Archives

ARCHIVES

Archivage électronique et analyse de risque : les nouveaux défis de l'archiviste

Antony Belin et Jean-Marc Rietsch

Volume 46, numéro 1, 2016

URI : https://id.erudit.org/iderudit/1035722ar
DOI : https://doi.org/10.7202/1035722ar

Aller au sommaire du numéro

Éditeur(s)

Association des archivistes du Québec (AAQ)

ISSN

0044-9423 (imprimé)
2369-9256 (numérique)

Découvrir la revue

Citer cet article

Belin, A. & Rietsch, J.-M. (2016). Archivage électronique et analyse de risque : les nouveaux défis de l'archiviste. *Archives*, *46*(1), 47–60. https://doi.org/10.7202/1035722ar

Résumé de l'article

L'ère du numérique a causé de profondes transformations à la discipline archivistique. De nouveaux enjeux font ainsi surface. C'est notamment le cas de la notion de risque, qui doit invariablement être prise en compte lors de la définition des besoins dans un organisme.

Dans leur article, Belin et Rietsch font d'abord référence à l'évolution du numérique. Depuis quinze ans, l'arrivée du numérique apporte, certes, beaucoup d'avantages au travail des archivistes, mais aussi tout un lot de nouvelles problématiques. En effet, réussir à assurer l'intégrité d'un document numérique, sa provenance, sa confidentialité, son accès ou sa préservation à long terme, sont tous des défis qui nous rappellent que cette nouvelle ère est parfois fondée sur des mécanismes de fonctionnement complexes et exigeant des coûts monétaires importants.

La seconde partie de l'article est dédiée à la présentation d'un cas concret : le succès de la mise en place d'un système d'archivage électronique (SAE) régional mutualisé au sein du syndicat mixte de coopération territoriale *Mégalis Bretagne*, en France. Le succès de cette opération repose principalement sur l'aspect de mutualisation des moyens, c'est-à-dire la mise commun d'un système détenant plusieurs infrastructures techniques. Ce type de système permet d'assurer l'optimisation des ressources disponibles et les risques sont ainsi partagés. Une politique d'archivage bien réfléchie est absolument nécessaire avant la mise en place d'un tel système. L'exemple du système de *Mégalis Bretagne* illustre bien l'association d'un projet d'archivage numérique et l'analyse du risque.

NOTE ET BILAN D'EXPÉRIENCE

Archivage électronique et analyse de risque : Les nouveaux défis de l'archiviste

Antony Belin
Jean-Marc Rietsch

Sous l'impulsion du numérique, l'archivage vit actuellement une profonde mutation qui l'amène, en particulier, à aborder d'autres aspects, tel le risque, comme éléments de définition des besoins. Par ailleurs, après bientôt quinze années d'existence, l'archivage sous sa forme électronique démontre, de plus en plus, la nécessité de mutualiser les moyens, afin de rester à un niveau économique acceptable, d'où une réorganisation partielle, voire importante, de bon nombre d'entités en la matière.

Après avoir détaillé cette évolution, nous nous attacherons à montrer comment il est désormais indispensable d'associer un projet d'archivage électronique avec une approche d'analyse du risque, afin de pouvoir définir ses besoins par rapport à différents niveaux de sécurité, en fonction des données/documents à traiter.

Un système d'archivage électronique (SAE) devrait donc reposer non sur une infrastructure unique, mais bien sur plusieurs infrastructures techniques, afin de répondre à ces attentes et, surtout, de permettre une optimisation économique des ressources, en fonction des besoins. Une telle organisation apporte, également, une évolutivité importante, absolument indispensable pour de tels projets. La politique d'archivage y revêt un rôle prépondérant et se positionne au centre de la méthodologie présentée, relayée par sa ou ses déclarations de pratiques d'archivage.

APPROCHE THÉORIQUE DU SUJET

Importance du détail en matière de numérique

Si le numérique nous apporte incontestablement beaucoup d'avantages et, en particulier, l'amélioration de nombreux processus, il est un paradoxe que nous avons encore du mal à percevoir, relevant de la complexification de certains aspects.

Alors que le binaire ne possède que deux états, pourquoi alors, particulièrement en matière de signature électronique et contrairement au monde classique, nous faut-il choisir parmi plusieurs niveaux de signature, en fonction des besoins, définis

essentiellement par rapport au risque à couvrir? Un tel choix peut paraître déroutant pour qui a l'habitude de sa signature manuscrite, demeurant toujours la même.

Même si le numérique nous paraît relativement simple à utiliser, les mécanismes à gérer derrière sont souvent extrêmement complexes, voire compliqués et onéreux. En conséquence, le numérique nous oblige à encore mieux poser nos problèmes et à définir plus en détail nos exigences, comme pour le cas de la signature où, au-delà du simple fait de devoir signer, il faut se poser la question du niveau de risque à couvrir, afin d'utiliser le bon dispositif.

Un système d'archivage électronique, mais plusieurs solutions techniques

Contrairement à ce que nous pourrions penser, l'archivage électronique n'échappe pas à la règle. Ainsi, compte tenu des multiples possibilités offertes de nos jours, pourquoi conserver un document peu significatif dans les mêmes conditions de coûts, d'accessibilité et de sécurité qu'un document extrêmement sensible?

