



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

---

# MÉMENTO

**Version du 16 mai 2006**

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

avec le concours

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

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

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

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](mailto:conseil.dcssi@sgdn.pm.gouv.fr)

## Historique des modifications

<b>Version</b>	<b>Objet de la modification</b>	<b>Statut</b>
01/03/2006	Création du document sur la base d'un marché public (N°CO05000012 du 20 juin 2005, sur la fourniture d'une étude relative à la sécurité globale des services d'archivage)	Version de travail
16/05/2006	Finalisation	Validé

# Table des matières

<b>1</b>	<b>CONTEXTE, OBJET ET OBJECTIFS DU PRÉSENT MÉMENTO .....</b>	<b>5</b>
1.1	FINALITÉ DE CE MÉMENTO .....	5
1.2	DÉMARCHE RETENUE .....	6
<b>2</b>	<b>PROBLÉMATIQUE DE L'ARCHIVAGE ÉLECTRONIQUE SÉCURISÉ.....</b>	<b>7</b>
<b>3</b>	<b>CONTEXTE ET ENJEUX DE L'ARCHIVAGE ÉLECTRONIQUE SÉCURISÉ.....</b>	<b>9</b>
3.1	ARCHITECTURE DE L'ARCHIVAGE ÉLECTRONIQUE .....	9
3.2	ENJEUX JURIDIQUES DE L'ARCHIVAGE ÉLECTRONIQUE .....	11
3.2.1	<i>Précisions sur la notion d'archives et le concept d'archivage électronique sécurisé..</i>	<i>11</i>
3.2.2	<i>Principes juridiques directeurs impactant l'archivage électronique sécurisé .....</i>	<i>12</i>
3.2.3	<i>Obligations juridiques et recommandations subséquentes en matière d'archivage électronique .....</i>	<i>14</i>
3.2.4	<i>Régimes de responsabilité .....</i>	<i>15</i>
<b>4</b>	<b>ASPECTS OPÉRATIONNELS DE L'ARCHIVAGE ÉLECTRONIQUE SÉCURISÉ DANS LA SPHÈRE PUBLIQUE .....</b>	<b>16</b>
4.1	LA COHÉRENCE DE L'ARCHIVAGE ÉLECTRONIQUE DANS L'ENSEMBLE DE L'ORGANISME.....	16
4.2	LES DOCUMENTS SUR LESQUELS REPOSE UN ARCHIVAGE ÉLECTRONIQUE SÉCURISÉ .....	17
4.2.1	<i>Une Politique d'archivage.....</i>	<i>17</i>
4.2.2	<i>Un cahier des charges.....</i>	<i>18</i>
4.2.3	<i>Une grille d'audit.....</i>	<i>18</i>
	<b>FORMULAIRE DE RECUEIL DE COMMENTAIRES.....</b>	<b>19</b>

# 1 Contexte, objet et objectifs du présent mémento

## 1.1 Finalité de ce mémento

Ce mémento présente les résultats d'une étude initiée par la DCSSI relative à l'archivage électronique sécurisé.

Cette étude est partie :

- d'un **constat** : l'archivage électronique est devenu incontournable du fait de la mutation des échanges et du patrimoine informationnel ;
- et d'une **préoccupation** : l'archivage électronique doit apporter un certain nombre de garanties. En ce sens, il faut dès aujourd'hui prendre en compte les contraintes, modalités et conditions applicables à l'archivage électronique afin que celui-ci permette de garantir dans le temps les archives électroniques.

**L'archivage électronique sécurisé peut ainsi être défini comme l'ensemble des modalités de conservation et de gestion des archives 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.** L'archivage électronique sécurisé revêt également une dimension patrimoniale certaine.

Dans le cadre de ce mémento, il s'agit de présenter de façon concise les éléments à prendre en compte en amont de la mise en place d'un projet d'archivage électronique sécurisé et les documents nécessaires à sa mise en œuvre.

Ce mémento permet à la fois de sensibiliser les décideurs à l'archivage électronique sécurisé qui est devenu incontournable dans la société de communication actuelle et d'apporter des informations stratégiques liées à la dimension pluridimensionnelle de l'archivage électronique sécurisé. Ce mémento peut également constituer un support intéressant pour les personnes en charge de l'archivage au sein de la structure concernée. Il pose en ce sens les bases qui doivent être prises en compte dans le cadre de l'archivage électronique sécurisé.

Au demeurant, si l'étude dont est issu ce mémento s'adresse aux acteurs de la sphère publique, avec sa législation et réglementation spécifiques et son organisation des archives publiques, la démarche présentée dans ce mémento pourra néanmoins s'étendre également au secteur privé et à ses propres spécificités.

## 1.2 Démarche retenue

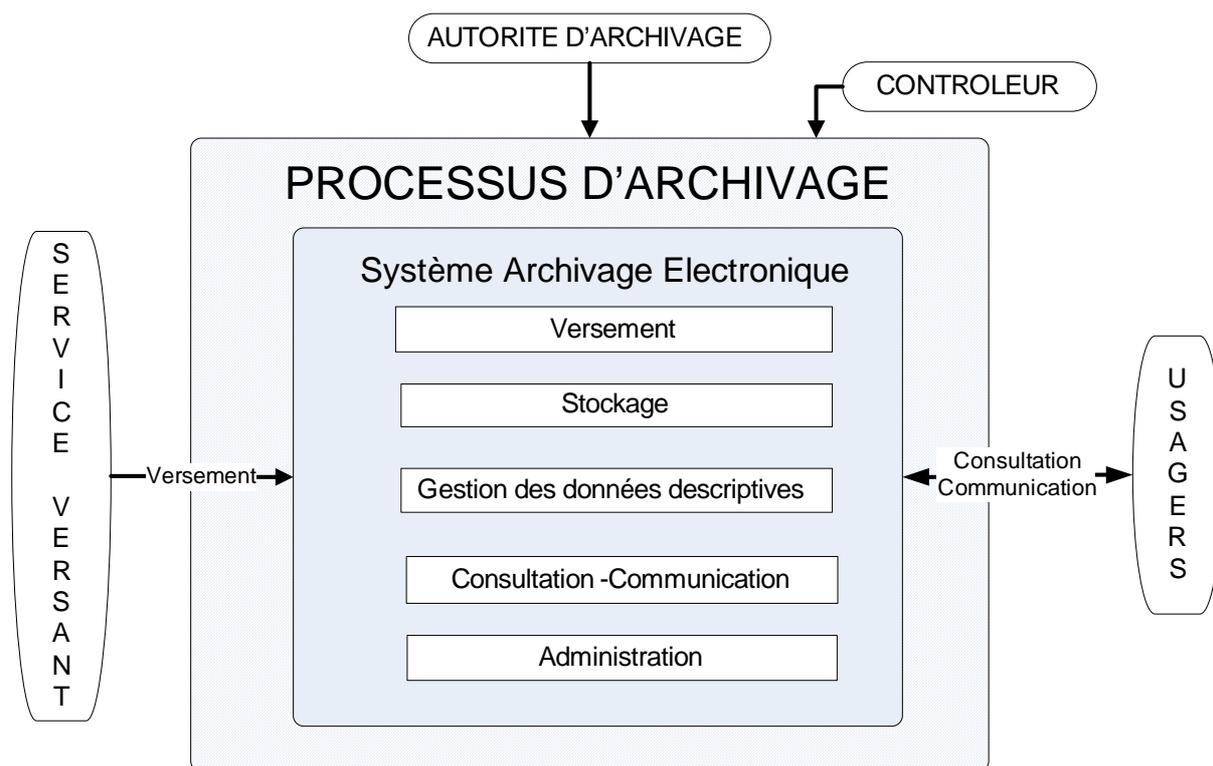
La démarche initiée par la DCSSI repose avant tout sur l'état de l'art dans le domaine, d'où la prise en compte de l'existant de façon exhaustive en matière de législation mais aussi de normes et de meilleures pratiques. Des « outils » complémentaires ont également été intégrés dans la réflexion. Tel a notamment été le cas du guide d'élaboration de politiques de sécurité des systèmes d'information (PSSI) publié par la DCSSI.

