (ou destruction) : opération autorisée par un visa d'élimination consistant, après tri, à détruire l'Objet d'archive
Objet d'archive : données qui font l'objet de l'archivage (définition issue du SEDA)
Opérateur d'archivage : entité qui fournit les services, liés au Service d'archivage, demandés et spécifiés par l'Autorité d'archivage au bénéfice de cette dernière, opérant dans un cadre hiérarchique, réglementaire ou contractuel.

10 Annexe 1 : Cadre législatif et réglementaire (à relire pour validation GP)

- Code civil :
  - Articles 1316 et suivants (loi 2000-230 du 13 mars 2000).
- Code de la santé publique et particulièrement :
  - Article R 1110 (alinéas 1 à 4) ;

  - Article R1111 (alinéas 1 à 16).
- Code pénal :
  - Articles 226-13 et 226-31.
- Code du patrimoine :
  - Livre II « Archives ».
- Code général des impôts, annexe 3 :
  - Article 96 F.
- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
- Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés « loi informatique et libertés »
- Réglementation et recommandations de l'Agence Nationale d'Accréditation et d'Evaluation en Santé (ANAES) - Juin 2003
- Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique
- Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
- Décret n° 2011-246 du 4 mars 2011 relatif à l'hébergement de données de santé à caractère personnel sur support papier et modifiant le code de la santé publique
- Circulaire n° DHOS/E1/2009/271 relative à la communicabilité des informations de santé concernant une personne décédée
- Circulaire DGP/SIAF/AACR/2010/011 du 27 juillet 2010 Accès aux origines personnelles : communicabilité des dossiers de pupille pour lesquels le secret de l'identité du parent biologique a été explicitement opposé
- Code de déontologie médicale
- Cadre d'interopérabilité des systèmes d'information de santé et matrice d'habilitation des professionnels de santé : dernière version V.1.3 du 18 octobre 2012.

+++ ???

11 Annexe 2 : Normes et référentiels

11.2 S'y retrouver dans les normes (à relire pour validation GP)

Différentes présentations des normes en usage dans le domaine de la gestion de l'information existent. On peut citer en particulier :

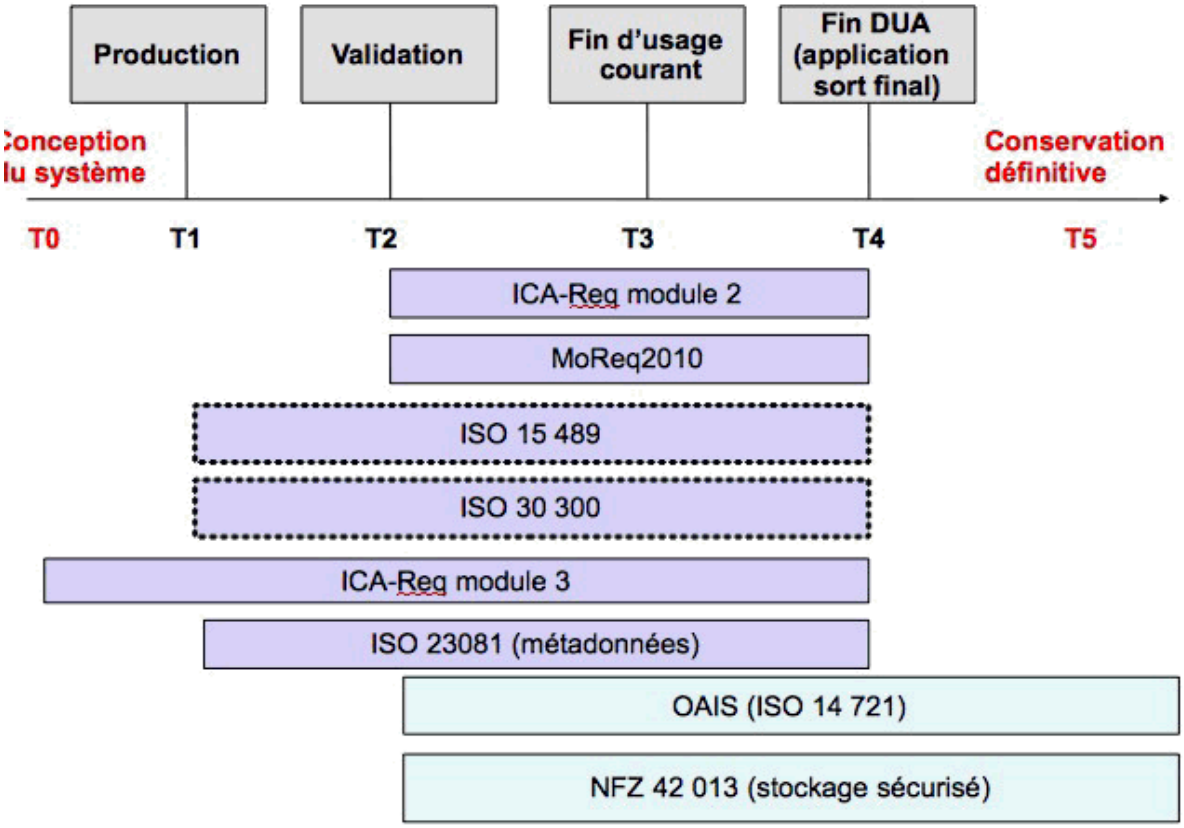
- Les trois documents de référence sur l'archivage électroniques (guide des bonnes pratiques, annexes, illustrations) publiés en 2012 par la direction interministérielle des systèmes d'information et de communication de l'Etat (DISIC) : http://www.references.modernisation.gouv.fr/archivage-numerique.

