Paris, le 13 septembre 2006

La directrice des Archives de France

à

Mesdames et Monsieur les responsables des centres des Archives nationales

Mesdames et Messieurs les directeurs d'archives départementales
sous couvert de Mesdames et Messieurs les présidents des conseils généraux

Mesdames et Messieurs les archivistes communaux
sous couvert de Mesdames et Messieurs les maires

Mesdames et Messieurs les archivistes régionaux
sous couvert de Mesdames et Messieurs les présidents des conseils régionaux

Instruction DITN/RES/2006/005

Objet : Publication de l'étude commanditée par la direction centrale de la sécurité des systèmes d'information (DCSSI) sur l'archivage électronique sécurisé dans le secteur public

Objectifs et portée de l'étude

La direction centrale de la sécurité des systèmes d'information (DCSSI), qui relève du Secrétariat général de la défense nationale auprès des services du Premier ministre, a confié au Cabinet Caprioli et associés, à JMR Consultants et à Oppida, une étude sur l'archivage électronique sécurisé, notamment dans le secteur public.

Cette étude, à laquelle la DAF et la DGME ont largement participé en tant que membres du groupe de travail constitué à cette occasion, vient d'être publiée sur le site de la DCSSI à l'adresse suivante (http://www.ssi.gouv.fr/fr/confiance/archivage.html). Ces travaux ont vocation, au moins en partie, à intégrer également le référentiel général d'interopérabilité tel que défini 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.

Il s'agit, pour le domaine de l'archivage électronique, d'un référentiel essentiel qui s'ajoute à la publication en mars 2006 du standard d'échange de données pour l'archivage[1].

Il est par conséquent indispensable que vous en preniez précisément connaissance et que vous le mettiez en œuvre.

En effet et en tout état de cause, sa mise en œuvre n'est pas limitée à l'archivage des données numériques. Ces standards sont parfaitement applicables, pour une très grande part, aux processus et procédures à mettre en œuvre pour la gestion des archives sur support papier. Si les risques supplémentaires caractéristiques des données numériques conduisent à élaborer des référentiels, dont la formalisation n'avait jamais été autant systématisée pour le papier, il n'en reste pas moins que les principes et les recommandations ainsi énoncés sont également à appliquer à la pratique quotidienne des services d'archives.

Par ailleurs et plus directement, même si vous n'êtes pas encore amenés à conseiller les services producteurs quant à la conservation de leurs données numériques ou à en conserver vous-mêmes, ces recommandations sont à appliquer pour la gestion informatisée des archives que vous avez mise en place ainsi que pour la gestion et conservation des archives que vous avez numérisées.

L'archivage électronique sécurisé est ainsi 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 dès lors que les délais d'utilité administration sont expirés. L'archivage électronique doit en particulier être en cohérence avec les autres référentiels existants dans l'organisme dont dépend le service d'archive : la politique de sécurité des systèmes d'information, le contexte législatif et réglementaire, le standard d'échange de données pour l'archivage.

L'objectif était par conséquent à travers cette étude de définir un référentiel documentaire sur lequel se reposer pour pouvoir mettre en œuvre une politique d'archivage garantissant que les archives sont conservées intègres, fiables, identifiables, intelligibles, accessibles, durant les délais de conservation requis et ce, en conservant la trace de toutes les opérations effectuées**.**

[1] Instruction DITN/RES/2006/001 en date du 8 mars 2006. Le standard est consultable à l'adresse suivante : https://www.ateliers.adele.gouv.fr/ministeres/projets_adele/a103_archivage_elect/public/standard_d_echange_d/folder_contents

Le référentiel a été élaboré pour le secteur public[2] (services producteurs d'archives des services de l'Etat centraux et déconcentrés, des établissements publics, des collectivités territoriales…, réseau des services publics d'archives) et **pour les archives électroniques**[3] **présentant dès leur établissement une valeur juridique**[4] dans la mesure où il a semblé indispensable de fixer les règles juridiques, techniques, les processus et les fonctionnalités nécessaires pour sécuriser un ensemble informationnel et patrimonial dont le risque d'altération est rendu bien plus grand que pour les archives sur support analogique.

