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

Archivage électronique sécurisé

P2A – POLITIQUE ET PRATIQUES D'ARCHIVAGE (SPHÈRE PUBLIQUE)

Version du 24 juillet 2006

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

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

avec le concours

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

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

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

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

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

conseil.dcssi@sgdn.pm.gouv.fr

Historique des modifications

Version	Objet de la modification	Statut
20/12/2005	Création du document sur la base d'un marché public (N°CO05000012 du 20 juin 2005, sur la fourniture d'une étude relative à la sécurité globale des services d'archivage)	Version de travail
24/07/2006	Finalisation	Validé

Table des matières

1 Introduction

1.1 Avant-propos

Le code du patrimoine définit les archives comme étant « *l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité* ».

L'archivage électronique répond principalement à deux objectifs juridiques :

- il permet aux administrations de s'appuyer sur des documents servant de pièces justificatives dans le cadre de contrôles (ex : fiscal ou sécurité sociale) ;
- il permet aux parties de produire des actes juridiques ayant une valeur juridique (preuve, légalité) en cas de litige devant les tribunaux.

L'archivage répond ainsi à une contrainte légale ou à un besoin juridique. L'archivage devient conservation dès le moment où il est réalisé dans une finalité juridique.

L'archivage prend également une dimension historique lorsqu'il répond à une finalité patrimoniale.

L'archivage électronique sécurisé peut être défini comme l'ensemble des modalités de conservation et de gestion de données électroniques ayant une valeur juridique lors de leur établissement ; cet archivage garantissant la valeur juridique jusqu'au terme du délai durant lequel des droits y afférents peuvent exister.

En conséquence, l'archivage électronique, objet du présent document, tend à conserver l'information en la restituant de manière intègre et conforme à l'information d'origine. Cette opération visant à conserver des Archives ayant une force probante et des effets juridiques concerne toutes les personnes juridiques sans exception, qu'elles soient physiques, morales, privées ou publiques.

Pour autant, les notions et les éléments développés dans le présent document peuvent également servir dans le cadre d'un archivage patrimonial.

Les archives électroniques sont gérées au sein d'un service d'archivage électronique sous la responsabilité d'une autorité d'archivage (cf. chapitres 2 et 3). Les objectifs et engagements de l'autorité d'archivage (en matière de services, de niveau de sécurité, de responsabilités,…) ainsi que les pratiques mises en œuvre au sein du service d'archivage électronique, pour répondre à ces objectifs et engagements, doivent être formalisées.

Une telle formalisation est l'objet des politiques d'archivage et des déclarations des pratiques traitées dans le présent document.

1.2 Objectif du document

L'objectif de ce document est double :

- décrire les concepts de politique d'archivage (PA) et de déclaration des pratiques d'archivage (DPA), ainsi que les différences et le positionnement entre ces deux concepts ;
- présenter un cadre pour aider les rédacteurs et les utilisateurs de PA et de DPA dans la rédaction et la compréhension de ces documents.

En particulier, ce document identifie les éléments à prendre en considération lors de la rédaction d'une PA ou d'une DPA.

1.3 Périmètre

Le présent document concerne uniquement la sphère publique, c'est-à-dire les Archives publiques telles que définies par le Code du patrimoine comme étant :

« a) Les documents qui procèdent de l'activité de l'État, des collectivités territoriales, des établissements et des entreprises publiques ;

b) Les documents qui procèdent de l'activité d'organismes de droit privé chargés de la gestion de services publics ou d'une mission de service public ;

c) Les minutes et répertoires des officiers publics ou ministériels. »

Ces Archives sont inaliénables et imprescriptibles.

Il s'ensuit que conformément à la législation en vigueur, une autorité d'archivage (désignée par AA et définie au chapitre 2 ci-après) responsable d'archives publiques (administration centrale, administration déconcentrée, collectivité territoriale, collectivité locale, personnes privées chargées d'une mission de service public…) devra notamment se conformer au Code du patrimoine et aux dispositions réglementaires applicables au service d'archives qui est un service public administratif.

Il est également précisé qu'au fil du temps, le changement de statut des archives (archives courantes, archives intermédiaires, archives définitives) selon leur âge peut conduire à un transfert de celles-ci vers une autre AA ; ce qui implique un changement d'AA. En outre, les niveaux de sécurité des PA adoptées pourront tenir compte de l'âge des archives, les exigences juridiques en la matière pouvant varier selon qu'il s'agisse d'archives courantes, intermédiaires ou définitives. Il appartiendra à chaque AA de s'assurer de la conformité de sa PA aux principes juridiques applicables en la matière.

En outre, la présente PA Type, liée à la sphère publique, ne fait pas référence au terme « restitution » dans la mesure où les archives publiques sont, par définition, inaliénables et imprescriptibles. En conséquence, une telle fonctionnalité n'entre pas dans le champ de la présente PA.

Enfin, il est important de relever que l'externalisation auprès d'une autorité d'archivage privée n'est pas autorisée, sauf dans certains cas très encadrés, limités et incertains juridiquement pour l'État. En revanche, il est envisageable que plusieurs personnes morales (notamment des collectivités locales) choisissent de « *mutualiser* » leur service d'archivage électronique au sein d'une structure juridique légale (structure visée par le code général des collectivités territoriales).

Le présent document tient compte de ces spécificités.

2 Définitions et abréviations

2.1 Définitions

- **Archive :** Paquet d'informations reçu, conservé et communiqué par un Service d'archives (cette définition issue du standard d'échange est la définition de référence dans le présent Cahier des charges).
- **Archives :** documents sous forme électronique, quels que soient leur date et leur support, produits ou reçus par tout service ou organisme public ou privé, dans l'exercice de leur activité (définition issue du code du patrimoine).
- **Archive courante** : les Archives qui sont d'utilisation habituelle pour l'activité des services, établissements et organismes qui les ont produites ou reçues.
- **Archive définitive** : les Archives qui ont subi les tris et éliminations définis aux articles 15 et 16 du décret n° 79-1037 du 3 décembre 1979.
- **Archive intermédiaire** : les Archives qui ont cessé d'être considérées comme des Archives courantes et les Archives qui ne peuvent encore, en raison de leur intérêt administratif, faire l'objet de tri et d'élimination conformément à l'article 16 du décret n° 79-1037 du 3 décembre 1979.
- **Attestation de validation :** document établi par l'Autorité de validation attestant de la validité de la Signature électronique et de l'horodatage (Signature électronique, Certificat et Jeton d'horodatage) de l'Archive et attachée à cette Archive dans le Paquet d'informations, puis l'Objet d'archives.
- **Authentification :** procédé visant à vérifier l'identification d'une personne physique par des moyens techniques, tels que mot ou phrase de passe, un code secret, une réponse à un défi ou encore une sécurisation numérique (Certificat).
- **Autorité d'archivage** : entité responsable de la gestion du service d'archive et du système d'archivage.
- **Certificat** : document sous forme électronique attestant du lien entre l'identité du titulaire et les données de vérification de signature électronique.
- **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.
- **Conservation** : opération(s) juridique(s) ou (et) matérielle(s) destinées à assurer la sauvegarde d'un droit, d'une chose, d'un patrimoine…
- **Consultation** : interrogation du Système d'archivage électronique destinée à vérifier l'existence ou non d'un Objet d'archives.
- **Contenu d'information :** ensemble d'informations constituant l'objet principal de la pérennisation.
- **Élimination** (ou Destruction) : opération autorisée par un visa d'élimination consistant, après tri, à détruire l'Objet d'archive.
- **Empreinte (empreinte numérique ou condensat ou hash)** : Résultat d'une fonction de hachage appliquée sur une chaîne de caractères de longueur quelconque visant à réduire celle-ci en une donnée de longueur fixe représentative de cette chaîne de caractères. L'empreinte est l'un des éléments permettant de vérifier l'intégrité d'un document, d'un flux, d'un lot, d'une transmission… (comparaison d'empreintes).
- **Information de pérennisation** : se décomposant en information de provenance, information d'identification, information d'intégrité et information de contexte, l'information de pérennisation accompagne le Contenu d'information afin qu'il puisse être correctement conservé.
- **Journaux d'évènement** : Enregistrement d'un ensemble de données relatives aux différentes opérations effectuées ou anomalies survenues au sein du SAE et destiné à assurer la traçabilité du service. Par ailleurs ces journaux doivent être conservés pendant une période à définir et donc faire l'objet d'une procédure de sauvegarde particulière.

- **Métadonnées** : description de l'Objet d'archives et éventuellement des parties de cet objet. Les métadonnées portent à la fois sur le contenu, la gestion et le format.
- **Migration de formats** : opération qui consiste à migrer le contenu de certains types de formats vers d'autres types afin que le format de fichier utilisé pour la conservation des Archives reste adapté compte tenu de l'évolution des technologies.
- **Migration de supports** : opération qui consiste à migrer le contenu de certains types de supports vers d'autres types, notamment afin d'anticiper l'obsolescence du support concerné.
- **Module de sécurité :** système de confiance basé sur une ressource cryptographique éprouvée. Une ressource sera considérée comme éprouvée si elle a subi une évaluation selon des critères d'évaluation de la sécurité des systèmes d'information en vigueur, avec une cible de sécurité et un niveau d'assurance et de résistance suffisant.
- **Objet d'archives** : Données qui font l'objet de l'archivage (définition issue de du Standard d'échange)
- **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.
- **Paquet d'Informations :** association du Contenu d'information et de son Information de pérennisation. A ce Paquet d'informations est associée une information d'empaquetage qui permet de relier et d'identifier les composants d'un Paquet d'informations.

  On distingue trois types de paquets :

  - Les Paquets d'information à verser : Paquets d'informations livrés par le Service producteur au Système d'archivage électronique pour l'élaboration d'un ou plusieurs Paquets d'informations archivés.
  - Les Paquets d'information archivés : Paquets d'informations conservés dans le Système d'archivage électronique et constitué d'un Contenu d'information et de l'Information de pérennisation associée.
  - Les Paquets d'informations diffusés : Paquets d'informations reçus par l'Utilisateur en réponse à sa requête au Système d'archivage électronique. Ce paquet provient d'un ou plusieurs Paquets d'informations archivés.
- **Politique d'archivage** : ensemble de règles portant un nom qui indique les exigences relatives à un archivage électronique sécurisé pour une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes.
- **Politique de sécurité** : ensemble de règles portant un nom qui définit les exigences physiques, techniques et logiques afin de garantir un niveau de sécurité déterminé pour une communauté particulière et/ou une classe d'applications.
- **Service d'archives** : désigne l'entité destinataire du Versement et assurant la gestion des Archives versées par les Services versants et destinées à être communiquées aux Services versants / producteurs, et, dans le respect des délais de communicabilité, aux Usagers. Le Service d'archives assure également une mission de conseil auprès des Services versants ou des Services producteurs.
- **Service producteur** : entité qui a initialement reçu ou produit l'Archive et qui en est propriétaire. Le Service producteur et le Service d'archives peuvent être assurés par une même personne juridique.
- **Service versant** : entité qui verse un Paquet d'informations à un Service d'archives.
- **Signature électronique :** une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil.
- **Signature numérique :** donnée sous forme électronique, jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification de l'origine des informations et garantit leur intégrité.
- **Support :** tout instrument permettant à l'Utilisateur de stocker des informations, de telle sorte que celles-ci puissent être consultées ultérieurement pendant une période adaptée à l'objectif de ces informations, et permettant la reproduction exacte des informations stockées.