La démarche s'appuie également sur les travaux actuellement en cours dans le cadre du référentiel général d'interopérabilité, visant notamment à élaborer un standard d'échange pour le versement, la communication et l'élimination des archives électroniques (travaux menés par la DAF et la DGME dans le cadre de l'action 103 du plan ADELE).

Compte tenu de la nécessité de traiter plusieurs disciplines en parallèle, l'approche a été globale avec la prise en compte de l'ensemble des phases de l'archivage électronique sécurisé : planification, mise en œuvre, vérification et amélioration continue.

Enfin, les documents présentés ci-après ont été conçus dans le souci d'être à la fois autonomes et autosuffisants.

Le schéma suivant récapitule les différents intervenants, phases et éléments pris en compte dans un archivage électronique sécurisé.



## 2 Problématique de l'archivage électronique sécurisé

Compte tenu de l'évolution des technologies et des avantages liés aux nouveaux moyens de communication qu'elles impliquent (notamment gain de temps et diminution des coûts), les échanges électroniques et l'utilisation des nouvelles technologies prennent une place de plus en plus importante au sein de la société. Les actes de la vie quotidienne (contrats, déclarations, décisions, notes d'informations...) sont ainsi réalisés de plus en plus souvent par voie électronique. Cela touche autant les acteurs de droit privé (entreprises particuliers) que les personnes publiques (administrations au sens large, usagers). Ce mouvement s'inscrit au demeurant dans une démarche globale, notamment avec les initiatives communautaires dont l'adoption de directives et le projet e-Europe.

Au niveau national, le droit a accompagné cette évolution des pratiques tant dans la sphère privée que publique. Les textes se sont ainsi succédés. A titre principal, on peut citer la loi du 13 mars 2000 portant réforme du droit de la preuve et introduisant dans le code civil l'écrit sous forme électronique et les signatures électroniques, la loi du 21 juin 2004 pour la confiance dans l'économie numérique reconnaissant la validité des actes et des contrats électroniques avec ses exceptions et ses adaptations, la loi de finances rectificative traitant des factures électroniques, l'article 56 du code des marchés publics et ses textes d'application, la loi du 9 décembre 2004 de simplification du droit, 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...

À l'analyse, il ressort de ces textes que, quand bien même le principe de neutralité technique est respecté, la sécurité juridique est indissociable, de fait et de droit, de la sécurité technique, c'est-à-dire de la sécurité des systèmes d'information.

**Mais, il serait vide de sens de reconnaître et de donner des effets juridiques aux échanges, actes et signatures électroniques, sans prendre en compte leur portée juridique dans le temps.** En d'autres termes, la question de l'archivage électronique doit accompagner toute démarche de dématérialisation dès lors que les éléments (faits, actes) concernés ont des effets juridiques.

La mise en place d'un « archivage électronique sécurisé » du patrimoine informationnel des organisations publiques devient ainsi une priorité.

**Or, la mise en place de services d'archivage électronique sécurisé repose sur une acception pluridimensionnelle :**

- des aspects techniques ;
- des aspects organisationnels ;
- des aspects fonctionnels ;
- et des aspects juridiques.

L'archivage recouvre au demeurant différentes finalités. Il peut ainsi répondre à une préoccupation informationnelle, historique ou statistique (on parle d'archivage patrimonial), à une obligation légale ou à un besoin juridique par exemple à des fins de preuve (dans ces deux derniers cas, on parle communément d'archivage à des fins juridiques).

L'archivage dans une finalité juridique peut servir à prouver ses droits, il peut être imposé à des fins de contrôle et répondre à une obligation légale. En tout état de cause, archiver des documents électroniques correspond à l'idée de pérennité de l'information dans le temps avec la possibilité de la restituer intacte, c'est à dire identique à celle de son origine.

De plus, **pour que la valeur juridique des archives ne puisse être déniée du seul fait de l'archivage électronique mis en place, il faut tenir compte de plusieurs paramètres pour apprécier et déterminer le cas échéant, les exigences et contraintes** en matière :

- d'identification/authentification de l'origine de l'archive ;
- d'intégrité des archives ;
- d'intelligibilité / lisibilité des archives ;
- de durée et pérennité de l'archive ;
- de traçabilité des différentes opérations (notamment versement, consultation, migration, élimination) ;
- de la disponibilité et de l'accessibilité des archives.

**L'archivage électronique sécurisé doit prendre en compte l'ensemble de ces paramètres pour être juridiquement efficient.** Toutefois, deux précisions doivent d'ores et déjà être apportées dans le cadre de l'archivage électronique. D'une part, l'archivage électronique ne saurait conférer à l'archive une valeur juridique si le document initial n'en avait aucune. D'autre part, à défaut de textes réglementaires précisant les modalités et les dispositifs pour qu'un archivage électronique soit regardé comme fiable, seules les décisions rendues par les juges en la matière auront un impact sur le droit positif.