En réalité, souvent nous ne nous posons même pas la question et, jusqu'à aujourd'hui, la tendance naturelle était de raisonner comme dans l'univers papier où certes les conditions de conservation ne sont pas toutes les mêmes, mais où globalement elles ne présentent pas autant de différences et de possibilités que dans le numérique. D'une certaine façon, le trop devient ainsi l'ennemi du bien, quoique…

Incontestablement, de par l'étendue des solutions offertes, l'environnement numérique nous impose de mieux préciser nos besoins, au risque de mettre en place une solution inadaptée, car surdimensionnée ou, plus grave, sous-dimensionnée. Ainsi, sans doute par souci de simplification, l'archivage électronique ne présente qu'exceptionnellement plusieurs niveaux, mais ce genre de raisonnement montre vite ses limites, en particulier à cause des coûts induits et, surtout, compte tenu des volumes de plus en plus conséquents à conserver avec une sécurité adaptée.

Au-delà des coûts, le fait de finalement mieux connaître son information ne relève-t-il pas d'une démarche on ne peut plus vertueuse, dans la mesure où le véritable problème face à l'augmentation des volumes de données n'est pas tant de pouvoir les conserver, mais plutôt de savoir qu'en faire, fondement de toute bonne gouvernance de l'information. La notion d'âge des archives (actives, semi-actives, définitives) est ainsi plus que jamais d'actualité, sachant que les exigences de conservation peuvent également être amenées à évoluer au cours du cycle de vie des documents, en fonction de l'évolution de leur caractère critique, dans un sens comme dans l'autre.

Archivage électronique et système d'information

Au-delà de l'archivage électronique, c'est de l'évolution du système d'information dans sa globalité qu'il s'agit. Ce système d'information est passé, ces dernières années, de la simple collecte de données à la production de valeur informationnelle stratégique, autre vaste sujet. Les besoins de l'utilisateur changent, eux aussi, en même temps que les possibilités offertes par les nouveaux outils mis à leur disposition.

Une grande différence se fait jour entre l'archivage physique et l'archivage électronique avec, en particulier, la prise en compte de la gestion du cycle de vie de

l'information ou *information lifecycle management*. L'archivage électronique correspond désormais à une approche par processus. Dès lors, nous ressentons beaucoup moins l'aspect de rupture au moment de l'archivage. La notion même de versement (processus de transferts de fichiers) apparaît de moins en moins significative au sein d'une organisation et est remplacée par l'action à entreprendre au moment où un document devient figé et où il faut absolument le protéger. Cette protection doit ainsi permettre de prouver son origine et son intégrité, au sens de son contenu informationnel, et ce, jusqu'à la fin de son cycle de vie.

C'est en cela que les systèmes de gestion électronique de documents ou de gestion intégrée de documents apparaissent comme complémentaires et non comme concurrents des SAE. Ces systèmes de gestion permettent dès la création du document, avant même que ce dernier ne soit figé, de lui appliquer des règles, notamment pour la communicabilité et pour le versionnage, au cours d'une période de préarchivage, puis d'initier l'archivage courant, avant de procéder au versement dans le SAE. Nonobstant, le transfert en archivage intermédiaire n'implique pas automatiquement l'élimination des données dans le système de gestion électronique de documents, celui-ci continuant de servir comme système de consultation. De son côté, le SAE a pour principale fonction, mais essentielle, d'assurer la pérennité de la valeur probatoire des données jusqu'à l'échéance d'une durée d'utilité administrative pouvant atteindre les cent ans, voire *ad vitam æternam* pour des données à conserver à titre patrimonial.

Besoin côté utilisateur

Vu du côté de l'utilisateur, le système d'information doit assurer la conservation et la préservation des données, mais doit surtout permettre de retrouver rapidement et facilement une information. Le fait de savoir que le document se trouve dans le système d'information depuis quelques minutes ou depuis plusieurs années apparaît dès lors comme secondaire, le plus important étant d'avoir toute confiance dans le document affiché. La confiance est en effet essentielle pour la valeur d'un document, au point d'y associer des tiers de confiance numérique (horodatage, signature électronique, archivage…) jouant le rôle de témoins officiels. Cela revient à disposer de la garantie du caractère authentique de ce dernier, en ce qui concerne à la fois son origine et son intégrité, au sens du contenu informationnel.

De l'importance de classifier des données

Comme vu précédemment, d'un point de vue qualitatif, toutes les données n'ont évidemment pas la même «importance», d'où la nécessité de les classifier, afin de pouvoir ensuite leur attribuer un niveau de sécurité/service adapté.

Une analyse qualitative des données se révèle souvent riche d'enseignements, sachant qu'il est néanmoins souvent compliqué d'attribuer une valeur à une donnée. Il existe diverses théories sur le sujet, dont la plus connue est sans doute l'*infonomics* (contraction d'*information* et d'*economics*) qui permet d'évaluer, de gérer et de manipuler l'information comme un véritable actif de toute organisation.

Sans tomber d'emblée dans un tel niveau de complexité, nous pouvons nous limiter à une approche par les risques et surtout au regard de leurs impacts. Le principe

consiste ainsi à évaluer les conséquences de la perte de telle ou telle donnée et ce qui en découlerait en matière d'impacts financiers, judiciaires, en termes d'image ou de réputation…

Remarque : Il va de soi que nous nous intéressons à la valeur informationnelle de la donnée en tant que telle, sachant que les mégadonnées (*big data*) sont en train de mettre à mal cette approche, dans la mesure où leur principe de base consiste à associer des informations, sans véritable valeur, prises séparément et isolément, mais dont l'importance devient significative dès lors qu'elles sont reliées « intelligemment » entre elles.