- **Stockage** : opération consistant à garder des Archives sur un Support pendant une durée déterminée et dans un format pérenne.
- **Système d'archivage électronique** : 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.
- **Usager** : personne physique ou morale autorisée à consulter les Archives conservées sur le Système d'archivage électronique dans le respect de la législation applicable en matière de communication des Archives.
- **Utilisateur :** toute personne physique ou morale autorisée à utiliser un Système d'archivage électronique.
- **Versement** : transmission par un Service versant d'un Paquet d'informations à un Service d'archives.

2.2 Abréviations

AA : Autorité d'Archivage
AC : Autorité de Certification
AH : Autorité d'Horodatage
AV : Autorité de Validation
DPA : Déclaration des Pratiques d'Archivage
EAD : *Encoded Archival Description*
OA : Opérateur d'Archivage
OAIS : *Open Archival Information System*
OID : *Object Identifier Denomination* (identificateur d'objet)
DAF : Direction des Archives de France
DCSSI : Direction Centrale de la Sécurité des Systèmes d'Information
DUA : Durée d'Utilité Administrative
PA : Politique d'Archivage
PRIS : Politique de Référencement Intersectoriel de Sécurité
RM : *Records Management*
SAE : Système d'Archivage Électronique
SP : Service Producteur
SV : Service Versant

3 Concepts

Ce chapitre présente les concepts de base liés au service d'archivage électronique, ainsi que les intervenants de l'archivage électronique, les principes liés à la présentation de l'information et la description fonctionnelle de l'archivage électronique.

3.1 Présentation des intervenants de l'archivage électronique sécurisé et obligations et responsabilités respectives

Il s'agit ici de présenter les fonctions des composantes ou entités sur lesquelles repose et s'organise l'archivage électronique sécurisé. L'organisation de l'archivage électronique sécurisé repose en ce sens sur plusieurs intervenants dont les rôles doivent être précisés. Afin de faciliter la compréhension de l'articulation entre ces différents intervenants, un schéma récapitulatif et des exemples viennent illustrer la présentation. Les obligations et responsabilités de chacun des intervenants au vu des rôles tenus sont ensuite traitées.

Le descriptif qui suit vise à présenter les intervenants sous l'angle **fonctionnel** dans un processus d'archivage électronique. Juridiquement, une ou plusieurs fonctions peuvent être mises en œuvre par une même personne juridique (voir les exemples du 3.2).

Nota - Il est précisé à toutes fins utiles que les opérations de vérification par une Autorité de validation n'entre pas dans le champ de la présente PA type. En effet, une Autorité de validation désigne l'entité en charge de s'assurer que les différents éléments relatifs à la Signature électronique d'un acte sont valides. Or, la vérification de la Signature électronique apposée sur l'acte doit être assurée avant le Versement de l'Archive. Cette opération en amont incombe donc au Service Versant qui pourra avoir recours à une Autorité de validation avant de constituer le Paquet d'informations à archiver. Il s'agit là d'une opération en amont de l'archivage qui n'est donc pas traitée dans la présente PA. Il en va de même pour les prestataires et procédés qui concernent les transmissions électroniques des Archives. En ce sens, chaque personne publique est responsable des intermédiaires techniques auquel elle a recours pour échanger et transmettre des Archives.

3.1.1 Autorité d'archivage / Opérateur d'archivage

L'Autorité d'archivage (AA) est responsable de l'ensemble des prestations rendu par le Service d'archivage électronique conformément à la présente PA. En conséquence, l'AA est la clé de voûte de l'archivage électronique sécurisé.

La fonction d'AA est exercée par le service qui a la responsabilité des archives. L'autorité d'archivage évolue généralement au cours du cycle de vie des archives.

L'AA aura techniquement recours à un Opérateur d'archivage (OA) pour la mise en œuvre de tout ou partie du SAE. Un Opérateur d'archivage désigne l'entité qui exploite tout ou partie du SAE dans sa mise en place et dans sa mise en œuvre conformément aux exigences édictées par l'AA. Cette entité opère dans un cadre hiérarchique, réglementaire ou conventionnel (Ex. convention de services). Il en sera ainsi, par exemple, pour l'OA qui exploitera un SAE mutualisé et externalisé dans le cadre d'un groupement intercommunal (par exemple une communauté d'agglomération) ; étant noté, selon les hypothèses, que :

- soit chacune des communes membres reste Autorité d'Archivage et seul l'OA est « *mutualisé* »,
- soit chacune des communes membres transmet également le Service d'archives lui-même au groupement intercommunal constitué dès lors qu'un tel transfert de compétences est permis par les textes applicables.

En tout état de cause, quelle que soit l'organisation opérationnelle adoptée, c'est l'Autorité d'Archivage qui sera responsable. La notion d'OA n'est donc pas reprise dans la suite de la présente PA Type.

Enfin, il est rappelé que le changement de statut des archives (archives courantes, archives intermédiaires, archives définitives) selon leur âge peut conduire à un transfert de celles-ci vers une autre AA ; ce qui implique un changement d'AA. Dans ce cas, l'AA initiale doit être regardée comme un Service versant et devra à ce titre respecter les obligations applicables au Versement conformément à la PA de l'AA destinatrice.

3.1.2 Service producteur

Le Service producteur désigne l'entité qui a initialement reçu ou produit l'Archive et qui en est propriétaire.

Le Service producteur est chronologiquement la première AA dès lors que l'on se situe au niveau des Archives courantes.

Ensuite, le Service producteur est, en principe, le Service versant.

Si le Service producteur a disparu ou si certaines de ses missions ont été confiées à d'autres services, c'est le service qui aura récupéré ces missions qui sera considéré comme le Service producteur et endossera à ce titre les obligations et responsabilités y afférent.

Par ailleurs, le Service producteur et le Service d'archives peuvent être assurés par une même personne juridique. Tel pourra être le cas par exemple au sein d'un même département. Ces deux fonctions pourront également être distinctes. Il en ira ainsi par exemple dans le cas d'un groupement intercommunal chargé de la gestion du service d'archives de plusieurs communes, ces dernières étant des services producteurs distincts.

3.1.3 Service versant

Le Service versant désigne l'entité qui verse un Paquet d'informations à une AA via le SAE.

Une AA peut être un Service versant. Ceci sera notamment le cas dans l'hypothèse où le changement d'âge de l'archive implique un changement d'AA. Ainsi, le Service versant assure une fonction exercée par l'autorité d'archivage qui verse ses archives à une autre autorité.

3.1.4 Contrôleurs

Les personnes habilitées par les textes législatifs et réglementaires en vigueur à contrôler les Archives publiques.

La fonction de Contrôleur est ainsi exercée par le service qui contrôle la manière dont les autorités d'archivage s'acquittent de leur mission (création, versement, stockage, communication des archives, administration).

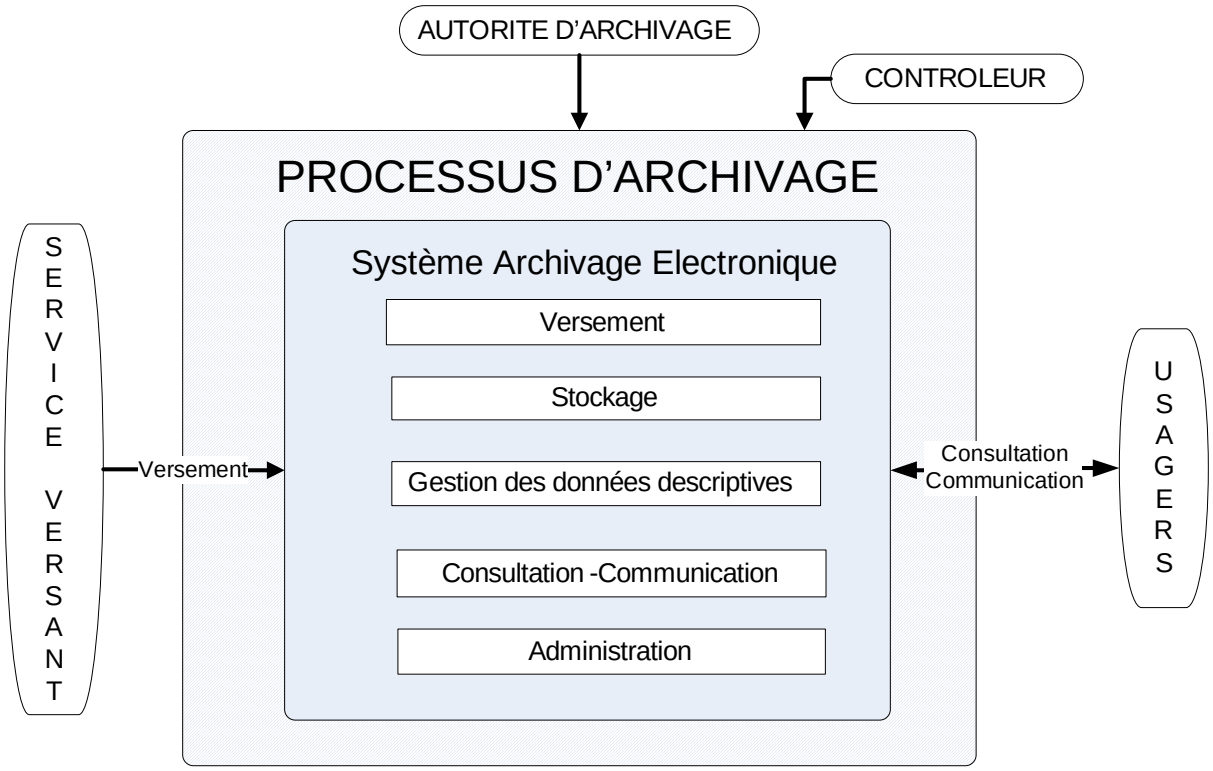
Dans le cadre de l'Archivage électronique, les Contrôleurs doivent bénéficier d'un accès au SAE.

3.1.5 Usager

Le terme Usager désigne toute personne physique ou morale autorisée à consulter les Archives conservées par l'AA dans le respect de la législation applicable en matière de communication des Archives.

3.1.6 Schéma récapitulatif

Le schéma ci-dessous synthétise les différents intervenants dans le processus d'archivage électronique :



Il peut y avoir un seule entité chargée de la mise en œuvre de l'ensemble des fonctionnalités de l'archivage ou les fonctionnalités peuvent être mise en œuvre par des entités différentes (par exemple, une entité a en charge la fonctionnalité de versement, une autre celle de stockage, etc.).

3.1.7 Illustrations

Dans la sphère publique, le rôle d'un service, en tant qu'intervenant dans le Service d'archivage électronique, est appelé à évoluer selon l'âge de l'Archive. Les cinq exemples donnés ci-après tendent à illustrer cette évolution suivant le cycle de vie des Archives.

Ministères (hors Défense et Affaires étrangères, qui relèvent d'un régime spécifique)

Les différents **services du ministère** créent des dossiers : ils en sont les Services producteurs. En même temps, ils ont la responsabilité de leur bonne conservation : ils sont donc Autorités d'archivage.

Une fois la période d'utilisation courante des dossiers échue, le Service producteur les remet généralement au **service d'archives du ministère**. Il joue alors un rôle de Service versant et le Service d'archives, en prenant la responsabilité de la bonne conservation de ces dossiers, devient leur Autorité d'archivage.

Si le Service d'archives du ministère est une mission des Archives nationales, le **conservateur en mission** exerce en outre, au nom de la direction des archives de France, un rôle de Contrôleur sur les archives du ministère. Sinon, le contrôle est exercé par la direction des archives de France.

Lorsque la période d'utilité administrative des dossiers s'achève, le Service des archives du ministère les remet au Centre des archives contemporaines de Fontainebleau. Il joue alors un rôle de Service versant et le Centre des archives contemporaines, en prenant la responsabilité de la bonne conservation de ces dossiers, devient leur Autorité d'archivage. Le contrôle sur le Centre des archives contemporaines est exercé par la direction des archives de France.