Ceci étant précisé, l'archivage électronique sécurisé conduit d'abord à s'interroger sur le contexte dans lequel il s'inscrit et les enjeux qu'il représente. Ensuite, sa mise en place doit reposer sur l'adoption d'un certain nombre de documents indispensables à la cohésion des aspects fonctionnels, opérationnels, organisationnels, juridiques et techniques pour que l'archivage électronique soit un archivage électronique sécurisé.

## 3 Contexte et enjeux de l'archivage électronique sécurisé

Avant la mise en place effective d'un archivage électronique sécurisé, il est indispensable de s'interroger sur l'existant en matière d'archivage électronique en tenant compte du contexte à la fois technique et juridique. Cette étude préalable doit permettre de déterminer et d'apprécier les enjeux de l'archivage électronique sécurisé, en identifiant les besoins et les contraintes générales à prendre en compte dans une approche nécessairement pluridimensionnelle.

### 3.1 Architecture de l'archivage électronique

L'architecture de l'archivage électronique doit être envisagée selon deux axes indissociables en la matière : les aspects juridiques et opérationnels (technique et sécurité).

La partie juridique est le fruit d'une approche pratique et pluridimensionnelle. Elle a pour objectif de faciliter l'appréhension de la relation étroite qui existe entre le juridique et le technique en matière d'archivage électronique. Ainsi, doivent être présentés et hiérarchisés, les textes et travaux internationaux, communautaires et nationaux, qui attirent au concept d'archivage électronique et plus largement à la dématérialisation (valeur probante, signature électronique, factures électroniques, marchés publics dématérialisés...). Sans se limiter à être un référentiel de textes, cette approche vise à préciser la portée, l'intérêt et/ou les implications que chacun d'entre eux est susceptible d'avoir sur l'archivage électronique.

Ce référentiel établi, le périmètre technique et opérationnel d'un service global d'archivage électronique et plus précisément d'un système d'archivage électronique ou SAE doit être appréhendé. Au préalable, afin d'éviter un certain nombre de confusions certains termes et concepts doivent être précisés. Tel est notamment le cas de l'intégrité, du stockage ou encore de la GED. En outre, avant d'entrer dans le détail de l'architecture, il est nécessaire d'aborder les contraintes techniques auxquelles toute personne souhaitant mettre en place un archivage électronique se trouve confrontée, puis les différentes organisations possibles pour un service d'archivage en s'appuyant sur les normes actuelles en la matière. Ensuite, le détail des fonctionnalités d'un SAE, notamment sur lequel reposera la mise en place de l'archivage électronique sécurisé, doit être déterminé en prenant en compte les aspects relevant de la sécurité logique et ceux liés à la sécurité physique du système. Enfin, les décideurs doivent prendre en compte les offres en matière de logiciels et services et analyser les coûts d'un d'archivage électronique sécurisé afin d'une part, de bien les appréhender et d'autre part, de pouvoir comparer différentes solutions. Les développements qui suivent présentent de façon synthétique le contenu de ces différentes phases.

En matière de contraintes, les notions de formats logiques doivent être prises en compte, c'est-à-dire sous quelle forme va se présenter une information à archiver. Par exemple, s'agit-il d'un texte ou d'une image ? Le format XML est largement recommandé compte tenu essentiellement de son aspect de standard ouvert et extensible mais aussi en tant que métalangage. Sur ce point, l'existence du cadre commun d'interopérabilité des systèmes d'information publics doit être prise en compte. Les formats physiques ou différents types de supports utilisables auxquels s'ajoute la notion de *WORM* (*Write Once Read Many*) doivent également être appréhendés. Le *WORM* peut être vu comme une référence à une méthode d'enregistrement dont la propriété intrinsèque est d'être non effaçable, non réinscriptible et non modifiable. Une distinction est d'ailleurs faite entre *WORM* physique et *WORM* logique résultant dans la manière de gérer les propriétés évoquées précédemment en ayant recours ou non à une transformation irréversible du substrat. Il en va de même des supports magnétiques (bandes et disques) et des supports optiques (CD, DVD) sachant que le choix se fera en fonction des exigences, comme la stabilité de ces supports ou encore leur large diffusion.

Après les formats, une autre contrainte est celle des accès au système qui se doivent d'être performants quelle que soit la volumétrie à traiter. Cette dimension est à prendre en compte le plus en amont possible.

Les problèmes de migration auxquels tout archivage électronique se verra confronté, notamment pour les archives publiques, qu'il s'agisse d'un changement de support ou d'un changement de format, constituent un paramètre et un enjeu primordiaux. L'évolutivité du système constitue également une des composantes de l'archivage électronique, d'autant qu'elle devra pouvoir se faire sans impact significatif sur la qualité du service rendu. Les aspects sécurité, outre la sauvegarde des informations archivées, sont à prendre en compte et induisent la notion de traçabilité

de l'ensemble des opérations et événements survenus au sein du système. Enfin, la prise en compte de la signature électronique se doit d'être soulignée afin de bien définir les contraintes afférentes. À ce titre, dans le cadre de la sphère publique, et ce, a priori à la différence de la sphère privée, il semble devoir être considéré qu'il appartient aux services producteurs de s'assurer de la validité des signatures électroniques apposées sur leurs archives (soit en effectuant cette opération en interne, soit en ayant recours à une autorité de validation qui établirait une attestation de validité, laquelle serait jointe à l'Archive au titre de ses métadonnées). Intervenant en amont des opérations de versement dans le cadre de l'archivage électronique, la question relative à la conservation des signatures électroniques des documents originaux apparaît ainsi hors du champ du système d'archivage électronique qui serait mis en place dans la sphère publique. En revanche, suivant les cas, il sera possible de signer le transfert entre un producteur et une autorité d'archivage, voire l'ensemble des échanges entre les différents partenaires entraînant une prise de responsabilité particulière (acceptation du transfert, élimination, communication, refus des services de contrôle...).

Au niveau organisationnel, les différents modèles et normes existants en matière d'archivage doivent servir la réflexion en tenant compte de leurs champs d'application, principaux avantages et inconvénients. Il en est ainsi de l'OAIS (*Open Archival Information System*) à la NF Z42-013 en passant par l'ISO 15489 et autre modèle Moreq (*Model requirements for the management of electronic records*).

C'est à l'issue de cette étude que l'architecture d'un service d'archivage électronique pourra pleinement être élaborée.