Des architectures techniques différentes en réponse

Si la valeur varie d'une donnée à l'autre, cela implique forcément des différences de besoins en termes de solutions à trouver, mais, heureusement, toutes les architectures, même si elles se ressemblent, n'assurent pas la même qualité de service en termes de pérennité, de disponibilité, d'intégrité, d'accessibilité et de confidentialité, et n'ont, évidemment, pas les mêmes coûts, tant en acquisition qu'en exploitation.

Dès lors, pourrons-nous définir des niveaux de sécurité/service afin de satisfaire, de façon cohérente et parfaitement adaptée, les besoins exprimés pour les données à traiter. Quoi qu'il en soit, il sera important de bien distinguer les aspects purement sécuritaires de ceux plus courants, relatifs à la qualité et à la performance des services proposés, tels la disponibilité ou les temps de réponse.

Une logique reprise en Europe

Avec une mise en application prévue en juillet 2016, il est intéressant de noter que le *Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et sur les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la Directive 1999/93/CE* suit la même logique et insiste bien quant à la nécessité d'assortir les solutions aux besoins, en particulier en matière de risque, allant jusqu'à proposer une échelle à trois niveaux : faible, substantiel et élevé. Ce règlement est particulièrement riche d'enseignement, car il constitue une véritable synthèse des bonnes pratiques reconnues après quelque quinze années d'expérience, bonnes ou mauvaises, au sein de l'Union européenne (UE). Il décrit également trois niveaux de signature/cachet électronique (qualifié, avancé et simple), mais, malheureusement, il ne traite pas encore de l'archivage ou, plus exactement, de la préservation, si ce n'est concernant les articles 24 et 34.

Article 24

Exigences applicables aux prestataires de services de confiance qualifiés

2. Un prestataire de services de confiance qualifié qui fournit des services de confiance qualifiés :

f) utilise des systèmes fiables pour stocker les données qui lui sont fournies, sous une forme vérifiable de manière que :

i) les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée par ces données ;

ii) seules des personnes autorisées puissent introduire des données et modifier les données conservées ;

iii) l'authenticité des données puisse être vérifiée ;

g) prend des mesures appropriées contre la falsification et le vol de données…

Article 34

Service de conservation qualifié des signatures électroniques qualifiées

1. Un service de conservation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique.

Nous retiendrons également de ce règlement européen que le fait d'être qualifié pour un des services de confiance identifiés lui confère une présomption de fiabilité, d'où de nouvelles opportunités en matière d'organisation des SAE.

Comment aborder les solutions

Prenons ici l'exemple du critère sécuritaire relatif à l'intégrité d'un document. La solution finale, visant à garantir cette intégrité, peut être obtenue à partir de plusieurs dispositifs :

- logiciel : on calcule l'empreinte du document et on la recalcule régulièrement ou au moment de l'interrogation du document pour vérifier sa non-altération ;
- stratégie de stockage : avec, en particulier, les solutions de type *Content Addressed Storage*, gérant automatiquement le contrôle d'intégrité, de façon régulière ou ponctuelle, selon le paramétrage retenu ;
- organisationnel : grâce, en particulier, au nouveau règlement européen (cf. *supra*), apportant une présomption d'intégrité à tout document horodaté par un prestataire de services de confiance qualifié. De ce fait, le service de stockage ne devra plus se préoccuper que de la pérennité du document. Attention toutefois qu'en cas d'altération d'un document, le système pourra certes la détecter, mais sera incapable de restaurer le document d'origine. Il y a donc lieu d'être extrêmement prudent quant à ce type d'organisation qui est satisfaisante pour des documents moyennement importants, mais certainement pas pour des documents critiques. Il conviendrait alors de compléter par d'autres dispositifs permettant, le cas échéant, de recouvrer les documents intègres, en particulier grâce à un troisième jeu de données en plus d'un système de réplication traditionnel.