Lorsqu'un ministère a obtenu, par convention, la possibilité de conserver ses archives définitives, son service d'archives est et reste Autorité d'archivage. Le contrôle sur ce service est exercé par la direction des Archives de France

Services déconcentrés de l'État

Les différents services de cette administration créent des dossiers. Ils en sont les Services producteurs. En même temps, ils ont la responsabilité de leur bonne conservation : ils sont donc Autorités d'archivage.

Une fois la période d'utilité courante des dossiers achevés, les Services producteurs soit continuent de gérer directement leurs dossiers durant la durée d'utilité administrative (âge intermédiaire). Dans ce cas, ils continuent d'être autorité d'archivage. Le contrôle durant ces âges est exercé par le directeur des archives départementales.

Si, à l'inverse, les dossiers sont versés dans un Service d'archives intermédiaire (par exemple un service géré au niveau de l'ensemble des services déconcentrés de l'État dans le département, ou encore la région), les Services producteurs deviennent Services versants et le Service d'archives intermédiaire devient à son tour Autorité d'archivage. Le contrôle est toujours exercé soit par le directeur des archives départementales soit par le directeur des archives départementales, chef-lieu de région (en cas de service géré au niveau régional).

À l'expiration de la DUA, en cas d'existence d'archives définitives, le Service d'archives intermédiaire devient un Service versant, vers la direction des Archives départementales compétente qui devient Autorité d'archivage. Le contrôle est alors exercé par la direction des Archives de France.

Régions

Les différents services du conseil régional créent des dossiers. Ils en sont les Services producteurs. En même temps, ils ont la responsabilité de leur bonne conservation : ils sont donc Autorités d'archivage.

À l'expiration de la durée d'utilisation courante, les services versent au Service d'archives régional qui devient Autorité d'archivage, sous le contrôle du directeur des archives départementales chef-lieu de région. À l'issue de cette durée, le Service d'archives régional a la possibilité de confier, par convention, les Archives définitives à la direction des archives départementales chef-lieu de région, ou bien de rester Autorité d'archivage.

Départements

Les différents services du conseil général créent des dossiers. Ils en sont les Services producteurs. En même temps, ils ont la responsabilité de leur bonne conservation : ils sont donc Autorités d'archivage.

À l'expiration de la durée d'utilisation courante, soit les services continuent d'assurer la gestion de leurs dossiers durant la période intermédiaire et ils restent Autorité d'archivage, sous le contrôle du directeur des archives départementales, soit ils versent à un Service d'archives intermédiaire, généralement sous la responsabilité de la direction des archives départementales. Dans ce cas, après versement, la direction des archives départementales devient Autorité d'archivage et le restera pour la partie des archives devenues archives définitives après la DUA. Le contrôle est alors exercé par la direction des Archives de France.

Communes

Les différents services de la commune créent des dossiers. Ils en sont les Services producteurs. En même temps, ils ont la responsabilité de leur bonne conservation : ils sont donc Autorités d'archivage.

À l'expiration de la durée d'utilisation courante, si un Service d'archives de la commune existe, les Services producteurs deviennent des Services versants pour le Service d'archives qui devient Autorité d'archivage et le reste si le Service d'archives a également la compétence sur les Archives définitives. Le contrôle est exercé par le directeur des archives départementales.

La commune peut également (c'est une obligation pour les communes de moins de 2000 habitants) déposer aux archives départementales des catégories d'archives ayant atteint une certaine ancienneté ou pour des archives manifestement mal conservées). La direction des archives départementales devient alors Autorité d'archivage, sous le contrôle de la direction des Archives de France.

Actuellement, même si des communautés urbaines ou des communautés d'agglomération se mettent en place, aucune n'a encore inscrit dans ses statuts la responsabilité des archives de la structure intercommunale, de la ville siège de la structure et également des communes membres de la communauté. Pourtant, il ne semble pas que les textes actuels empêchent un tel montage juridique et ce serait évidemment une piste intéressante pour les archives numériques. Néanmoins, la question juridique devrait être affinée. Dans une telle hypothèse, la structure intercommunale deviendrait Autorité d'archivage après un versement par la commune (ou son service d'archives) et un contrôle serait exercé par le directeur des archives départementales concerné.

3.2 Principes relatifs à la représentation de l'information

Il est important de préciser qu'il s'agit de traiter ici du Service d'archivage électronique sécurisé. En ce sens, ce sont les différentes opérations successives identifiées dans le processus d'archivage électronique qui sont décrites. Ce service qui repose sur des intervenants fonctionnels dont les rôles ont été précisés au chapitre 3.1 du présent document, reposera également sur un SAE (système d'archivage électronique). De la sorte, il existe un lien étroit entre le Service d'archivage électronique et le SAE. Toutefois, les spécifications relatives au SAE doivent être traitées dans un document à part (notamment certains aspects seront précisés dans la DPA et les modalités opérationnelles, mais également et surtout dans le cahier des charges qui devra être adopté par la personne publique afin de déterminer les exigences attendues du SAE).

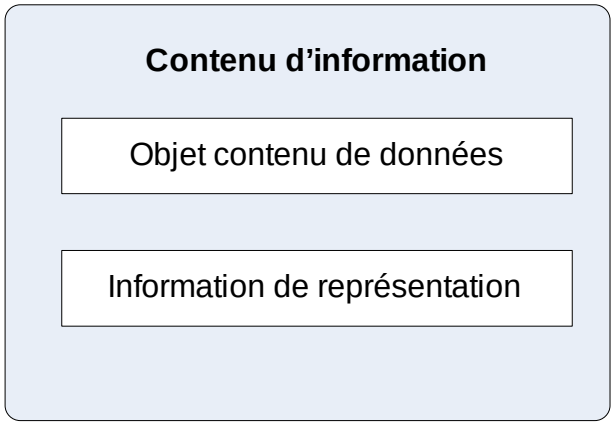
La présente partie décrit ainsi qu'elles sont les exigences fonctionnelles relatives au Service d'archivage électronique selon les différentes étapes à prendre en compte.

À cet égard et au préalable, il est nécessaire de rappeler certains principes relatifs à la représentation de l'information.

Afin de clarifier la suite du présent document, sont reprises ci-après les définitions de certains termes utilisés ainsi que leur interconnexion.

3.2.1 Contenu d'information

Si l'on se réfère au modèle OAIS, un **contenu d'information** (*Content Information*) est un ensemble d'informations constituant l'objet principal de la pérennisation dévolue au SAE. Il est composé d'un **objet contenu de données** (*Content Data Object*) et de son **information de représentation** (*Representation Information*).



Un objet contenu de données peut être un objet physique ou un objet numérique sachant que ne sont traités ici que des objets numériques. Un objet numérique (*Digital Object*) est un objet constitué d'une suite de bits qui prend la forme d'un fichier électronique généré dans un format donné (par exemple un format image ou un format texte).

L'information de représentation (*Representation Information*) est l'information qui traduit un objet contenu en des concepts plus explicites. Il pourra s'agir par exemple de la définition et de la description du format image dans lequel a été généré le fichier et qui permettra de convertir la séquence de bits dont il se compose sous une forme intelligible par l'utilisateur. Cette information de représentation peut, soit être fournie par le service versant avec l'objet contenu de données, soit être gérée séparément par le service d'archives dans une base de connaissances. Dans ce dernier cas le service d'archives a la charge de contrôler, lors des versements, l'existence de la documentation correspondante dans sa base de connaissances.

Par exemple dans le cadre de délibérations transmises par les collectivités aux préfectures pour le contrôle de légalité, la correspondance avec les définitions précédentes pourrait être :

- Objet contenu de données : fichiers PDF correspondant aux délibérations transmises et les informations de signatures éventuelles associées
- Informations de représentation : indication du format PDF

3.2.2 Information de pérennisation

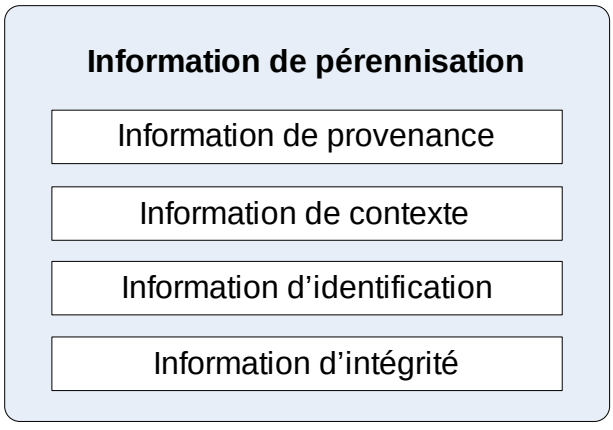
Afin qu'un contenu d'information puisse être correctement conservé, il doit être accompagné d'une **information de pérennisation** (*Preservation Description Information* - PDI) qui se décompose de la façon suivante :

- Information de provenance (Provenance Information) : information qui documente l'historique du contenu d'information. Cette information renseigne sur l'origine ou la source du contenu d'information, sur toute modification intervenue depuis sa création et sur ceux qui en ont eu la responsabilité. Exemple : nom du principal responsable de l'enregistrement des données, informations relatives au stockage, à la manipulation et à la migration des données.

- Information de contexte (*Context Information*) : information qui décrit les liens entre un contenu d'information et son environnement. Elle inclut entre autres les raisons de la création de ce contenu d'information et son rapport avec d'autres objets contenus de données.

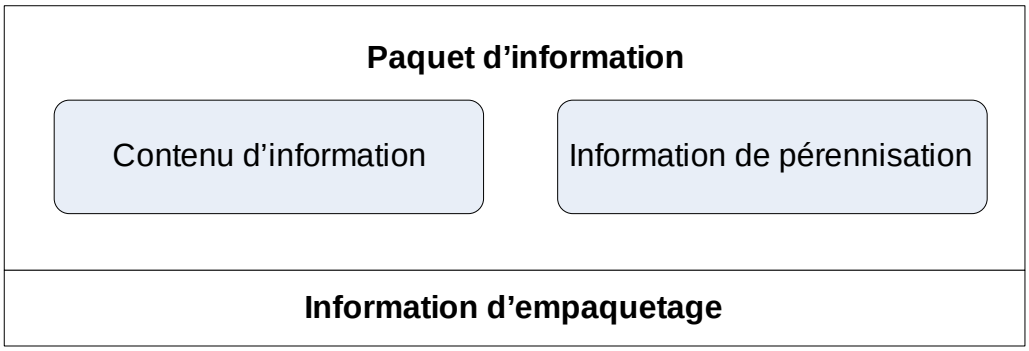
- Information d'identification (*Reference Information*) : information qui identifie et si nécessaire décrit le ou les mécanismes d'attribution des identificateurs au contenu d'information. Elle inclut aussi les identificateurs qui permettent à un système externe de se référer sans équivoque à un contenu d'information particulier. Exemple : un ISBN (*International Standard Book Number*).

- Information d'intégrité (*Fixity Information*) : description des mécanismes et des clés d'authentification garantissant que le contenu d'information n'a pas subi de modification sans que celle-ci ait été tracée. Par exemple, le code CRC (contrôle de redondance cyclique) pour un fichier ou mieux le calcul d'empreinte.



3.2.3 Définition d'un paquet d'information (ou lot)

D'après l'OAIS, l'ensemble des échanges d'informations effectués entre le système d'archivage et l'extérieur s'effectue par l'intermédiaire de paquets d'informations.
Un paquet d'informations *(Information Package IP*) est l'association du Contenu d'information et de son Information de pérennisation (PDI). À ce paquet d'informations est aussi associée une Information d'empaquetage qui permet de relier et d'identifier les composants d'un Paquet d'informations.