Il s'ensuit que les grandes fonctions d'un archivage électronique sécurisé et d'un système d'archivage électronique, doivent être :

- le versement,
- le stockage,
- la gestion des données descriptives,
- la consultation/communication
- et une dernière et cinquième fonction : l'administration au sens large y compris la gestion de la relation avec les services producteurs, la veille technologique et juridique ou encore les projets d'évolution et de migration.

En matière de sécurité, l'administration générale et l'organisation, les aspects physiques, la sécurité des locaux, les contrôles d'accès des personnels aux bâtiments et aux différents matériels, la sécurité des personnels, du matériel et du logiciel sont également des aspects indispensables à prendre en considération. Ceci étant, le SAE doit aussi reposer sur des règles de sécurité spécifiques mais qui viennent s'ajouter à celles définies à titre général dans la politique d'archivage électronique sécurisé et dans la politique de sécurité des systèmes d'information si cette dernière existe. À ce titre, le SAE qui est un système d'information doté d'une finalité particulière doit intégrer une analyse des risques tout au long du processus d'archivage.

En ce qui concerne les offres logicielles, le marché propose aujourd'hui un panel assez large et diversifié de solutions d'archivage qui se précise et se complète d'année en année. La typologie des produits va du coffre-fort à la solution générale qui englobe l'archivage dans la gestion du cycle de vie complet des données (ILM). Les produits du marché mettent tantôt l'accent sur la gestion de contenu, tantôt sur l'archivage légal (l'expression est répandue mais il serait plus exact de dire « archivage à des fins de preuve »). Ils visent soit l'ensemble des données d'une organisation (incluant parfois les données sur les archives papier), soit un type d'information ou un format de document bien spécifique, tel que les messages électroniques. Dans le secteur technique et scientifique, existent également des offres notamment en terme d'infrastructures de stockage (très grandes volumétries) et d'outils performants d'accès et de consultation des données archivées. En revanche, il existe encore très peu de briques logicielles prenant notamment en compte la partie gestion des versements sur la plateforme d'archivage suivant un format donné, le contrôle des formats, leur conversion éventuelle..., ainsi que l'alimentation automatique d'une base de données descriptive à partir notamment des métadonnées des objets archivés accompagnant le versement.

Au niveau logiciel, il faut également choisir entre une solution du marché, un logiciel libre ou encore un développement spécifique. L'essentiel est de bien prendre la mesure de ses choix, étant entendu que les changements de politique auront un coût qu'il vaut mieux connaître à l'avance et si possible éviter ou, à tout le moins, anticiper. Il est également important de considérer les questions techniques de récupération des données et de maintenance.

En complément à l'offre logiciel, un certain nombre de critères à analyser et à vérifier dans le processus de choix d'une solution doit être retenu, à savoir : l'interopérabilité et le partage de ressources, critères très importants pour la pérennité du service et sa continuité, la facilité de prise en compte des données descriptives pour les consultations ultérieures, les temps et les contrôles d'accès, la montée en charge tant pour les accès que pour la volumétrie, le stockage de sorte qu'il corresponde bien aux besoins et aux souhaits de l'organisation (*on line, off line, near line*), la prise en compte des possibilités de migrations tant de supports que de format, l'évolutivité sous les aspects à la fois des volumes et des accès mais également la capacité à changer de système facilement en tout ou partie, le coût direct du logiciel et les coûts associés du type support et maintenance, la pérennité du fournisseur/éditeur.

En ce qui concerne les coûts la réflexion et l'approche doivent essentiellement permettre de choisir une solution parmi d'autres. Dans ce cadre, le fait de répertorier l'ensemble des coûts de façon exhaustive, tant en matière d'investissement direct (matériel informatique, réseau, sécurité, prestations...) qu'en exploitation (télécommunications, locaux, personnel, maintenance...) ou autres coûts comme les consommables, apparaît comme une opération délicate qu'il conviendra de mener avec rigueur.

**À partir du moment où le décisionnaire dispose de l'ensemble des données, il s'agit de mettre en place une véritable simulation du fonctionnement du système d'archivage, en terme de coûts et pour une période donnée.** L'avantage de disposer d'un système de simulation est avant tout de permettre la prise en compte à la fois des coûts ponctuels et des coûts récurrents et éventuellement de pouvoir analyser la sensibilité des paramètres identifiés.

## 3.2 Enjeux juridiques de l'archivage électronique

Le contexte et les enjeux juridiques de l'archivage électronique à des fins juridiques, également dénommés archivage électronique « sécurisé », doivent être appréhendés eu égard aux textes et concepts juridiques qui s'imposent en matière d'archivage.

Dresser le panorama juridique de l'archivage électronique sécurisé conduit à prendre en compte le régime juridique applicable aux archives électroniques afin qu'elles conservent la valeur juridique que l'acte recouvrait lors de son établissement. En ce sens, il s'agit **dans un premier temps d'identifier les exigences juridiques que l'archivage électronique devait garantir dans le temps pour que l'acte réponde aux contraintes posées à des fins de validité ou de force probante pendant tout son cycle de vie, c'est-à-dire dans le cadre de l'archivage, jusqu'à la fin de la durée de conservation nécessaire** (qui soit est imposée par un texte, soit est déterminée à des fins de preuve). Dans un second temps, **l'analyse doit prendre en compte les modalités de l'archivage électronique qui trouvent à s'imposer au-delà de l'objet archivé et qui portent directement sur les obligations et responsabilités des différents acteurs de l'archivage.** Si la sphère publique est au cœur des préoccupations, les aspects de droit privé doivent également être appréhendés afin de présenter un panorama le plus exhaustif possible quant aux contraintes de l'archivage électronique sécurisé.

Le présent mémento du contexte et des enjeux juridiques met en exergue un « *panorama* » juridique de l'archivage électronique sécurisé à travers lequel les critères juridiques d'un tel archivage sont identifiés et définis au vu du droit positif et de ses éventuelles évolutions. En effet, la problématique posée par l'archivage électronique naît de la combinaison des conditions légales de conservation et des exigences propres à l'archivage sous forme électronique.

### 3.2.1 Précisions sur la notion d'archives et le concept d'archivage électronique sécurisé

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

Il ressort de cette définition que les documents acquièrent la qualité d'archives dès leur création dans le cadre d'une activité et que la forme ou la nature du support est indépendante de la notion d'archives. En ce sens, que le document soit sur support papier ou qu'il s'agisse d'un document électronique, la notion d'archives aura vocation à s'appliquer.