- Note d'information DGP/SIAF/2012/005 du 15 février 2012 relative à l'actualité de la normalisation en matière de records management (http://www.archivesdefrance.culture.gouv.fr/static/5570).
- On peut ajouter : note d'information DGP/SIAF/2011/010 du 8 juin 2011 relative au modèle de référence pour un système ouvert d'archivage d'information OAIS

  http://www.archivesdefrance.culture.gouv.fr/static/4940
- Chapitre zéro de Moreq2 (version française publiée en 2008) (http://www.archivesdefrance.culture.gouv.fr/gerer/archives-electroniques/standard/moreq2/).
- 2e livre blanc de la CN11 de l'AFNOR intitulé *Intégration du records management et perspectives d'évolution de l'ISO 15489* (Octobre 2011) : http://www.bivi.fonctions-documentaires.afnor.org/livres-blancs/publication-d-une-deuxieme-version-du-document-introduction-a-la-serie-de-normes-iso-30300-systeme-de-gestion-des-documents-d-activite.

? Signaler le 3ème libre blancde la CN11 de l'AFNOR de mai 2012 intitulé ISO 30300 – 30301 – Système de gestion des documents d'activité Définition, modélisations, intégration aux autres normes de système de management

http://www.bivi.fonctions-documentaires.afnor.org/livres-blancs/publication-d-un-3e-livre-blanc-sur-le-records-management-iso-30300-30301-systeme-de-gestion-des-documents-d-activite



précision sur source du schéma ?

Autre schéma possible issu de la note d'information DGP/SIAF/2012/005 citée ci-dessus

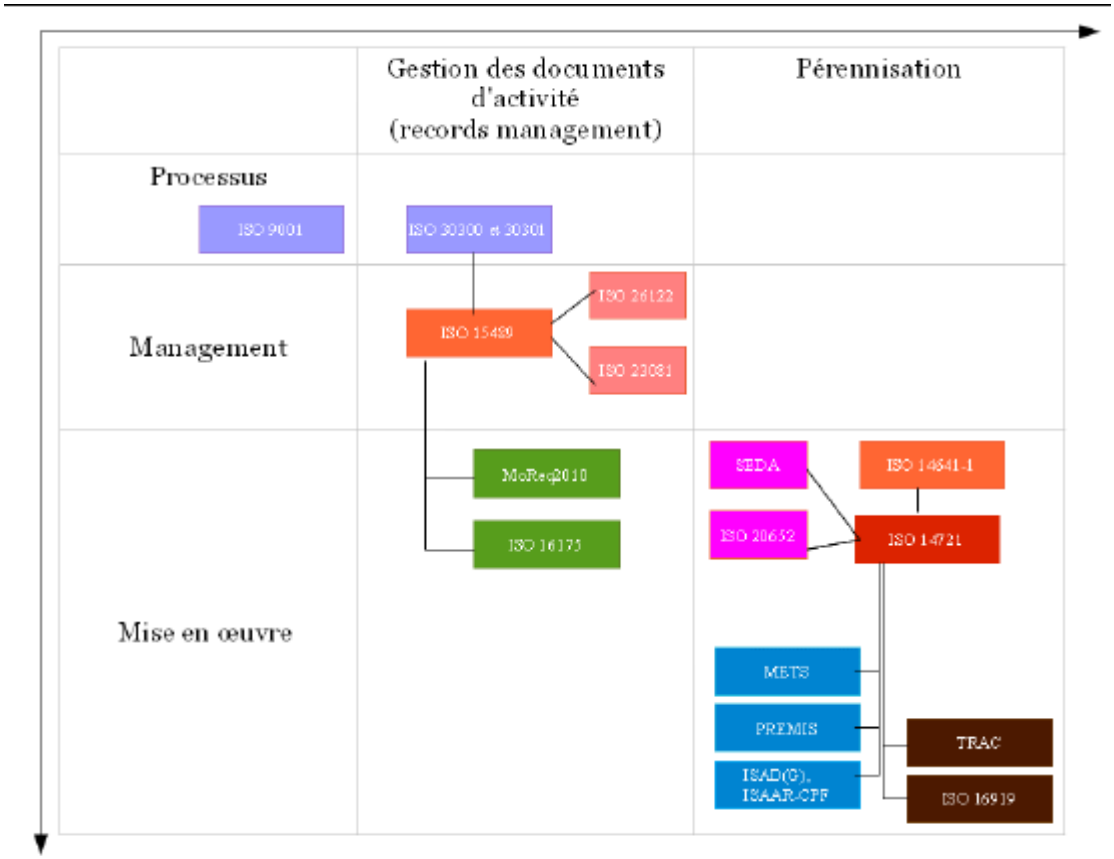


Schéma des principales normes relatives au records management et à l'archivage électronique

11.2 Les principales normes en matière de gestion de l'information

11.2.1 Normes de gouvernance des processus

ISO 30 300 : information et documentation – Systèmes de gestion des documents d'activité – Principes essentiels et vocabulaire.