La participation de la DAF et de la DGME à cette étude a permis d'étendre sa portée, au-delà des aspects juridiques et techniques qui constituaient à l'origine le cœur de la commande de la DCSSI, aux aspects archivistiques métier en introduisant l'organisation en place au sein des Archives publiques en France, les finalités de l'archivage, les acteurs concernés, les processus et les fonctionnalités couvertes. Vous y retrouverez par conséquent votre pratique quotidienne. De même, à l'instar du standard d'échanges des données pour l'archivage, le service d'archivage électronique (SAE) repose sur le modèle conceptuel de l'OAIS[5] et par conséquent sur les cinq grandes fonctions que sont le versement ; le stockage ; la gestion des données descriptives ; la consultation/communication ; l'administration (relation avec les services producteurs, veille technologique et juridique, projets d'évolution et migration des supports et des formats).

De même ont été intégrés dans l'étude deux points essentiels : d'une part la nécessité de devoir procéder à des migrations de supports et de formats des documents électroniques tout au long de leur cycle de vie, et, d'autre part, le fait que les services d'archives publics n'ont pas, dans leurs missions, à vérifier les signatures originelles des documents numériques qui leur sont versés, cette vérification intervenant en amont (par les services producteurs) et les résultats de cette vérification devant figurer dans les métadonnées du document.

Portée du référentiel

Le résultat de cette étude consiste en la production de plusieurs livrables de différents niveaux. Une plaquette de communication et un memento permettent de synthétiser l'ensemble de l'étude et de présenter l'articulation entre ses différents éléments. Des analyses préalables ont été dans une première étape réalisées, soit une synthèse des enjeux juridiques ainsi que l'état de l'art juridique, technique et organisationnel. Enfin les documents d'aides à l'élaboration du référentiel sur lequel repose cet archivage électronique sécurisé, comportent une politique d'archivage et sa grille d'audit, ainsi qu'un cahier des charges.

---

[2] Ceci étant, un grand nombre de préconisations contenues dans ces documents sont transposables au secteur privé.

[3] De même que pour le standard d'échange de données pour l'archivage, ces documents sont parfaitement valables, pour une très grande part, pour la sécurisation des archives sur support papier.

[4] Ce qui, dans le domaine des archives publiques, recouvre une grande proportion des documents produits ou reçus dans le cadre des missions des services.

[5] Norme ISO 14721:2003 (Systèmes de transfert des informations et données spatiales -- Système ouvert d'archivage de l'information -- Modèle de référence), plus connue sous le nom de modèle OAIS (Open Archival Information System). Pour plus de renseignements, je vous renvoie au standard d'échange de données pour l'archivage, annexe, partie 8.4.

La plaquette (2 pages) est un document de communication destiné en quelques lignes à présenter les enjeux et le contenu d'une politique pour un archivage électronique sécurisé. Je vous engage vivement à la transmettre largement auprès de l'ensemble de vos partenaires et de les inciter ainsi à prendre connaissance de ce très important référentiel.

Le memento est une synthèse de 20 pages de l'ensemble des livrables. Sa lecture sera une introduction utile et indispensable.

Etat de l'art juridique, technique et organisationnel

Ce document de 69 pages est constitué de 5 parties : une partie juridique qui recense l'ensemble des textes juridiques[6] au niveau international, européen et national ayant un impact sur l'archivage en droit privé et en droit public (textes centrés sur l'archivage et le "record management" bien évidemment, mais également sur la communication et l'accès à l'information, la protection des données personnelles, l'interopérabilité, les signatures électroniques, la traçabilité et la sécurité de l'information, le commerce électronique, l'administration électronique…).

Cette première partie est suivie par une partie technique : précisions sémantiques, présentation des formats les plus connus ainsi que des supports avec leurs caractéristiques.

Une troisième partie concerne les aspects organisationnels avec une présentation notamment du modèle OAIS et de ses différents concepts ; de la norme ISO 15489 relative au record management et de Moreq[7]. Des premiers élements sont donnés quant à l'architecture et aux fonctionnalités d'un services d'archivage électronique (SAE) qui seront détaillés dans le cahier des charges livré dans le cadre de cette étude. Enfin quelques éléments quant aux offres et aux coûts sont donnés : offres logicielles, offres de service (tiers-archiveurs[8]).