APPROCHE CONCRÈTE : EXEMPLE DU SYSTÈME D'ARCHIVAGE ÉLECTRONIQUE RÉGIONAL MUTUALISÉ MÉGALIS BRETAGNE

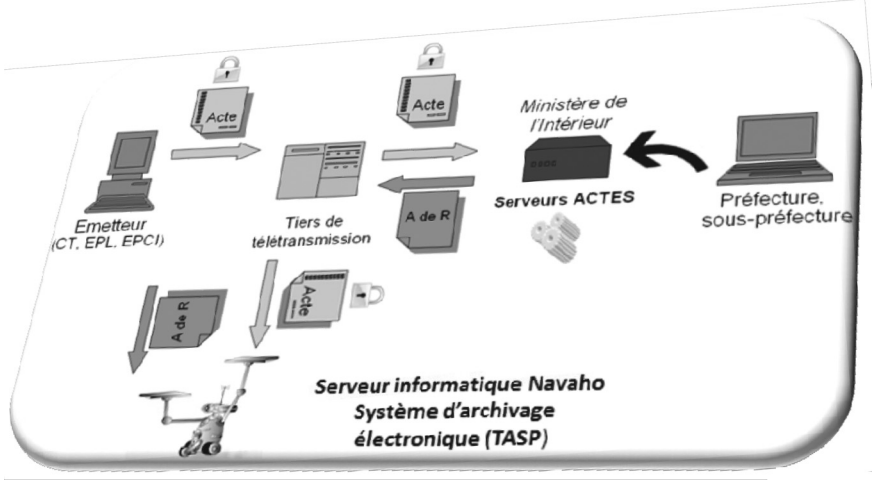
Mégalis Bretagne rassemble les collectivités bretonnes, au service d'un projet d'aménagement numérique du territoire et du développement de services numériques. Ce projet de mutualisation d'un système d'archivage électronique au niveau régional est considéré comme pionnier en France de par son ampleur. Il implique potentiellement toutes les communes et tous les établissements publics à compétence intercommunale (EPCI) adhérents de Mégalis Bretagne, supposant dès lors l'harmonisation avec quatre départements (Côtes-d'Armor, Finistère, Ille-et-Vilaine et Morbihan).

Association entre tiers de télétransmission, gestion électronique de documents et système d'archivage électronique

Dans notre exemple, divers tiers de télétransmission (TDT) et le système d'archivage électronique mutualisé régional sont associés afin de permettre un archivage à valeur probante pour trois flux documentaires en production :

- contrôle de légalité des actes : en France, le représentant de l'État compétent (le préfet pour les communes, les départements et leurs établissements publics, le préfet de région pour les régions) exerce le contrôle de légalité sur les actes des collectivités territoriales (CT). Il examine la conformité de ceux-ci avec la loi. Le programme d'Aide au contrôle de légalité dématérialisé (ACTES) a pour but de permettre aux collectivités territoriales de communiquer par télétransmission leurs actes à la préfecture pour le contrôle de légalité *a posteriori*. Les collectivités souhaitant mettre en place cette démarche peuvent soit investir pour se doter en propre de l'infrastructure nécessaire (ce qui est rarement le cas étant donnée l'ampleur des dépenses à engager), soit être reliées aux serveurs du ministère de l'Intérieur par l'intermédiaire d'un tiers de télétransmission (un organisme homologué pour effectuer, dater et authentifier la télétransmission, par un procédé de signature électronique) ;

Tableau 1 – Le flux ACTES



- flux comptables : Hélios est une application créée et gérée au sein de la Direction générale des finances publiques (DGFiP). En transformant des flux papiers en échanges de données, *via* l'informatique, Hélios facilite le travail des comptables de l'administration de l'État français et leur rapport aux ordonnateurs des dépenses publiques, dans les collectivités territoriales. Le protocole d'échange standard d'Hélios version 2 (PES v2) est la solution de dématérialisation des titres de recette, des mandats de dépense et des bordereaux récapitulatifs, validée par les partenaires nationaux dès 2005. Il constitue, en outre, la seule modalité de transmission des pièces justificatives dématérialisées. Les caractéristiques du PES v2 sont précisées par l'*Arrêté du 27 juin 2007 portant application de l'art. D. 1617-23 du* Code général des collectivités territoriales *(CGCT) relatif à la dématérialisation des opérations en comptabilité publique* ;
- appels d'offres (AO) dans le cadre des marchés publics.

Nombre de projets actuels ont une vision de ces marchés de dématérialisation de leurs archives et de leurs procédures administratives associant désormais un système d'archivage électronique intermédiaire à des tiers de télétransmission, voire à une gestion électronique de documents en amont, tandis qu'un système d'archivage électronique définitif hébergé par les Archives départementales (AD) termine la chaîne documentaire. Il est à noter que certaines Archives départementales, du fait d'être aussi responsables de la conservation des archives du conseil départemental (CD) et de ses entités rattachées, voire de services déconcentrés de l'État, ont tendance à ne vouloir qu'un seul système d'archivage électronique assurant l'intermédiaire et le définitif. Dans la mesure où le coût engendré reste minime, nous leur conseillons néanmoins de dissocier sur la même plateforme un système d'archivage électronique intermédiaire et un système d'archivage électronique définitif : le premier ayant une portée juridique essentielle concernant la préservation de la valeur probante, tandis que le second a une portée patrimoniale, plus contraignante en matière de pérennité.

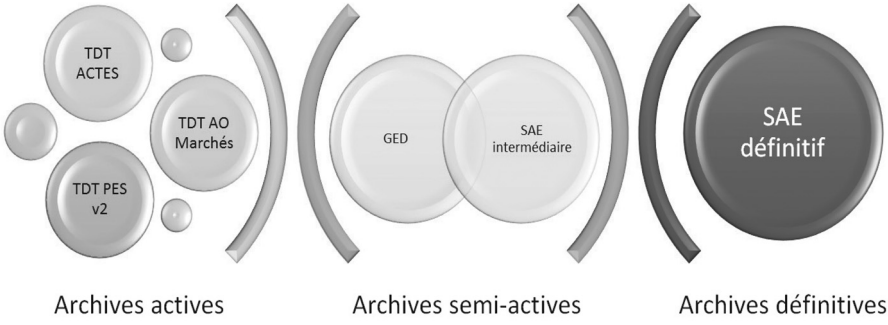
Ceci implique que les éditeurs nouent des partenariats techniques et financiers, afin que leurs solutions communiquent parfaitement, facilitant dès lors les transferts d'archives d'un environnement à un autre : que ce soit des tiers de télétransmission vers les systèmes d'archivage électronique intermédiaires ; ou de ces derniers vers d'autres systèmes d'archivage électronique intermédiaires (rupture contractuelle, besoin de niveau de conservation différent…) ; ou, plus naturellement, vers des systèmes d'archivage électronique définitifs. Ces harmonisations techniques sont, par ailleurs, encouragées par le respect des deux parties du *Référentiel général d'interopérabilité* (RGI) (cadre de recommandations référençant des normes et des standards favorisant l'interopérabilité au sein des systèmes d'information de l'administration française), notamment concernant le format d'échange des données et, tout particulièrement, le Standard d'échange de données pour l'archivage (SEDA).