Si cette première définition vise tant les archives publiques que privées, les articles L. 211.4 et L. 211-5 du Code du patrimoine distinguent les archives publiques des archives privées. Ainsi, constituent des **archives publiques**, « *les documents qui procèdent de l'activité de l'État, des collectivités territoriales, des établissements et entreprises publiques* », de celle « *des organismes de droit privé chargés de la gestion des services publics ou d'une mission de service public* ». Entrent également dans cette définition, les « *minutes et répertoires des officiers publics ou ministériels* » (sont ainsi concernés les actes authentiques). La qualification d'archives publiques est importante puisque celles-ci sont régies par un régime juridique spécifique et précisément encadré. A titre principal, les archives publiques sont imprescriptibles et inaliénables ; elles font partie du domaine public mobilier. De plus, elles font l'objet d'une réglementation particulière tant en termes de délais de conservation que de gestion (autorités compétentes, contrôles reposant sur des textes réglementaires, phases successives d'archivage selon l'âge de l'archive, procédures de versement, de tri, d'élimination, absence de restitution...).

Ceci ayant été précisé, l'analyse conduit à considérer que :

- Il n'existe pas de cadre juridique spécifique à l'archivage électronique : il est donc nécessaire de partir des principes juridiques généraux qui trouvent à s'appliquer pour en apprécier la portée dans le contexte de l'archivage électronique ;
- 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 électroniquement. En revanche, un acte doté d'une valeur juridique peut la perdre au motif qu'il a été conservé dans de mauvaises conditions. **C'est pourquoi, seul un « archivage électronique sécurisé » permettra au juge d'apprécier la valeur juridique du document conservé, la conservation réalisée devant répondre aux exigences légales ou jurisprudentielles et conditionnant le fait que cet acte produise des effets juridiques.**

Cette approche conduit à donner la définition suivante de **l'archivage électronique sécurisé** : **l'ensemble des modalités de conservation et de gestion des archives 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.**

Cette définition est déterminée au vu des principes juridiques impactant l'archivage électronique sécurisé et des obligations et responsabilités qui en découlent pour les personnes intervenant en la matière.

### 3.2.2 Principes juridiques directeurs impactant l'archivage électronique sécurisé

#### Dans la sphère privée

Les principes directeurs de l'archivage électronique dans la sphère privée permettent de mettre en exergue :

- la nécessité d'identifier le **domaine juridique** dans lequel s'inscrit le document. Durée de conservation, finalité (validité, preuve...), formalisme connexe (LRAR, double exemplaire...) sont autant de paramètres à prendre en compte pour définir les bonnes modalités d'archivage ;
- lorsque **l'identification de l'auteur ou de l'origine de l'acte** fait partie intégrante de sa valeur juridique, l'archivage électronique doit prendre en compte et traiter l'ensemble des éléments participant à l'imputabilité de l'acte conservé (signature électronique, certificat...) ;
- les écrits électroniques (à titre de preuve, de validité, qu'il s'agisse de contrat ou facture par exemple) doivent être conservés de telle sorte que leur **intégrité** soit garantie. L'archivage électronique devra respecter cette exigence commune à la reconnaissance juridique des écrits électroniques en droit privé ;

- l'archivage électronique représente un enjeu majeur : **si la conservation ne garantit pas les conditions exigées pour la reconnaissance d'un écrit électronique et remplies à la date de son établissement, l'écrit électronique perd sa valeur juridique** ;
- les conditions **d'intelligibilité**, d'imputabilité, d'intégrité et de respect de formalités parfois connexes (type LRAR) doivent être garanties dans le cadre d'un archivage électronique à des fins juridiques. L'archivage doit les garantir dans le temps. **Ainsi, le contenu informationnel doit être maintenu dans son intégrité mais pas forcément dans les mêmes formes et sur les mêmes supports**. Mais, comment allier l'évolution des technologies qui a une incidence directe sur l'intelligibilité des actes avec la garantie d'intégrité dans le temps ? **C'est là la problématique majeure de l'archivage électronique**.
- en tout état de cause, l'archivage électronique doit reposer sur une **traçabilité** des documents et des opérations afférentes. Elle doit être garantie aux différentes phases concernées et dépasse la question des supports utilisés.

### Dans la sphère publique

Il est certain que dans le cadre de l'archivage d'actes électroniques, l'archivage effectué devra porter sur l'ensemble des éléments permettant d'apprécier la légalité et/ou la valeur probante de cet acte. En ce sens, **pour que l'archivage remplisse sa finalité juridique, il faudra que les modalités mises en place permettent de garantir les conditions imposées pour la reconnaissance juridique des documents eux-mêmes**.

Dans le cadre d'un archivage électronique dans une finalité juridique, le juge administratif pourra être convaincu de la valeur juridique du document archivé aux conditions cumulatives que :

- l'acte soit **intelligible** par lui ;
- l'auteur du document électronique puisse être **dûment identifié** (garantie de la compétence juridique de l'auteur de l'acte) ;
- le document ait été établi et conservé dans des conditions de nature à en garantir **l'intégrité** (toute altération ou modification du document doit être détectable, à défaut le juge pourra douter de la fiabilité de l'écrit électronique et donc de sa valeur juridique, que ce soit à titre de preuve ou de légalité).

De plus, pour que l'archivage électronique soit regardé comme fiable d'un point de vue juridique, il apparaît nécessaire que **les procédures mises en place soient précisément décrites et mises en œuvre** (il en va ainsi des métadonnées qui font à ce titre l'objet d'un standard d'échange<sup>1</sup>). L'automatisme de certaines opérations dont la datation des versements constitue en ce sens une sécurité. De même, il pourrait être envisagé qu'un certain nombre de documents soit scellé à la date de leur versement aux archives. De la sorte, si les administrations ont la maîtrise de l'archivage de leurs documents, elles en garantissent l'efficacité et la fiabilité du fait de processus externes (logiciels...) dont elles n'ont pas la maîtrise.

D'une façon générale, **l'ensemble des opérations devra être tracé**. A cet effet des procédures devront être définies en tenant compte des prescriptions applicables à l'archivage en général (DUA, bordereau de versement, opération de tri, bordereau d'élimination...) et des règles relatives à la consultation et à la communication des documents archivés (accès réservé, liberté de communication...).