Les enjeux juridiques

Ce document de 52 pages est une étude juridique énonçant dans un premier temps les principes juridiques directeurs en matière d'archivage électronique dans la sphère privée, puis dans la sphère publique et dans un second temps, les obligations juridiques et les recommandations subséquentes en découlant, ainsi que les régimes de responsabilité y afférents.

On retiendra plus particulièrement les points suivants :

Si à son établissement le document ne répondait pas aux définitions législatives pour être admis juridiquement, l’archivage ne saurait lui conférer une valeur juridique qu’il n’avait pas à la date de son établissement.

[6] Les textes sont listés et commentés pour les plus importants, du point de vue de l'archivage bien évidemment.
[7] Model Requirements for the management of electronic records.
[8] Avec des éléments sur le contenu des contrats à passer avec eux.

C’est l’ensemble du document qui doit être archivé dans des conditions de nature à préserver les qualités qu’il remplit à son établissement (imputabilité, intégrité le cas échéant). C’est pour cette raison que l’archivage électronique ne se borne pas à l’archivage du document *stricto sensu*[9].

Il est nécessaire d'entendre l'archivage électronique comme une conservation "active" à même de garantir pendant toute la durée de conservation, les exigences juridiques requises. Ainsi les migrations sont admises, à condition que les caractéristiques de la conservation assurent la conservation de l'imputabilité et de l'intégrité du document.

Concernant les notions d'original/copie, il est énoncé que la numérisation d'originaux papier ne génère que des copies et qu'il appartient au juge d’en apprécier la valeur juridique. L'étude recommande fortement de conserver les originaux papier dans ce cadre. En effet, elle n’a en tout état de cause que la valeur de copie et l’original électronique qui présente les garanties d’intégrité sera seul à emporter pleinement la conviction du juge.

Parmi les obligations, l'étude recommande notamment :

Une formalisation des procédures et notamment des formats et des métadonnées (remplacement des anciens bordereaux papier), suivant le standard d'échange de données pour l'archivage.

L'obligation du secret professionnel induit de mettre en œuvre des procédures et des outils de nature à protéger ce secret professionnel (du simple mot de passe au chiffrement suivant la nature des documents). De même la sécurité des systèmes d'information[10] devra être assurée à titre préventif, réactif ou encore curatif. Enfin sont pointées les obligations relatives aux données à caractère personnel traitées.

Les recommandations portent par conséquent sur l'obligation d'assurer la traçabilité de l'ensemble des opérations, d'assurer comme énoncé ci-dessus, une conservation "active", de mettre en œuvre une interopérabilité des systèmes d'archivage[11], adopter une politique d'archivage[12] et réaliser en parallèle des audits réguliers. Concernant plus spécifiquement le secteur public, la question du recours à un tiers-archiveur est clairement analysée en l'excluant en principe, sauf à titre exceptionnel et de manière très encadrée. Il est noté que le recours à une externalisation pour les services de l'Etat ne repose que sur une base juridique faible (une simple circulaire).

[9] Eléments de signature, de datation, de traçabilité, caractéristiques du document, opérations l'encadrant.
[10] Atteinte aux systèmes de traitement automatisés de données (STAD).
[11] Objectif du standard d'échange de données pour l'archivage.
[12] Voir ci-dessous la partie consacrée à la politique d'archivage dans le secteur public à mettre en œuvre.

L'étude se termine par un aperçu des différents régimes de responsabilité. Ainsi, en droit public, peuvent être déclarés responsables :

- les producteurs d'archives : ils sont les créateurs des archives et l'efficacité juridique de l'archivage électronique repose en amont sur eux, c'est pourquoi ils doivent être sensibilisés à la problématique de l'archivage électronique et aux enjeux y afférents ;
- les gestionnaires des archives (services d'archives publiques qui sont directement impliqués dans l'archivage électronique – procédures, systèmes…) ;
- la direction des Archives de France, en tant que gestionnaire des archives de l'État (hors Ministère de la défense et Ministère des affaires étrangères), soit au titre du contrôle scientifique et technique.

La responsabilité pour faute de l'administration ou de la collectivité dont dépend le service chargé des obligations en matière d'archivage pourra être valablement mise en cause si :

- une faute a été commise dans la gestion des archives ;
- un préjudice a été causé ;
- il existe un lien direct entre la faute et le préjudice.