Ainsi, de nombreux projets intègrent désormais le choix d'un système d'archivage électronique intermédiaire, mutualisé pour l'ensemble des collectivités territoriales, associé à un système d'archivage électronique à caractère définitif. Le premier est géré par des établissements publics de coopération intercommunale, par des centres de gestion départementaux (CDG) ou par des conseils départementaux. Tandis que

le second système d'archivage électronique est sous la responsabilité des Archives départementales. Ces systèmes d'archivage électronique utilisent majoritairement des solutions identiques, facilitant d'autant les échanges de l'un à l'autre lors du changement d'âge des archives. La tendance, dans le domaine public, est donc, *a minima*, de se retrouver avec plusieurs environnements, comme l'illustre le présent schéma (à simple titre d'exemple) :

- les archives actives sont conservées par les tiers de télétransmission ;
- ensuite, les archives semi-actives sont disponibles pour des communications fréquentes sur la gestion électronique de documents, mais conservées sur le système d'archivage électronique intermédiaire afin de garantir leur valeur probatoire, une plateforme commune permettant un accès transparent pour les utilisateurs, car certaines archives plus sensibles au niveau de leur confidentialité imposent de ne les rendre consultables que sur un système d'archivage électronique gérant les droits d'accès de façon plus sécurisée que ne le ferait une gestion électronique de documents ;
- enfin, les archives historiques sont conservées sur un système d'archivage électronique définitif, assurant la conservation patrimoniale *ad vitam æternam*.

Tableau 2 – Les 3 âges des archives et leurs environnements de conservation



Mutualisation des moyens pour un modèle économique viable

La gageure de Mégalis Bretagne, dans un contexte économique assombri par la crise financière et par des restrictions budgétaires drastiques dans le domaine public, était d'obtenir d'un tiers archiveur privé agréé, un système d'archivage électronique conforme aux exigences du Service interministériel des Archives de France (SIAF) pour la sphère publique.

C'est donc par un dialogue compétitif entre quatre acteurs que Mégalis Bretagne a décidé d'atteindre cet objectif ambitieux. Pas moins de sept mois (de janvier à juillet 2012) et de cinq auditions des groupements retenus furent nécessaires à la bonne élaboration des exigences légales, réglementaires et normatives, des besoins fonctionnels archivistiques, des questions techniques et de déploiement, des aspects

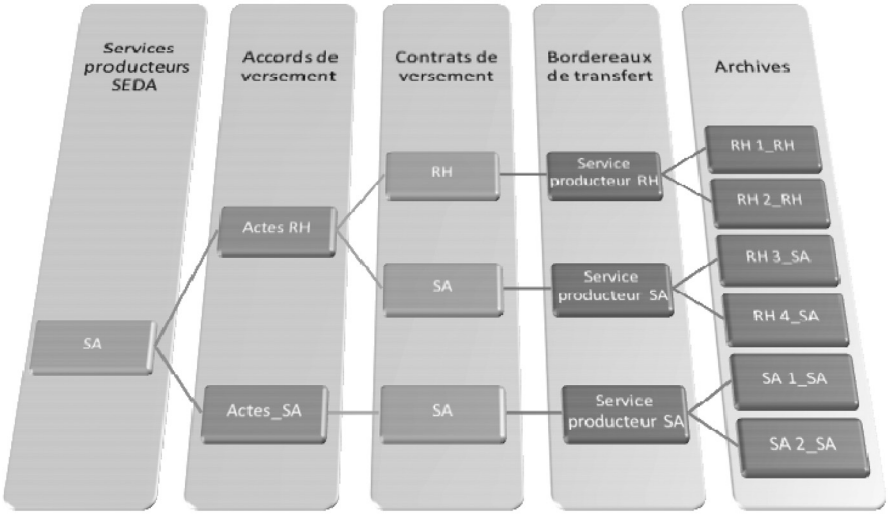
financiers et des cahiers des clauses administratives et techniques particulières (CCAP et CCTP). Le marché fut finalement attribué en juillet 2012 au groupement constitué :

- de l'intégrateur Logica, racheté peu après par la multinationale canadienne CGI ;
- du tiers archiveur agréé par le Service interministériel des Archives de France, pour sa solution de Tiers archivage pour la sphère publique (TASP), Risc Group IT Solutions (ITS), devenu quelques mois après Navaho et désormais filiale de Sewan Communications ;
- de l'éditeur du logiciel, en code source libre, ADULLACT solution libre d'archivage électronique (AS@LAE), ADULLACT Projet, filiale de l'Association des développeurs et des utilisateurs de logiciels libres pour les administrations et pour les collectivités territoriales (ADULLACT).