Enfin, s'il n'existe pas de règles juridiques spécifiques à l'archivage électronique, il est nécessaire de prendre en compte les **règles de droit commun applicables à l'archivage papier**, en adaptant les modalités de l'archivage électronique afin de préserver les spécificités liées à la nature électronique des documents. De même, la question des formats et des supports utilisés doit faire l'objet d'une réflexion adéquate en fonction de la nature des archives et de la durée de conservation fixée. **La problématique de la migration des documents constitue là encore un des enjeux**

---

<sup>1</sup> Direction des Archives de France et ADAE, Standard d'échange de données pour l'archivage électronique – versement – communication – élimination, appel à commentaires en septembre 2005.

**majeurs de l'archivage électronique à des fins juridiques.** Et les observations faites à cet égard en droit privé se retrouvent de façon similaire.

### 3.2.3 Obligations juridiques et recommandations subséquentes en matière d'archivage électronique

Quel que soit l'acteur en cause (sphère publique / sphère privée), un ensemble d'obligations techniques, organisationnelles et juridiques conditionne la mise en place d'un archivage électronique sécurisé et sa fiabilité afin de conserver la valeur juridique aux archives électroniques traitées. Parmi ces obligations, certaines sont générales, d'autres propres à l'environnement numérique (atteinte aux STAD, traitement de données à caractère personnel, données de connexion...) ou propres à la sphère publique. L'on peut ainsi distinguer :

- **les obligations générales** à respecter compte tenu des exigences juridiques, notamment :
  - Le respect des durées de conservation imposées par les textes. Il sera ainsi nécessaire de déterminer la durée de conservation de l'archive en cause qui est fonction de son régime juridique. Un travail en amont permettant d'établir une typologie des différentes durées de conservation est alors indispensable. A cet égard, pour les archives privées, il conviendra de se conférer aux différents textes juridiques dont l'acte relève ; pour les archives publiques, les durées d'utilité administrative fixées par les services compétents devront être pris en compte ;
  - Le respect du secret professionnel : cette obligation est clairement imposée pour les archives publiques et privées qui ne peuvent être mises à la disposition du public. En cas de manquement, des sanctions pénales sont encourues.
  - Le respect de la confidentialité des correspondances : dans la mesure où les correspondances constituent des archives, les principes applicables en la matière doivent être respectés même lorsqu'elles sont sous forme électronique.
- **les obligations spécifiques à l'environnement numérique :**
  - L'obligation de sécurité en vue d'éviter les atteintes aux Systèmes de Traitement Automatisé de Données. Cette obligation nécessite de prévoir les procédures et moyens à mettre en place à titre préventif, réactif et répressif le cas échéant. Le lien avec la Politique de sécurité des systèmes d'information, si elle existe, est ici primordial ;
  - Les obligations de protection relatives aux traitements de données à caractère personnel ;
  - Le respect de la législation en matière de cryptologie.
- **les obligations spécifiques aux archives publiques :**
  - Les obligations dont le non respect est constitutif d'infractions spécifiques ;
  - Les obligations tenant à la gestion des archives publiques notamment en ce qui concerne les modalités de versement, de communication, d'élimination ou de contrôle des archives publiques. À ce titre, il convient donc de prendre en compte et de transposer les formalités et procédures requises pour le papier et de les adapter (exemple : lieu du « dépôt », lieu d'hébergement de la plate-forme d'archivage électronique...);
  - L'exclusion de principe du recours à un tiers archiveur.

**L'analyse de ces obligations met en avant certaines recommandations valables en tout état de cause :**

- assurer la traçabilité de toutes les opérations concernant les archives versées (communication, migration, éventuelle élimination...);
- veiller à l'interopérabilité des systèmes d'archivage ;
- suivre l'état de l'art pour les migrations ;
- établir et mettre en œuvre une politique d'archivage électronique visant à définir les rôles de chaque intervenant dans le processus d'archivage électronique (service

- versant, autorité d'archivage, contrôleurs...), les obligations et responsabilités y afférent ;
- procéder ou faire procéder aux audits adéquats.

**En pratique, les obligations précitées ont des implications fonctionnelles et opérationnelles qui se retrouvent à chacune des phases de l'archivage** (versement, stockage, tri, élimination, administration, accès, communication....).

**C'est pour cette raison que** l'identification préalable des rôles de chaque intervenant est fondamentale. A cet égard, alors qu'il existe une **grande liberté organisationnelle et structurelle dans la sphère privée**, il convient de constater que **les procédures dans la sphère publique sont strictement encadrées** (procédures de versement, procédures de tri, procédures d'élimination, procédures de communication...). Ceci d'autant plus que les responsabilités dans la sphère publique sont étroitement liées aux règles organisationnelles imposées par le code du patrimoine et le code général des collectivités territoriales.

**Il en va ainsi du recours à des tiers archiveurs** qui est prohibé pour les archives publiques (sauf deux exceptions dont le fondement juridique reste fragile) alors qu'il permet aux personnes privées de transférer contractuellement la charge de certaines obligations et donc de limiter leur responsabilité en interne.

### 3.2.4 Régimes de responsabilité

Les régimes de responsabilité sont très différents selon qu'il s'agisse d'une personne privée ou d'une personne publique. Partant de ce préalable, les régimes de responsabilités doivent être appréhendés distinctement pour chacun de ces acteurs et suivant les modalités pouvant être retenues pour effectuer cet archivage électronique.

Ainsi, **dans la sphère privée**, ce sont les principes de la responsabilité civile qui sont applicables tant pour les personnes morales que pour les salariés (étant noté les effets juridiques des délégations) et les liens contractuels qui peuvent exister avec des prestataires externes.

**Pour les archives publiques**, c'est le régime de responsabilité administrative qui s'applique pour les personnes morales concernées (personnes publiques, personnes privées chargées d'une mission de service public) et les agents (régime de la faute / droit disciplinaire).

La responsabilité pénale est également un des aspects à prendre en compte.