On distingue ainsi trois types de paquets :

- Les paquets d'informations à verser (*Submission Information Package* - SIP) : Paquet d'informations livré par le service producteur ou service versant au système d'archivage pour l'élaboration d'un ou plusieurs Paquets d'informations archivés (AIP).

- Les paquets d'informations archivés (*Archival Information Package* - AIP) : Paquet d'informations conservé dans le système d'archivage et constitué d'un Contenu d'information et de l'Information de pérennisation (PDI) associée.

- Les paquets d'informations diffusés (*Dissemination Information Package* - DIP) : Paquet d'informations reçu par l'Utilisateur en réponse à sa requête au système d'archivage. Ce paquet provient d'un ou de plusieurs Paquets d'informations archivés (AIP).

3.2.4 Information de description

Enfin, l'Information de description (Descriptive Information) est un ensemble d'informations, extraites de l'information de représentation et des informations de pérennisation, constitué principalement de descriptions de paquets et permettant aux utilisateurs de rechercher, commander et récupérer des informations du système d'archivage.

Par exemple dans le cadre du contrôle de la légalité cette information descriptive, destinée à identifier une délibération, pourrait être la date de la délibération et le nom de la collectivité émettrice.

3.2.5 Contenu d'un paquet d'information

Afin de préciser le détail du contenu effectif de chaque paquet d'information, l'Administration pourra se référer au standard d'échange sachant que le principe de base retenu est de s'appuyer sur le modèle OAIS et les possibilités offertes par la DTD EAD, pour la description de l'Objet archivé.

Dans le cas du Versement il est ainsi proposé que soient transférés les différents fichiers constituant l'Objet à archiver, ainsi que l'information de pérennisation associée décrite suivant les règles de la DTD EAD, l'ensemble étant rassemblé sous un numéro unique d'identifiant du versement.

Dans certains cas, l'objet à archiver correspondra à un fichier XML, pouvant encapsuler, en Base64, les différents fichiers si ceux-ci étaient initialement sous un format binaire.

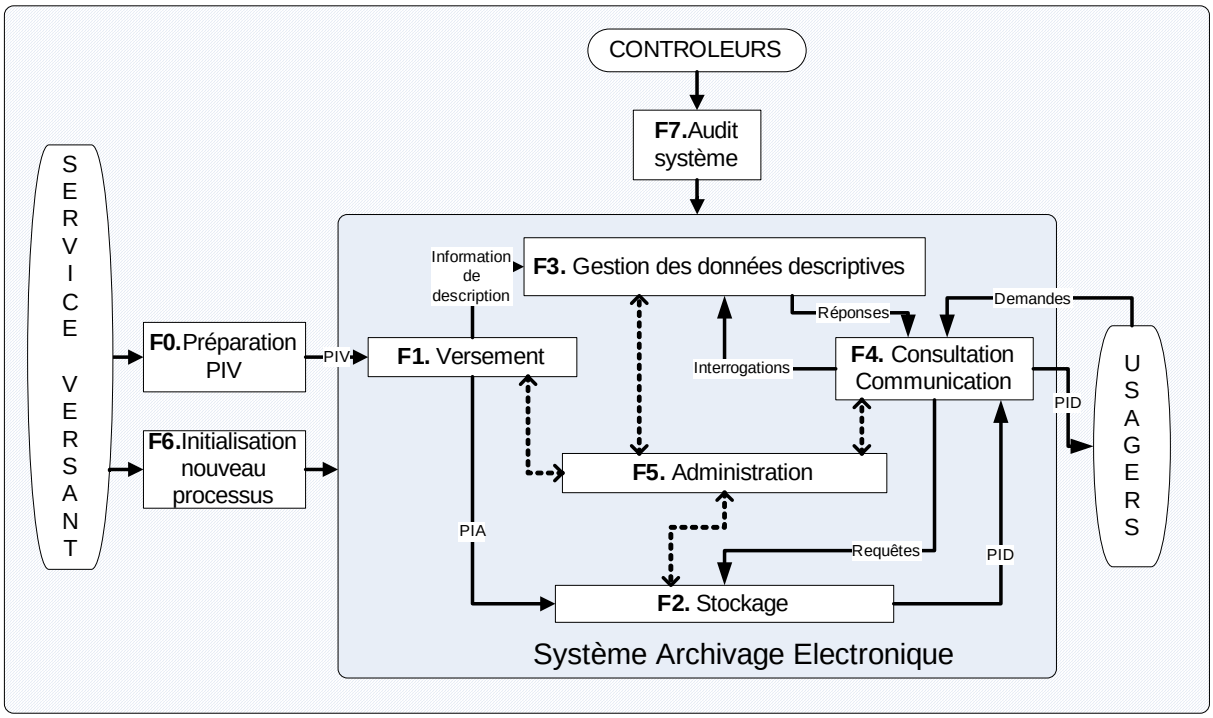
Devront par ailleurs être spécifiés, à partir d'un référentiel à élaborer par la direction des Archives de France, à partir d'une part du cadre commun d'interopérabilité et, d'autre part du registre de formats PRONOM, les formats des fichiers, les seuls formats acceptés pour l'archivage à moyen et long terme étant des formats dont les spécifications sont publiques.

Enfin, il convient de rappeler que la présente PA Type, liée à la sphère publique, ne fait pas référence au terme « restitution » dans la mesure où les archives publiques sont par définition inaliénables et imprescriptibles et où l'utilisation de ce terme risquerait d'être source de confusions.

3.3 Description fonctionnelle de l'archivage électronique sécurisé

Est brièvement rappelé ci-dessous le détail des fonctions intervenant pour le service d'archivage.

SERVICE D'ARCHIVAGE



PIV : Paquet d'information versé
PIA : Paquet d'information archivé
PID : Paquet d'information diffusé

F0. Préparation des PIV - Revient à constituer les paquets d'informations avant versement.

F1. Versement - Permet le traitement des paquets d'informations en provenance des Services versants dans son ensemble. Cette fonction inclut tous les mécanismes de préparation, transmission, contrôle, rejet, complément d'information ainsi que tous les traitements de ces informations pour une intégration dans le dispositif de Stockage des contenus et celui de gestion des données descriptives.

F2. Stockage - Gère l'ensemble des services liés à la conservation des paquets d'informations archivés à partir du moment où ils sont mis à sa disposition par la fonction de Versement jusqu'à leur destruction/élimination s'il y a lieu tout en garantissant leur intégrité. Cette fonction prend entre autres en compte les aspects de choix de supports et de gestion de l'ensemble des migrations.

F3. Gestion des données descriptives - assure la conservation, la mise à disposition et la mise à jour des informations descriptives associées aux contenus d'informations, conservés par la fonction Stockage. Ces informations doivent servir aux utilisateurs comme point d'entrée au SAE et permettre de retrouver les données qu'ils recherchent en assurant le lien avec leur identification de localisation dans le système de stockage.

F4. Consultation et communication - prévoit l'ensemble des mécanismes permettant 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 comprend la mise à disposition d'une interface de consultation, un système de recherche effectuée à partir des données descriptives, un principe de visualisation du résultat, la sélection de contenus à communiquer et la livraison effective de ces contenus sous forme de paquets d'informations diffusés. Dans la mesure où la communication du contenu peut être différée par rapport au moment de l'interrogation, cette fonction doit également prévoir un mécanisme de commandes à destination des utilisateurs, le suivi étant assuré par la fonction Administration.

F5. Administration - permet d'assurer l'exploitation d'ensemble du Système d'archivage électronique et sa pérennisation ainsi que la gestion des utilisateurs du SAE au sens de leurs droits d'accès.

F6. Initialisation d'un nouveau processus - consiste à intégrer un nouveau Service versant dans le réseau des Services producteurs utilisateurs du SAE et à définir et mettre en œuvre un nouveau flux de versements au sein de ce service versant.

F7. Audit - permet de vérifier la conformité de l'ensemble du service par rapport aux spécifications attendues.

3.4 Politique d'archivage (PA)

Lorsqu'une personne publique (ou privée chargée d'une mission de service public) entend mettre en place un archivage électronique sécurisé, elle doit, en tant qu'AA, élaborer sa propre politique d'archivage (PA), dans laquelle elle définit le niveau de sécurité et les exigences qu'elle s'engage à respecter.

La présente PA Type définit les exigences minimales, en termes juridiques, fonctionnels, opérationnels, techniques et de sécurité, qu'une autorité d'archivage doit respecter afin que l'archivage électronique mis en place puisse être regardé comme fiable. Cette fiabilité a pour objectif de conserver aux Archives leur force juridique originelle tant en termes de preuve que de légalité. En conséquence, un acte électronique n'ayant aucune valeur juridique lors de son établissement ne pourra se voir conférer une telle valeur au seul motif qu'il a été archivé conformément à la présente PA Type. En outre, à défaut de texte juridique venant préciser les modalités pour qu'un archivage électronique soit regardé comme fiable, le juge reste seul compétent pour se prononcer sur ce point.

Ceci étant précisé, cette PA Type repose sur des contraintes « standard » à mettre en place. Il en est ainsi :

- des contraintes en matière d'identification/authentification de l'origine de l'Archive ;
- de l'intégrité des Archives, des Paquets d'informations et des Objets d'archives ;
- de l'intelligibilité / lisibilité des Archives ;
- de la durée / pérennité de l'Objet d'archives ;
- de la traçabilité des différentes opérations (notamment versement, consultation, élimination) ;
- de la disponibilité et de l'accessibilité des Archives.

La présente PA Type constitue donc un référentiel de la sécurité de l'archivage électronique pour qu'il puisse être qualifié de « fiable ». Ce référentiel définit les principes minimaux à respecter par l'AA et les entités opérant les différentes composantes du service d'archivage.

L'ajout de principes de sécurité supplémentaires ainsi que la déclinaison des principes (minimaux et supplémentaires) en mesures de sécurité (techniques et non-techniques) dépend de l'environnement, de l'organisation opérationnelle, des technologies mises en œuvre et doivent être déterminés à l'issue d'une analyse des risques sécurité qui doit être menée sous la responsabilité et le contrôle de l'AA.

L'Autorité d'archivage devra donc intégrer dans sa propre PA l'ensemble des exigences qui sont définies dans la présente PA Type.

Enfin, dans le prolongement de la PA, l'AA pourra élaborer un cahier des charges portant sur le Système d'archivage électronique (SAE). Un guide sectoriel d'aide à la rédaction d'un cahier des charges à cette fin a été élaboré. La personne publique ou la personne privée chargée d'une mission de service publique pourra se faire aider dans ce cadre par une assistance à maîtrise d'ouvrage.

La politique d'archivage formalise les objectifs à atteindre par l'AA et les engagements qu'elle doit respecter. La PA doit être cohérente avec les exigences juridiques et, éventuellement, conventionnelles ou contractuelles, liées au service d'archivage de la responsabilité de l'AA, ainsi qu'avec la présente PA Type. De plus, la PA doit également être cohérente avec l'architecture fonctionnelle du service d'archivage.

La PA doit ainsi définir :

- Les prestations fournies aux services versant / producteur et aux usagers / utilisateurs en matière d'archivage électronique : périmètre des prestations, niveaux de service, type d'archivage (courant / intermédiaire / définitif),…

- Les obligations pesant sur les intervenants, à commencer par l'AA, mais également les autres intervenants (Services producteurs / versants, Usagers / utilisateurs, Contrôleurs). Les obligations concernant les autres intervenants constituent les obligations minimales qu'ils doivent respecter afin que l'AA puisse fournir les prestations d'archivage conformément à sa PA.