Le défi pour le groupement était de constituer un nouveau modèle économique, adapté à une sphère publique dont les codes et les enjeux ne lui étaient pas familiers de prime abord. Il était dès lors essentiel de s'appuyer sur des éléments tangibles. C'est ainsi que la mutualisation des instances de production entre plusieurs collectivités s'est imposée comme le seul moyen possible pour réduire suffisamment les coûts, tout en se devant impérativement de respecter la parfaite étanchéité des fonds et la confidentialité des accès aux données. La mise en œuvre de ce dernier aspect fut facilitée par les principes archivistiques du Standard d'échange de données pour l'archivage, basés sur une série d'échanges formalisés (transferts entrants, communications, restitutions, transferts sortants et éliminations) entre cinq acteurs (producteur, versant, archives, demandeur, contrôleur) et sur la contractualisation des versements, grâce à des accords de versement par flux entre le Service versant et le Service Archives, auxquels sont associés des contrats de versements greffant les Services producteurs.

De plus, l'harmonisation des profils d'archives (un profil étant lié à un flux documentaire) par les pilotes du projet permit de simplifier les acteurs, en particulier en mutualisant les Services versants. Mégalis Bretagne devint ainsi le seul service versant, commun à l'ensemble des adhérents au système d'archivage électronique régional. En outre, le système d'archivage électronique étant géré par un opérateur de tiers archivage (OTA), sous la responsabilité de l'Autorité de tiers archivage (ATA), le tiers archiveur Navaho devint également le Service Archives commun à l'ensemble des adhérents du système d'archivage électronique. En revanche, la mutualisation des Services producteurs est quasiment impossible, au risque majeur de mettre à mal la confidentialité de l'accès aux archives, voire de déroger gravement aux règles imposées par la Commission nationale informatique et libertés (CNIL) concernant la confidentialité de l'accès aux données à caractère personnel (DCP), sans compter l'impossibilité technique, en cas de séparation des services (lors des fusions de collectivités, par exemple), de réaffecter l'arriéré à ces services, par trop fastidieux.

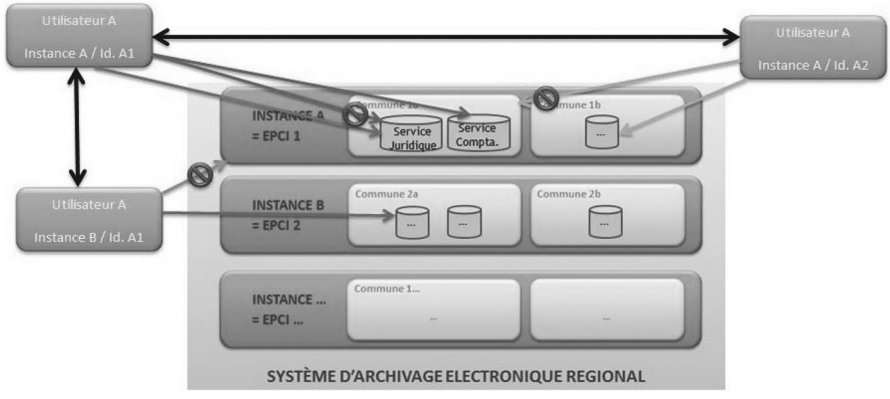
Tableau 3 – L'étanchéité par Services producteurs



Le défi le plus conséquent à relever était une mutualisation des instances, néanmoins garante de l'étanchéité des fonds. La solution AS@LAE a ainsi été architecturée pour s'adapter au mieux au contexte des établissements publics à compétence intercommunale, permettant, sur une seule instance dédiée à cet établissement, une étanchéité non seulement entre les collectivités ou tout établissement adhérents, mais aussi une étanchéité par Service producteur, le tout sécurisé par des droits paramétrables alloués par collectivité, par rôle utilisateur (profil défini selon la fonction de l'utilisateur sur le système : archiviste, administrateur, membre du Service producteur…) et par utilisateur. Ces droits s'affinent du premier vers le dernier, tout en considérant que l'entité inférieure (utilisateur par exemple) ne puisse avoir de droits plus élevés que l'entité supérieure (rôle utilisateur dans notre exemple).

En synthèse, le cloisonnement suivant est alors possible, bien que nous ayons affaire au même utilisateur.

Tableau 4 – L'étanchéité par utilisateur



Une mise en production sans accrocs

Moins d'un an aura été nécessaire à la mise en production opérationnelle du système d'archivage électronique, grâce, notamment, à une relation parfaitement maîtrisée entre Mégalis Bretagne et le groupement CGI-Navaho-ADULLACT, ainsi qu'à une excellente conduite du projet de Mégalis Bretagne vis-à-vis des collectivités pilotes retenues.

La validation de service régulier (VSR) fut notifiée le 14 août 2013. Les premiers transferts d'archives réelles (portant sur le contrôle de légalité d'actes liés aux ressources humaines) se déroulèrent sur les instances de production de Mégalis Bretagne et du conseil départemental du Morbihan (CD 56) dès le 25 juin. Le 27 juin, suivirent les premiers transferts de flux comptables et financiers, dans le cadre du Protocole d'échange standard, sur l'instance de production de Brest Métropole Océane (BMO). Le 1er août 2013, ceux des flux marchés eurent lieu sur l'instance de production du conseil départemental des Côtes d'Armor (CD 22).