ISO 30 301 : Information et documentation – Systèmes de gestion des documents d'activité – Exigences.

11.2.2 Normes de gestion des processus

11.2.2.1 Archives papier et électroniques

ISO 15489 : Information et documentation – « Records management », partie 1 : principes directeurs ; partie 2 : guide pratique.

11.2.2.2 Archives électroniques

ISO 14 721 (modèle OAIS) : systèmes de transfert des informations et données spatiales - Système ouvert d'archivage d'information (Modèle de référence pour la pérennisation des archives électroniques).

ISO 20652 : Systèmes de transfert des informations et données spatiales - Interface entre producteur et archives (PAIMAS).

11.2.2.3 Sécurité des systèmes d'information

ISO/CEI 27 001 : Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences.

11.2.3 Normes techniques de mise en œuvre

11.2.3.1 Spécifications pour la conception d'un système d'archivage électronique

ISO 14641-1 (NF 42 013) : gestion de document électronique - Conception et fonctionnement d'un système d'informations pour la conservation de documents électroniques - Partie 1 : spécification.

MoReq 2010 (Modular Requirements for Records Systems), vol. 1 : core services & plug-in module.

ISO 16175 : Principes et exigences fonctionnelles pour l'archivage dans un environnement électronique (ICA-Req).

11.2.3.2 Métadonnées

ISO 23081 : Information et documentation - Gestion des métadonnées pour l'information et les documents.

METS (standard de la bibliothèque du Congrès des Etats-Unis) : Metadata Encoding and Transmission Standard.

PREMIS – Preservation metadata.

11.2.3.3 Echange et interopérabilité

SEDA : Standard d'échange des données pour l'archivage (www.archivesdefrance.culture.gouv.fr/seda/). Ce standard fait partie du RGI et est donc exigible pour tout versement d'archives publiques dans un service d'archives publiques.

11.2.3.4 Coffre-fort électronique

NF Z42-020 : Spécifications fonctionnelles d'un composant Coffre-Fort Numérique destiné à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps.

11.2.3.5 Formats de représentation de l'information

Nous donnons ci-après la liste des formats de représentation de l'information donnée dans les annexes du Guide de bonnes pratiques sur l'archivage électronique de la DISIC (**http://references.modernisation.gouv.fr/sites/default/files/DISIC_AE_Annexes_Guide_0.pdf** voirpage 56). Cette liste est également issue des travaux du CINES (Centre informatique national de l'enseignement supérieur) dans le domaine.

11.2.3.5.1 Formats bureautiques et non structurés

HTML, Hypertext Markup Language pour les pages Web
Standardisé par le consortium W3C
Normalisé par l'ISO en 2000 (ISO 15445:2000)

PDF – PDF/A
PDF - format propriétaire (ADOBE)
PDF/A-1 est devenu la norme ISO 19005-1 en 2005
PDF 1.7 est devenu la norme ISO 32000-1 en 2008
PDF/A-2 nouvelle version de PDF-A publiée en juin 2011 : elle s'appuie sur la version 1.7 de PDF lui-même normalisé en ISO 32000-1

ODF, Open Document Format, pour les documents bureautiques
La version 1.0 est standardisée par OASIS en 2005 puis normalisée par l'ISO en 2006 (ISO 26300)
La version 1.1 est standardisée par Oasis en 2007 puis l'ISO en 2012.
La version 1.2 est actuellement un standard Oasis depuis 2011.

OOXML, Office Open XML, pour les documents bureautiques
Standardisé par ECMA en 2006
Normalisé par ISO en 2008 (ISO 29500)

11.2.3.5.2 Formats image

PNG, Portable network Graphics, pour les images matricielles. A l'origine, format créé pour offrir une alternative libre au format GIF qui utilise une technique de compression sans perte LZW soumise à un brevet.
Standardisé par le W3C en 1996
Normalisé par l'ISO en 2004 (ISO 15948:2004)

GIF, Graphics Intergange Format est un format ouvert de la société CompuServe pour la représentation d'images matricielles. Il utilise une compression sans perte LZW dont le brevet a maintenant expiré.
Version GIF87a
Version GIF89a permet l'inclusion de plusieurs images dans un fichier

JFIF, JPEG File Interchange Format est un format pour la représentation d'images matricielles compressées avec l'algorithme JPEG (Joint Photographic Experts Group)
L'algorithme JPEG est défini par la norme ISO 10918-1 en 1993

JPEG2000, Norme ISO 15444-1 de 2000 utilisant pour la compression (avec ou sans perte) des images un algorithme une transformée en ondelettes permettant des meilleurs taux que l'algorithme de la norme ISO 10918-1.

TIFF, Tagged Image File Format est un format conteneur propriétaire de Adobe pour des images numériques.