\*\*\*\*\*

**Cette première démarche, nécessaire en amont de tout projet, permet d'identifier concrètement les enjeux et le contexte de l'archivage électronique sécurisé. La définition des besoins, l'identification de l'existant, des moyens, des exigences et du contexte doivent précéder puis accompagner la mise en place opérationnelle de l'archivage électronique sécurisé.**

**L'analyse du contexte et des enjeux de l'archivage électronique sécurisé permet également de relever que, si des points de similitude existent, qu'il s'agisse d'archives électroniques publiques ou privées, les points de divergence entre les deux sphères commandent de traiter distinctement les documents à adopter pour organiser l'archivage électronique sécurisé.**

**En effet, alors que les acteurs privés bénéficient d'une certaine souplesse quant aux modalités organisationnelles de leurs archives, l'organisation des archives publiques est strictement encadrée (notamment par le code du patrimoine et les textes réglementaires).**

**De plus, la spécificité de l'organisation dans la sphère publique a des implications directes sur les modalités de mise en place de l'archivage électronique et sur son architecture, compte tenu des rôles des différents intervenants tant d'un point de vue fonctionnel que juridique.**

**Les aspects opérationnels doivent tenir compte de ces divergences.**

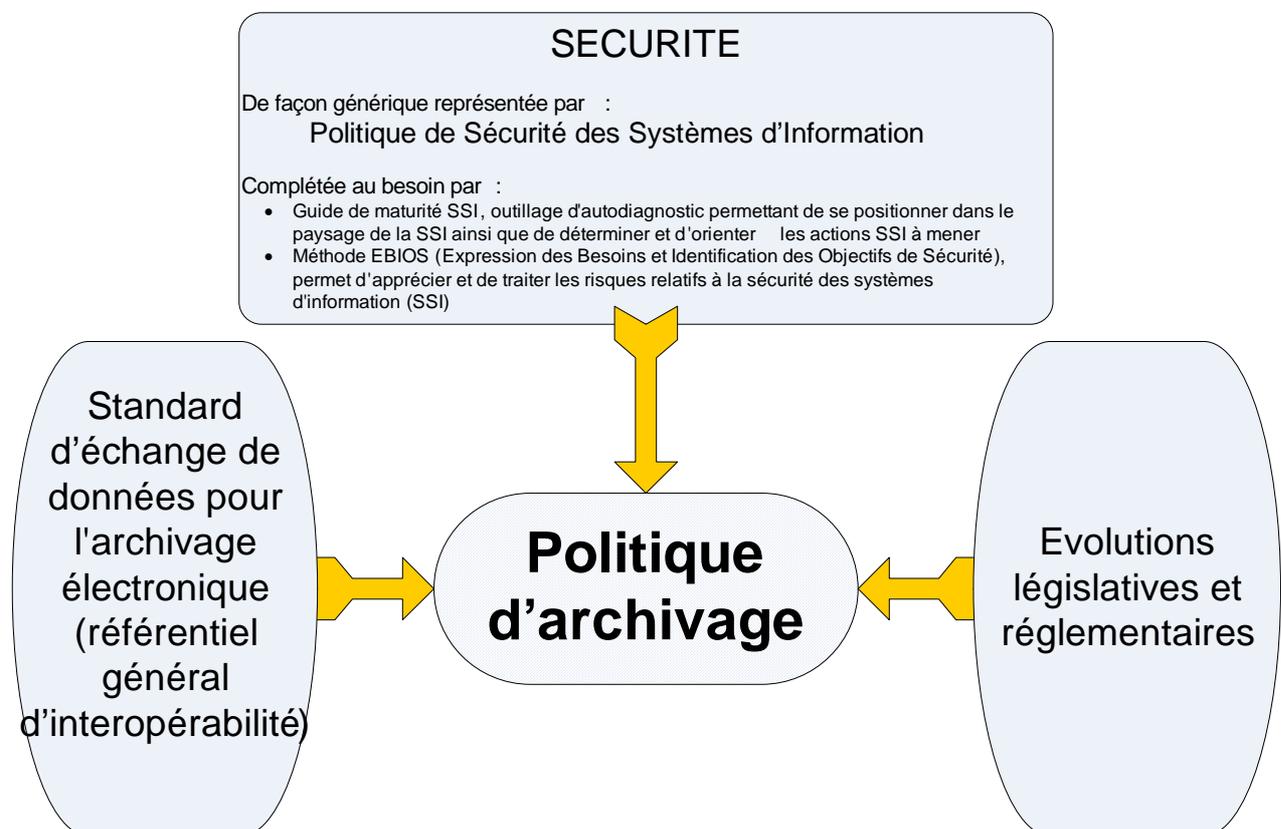
## 4 Aspects opérationnels de l'archivage électronique sécurisé dans la sphère publique

La mise en place d'un archivage électronique sécurisé doit se faire *in concreto*. À ce titre, il faut tenir compte de l'environnement dans lequel il va être mis en œuvre. De plus, il doit reposer sur un ensemble de documents opérationnels.

### 4.1 La cohérence de l'archivage électronique dans l'ensemble de l'organisme

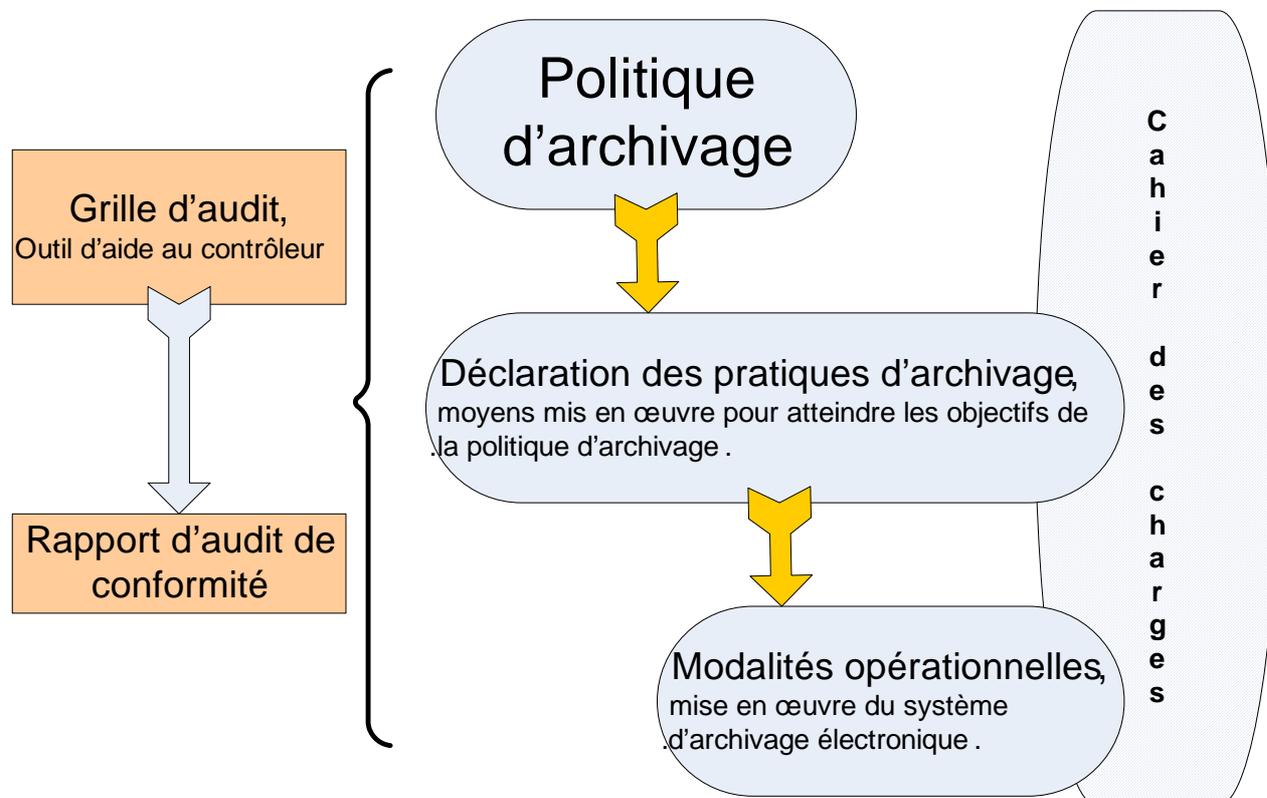
La cohérence avec le schéma directeur des systèmes d'information défini, la politique de sécurité adoptée le cas échéant, les technologies utilisées, la structure concernée et les besoins et moyens identifiés doit être prise en considération.