- Les fonctionnalités mises en œuvre au sein du service d'archivage, sous la responsabilité de l'AA, afin de fournir ces prestations (fonction de versement, fonction de stockage,…) et l'organisation fonctionnelle correspondante (liens entre fonctions, flux d'information,…).

- Les principes de sécurité à respecter au niveau de l'AA et par les différentes fonctions, basés sur les trois catégories définies dans [PSSI] (principes organisationnels, principes de mise en œuvre, principes techniques).

Une PA se situe donc au niveau fonctionnel et doit être indépendante des implémentations opérationnelle et technique permettant la mise en œuvre des différentes fonctions.

Une PA est a priori un document public permettant aux différents intervenants concernés, internes et externes à l'AA, de prendre connaissance des engagements de l'AA. Une PA peut être soit être directement conventionnelle ou contractuelle entre les intervenants, soit être reprise, pour les parties pertinentes, dans des "conditions générales d'utilisation", ou document équivalent, spécifiques à chaque catégorie d'intervenants. Compte tenu de la complexité de lecture d'une PA pour des non spécialistes, c'est cette seconde approche qui est recommandée.

3.5 Déclaration des pratiques d'archivage (DPA)

La déclaration des pratiques d'archivage (DPA) vise ensuite à définir comment l'AA s'organise pour répondre aux objectifs et engagements de la (des) PA ainsi qu'à identifier les procédures opérationnelles et les moyens mis en œuvre pour cela.

Une même DPA peut en effet permettre de couvrir les objectifs et engagements de plusieurs PA et les objectifs et engagements d'une même PA peuvent être couverts par des procédures et moyens différents, donc par des DPA différentes.

En matière de sécurité, la DPA doit décliner les principes de sécurité identifiés dans la (les) PA, en principes de sécurité opérationnels au niveau des différentes composantes du service d'archivage, et en règles de sécurité à mettre en œuvre pour respecter ces principes.

Ces principes et règles peuvent être identifiés directement dans la DPA, notamment s'ils sont dédiés au service d'archivage, ou la DPA peut renvoyer sur un document plus global de politique de sécurité des systèmes d'information (cf. [PSSI]). Dans tous les cas, la DPA doit au minimum faire le lien entre les principes identifiés dans la ou les PA auxquelles la DPA répond et les principes et règles opérationnelles de sécurité (qu'ils soient dans la DPA ou une PSSI séparée), de manière à en démontrer la couverture exhaustive.

Une DPA est à priori un document confidentiel interne à l'AA et ses composantes, qui n'a pas à être rendue public. Pour appuyer ou compléter la ou les PA auxquelles elle se conforme, une AA peut éventuellement communiquer des extraits de sa DPA.

La mise en œuvre concrète et opérationnelle est ensuite réalisée, en conformité avec ce qui est identifié dans la DPA, au travers des procédures opérationnelles, des spécifications techniques des systèmes et des éventuels services externes, des cahiers des charges correspondants, des contrats, y compris les contrats de travail des personnels…

3.6 Liens entre PA, DPA et d'autres documents

Une PA identifie les principes que s'engage à respecter une AA dans la mise en œuvre d'un service d'archivage électronique sécurisé (la "cible"). Une PA peut être rédigée par l'AA elle-même ou par une entité tierce (par exemple, autorité hiérarchique de l'AA ou client de l'AA) et prise en compte et acceptée par l'AA. Dans tous les cas, à partir du moment où une AA s'engage à respecter une PA, elle est responsable de la conformité du service d'archivage électronique

La DPA est rédigée par ou sous la responsabilité de l'AA.

4 Contenu d'une PA

Le présent chapitre décrit le contenu attendu d'une PA : plan du document et pour chaque élément du plan, contenu requis.

Ce plan est également applicable à la rédaction d'une DPA.

Il est fortement recommandé que les rédacteurs de PA et DPA se conforment à ce plan commun. Un tel plan commun facilité en effet :

- la comparaison entre deux PA ou entre deux DPA (par exemple, dans le cas de la détermination d'équivalence entre deux AA lors du transfert d'archives d'une AA à une autre) ;
- la comparaison entre une DPA et une PA, afin de vérifier que les pratiques annoncées dans la DPA sont conformes aux objectifs et engagements définis dans la PA.

Pour chaque sous-chapitre, à l'exception de ceux du chapitre d'introduction, les principes devant / pouvant être retenus dans une PA, et à décliner dans une DPA, sont présentés sous la forme suivante :

<<Nom du principe>>
Description : <<Description du principe>>
Explication / Justification : <<Présentation de l'intérêt, de l'importance et de la portée du principe>>

4.1 Introduction

4.1.1 Objet du document

Ce chapitre doit présenter la portée du document, en particulier le ou les types d'archive qui sont couvertes ainsi que l'AA ou les types d'AA auxquelles il peut s'appliquer.

4.1.2 Nom et identification du document

Ce chapitre doit préciser le nom de la PA ainsi que, éventuellement, un identifiant d'objet (OID) pour le document. L'utilisation d'un OID permet de fournir au document une référence normalisée et unique qui peut ensuite être utilisée, par exemple, dans un paquet d'information pour préciser que ce paquet respecte la PA considérée.

4.2 Principes organisationnels

4.2.1 Politique d'archivage

Ce chapitre doit préciser les principes appliqués par l'AA pour la gestion de la PA.

PA-DIFF - Diffusion de la PA
Description :
La PA doit être diffusée à l'ensemble des parties concernées par le service d'archivage correspondant.
Explication / Justification :
La PA permet à chaque partie de prendre connaissance des principes que l'AA s'engage à respecter dans la délivrance du service d'archivage électronique.

PA-EVOL - Évolution de la PA
Description :
La PA doit être tenu à jour aussi bien vis-à-vis des évolutions internes qu'externes au service d'archivage.
Les principes mis en œuvre au sein du service d'archivage doivent être en permanence conformes à ceux présentés dans la PA correspondante. En cas d'écart, soit la mise en œuvre des principes doit être corrigée pour être conforme à la PA, soit la PA doit être corrigée pour être conforme aux principes effectivement mis en œuvre.
Explication / Justification :
La PA est le document de référence du service d'archivage et doit donc parfaitement refléter la réalité.

PA-CONT - Contrôle d'application de la PA
Description :
L'AA doit prévoir et mettre 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 PA et déclinés dans la DPA.
Explication / Justification :
Cf. principe PA-EVOL : la PA est le document de référence du service d'archivage.

4.2.2 Organisation et responsabilité du service d'archivage électronique

Ce chapitre doit présenter les principes mis en œuvre concernant l'organisation et les responsabilités des intervenants liés au service d'archivage. Au niveau de la PA, il s'agit de l'organisation fonctionnelle du service d'archivage, l'organisation opérationnelle et technique devant être décrite au niveau de la DPA. Pour la description de l'organisation fonctionnelle, le rédacteur peut utilement s'appuyer sur les éléments présentés aux chapitres 3.1 et 3.3 ci-dessus.

ORG-PA - Responsabilité de la PA
Description :
L'AA n'est pas forcément elle-même responsable de la rédaction et la tenue à jour de la PA. L'entité responsable de la PA doit donc être explicitement identifiée.
Explication / Justification :
La PA est le document de référence du service d'archivage. Les responsabilités concernant son élaboration et sa mise à jour doivent être claires.

ORG-AA - Responsabilité de l'AA

Description :

Quelque soit l'organisation opérationnelle interne du service d'archivage électronique, l'AA est responsable, vis-à-vis des intervenants externes au service (services versant, utilisateurs, contrôleurs,…) du respect des principes présentés dans la PA.

L'AA est notamment responsable de la DPA (élaboration, mise à jour, application, conformité avec la ou les PA concernées).

L'Autorité d'archivage est responsable des obligations qui lui incombent, en application de la ou des PA considérées, tant qu'elle tient son rôle d'Autorité d'archivage. En ce sens, dès lors que les Archives concernées sont transmises à une autre Autorité d'archivage (ce qui pourra notamment être le cas avec le changement d'âge de l'Archive), c'est cette nouvelle Autorité d'archivage qui endossera les responsabilités déterminées dans la PA qu'elle aura adoptée et qui trouvera à s'appliquer. La responsabilité de l'Autorité d'archivage vis à vis du Service versant jouera pleinement dès lors qu'elle aura émis l'accusé de réception de l'Archive versée.

Explication / Justification :

Les responsabilités respectives des différents intervenants liés au service d'archivage doivent être clairement définies.

ORG-PROD - Responsabilité du Service producteur

Description :

Le Service producteur s'il existe et lorsqu'il n'est pas le Service versant doit fournir toutes les informations utiles au Service versant et notamment les informations relatives à la nature et à la durée de vie de l'Archive ainsi que son éventuel caractère confidentiel et/ou les accès limités à l'Archive concernée, le cas échéant.

Le Service producteur est responsable de l'exactitude de ces informations et de leur bonne transmission au Service versant.

Explication / Justification :

Les responsabilités respectives des différents intervenants liés au service d'archivage doivent être clairement définies.

ORG-VERS - Responsabilité du Service versant

Description :

Le Service versant doit fournir les Archives à l'AA de destination.

Le Service versant s'engage à fournir toutes les informations relatives à la nature et à la durée de vie de l'Archive ainsi que leur éventuel caractère confidentiel et/ou les accès limités à l'Archive concernée, le cas échéant.

Le Service versant est responsable de l'exactitude de ces informations et de leur bonne transmission.

Pour préciser les conditions techniques mises en œuvre, le Service versant et l'Autorité d'archivage doivent passer un accord (convention, charte d'archivage,…) relative aux Versements, aux traitements et aux accès des Archives. Dans ce cadre, il convient de noter que la responsabilité du Service versant sera dégagée dès lors que l'accusé de réception de l'Autorité d'archivage sera émis, et ce, selon les modalités prévues dans leur accord. Cet accord doit être totalement conforme à la PA et à la DPA applicables.

Il appartient au Service versant de vérifier le caractère communicable de l'Archive ou de l'Objet d'archives 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).

Le cas échéant, le Service versant garantit que les supports et les Archives qu'ils contiennent sont en parfait état et exempts de tout virus ou autre dysfonctionnement susceptible d'avoir un impact sur la bonne exécution de la Politique d'Archivage et notamment sur les obligations de l'Autorité d'archivage ou sur les moyens informatiques utilisés.

Explication / Justification :

Les responsabilités respectives des différents intervenants liés au service d'archivage doivent être clairement définies.

ORG-CONT - Responsabilité des Contrôleurs
Description : Les Contrôleurs sont tenus d'exercer leurs contrôles dans le respect des textes législatifs et réglementaires qui encadrent leurs compétences. Ils s'engagent à respecter les procédures et procédés déterminés dans la présente PA pour mener leurs contrôles. Il leur appartient, dès lors qu'ils relèveraient des difficultés pour exercer leurs contrôles, d'en avertir par tout moyen l'AA compétente afin qu'elle y remédie. Le contrôleur peut donner une autorisation lorsqu'un Utilisateur souhaite consulter une Archive avant l'expiration du délai de non communicabilité.
Explication / Justification : Les responsabilités respectives des différents intervenants liés au service d'archivage doivent être clairement définies.