En principe, la réparation du préjudice subi sera alors à la charge de la collectivité dont le fonctionnement du service a causé le dommage.

La responsabilité personnelle des fonctionnaires ou des agents est très rarement retenue. Un agent sera susceptible d'être tenu personnellement de réparer le préjudice subi du fait d'un manquement lui incombant dans les hypothèses suivantes :

- faute commise en dehors du service ;
- faute lourde (faute ayant caractère intentionnel ou une extrême gravité) commise dans le cadre du service.

La responsabilité pénale[13] peut être mise en cause lorsque l'agent a personnellement et intentionnellement commis des manquements aux obligations constitutifs d'infractions.
Le droit disciplinaire pourra également trouver à s'appliquer.

Par conséquent, il est fondamental que chaque rôle soit bien identifié, que les procédures soient listées et tracées, que seules les autorités compétentes puissent intervenir et que le système d'archivage électronique permette de respecter les obligations applicables en la matière. À défaut en effet, la responsabilité administrative des différents intervenants, voire la responsabilité pénale des agents, pourra être recherchée.

La politique et pratiques d'archivage (PA)-sphère publique

Ce document de 43 pages 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. Ainsi cette PA Type repose sur des contraintes "standard" à mettre en place dans les domaines suivants que sont l'identification et l'authentification de l'origine de l'Archive, l'intégrité des objets archivés, leur intelligilité et lisibilité, leur pérennité, leur disponibilité et accessibilité, ainsi que la traçabilité des opérations les concernant. La PA Type constitue donc un référentiel de la sécurité de l'archivage électronique pour qu'il puisse être qualifié de fiable.

[13] Régime de droit commun qui s'impose.

Cette PA devra s'accompagner d'une déclaration des pratiques d'archivage (DPA) qui vise ensuite à définir comment l'Autorité d'archivage (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 oeuvre pour cela. Cette DPA est spécifique aux différents environnements et doit donc être déclinée par chacun mettant en œuvre une politique d'archivage.

La PA s'ouvre sur une présentation des différents acteurs. Cinq rôles sont distingués : les services producteurs d'archives ; les services versants ; les autorités d'archivage (responsables de la conservation des archives) ; les services contrôleurs (exerçant le contrôle scientifique et technique sur les archives publiques); les usagers.

Ainsi, par autorités d'archivage, on entend les entités qui prennent la responsabilité du processus d'archivage que ce soit dans les administrations centrales, les administrations déconcentrées, collectivités territoriales, collectivités locales, personnes privées chargées d'une mission de service public. Ces responsables changent suivant le cycle de vie de l'archive. Il peut s'agir par exemple d'un service producteur tant que l'archive est courante, puis d'un service d'archives intermédiaires dès lors que le producteur lui verse ses archives et que le service les prend en charge, puis d'un service d'archives public qui, tel que le vôtre, à son tour, prend en charge les archives définitives transférées par le service d'archives intermédiaires. Des cas de figure sont fournis suivant le type de service producteur.

Une description fonctionnelle de l'archivage électronique sécurisé est donnée, à partir des grandes fonctions figurant dans l'OAIS et qui seront reprises dans le cahier des charges pour la mise en œuvre d'un SAE.

La partie 4 présente précisément quel doit être le contenu de la PA : plan type et contenu requis. C'est une partie essentielle.

Un premier chapitre concerne l'organisation et la responsabilité de chacun des acteurs en présence et les transferts de responsabilité intervenants tout au long du cycle de vie des archives. *Je vous engage à prendre soigneusement connaissance de cette partie afin d'une part, d' informer les services producteurs et les services versants avec lesquels vous travaillez quant à leurs responsabilités en tant qu'autorités d'archivage, producteurs, services versants, suivant les cas*. Sont ainsi précisés les contenus des contrats de service que doivent passer les services producteurs et les autorités d'archivage, préalablement au versement d'une catégorie de documents donnée. Ces éléments peuvent ainsi vous permettre, au-delà des relations que vous entretenez avec les services producteurs et versants, de mettre en place de tels contrats qui facilitent la mise en place de procédures rigoureuses, systématiques et harmonisées.