Les premiers retours d'expérience de Mégalis Bretagne ne tardèrent pas, notamment :

- aux *Rencontres de l'administration électronique en Bretagne*, à Dinan, (7 décembre 2012), réunissant élus, acteurs publics, institutionnels, responsables associatifs, entreprises et journalistes autour des grandes questions de l'administration électronique. Parmi les thématiques : les impacts et les perspectives de l'administration électronique, l'évaluation des politiques publiques, les enjeux juridiques de la dématérialisation de bout en bout, la Loi informatique et libertés (LIL), la coopération territoriale, la modernisation des systèmes d'information des collectivités… Les partenaires et les prestataires de l'évènement étaient réunis autour du *Carrefour des Rencontres*, lieu d'exposition, d'échanges et de démonstrations ;
- lors du colloque *Système d'archivage électronique des archives publiques : Histoires de conduites de projets réussis* organisé par Mégalis Bretagne, en partenariat avec la mission Écologie et territoires (ÉcoTer) et avec la FedISA, à Rennes (31 janvier 2013) ;
- lors du 5e Congrès international de la Fédération de l'*Information Lifecycle Management*, du stockage et de l'archivage (FedISA), à Paris (17 juin 2013).

Le 10 avril 2013, les instances de production des pilotes (Mégalis Bretagne, les conseils départementaux des Côtes d'Armor, du Finistère et du Morbihan, ainsi que Brest Métropole Océane) démarrèrent. Le 20 juin 2013, ce fut au tour des huit instances de formation et des quatre instances de test de commencer leur activité.

Volumes de conservation sécurisée et écriture en Y

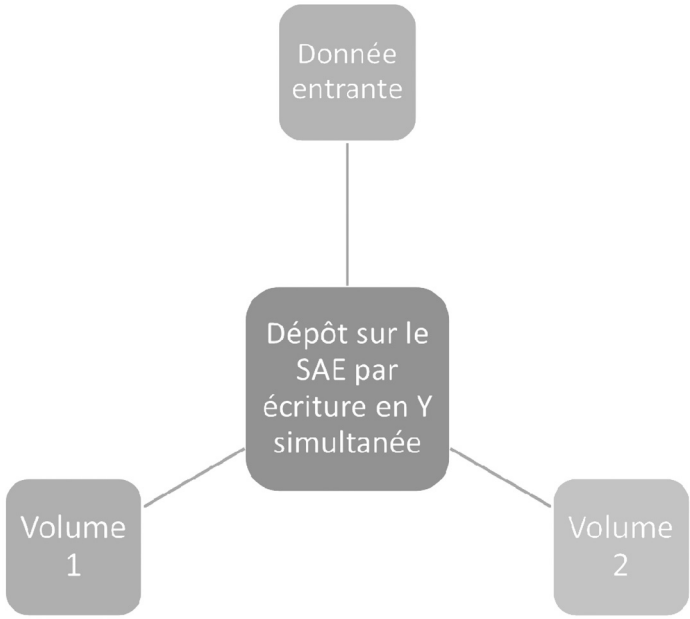
Dans le but d'accroître les performances du contrôle d'intégrité sur la solution, il a fallu développer AS@LAE, afin qu'il embarque directement la fonction de conservation sécurisée, *via* la gestion de simples machines virtuelles (VM) directement par le système d'archivage électronique, ce mode de stockage sécurisé s'avérant suffisant dans le contexte des collectivités territoriales et étant désormais défini par le tiers archiveur comme niveau de service standard. Environnement informatique séparé, autonome

et complet, virtuellement créé à partir d'une allocation dynamique de ressources logicielles ou matérielles disponibles sur un ou plusieurs serveurs, les machines virtuelles peuvent donner l'illusion d'environnements informatiques complètement séparés, mis à la disposition exclusive d'un ou de plusieurs utilisateurs, alors qu'en réalité, elles existent grâce à un système de partage de ressources et à des mécanismes d'exploitation multitâche, localisés dans des serveurs et leur permettant de fonctionner séparément. Ainsi, le couplage avec des coffres-forts numériques (CFN), à niveaux de sécurité différents selon les paramétrages et selon les technologies et les supports utilisés, demeure tout à fait possible pour les cas pertinents. Néanmoins, le coût induit est plus élevé, voire bien plus élevé.

La gestion des volumes de conservation sécurisée permet de séparer le stockage des fichiers par Services Archives, puis le plan de rangement défini dans AS@LAE permet de séparer le stockage des fichiers par Services producteurs. Sur une plateforme mutualisée de système d'archivage électronique, chaque volume de conservation sécurisée est cloisonné de façon logique, individualisant ainsi chaque collectivité ou organisme hébergé sur cette plateforme.

Parallèlement, un système d'écriture en Y (redondance) a été déployé en standard sur la solution. Le système d'archivage électronique effectue une écriture simultanée sur des supports de conservation sécurisée distincts (une écriture sur un support local et une seconde sur un support distant), autres que ceux supportant l'application elle-même. Il n'y a pas de notion de volume primaire ni secondaire, mais bien deux volumes homologues. Les opérations sont faites de façon simultanée au sein d'une même transaction, afin d'en garantir l'intégrité.