Le schéma qui suit présente les documents avec lesquels il convient de mettre en cohérence la mise en place d'un archivage électronique sécurisé.



## 4.2 Les documents sur lesquels repose un archivage électronique sécurisé

Le schéma suivant récapitule les documents à adopter en vue de la mise en œuvre d'un archivage électronique sécurisé :



### 4.2.1 Une Politique d'archivage

Pour mettre en place un archivage électronique sécurisé dont la fiabilité puisse être étayée, il apparaît nécessaire d'élaborer une Politique d'archivage. De la sorte, les personnes en charge des archives publiques disposeront d'un document posant les règles de base en matière de sécurité pour un archivage électronique sécurisé. **Cette Politique d'archivage doit définir les contraintes juridiques, fonctionnelles, opérationnelles et techniques à respecter par les différents acteurs afin que l'archivage électronique mis en place puisse être regardé comme fiable.** Ce document, en l'absence de textes précisant les critères de fiabilité de l'archivage électronique, permettra, le cas échéant, de rapporter devant le juge la preuve de la fiabilité du procédé et des procédures mis en œuvre et par là-même de l'archivage électronique réalisé.

La Politique d'archivage électronique sécurisé publiée par la DCSSI a été établie pour la sphère publique. Elle relève à la fois d'une démarche pédagogique puisqu'elle est enrichie d'exemples et de préconisations, et d'une démarche pratique puisqu'y sont décrites les règles de sécurité standard qu'il convient de respecter (rôles, obligations, responsabilité, fonctionnalités, architecture, aspects sécurité...). Cette Politique d'archivage porte donc sur l'organisation du service d'archivage électronique sécurisé. **Elle devra être adaptée et adoptée par l'autorité d'archivage responsable des archives publiques.** L'adaptation est indispensable car, en terme de sécurité, chaque personne publique dispose de ses propres enjeux et de sa propre culture. Cet aspect est primordial, il doit donc être appréhendé pleinement tant lors de la définition des besoins que lors de la rédaction des documents afférents au système d'archivage électronique.

De plus, **ce document devra être complétée par une Déclaration de Pratiques d'Archivage (DPA).** En pratique, la DPA est un document qui décrit les moyens mis en œuvre pour atteindre les objectifs fixés dans la politique d'archivage.

Ensuite, un document visant les modalités opérationnelles de mise en œuvre du système d'archivage électronique doit être dressé afin que ce dernier soit conforme à la DPA et par la même à la Politique d'archivage.

**En pratique, la DPA comme les modalités opérationnelles ne peuvent faire l'objet d'un document type** dans la mesure où elles sont intimement liées à l'expression des besoins spécifiques de la personne publique concernée, aux modalités choisies par cette dernière pour y répondre et aux moyens dont elle dispose. C'est pourquoi, il appartiendra à chaque autorité d'archivage de les rédiger.

#### 4.2.2 Un cahier des charges

En ce qui concerne la mise en place du système d'archivage électronique sur lequel va reposer l'archivage électronique sécurisé, l'élaboration et l'adoption d'un cahier des charges par l'autorité administrative semble indispensable.

Afin de faciliter la rédaction d'un tel cahier des charges, un guide a été élaboré. Dans ce cadre, les différentes phases à prendre en compte et les exigences minimales que doit remplir le système d'archivage ont été appréhendées. Ce guide précise ainsi les besoins et les contraintes essentiels de l'administration et permet à celle-ci, tout à la fois de :

- progresser dans la conception d'un système d'archivage électronique ;
- définir les critères de choix lorsque plusieurs solutions sont en compétition ;
- établir les bases du cadre contractuel avec le Prestataire retenu.

**Enfin, certaines autorités administratives ne disposeront pas, en interne, des compétences techniques et/ou des ressources humaines nécessaires** à la réalisation de l'ensemble du processus de mise en place d'un système d'archivage électronique ou plus spécifiquement à la réalisation de l'une des étapes y concourant. Dans une telle hypothèse, ces dernières pourront recourir à une assistance à maîtrise d'ouvrage. L'assistance à maîtrise d'ouvrage peut consister en l'accompagnement de la personne publique dès la phase d'expression des besoins et ceci jusqu'à la recette du système d'archivage électronique, ou bien peut viser seulement certaines étapes spécifiques du processus.

#### 4.2.3 Une grille d'audit

La grille d'audit constitue un outil d'aide aux contrôleurs afin de vérifier la conformité d'une autorité d'archivage à la Politique d'archivage type.

Elle reprend, sous forme de "*check-list*", les exigences définies dans la Politique d'archivage et permet de suivre facilement les non-conformités majeures / non-conformités mineures / remarques correspondant à l'autorité d'archivage contrôlée. Un tableau récapitulatif, généré automatiquement, présente une synthèse des résultats du contrôle. Disponible sous format XML, elle permettra d'effectuer un audit « assisté » et servira de base à la rédaction du rapport d'audit qui devra être dressé suite au contrôle de conformité.

## 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](mailto: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