Sont ensuite donnés des éléments sur la gestion des risques de sécurité des systèmes d'information. *Il s'agit là d'éléments à faire connaître à vos services informatiques ainsi qu'aux personnes responsables de la sécurité des systèmes d'information*. Plusieurs sous-thèmes sont abordés : identification des besoins de sécurité notamment en terme de disponibilité, d'intégrité et de confidentialité, appréciation des risques et traitement des risques[14]. La sécurité et le cycle de vie du SAE sont ensuite abordés : nécessité d'intégrer la sécurité des systèmes d'information (de l'organisme auquel l'autorité d'archivage appartient) à la mise en place du SAE ou à son évolution, nécessité d'effectuer des tests d'intégration avant toute mise en œuvre d'un nouveau composant, contrôles permanents de sécurité à mener, mise en place d'auto-évaluations et d'audits.

Les principes de mises en œuvre sont ensuite définis : aspects humains (critères de sélection des personnels du SAE, habilitations pour l'accès au SAE, définition des rôles de confiance[15], cloisonnement des postes sensibles) ; planification de la continuité des activités, l'AA devant disposer d'un plan de continuité des activités (PCA) à tester régulièrement ; gestion des incidents ; sensibilisation (notamment à la sécurité des systèmes d'information) et formation ; exploitation (documentation des procédures, maintenance des systèmes à tracer, lutte contre les virus et les codes malveillants..) ; aspects physiques et environnement (contrôle d'accès physique, protection contre les accidents et les pannes).

Enfin des principes techniques sont définis, relatifs à l'identification et l'authentification des utilisateurs, aux contrôles d'accès logiques, à l'intégrité des Archives versées, journalisation d'un certain nombre d'opérations, horodatage des opérations.

Une grille d'audit à destination des contrôleurs intervenant dans la sphère publique, reprend, sous forme de points de contrôle, les exigences définies dans la PA et leur permet ainsi de recenser 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, cette grille permet d'effectuer un audit *assisté* et sert de base à la rédaction du rapport d'audit qui devra être dressé.

Le cahier des charges pour un système d'archivage électronique

La PA s'accompagne également d'un modèle de cahier des charges (document de 46 pages) pour la mise en œuvre d'un service d'archivage électronique. Ce document est destiné à faciliter la mise en place du système d'archivage électronique par l'autorité d'archivage. Il décrit les phases à respecter, les fonctionnalités du système, les besoins, contraintes et exigences minimales.

[14] Refus du risque (évitement de la situation de risque), réduction du risque, transfert vers des tiers, prise de risque en prenant en compte son contexte particulier.
[15] Responsable de sécurité, responsable d'application/de base de données, ingénieur système, opérateur.

Le cahier des charges comporte plusieurs parties et sous-parties visant à guider celui qui aura en charge, au sein d'un service d'archives, la rédaction d'un tel document. Sont listées précisément les fonctionnalités d'une SAE autour des cinq grandes fonctions énumérées ci-dessus, chaque fonction étant elle-même décomposée en processus[16]. Des conseils sont également donnés sous forme d'encadrés. Quelques développements explicitent des processus[17]. Une proposition d'architecture générale est faite avec plusieurs scénarii suivant le type de sauvegarde/réplication, nombre de sites concernés[18].

Le cahier des charges fournit encore des précisions sur le mode de conduite du projet, son découpage, les livrables associés à chaque étape[19]. Enfin, des dispositions juridiques permettent notamment de préciser des notions concernant la fiabilité du système, le régime de propriété intellectuelle, l'interopérabilité et la réversibilité du SAE…

Martine de BOISDEFFRE

Directrice des Archives de France

[16] Par exemple, pour le versement : recevoir le versement, vérifier la transmission, contrôler la conformité, journaliser, consulter, convertir, générer un objet pour l'archivage, coordonner les mises à jour.
[17] Par exemple, ce que recouvre l'écriture effective sur les supports de stockage des objets archivés, ce que signifie le hierarchical storage management (HSM), que doit-on comprendre par destruction, par contrôle d'intégrité, définition des différents types de migrations, explications concernant les statistiques, l'interopérabilité des plates-formes.
[18] Un tableau synthétise les différents modes d'architecture et les risques plus ou moins importants associés à chacun en terme de perte de données et/ou de disponibilité des données.
[19] A l'instar de tout projet informatique.