Tableau 5 – L'écriture en Y



Le stockage des deux exemplaires est enregistré dans le journal de cycle de vie des archives. Les contraintes de destruction du deuxième exemplaire sont identiques à celles du premier, les deux opérations de destruction s'effectuent également dans la même transaction et doivent être validées préalablement par l'utilisateur comme pour toute destruction d'archives.

Ainsi, un contrôle d'intégrité de type logiciel est systématiquement effectué sur les deux branches du Y lors du transfert entrant, de la consultation, de la communication, de la restitution, du transfert sortant et de la destruction. Toute corruption détectée sur l'une des deux branches entraîne la suspension de l'opération et l'alerte de l'administrateur. Une tâche planifiée permet, par ailleurs, un contrôle d'intégrité régulier des archives et peut aussi être lancée manuellement, assurant un contrôle d'intégrité de type *Content Addressed Storage* (cf. *supra*).

Tous ces contrôles sont tracés dans le journal de cycle de vie. Il est, *de facto*, possible d'attribuer des niveaux de conservation des archives par l'utilisation de volumes (systématiquement redondants) différemment sécurisés, selon le contexte. Le principe consiste à ce que chaque flux documentaire soit relié à un type de volume de conservation, défini en fonction de son niveau de sécurité, grâce à l'accord de versement.

Migration des supports

Les changements pour la fonction stockage induisent de migrer les données de l'ancien coffre-fort numérique vers les nouveaux volumes de conservation sécurisée.

La plateforme fut d'abord mise à niveau, avec les nouveaux composants, le 10 novembre 2014. La migration des archives fut achevée en seulement trois jours sans aucun incident majeur. Les données archivées furent migrées d'un volume vers un autre volume de conservation sécurisée. Le contrôle d'intégrité des fichiers fut effectué après chaque lecture en amont et après chaque écriture en aval. L'opération de migration achevée, un contrôle d'intégrité a été réalisé sur l'ensemble des données migrées, avant de rouvrir le service.

Afin de préparer au mieux cette opération potentiellement risquée, toute la procédure fut préalablement testée, non seulement sur les instances de développement de Navaho, mais aussi sur la plateforme de préproduction du client. Enfin, après un arrêt de la plateforme de production, une migration virtuelle fut préalablement réalisée, afin d'analyser le comportement de l'environnement. Le seul accroc a concerné l'intégrité des journaux d'évènements (notamment du fait de leur chaînage), sur la partie coffre-fort numérique. Aussi, le parti fut pris de ne pas les prendre en compte et de les régénérer intégralement à la fin de l'opération, avant de rouvrir la plateforme, le système d'archivage électronique autorisant une telle opération.

De très rares erreurs relevées provinrent en réalité de transferts d'archives mal formées en amont (profils à modifier en conséquence) et, par conséquent, indépendantes du système d'archivage électronique lui-même.

CONCLUSION

La conservation d'une archive ne se limite pas, comme nous l'entendons trop souvent chez nombre d'éditeurs, à deux, cinq ou dix ans, mais aussi à trente, soixante

voire au-delà de cent ans de durée d'utilité administrative, quand ce n'est pas *ad vitam aeternam* dans un cadre patrimonial indispensable à la préservation de la mémoire d'une société. *De facto*, la valeur informationnelle de l'archive évolue tout au long de son cycle de vie dans un sens comme dans l'autre, imposant des exigences à rapprocher à des niveaux de service/sécurité adaptés, proposés à l'intérieur d'un même système d'archivage électronique ou par des systèmes d'archivage électronique différents.

Quoi qu'il en soit, pour l'utilisateur, ces technologies doivent s'avérer transparentes, celui-ci n'aspirant qu'à accéder aux données et à être sûr de leur intégrité et de leur origine. L'exemple de la migration des archives de Mégalis Bretagne l'illustre bien, la technologie étant passée d'un coffre-fort numérique externe à une fonction de conservation sécurisée interne au système d'archivage électronique, sans que l'utilisateur n'y voie un quelconque changement que ce soit au moment de la consultation ou de la communication. Le résultat, positif sur toute la ligne, étant que la solution s'en trouve finalement considérablement renforcée, Mégalis Bretagne ayant renouvelé le marché en décembre 2014 et ce jusqu'à juin 2017, et l'agrément comme tiers archiveur de Navaho ayant été renouvelé par le Service interministériel des Archives de France, pour une durée de trois ans, en février 2015.

Tous ces dispositifs doivent enfin obéir à des logiques de coûts rationnels, sans surseoir pour autant aux impératifs de sécurité réglementaires et technologiques. Bien sûr, il est possible de sauvegarder ses données gratuitement sur des services de type Drop Box ou encore Google… mais sans aucune garantie réelle, non seulement quant à leur intégrité, mais aussi quant à la confidentialité de leur accès et à leur réversibilité. La sécurité a un coût et soyons alors attentifs à le rendre le plus juste possible par rapport à nos besoins. Désormais des solutions abordables existent et permettent la mutualisation des moyens et donc du financement, tout en assurant le cloisonnement des données (garant du respect des fonds) et le respect de leur intégrité au fil du temps, associant des contrôles logiciels tout autant que des contrôles de type *Content Addressed Storage* en attendant l'intervention de tel ou tel tiers de confiance comme l'horodateur.

Antony Belin Archiviste expert en dématique, ABC-D@E.

Jean-Marc Rietsch Expert international en dématique, président de la FedISA.