ORG-UTIL - Responsabilité des Utilisateurs et Usagers
Description : Les Utilisateurs et les Usagers doivent respecter les conditions de consultation et de communication afférentes au Service d'archivage électronique, au SAE et aux Objets d'archives traités. Ils doivent également respecter la confidentialité, le cas échéant, des Objets d'archives traités et ne pas tenter d'y accéder s'ils ne disposent pas des droits associés. A titre d'exemple, lorsqu'un Usager bénéfice d'une autorisation de consultation d'Archives dérogeant aux délais légaux de communicabilité, il doit s'engager formellement à ne pas publier et à ne communiquer aucune information recueillie dans ce cadre et qui pourrait porter atteinte à la sûreté de l'État, à la Défense nationale ou à la vie privée. Dans la mesure où l'Utilisateur ou l'Usager dispose d'un mode d'accès spécifique et personnel (Authentification par login, mot de passe, Certificat ou autres), il s'engage à le conserver confidentiel et en faire un usage sous son contrôle exclusif. De même, les Utilisateurs et les Usagers ne doivent pas tenter de détériorer tout ou partie du service d'archivage électronique sécurisé, du SAE et/ou de son contenu.
Explication / Justification : Les responsabilités respectives des différents intervenants liés au service d'archivage doivent être clairement définies.

ORG-SSI - Organisation de la sécurité des systèmes d'information (SSI)
Description : Chaque entité intervenant dans le service d'archivage électronique sécurisé doit avoir une organisation couvrant la sécurité des systèmes d'information (SSI) de ce service d'archivage électronique. Cette organisation peut être soit spécifique à aux activités d'archivage électronique, soit plus globale à l'entité, mais dans ce cas bien couvrir explicitement l'ensemble du périmètre lié au service d'archivage électronique.
Explication / Justification : Les responsabilités respectives des différents intervenants liés au service d'archivage doivent être clairement définies.

4.2.3 Gestion des risques de sécurité des systèmes d'information (SSI)

GER-BESOINS - Identification des besoins de sécurité du service d'archivage
Description : L'AA doit mener (ou faire mener) une identification des besoins de sécurité sur l'ensemble du service d'archivage électronique. Les besoins de sécurité doivent être exprimés pour les informations et fonctions du service d'archivage au moins en termes de disponibilité, d'intégrité et de confidentialité (en ajoutant éventuellement d'autres critères de sécurité tels que la traçabilité). Les besoins de sécurité ainsi validés par l'AA doivent servir de base aux études de risques au niveau des différentes entités. L'expression des besoins de sécurité doit être mise à jour au moins une fois par an et à chaque évolution significative du service d'archivage. Pour définir ces besoins de sécurité, il est recommandé de s'appuyer sur les étapes 1 et 2 de la méthode EBIOS[1] de la DCSSI.
Explication / Justification : La mise en place de mesures de sécurité doit être cohérente avec les besoins de sécurité.

GER-APPR - Appréciation des risques SSI
Description : Les entités en charge de la mise en œuvre des fonctions de stockage et de consultation / communication doivent apprécier les risques (les mettre en évidence et estimer leur importance) relatifs à la sécurité des systèmes d'information liés à leurs activités. Les besoins de sécurité validés par l'AA doivent servir de point d'entrée à cette étude, pour laquelle, il est recommandé de s'appuyer sur les étapes 3 et 4 de la méthode EBIOS de la DCSSI. L'AA doit valider la liste hiérarchiser des risques.
Explication / Justification : La mise en place de mesures de sécurité doit correspondre aux risques réels pesant sur le système, qu'il convient donc d'identifier objectivement.

GER-TRAIT - Traitement des risques SSI
Description : L'AA doit identifier (ou faire identifier) les objectifs de sécurité exprimant la volonté de traiter les risques mis en évidence. Elle doit choisir entre un refus (évitement de la situation à risque), une réduction, un transfert (vers des tiers) ou une prise de risques, en prenant en compte son contexte particulier. Les entités en charge de la mise en œuvre des fonctions de stockage et de consultation / communication doivent ensuite proposer des mesures de sécurité techniques ou non techniques pour traiter les risques identifiés en fonction des objectifs de sécurité identifiés par l'AA, et mettre en évidence les éventuels risques résiduels subsistant au traitement des risques. L'AA doit enfin valider les mesures de sécurité, éventuellement suite à plusieurs révisions des propositions, jusqu'à ce qu'elle soit satisfaite. Il est recommandé de s'appuyer sur les étapes 4 et 5 de la méthode EBIOS de la DCSSI.
Explication / Justification : Le traitement des risques doit être basé sur un arbitrage par l'AA des solutions proposées.

[1] Expression des Besoins et Identification des Objectifs de Sécurité

4.2.4 Sécurité et cycle de vie du SAE

CDV-PROJ - Intégration de la SSI dans les projets
Description : Tout projet lié à tout ou partie du SAE (nouveau composant, évolution d'un composant, remplacement d'un composant existant) doit prendre en compte les aspects SSI dans l'ensemble du cycle de vie projet (de la définition des besoins jusqu'au retrait du service). Cette prise en compte concerne l'identification des exigences de sécurité et des mesures correspondantes à implémenter dans les systèmes objet du projet ainsi que la sécurité du projet lui-même (sécurité des développements, sécurité de la documentation,…). Les responsabilités concernant la prise en compte et le traitement des aspects de sécurité au sein du projet doivent être cohérentes et en relation avec l'organisation et les responsabilités de sécurité au sein de la ou des entités concernées par le projet (cf. ORG-SSI). Les besoins de sécurité du service d'archivage, tels que validés par l'AA, qui concernent le projet considéré doivent être pris en compte dans la démarche de sécurité. Si le projet concerne une fonction faisant l'objet d'une analyse de risques (notamment, les fonctions de stockage et de consultation / communication), les exigences de sécurité à prendre en compte doivent être cohérentes avec les résultats de cette analyse. Si nécessaire, cette analyse doit être mise à jour.
Explication / Justification : Un nouveau composant ou l'évolution d'un composant existant peuvent entraîner, au niveau de tout ou partie du SAE, l'introduction de nouvelles vulnérabilités qu'ils convient de connaître et, si nécessaire, de traiter.

CDV-EXPLOIT - Conditions et contrôles de mise en exploitation
Description : La mise en exploitation en environnement de production de tout nouveau composant du SAE (logiciel ou matériel) doit préalablement faire l'objet de tests d'intégration sur une plate-forme de tests distincte de la plate-forme de production. De plus, les logiciels doivent faire l'objet de contrôle, avant toute mise en exploitation, vis-à-vis des virus et codes malicieux. L'entité concernée doit, au minimum, vérifier les fichiers correspondants au travers d'un antivirus à jour.
Explication / Justification : Tout nouveau logiciel peut contenir des codes malicieux, quelque en soit la source. De plus, tout nouveau logiciel peut poser des problèmes de compatibilité avec les logiciels existants et rendre ainsi le système instable.

CDV-CONTR - Contrôles de sécurité
Description : Chaque entité du service d'archivage, dans le cadre de son organisation de la sécurité (cf. ORG-SSI), doit mener des contrôles permanents de la sécurité au niveau opérationnel, portant notamment sur le respect des procédures d'exploitation et de sécurité, l'utilisation adéquate et le non-contournement des mécanismes de sécurité en place (journaux d'évènements), … Des contrôles réguliers doivent également être menés afin de vérifier le niveau de sécurité, au travers d'audit techniques et organisationnels et de tests d'intrusion.
Explication / Justification : La sécurité doit être appliquée de manière continue et il convient de la contrôler. Le niveau de sécurité doit être régulièrement revu afin de s'assurer de son adéquation.

CDV-AUDIT - Audit par l'AA
Description : L'AA doit s'assurer régulièrement du respect, par chaque entité du service d'archivage, des principes définis dans la PA et des exigences de la DPA correspondante. Ces vérifications peuvent se faire au travers d'auto-évaluations, réalisées par chaque entité et dont les résultats sont transmis à l'AA, complétés par des audits sur site diligentés par l'AA.
Explication / Justification : L'AA est responsable de l'ensemble du service d'archivage et doit donc s'assurer que les engagements qu'elle prend sont bien respectés.

4.2.5 Aspects légaux et métiers

ALM-SECR - Secret professionnel
Description : 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 électronique doit respecter ces obligations.
Explication / Justification : Le secret professionnel doit être respecté en permanence et en toutes circonstances.

ALM-PERS - Protection des données personnelles
Description : 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.
Explication / Justification : La protection des données à caractère personnel doit être respectée en permanence et en toutes circonstances.

ALM-COMM - Obligation sur le caractère communicable des Archives
Description : Chaque intervenant s'engage à respecter les règles législatives et réglementaires applicables en matière de communicabilité des documents administratifs et des Archives publiques. 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). 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.
Explication / Justification : Cette obligation doit être respectée en permanence et en toutes circonstances.

ALM-PROPR - Droits sur la propriété intellectuelle et industrielle
Description : 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 électronique 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 doivent être respectés. Dans ce cadre, la responsabilité civile et pénale de celui qui violerait ces droits est susceptible d'être engagée.
Explication / Justification : Ces droits doivent être respectés en permanence et en toutes circonstances.

ALM-FORCE - Force majeure
Description : 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.
Explication / Justification : Cette limitation de responsabilité est applicable en permanence et en toutes circonstances.

ALM-CRYP - Régime juridique des moyens de cryptologie
Description : La confidentialité des Archives et Objets d'archives peut nécessiter le recours à des moyens de cryptologie. Le cas échéant, le service concerné devra s'assurer du respect du régime juridique applicable en la matière conformément aux articles 29 à 32 de la loi pour la confiance dans l'économie numérique.
Explication / Justification : Cette obligation s'applique si des moyens de cryptologie sont mis en œuvre.

4.3 Principes de mise en œuvre

4.3.1 Aspects humains

ASH-SELEC - Critères de sélection du personnel travaillant sur le SAE
Description : Le travail de tout personnel intervenant sur le SAE, à quelque niveau que ce soit (opérateur, administrateur, maintenance, etc.) doit faire l'objet d'une fiche de poste définissant clairement les rôles, obligations et responsabilités du personnel concerné. L'adéquation entre le personnel et la fiche de poste doit faire l'objet de vérifications préalables vis-à-vis des compétences requises ainsi que des antécédents qui pourraient être en contradiction avec les exigences du poste (honnêteté, probité, absence de conflits d'intérêts,…). Chaque fiche de poste doit être formellement acceptée par le personnel concerné. La fiche de poste doit être en permanence conforme aux attributions effectives du personnel concerné. En cas d'évolutions des attributions, il peut être nécessaire de procéder à des vérifications supplémentaires en fonction de la nouvelle fiche de poste.
Explication / Justification : Le SAE dans son ensemble constitue un système d'information sensible et les personnels amenés à intervenir sur ce système doivent être sélectionnés en conséquence afin d'éviter les risques de malversation et d'erreurs de manipulation.

ASH-RESP - Habilitations
Description : Le SAE ne doit être accessible, physiquement et logiquement, qu'à des personnes nominativement autorisées. Ainsi, des restrictions d'accès aux systèmes et informations doivent être définies conformément à leur besoin de sécurité et à la criticité des actions autorisées sur ces données et ressources (cf. identification des besoins de sécurité et analyses de risques). Les habilitations doivent être attribuées à une personne physique et être incessibles. Elles doivent être totalement cohérentes avec la fiche de poste correspondante. La définition et l'attribution des habilitations doit se faire dans le cadre de l'organisation SSI que chaque entité du service d'archivage doit mettre en place (cf. ORG-SSI). Elles doivent respecter les principes de moindre privilège et de besoin d'en connaître : tout personnel doit avoir accès exclusivement aux fonctions et informations nécessaires à son travail tel que défini dans sa fiche de poste.
Explication / Justification : Le SAE dans son ensemble constitue un système d'information sensible et l'accès par des personnes non autorisés à des fonctions ou informations sensibles peut se traduire par une perte de confidentialité, d'intégrité et/ou de disponibilité sur ces fonctions / informations soit par malveillance, soit par erreur (personne non compétente / non formée pour les fonctions / les informations considérées).

ASH-CONF - Définition des rôles de confiance

Description :

Chaque entité intervenant dans le service d'archivage doit identifier et définir explicitement les rôles de confiance requis pour assurer le fonctionnement et la sécurité de la partie du service d'archivage qui lui incombe. Un rôle de confiance est un rôle qui intervient sur la définition, la mise en œuvre et / ou la vérification des opérations du service d'archivage. Peuvent notamment être distingués les rôles suivants :

- Responsable de sécurité (mise en œuvre de la politique de sécurité de l'entité et couvrant le service d'archivage ; analyse des journaux d'évènements afin de détecter tout incident / anomalie / tentative de compromission).
- Responsable d'application / de base de données (mise en œuvre, pour l'application dont il a la responsabilité, de procédures correspondant aux pratiques d'archivage ; définition et gestion des droits sur l'application / la base de données)
- Ingénieur système (mise en route / configuration / maintenance / administration des systèmes d'information et des réseaux de l'entité)
- Opérateur du SAE (mise en œuvre et exploitation de tout ou partie des opérations du SAE)

S'agissant de rôles fonctionnels, une même personne physique peut détenir plusieurs rôles de confiance et un même rôle peut être détenu par plusieurs personnes physiques. Pour chaque rôle de confiance, l'entité concernée doit formellement et explicitement désignée quelle(s) personne(s) a en charge quel(s) rôle(s).

Explication / Justification :

Un rôle de confiance, de par les droits qui lui sont conférés, peut être amené à réaliser des actions au niveau du service d'archivage qui peuvent se traduire par des accès aux archives, des modifications d'archives, des destructions d'archives,… Il est donc indispensable que ces rôles et les personnes qui en ont la charge soient clairement et formellement identifiés et qu'il y ait un minimum de cloisonnement entre ces rôles afin d'éviter qu'une seule personne détienne suffisamment de droits pour mener des actes malveillants sans que l'entité ne puisse le prévenir ou le détecter.

ASH-CLOIS - Cloisonnement des postes sensibles

Description :

Si une même personne peut détenir plusieurs rôles de confiance, l'entité doit cependant définir une séparation minimale à respecter entre fonctions afin de s'assurer que toute opération sensible fera bien intervenir au moins deux personnes physiques différentes (pour la réalisation elle-même, ou bien pour la réalisation puis la vérification). Typiquement, le rôle de "responsable sécurité", en charge notamment de l'analyse des journaux d'activités, devrait être exclusif de tout autre rôle.

Explication / Justification :

Un rôle de confiance, de par les droits qui lui sont conférés, peut être amené à réaliser des actions au niveau du service d'archivage qui peuvent se traduire par des accès aux archives, des modifications d'archives, des destructions d'archives,… Il est donc indispensable que ces rôles et les personnes qui en ont la charge soient clairement et formellement identifiés et qu'il y ait un minimum de cloisonnement entre ces rôles afin d'éviter qu'une seule personne détienne suffisamment de droits pour mener des actes malveillants sans que l'entité ne puisse le prévenir ou le détecter.

4.3.2 Planification de la continuité des activités

PSS-PCA Élaboration du plan de continuité des activités
Description : L'AA doit disposer d'un plan de continuité d'activités (PCA) couvrant l'ensemble des activités du service d'archivage électronique. Le plan de continuité d'activité doit être réalisé à partir d'une analyse de risques. Le PCA doit être composé d'une analyse d'impacts métiers (*Business Impact Analysis* - BIA) et d'un ensemble de plans spécifiques, chacun destiné à décrire les procédures de réaction à des événements particuliers (par exemple un plan de reprise informatique, un plan de restauration des informations…). Les procédures définies dans les différents plans doivent permettre de maintenir les activités du service d'archivage conformément aux besoins en continuité exprimés par l'AA (cf. GER-BES-SEC). Le PCA doit être régulièrement testé (au moins une fois par an) et mis à jour en fonction des résultats de ces tests.
Explication / Justification : L'AA, en tant que responsable de l'ensemble du service d'archivage électronique, doit prévoir la conduite à tenir en cas de désastre, notamment la défaillance d'une des entités.

4.3.3 Gestion des incidents

INC-DETECT - Détection et traitement des incidents de sécurité
Description : Chaque entité intervenant dans le service d'archivage électronique doit définir l'organisation et les procédures à suivre en cas d'incident de sécurité. Il s'agit, dans un premier temps, de définir les situations anormales à prendre en compte (panne, défaillance, intrusion,…), puis de définir qui doit faire quoi lorsqu'une de ces situations apparaît.
Explication / Justification : Afin de limiter les conséquences des incidents de sécurité, les démarches à suivre doivent être préalablement définies et connues pour permettre une réaction rapide.

INC-AA - Remonté d'information à l'AA
Description : L'AA doit définir les informations sur les incidents de sécurité qui doivent lui être transmis ainsi que la fréquence des ces transmissions.
Explication / Justification : L'AA, en tant que responsable de l'ensemble du service d'archivage électronique, doit pouvoir suivre les principales anomalies survenues et pouvant impacter le service.

INC-CAPIT - Capitalisation sur les incidents de sécurité
Description : Les incidents de sécurité survenus, et les traitements correspondants, doivent être pris en compte pour améliorer de manière continue les opérations et la sécurité du SAE.
Explication / Justification : La capitalisation sur les incidents de sécurité survenus est indispensable pour éviter qu'ils ne se reproduisent.

4.3.4 Sensibilisation et formation

FOR-OPER - Formation aux opérations
Description :
Chaque intervenant dans le service d'archivage électronique doit être préalablement formé aux opérations qu'il aura à mener. Cette formation doit être régulièrement mise en jour, en fonction des évolutions des systèmes et des procédures.
Explication / Justification :
Une mauvaise manipulation sur les systèmes ou une mauvaise application des procédures peut se traduire par des conséquences graves (pertes de données, divulgation d'informations confidentielles,…).

FOR-SSI - Sensibilisation à la SSI
Description :
Chaque intervenant dans le service d'archivage électronique doit avoir conscience des enjeux en matière de sécurité des systèmes d'information ainsi que des obligations et responsabilités correspondantes qui lui incombent. Chaque entité doit définir ses objectifs en matière de sensibilisation à la SSI, en fonction éventuellement de différents types de population. Les personnels en charge de rôles de confiance doivent faire l'objet d'une attention particulière. Cette sensibilisation doit comporter un volet sur le traitement des incidents et la gestion des situations de crise.
Explication / Justification :
L'adhésion des intervenants à la démarche de SSI ne pourra se faire que si ceux-ci comprennent les enjeux correspondants et connaissent effectivement les éléments liés à cette démarche.

4.3.5 Exploitation

EXP-PROC - Procédures et règles d'exploitation
Description :
Chaque entité intervenant dans le service d'archivage doit documenter les procédures et règles d'exploitation des parties du SAE qui lui incombent. Les règles correspondantes en matière de SSI doivent y être intégrées.
Explication / Justification :
Une exploitation adéquate des systèmes et une application des règles de sécurité par les utilisateurs nécessitent que ces éléments soient formalisés.

EXP-DEV - Développement des systèmes
Description :
Les activités de développement, d'intégration et de test de nouveaux systèmes, ou de nouvelles versions de systèmes existants, doivent être séparées (tâches et environnement physique) des activités d'exploitation opérationnelle. La mise en production opérationnelle d'un nouveau système ou d'une nouvelle version doit faire l'objet d'un processus de validation formelle.
Explication / Justification :
Les aspects de développement et de test peuvent entraîner une instabilité des systèmes, ils doivent donc être menés séparément des environnements d'exploitation.

EXP-MAINT - Maintenance des systèmes
Description : Les opérations de maintenance sur les systèmes en exploitation doivent être préparées. Les procédures d'intervention sur les systèmes (à chaud ou à froid) doivent être formalisées et les éléments objet de la maintenance doivent être préalablement testés dans un environnement séparé avant leur mise en exploitation. Les opérations de maintenance doivent être réalisées sous le contrôle de personnels dans des rôles de confiance. Les opérations de maintenance doivent faire l'objet d'une traçabilité complète.
Explication / Justification : La maintenance d'un système est un élément clé pour permettre d'assurer, dans le temps, un niveau de performance et de sécurité adéquat. Cependant, les opérations de maintenance peuvent entraîner des perturbations sur les systèmes qu'il convient de contrôler et de minimiser.

EXP-VIRUS - Lutte contre les virus et les codes malveillants
Description : Chaque entité du service d'archivage doit mettre en place une organisation et des outils de lutte contre les virus et les codes malveillants. Tout fichier (logiciels, données) provenant de l'extérieur de l'entité doit être contrôlé, quelque soit son point d'entrée (réseau, disquette, CD,...).
Explication / Justification : L'introduction de codes malveillants dans le système peut entraîner des problèmes allant de la perturbation du fonctionnement des systèmes jusqu'à leur arrêt complet, en passant par la divulgation d'informations confidentielles.

EXP-SUPP - Gestion des supports
Description : Les supports d'information (informatiques et papiers) doivent faire l'objet d'une gestion formalisée conforme aux besoins de sécurité correspondants, afin d'assurer la confidentialité mais également la disponibilité / intégrité / pérennité des informations qui y sont stockées. Tout support provenant de l'extérieur doit être contrôlé (cf. EXP-VIRUS). La réutilisation / mise au rebut / sortie des locaux (maintenance) de supports doit faire l'objet de procédures strictes liées à l'effacement sécurisé des données contenues sur le support ou la destruction physique du support.
Explication / Justification : Les supports d'informations sont soumis à différents risques pouvant avoir des conséquences sur les informations stockées : dégradation des informations, divulgation à des personnes non autorisées,…

4.3.6 Aspects physiques et environnement

ENV-PHY - Contrôle d'accès physique
Description : Les locaux abritant le SAE doivent faire l'objet de contrôle d'accès physique empêchant l'accès à des personnes non autorisées aux ressources du SAE. Les contrôles d'accès doivent être complétés par des mécanismes de surveillance au moins en dehors des heures ouvrables : alarme et vidéo-surveillance.
Explication / Justification : L'accès physique aux machines peut permettre à une personne malintentionnée de tenter de piéger physiquement la machine ou de contourner les contrôles d'accès logiques. Les contrôles d'accès physique sont un complément indispensable aux contrôles d'accès logiques.

ENV-ACC - Protection contre les accidents et pannes
Description : Les locaux hébergeant le SAE doivent être protégés contre les accidents et pannes dus à l'environnement : dégâts des eaux, incendies, pannes électriques, panne de la climatisation, panne des réseaux de télécommunication. Les exigences concernant ces éléments doivent être conformes aux besoins de sécurité, définis par l'AA, des éléments du service d'archivage auxquels ils sont liés ainsi qu'aux résultats des éventuelles analyses de risques.
Explication / Justification : Les éléments liés à l'environnement peuvent entraîner des pertes de disponibilité des équipements et des pertes de données.

4.4 Principes techniques

4.4.1 Identification / authentification

AUT-UTIL - Identification / authentification des utilisateurs
Description : Les utilisateurs du SAE doivent faire l'objet d'une identification personnelle et unique. Les rôles de confiance doivent faire l'objet d'une authentification forte. Dans le cas d'une authentification par mot de passe, l'usage de ce mot de passe pour d'autres applications que le SAE doit être proscrit. La gestion des mots de passe et moyens d'authentification doit se faire dans le cadre de l'organisation sécurité de l'entité, sous le contrôle du responsable sécurité, et en cohérence avec les engagements et habilitations des personnels (cf. ASH-RESP).
Explication / Justification : L'identification / authentification des utilisateurs est la base pour la gestion des contrôles d'accès logique aux applications et informations et la traçabilité des actions.

4.4.2 Contrôle d'accès logique aux biens

CAL-UTIL - Gestion des accès des utilisateurs
Description : La gestion des accès d'un utilisateur authentifié est du ressort du responsable de l'application. Cette gestion doit être strictement conforme aux habilitations accordées (cf. ASH-RESP) et respecter notamment le principe de moindre privilège. Les droits d'accès doivent être gérés conformément aux procédures d'arrivée / départ des personnels et ils doivent faire l'objet de revues régulières (au moins une fois par trimestre) afin de supprimer les éventuels droits qui seraient restés ouverts inutilement.
Explication / Justification : Les droits d'accès sont l'élément central de la sécurité du système. Ils doivent donc faire l'objet d'une gestion très rigoureuse.

CAL-INTEG - Intégrité des Archives / Paquets d'information / Objets d'archive
Description : Le contrôle d'intégrité doit avoir lieu à plusieurs niveaux du processus d'archivage. Tout d'abord au moment du Versement afin de s'assurer que les Paquets d'information reçus et prêts à intégrer le SAE sont bien ceux envoyés par le Service versant. Si le Paquet d'information fait l'objet d'une signature électronique, une vérification de cette signature devra être effectuée dans le cadre du SAE. Ensuite, le contrôle d'intégrité doit être opéré tout au long de la conservation des Objets d'archives sans attendre des migrations éventuelles ou l'interrogation par des Utilisateurs ou Usagers. Des dispositifs de vérification d'intégrité basés sur l'empreinte des documents doivent ainsi être régulièrement réalisés par sondage dans le cadre du SAE.
Explication / Justification : La garantie d'intégrité des informations archivées tout au long de leur cycle de vie est un élément fondamental du service d'archivage électronique sécurisé.

4.4.3 Journalisation

JRN-CONSTIT - Constitution des données de traçabilité
Description : Afin de constituer un ensemble de données à la fois suffisantes et cohérentes en matière de traçabilité, les opérations suivantes doivent être effectuées et validées avant la mise en place de tout SAE : - Identifier les différents types d'événements à enregistrer ; - Définir les informations enregistrées pour chaque type et évènement ; - Décider d'une notification ou non de l'enregistrement d'un événement au responsable de l'événement, par type d'évènement et selon quelles modalités ; - Définir une fréquence a priori minimum de traitements des journaux d'événements même si toute latitude doit être laissée à ce niveau. Comme traitements devront être entre autres analysées la recherche d'anomalies ou encore la migration dans un mode de conservation à plus long terme ; - Par rapport à ce dernier point, définir une période de conservation des journaux d'événements ; - Vérifier les dispositifs de sécurité mis en place et destinés à assurer la protection des journaux d'événements ; - Vérifier en particulier, en complément au point précédent, la procédure de sauvegarde des journaux d'événements.
Explication / Justification : Compte tenu des obligations et engagements de l'AA vis-à-vis des intervenants externes au service d'archivage, et des entités du service d'archivage vis-à-vis de l'AA, la journalisation des évènements est indispensable pour s'assurer et démontrer que les opérations ont bien été effectuées conformément aux PA / DPA / Procédures applicables et, en cas de problème, en déterminer la cause et les responsabilités éventuelles.

JRN-HORO - Horodatage des opérations
Description : Afin d'éviter toute remise en cause de l'horodatage réalisé par le SAE, ce dernier reposera sur un procédé conforme à l'état de l'art (soit actuellement la RFC 3161) et à tout le moins aura recours à deux sources de temps distinctes afin de dater les différentes opérations réalisées (Versement, Communication, Consultation, Élimination).
Explication / Justification : Le rapprochement entre les différents journaux d'évènements afin de remonter à la cause d'un problème nécessite une synchronisation des horloges des différents systèmes vis-à-vis d'une source de temps fiable.

5 ANNEXE – Liste des textes et documents de référence

5.1 Conservation des documents électroniques dans la sphère publique

Outre le Code du patrimoine et le Code général des collectivités territoriales et notamment leurs parties réglementaires, il convient de se reporter aux textes suivants :

- **Loi n° 78-753 du 17 juillet 1978** portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal (J.O. du 18 juillet 1978, p. 2851 et s.) modifiée.

- **Loi n° 79-18 du 3 janvier 1979 sur les archives** (J.O. du 5 janvier 1979, p. 43 et s.).

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

- **Loi n° 2000-321 du 12 avril 2000** relative aux droits des citoyens dans leurs relations avec les administrations (J.O. du 13 avril 2000, p. 5646 et s.).

- **Loi n° 2001-1246 du 21 décembre 2001 de financement de la sécurité sociale pour 2002** (J.O. du 26 décembre 2001, p. 20552).

- **Loi n° 2002-276 du 27 février 2002** relative à la démocratie de proximité (J.O. du 28 février 2002, p. 3808 et s.).

- **Loi n° 2003-591 du 2 juillet 2003** habilitant le Gouvernement à simplifier le droit (J.O. du 3 juillet 2003, p. 11192 et s.).

- **Loi n° 2004-809 du 13 août 2004** relative aux libertés et responsabilités locales (J.O. du 17 août 2004, p. 14545).

- **Loi n° 2004-1343 du 9 décembre 2004** de simplification du droit (J.O. du 10 décembre 2004, p. 20857).

- **Ordonnance n° 2004-164 du 20 février 2004** relative aux modalités et effets de la publication des lois et de certains actes administratifs (J.O. du 21 février 2004, p. 3514)**..**

- **Ordonnance n° 2004-178 du 20 février 2004** relative à la partie législative du code du patrimoine (J.O. du 24 février 2004, p. 37048 et s.).

- **Ordonnance n° 2005-650 du 6 juin 2005** relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques (J.O. du 7 juin 2005, p. 10022 et s.).

- **Ordonnance n° 2005-1516 du 8 décembre 2005** relative aux échanges électroniques entre usagers et autorités administratives et entre autorités administratives (J.O. du 9 décembre 2005).

- **Décret n° 79-1037 du 3 décembre 1979** relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques (J.O.R.F. du 5 décembre 1979).

- **Décret n° 79-1038 du 3 janvier 1979** relatif à la communicabilité des documents d'archives publiques (J.O. du 5 décembre 1979, p. 3058).

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

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

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

- **Décret n° 2001-492 du 6 juin 2001** pris pour l'application du chapitre II du titre II de la loi n° 2000-321 du 12 avril 2000 et relatif à l'accusé de réception des demandes présentées aux autorités administratives (J.O. du 10 juin 2001, p. 9246 et s.).

- **Décret n° 2001-493 du 6 juin 2001** pris pour l'application de l'article 4 de la loi n° 78-753 du 17 juillet 1978 et relatif aux modalités de communication des documents administratifs (J.O. du 10 juin 2001, p. 9246 et s.).

- **Décret n° 2001-846 du 18 septembre 2001** pris en application du 3° de l'article 56 du code des marchés publics et relatifs aux enchères électroniques (J.O. du 19 septembre 2001, p. 14847 et s.).

- **Décret n° 2002-535 du 18 avril 2002** relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information (J.O. du 19 avril 2002, p. 6944).

- **Décret n° 2002-692 du 30 avril 2002** pris en application du 1° et du 2° de l'article 56 du code des marchés publics et relatifs à la dématérialisation des procédures de passation des marchés publics (J.O. du 3 mai 2002, p. 8064).

- **Code des marchés publics issu du décret n° 2004-15 du 7 janvier 2004** (J.O. du 8 janvier 2004, p. 37003).

- **Décret n° 2004-617 du 29 juin 2004** relatif aux modalités et effets de la publication sous forme électronique de certains actes administratifs au Journal officiel de la République française (J.O. du 30 juin 2004).

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

- **Décret n° 2004-1298 du 26 novembre 2004** relatif à diverses dispositions concernant les marchés de l'État et des collectivités territoriales (J.O. du 30 novembre 2004, p. 20310 et s.).

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

- **Décret n° 2005-324 du 7 avril 2005** relatif à la transmission par voie électronique des actes des collectivités territoriales soumis au contrôle de légalité et modifiant la partie réglementaire du code général des collectivités territoriales (J.O. du 8 avril 2005, p. 6340).

- **Décret n° 2005-222 du 10 mars 2005** relatif à l'expérimentation de l'introduction et de la communication des requêtes et mémoires et de la notification des décisions par voie électronique (J.O. du 11 mars 2005, p. 4212 et s.).

- **Décret n°2005-972 du 10 août 2005** modifiant le décret n°56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice, (J.O. du 11 août 2005, p. 13095) et **décret n°2005-973 du 10 août 2005** modifiant le décret n°71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, (J.O. du 11 août 2005, p. 13096).

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

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

- **Circulaire du 2 novembre 2001 relative à la gestion des archives dans les services et établissements publics de l'État** (PRMX0105139C).

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

- **Circulaire du 4 décembre 2002** du Premier ministre, précisant les conditions de la mise en œuvre du cadre commun d'interopérabilité définit par le circulaire du 21 janvier 2002 (version 2)

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

- **Note d'information du 18 octobre 2004** rédigée par F. BANAT-BERGER, intitulée « *Résumé du rapport de J.-F. BLANCHETTE sur "la conservation de la signature électronique : Perspectives archivistiques*, septembre 2004*"* » (DITN/RES/2004/04).

- **Instruction du 14 janvier 2005** relative aux modalités de délivrance du visa d'élimination des documents papier transférés sur support numérique ou micrographique (DITN/DPACI/RES/2005/001).

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

- **Recommandations du 29 mars 2005** relatives à la gravure, à la conservation et à l'évaluation des CD-R (DITN/RES/2005/004) **Référentiel général d'interopérabilité** visé par le projet d'ordonnance pris en application de l'article 3 de la loi n° 2004-1343 du 9 décembre 2004 de simplification du droit (J.O. du 10 décembre 2004, p. 20857).

5.2 Données à caractère personnel

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

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

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

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

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

5.3 Autres documents

À titre principal :

- **Le guide « *Conservation des informations et des documents numériques pour les téléprocédures, les intranets et les sites internet : format, support, métadonnées, organisation, XML et normalisation* »** de l'Agence pour les Technologies de l'Information et de la Communication dans l'Administration (ATICA) repris par l'Agence pour le Développement de l'Administration Électronique (ADAE).

- **Politique de Référencement Intersectorielle de Sécurité (PRIS) - V1 -** relative à la mise en place d'un référentiel documentaire identifiant des niveaux croissants de sécurité s'appliquant à différents services de confiance et disponible sur le site www.adele.gouv.fr.

- **Politique de Référencement Intersectorielle de Sécurité (PRIS) – V2,** disponible sur le site www.adele.gouv.fr, en matière d'archivage, la PC Type – Authentification.

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

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

- **Les archives électroniques,** Manuel pratique publié par la Direction des archives de France, Catherine Dhérent, 2002, disponible sur commande à l'adresse suivante : http://larecherche.servicepublic.fr/df/oxide?criteriaContent=dherent&page=resultsdfB&action=launchsearch&DynRubrique=Catalogue&DynCorpus=&DynDomain=Catalogue

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

- La méthode d'expression des besoins et d'identification des objectifs de sécurité (EBIOS), DCSSI, février 2004, disponible sur le site de la DCSSI http://www.ssi.gouv.fr.

- **Le guide pour l'élaboration d'une politique de sécurité de système d'information** (PSSI), DCSSI, mars 2004, disponible sur le site de la DCSSI http://www.ssi.gouv.fr.

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

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

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

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

Si oui :

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

Si oui :

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

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

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

Si oui :

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

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

Si non :

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

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

Remarques particulières sur le document

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

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

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

La seconde lettre précise son caractère :

- m mineur
- M Majeur

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

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

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

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

Merci de votre contribution