



Pineappli by FISAM

**LA CONSERVATION SECURISEE,
L'ARCHIVAGE DE DONNEES
NUMERIQUES**

Jean-Marc RIETSCH - Février 2021

PLAN DU DOCUMENT

INTRODUCTION	1
1. Objectifs et principales exigences de la conservation sécurisée	2
1.1. Exigences légales et réglementaires	2
1.2. Cloud et tiers archiveurs	3
2. Les solutions proposées	4
2.1. La solution de demain avec Pineappli :.....	4
2.2. Le bureau numérique du futur :	4
2.3. Le bureau numérique du futur	5
3. Représentation d'un système d'archivage électronique	6



INTRODUCTION

Le numérique est en train de bousculer bon nombre de nos habitudes. Il en est ainsi pour la conservation des documents numériques qui suivent leur cycle de vie de façon continue, contrairement à l'environnement papier où l'archivage rime souvent avec rupture concomitamment à un changement d'espace physique de stockage. Cette forme de fluidité dans la gestion des documents numériques et leur conservation engendre souvent un manque de considération de l'importance que revêt pourtant la « conservation sécurisée » des documents numériques dont les enjeux sont multiples :

- **Incapacité de retrouver un document** : Le premier enjeu est lié aux conséquences d'une incapacité de produire un document important qui aurait pourtant permis de se défendre dans le cadre d'un litige. De même les magistrats tireront toutes les conséquences, de l'impossibilité à produire le document réclamé. C'est également le cas de documents qui font l'objet d'obligations de conservation à des fins de contrôles administratifs pour lesquels l'absence de fourniture du document entraîne une pénalité.
- **L'enjeu lié à la valeur probante** : Pour être recevable il faut pouvoir démontrer l'origine du document, mais aussi que son intégrité a été conservée tout au long de son cycle de vie. En cas de contestation un document pourrait être rejeté et ainsi permettre à la partie adverse d'obtenir gain de cause.
- **L'enjeu lié à l'ignorance des contraintes réglementaires** : Enfin de nombreuses applications métier sont encadrées par des règles de conformité qui sont propres soit à un secteur d'activité soit à un type de document particulier. A ce sujet le RGPD (règlement général sur la protection des données) impose des règles très strictes en matière de conservation des données personnelles. Ignorer ces contraintes réglementaires revient à prendre des risques financiers et/ou pénaux.

I. OBJECTIFS ET PRINCIPALES EXIGENCES DE LA CONSERVATION SECURISEE

La qualité du système d'archivage et de façon plus large du système de conservation sécurisée d'informations numériques, détermine de façon structurante votre capacité à prouver vos droits dans toute situation litigieuse. Ainsi l'information doit être conservée de manière intègre tout au long de son cycle de vie et doit pouvoir être retrouvée à tout moment et en toute confiance quant à son origine, que l'information ait quelques minutes d'existence, quelques mois ou plusieurs années.

La confiance fait ici référence au caractère **authentique** d'un document, c'est-à-dire la garantie de son **origine**, de son **intégrité** et de son antériorité. En d'autres termes cela revient à garantir la valeur probante du document dans le temps. Même si un document n'a pas de valeur probante en tant que telle, il sera néanmoins important de pouvoir prouver à tout moment qu'il est intègre et que son origine est la bonne, au risque d'être totalement inutilisable.

Il est également nécessaire de veiller à la **pérennité** des documents numériques mais pas uniquement en regard des technologies de stockage. En effet l'attention devra être portée essentiellement sur les **formats logiques** destinés à assurer l'intelligibilité des documents dans le temps.

Enfin la **traçabilité** constitue un critère important de sécurité consistant à enregistrer tout ce qui se passe sur un document tout au long de sa période de conservation. La façon de gérer les traces doit également être irréfutable afin d'être retenu comme élément de preuve.

I.1. Exigences légales et règlementaires

La conservation sécurisée de données numériques doit répondre à des exigences techniques mais également organisationnelles. Il existe ainsi une multitude de normes et autres référentiels relatifs à la conservation sécurisée de données numériques et à leur archivage dont la plus connue en France est représentée par la NF Z42-013 et la certification correspondante NF461. En plus de ces référentiels l'on trouve également des agréments spécifiques comme celui dit HDS pour hébergeurs données de santé de l'ASIP Santé (agence française de la santé numérique).

1.2. Cloud et tiers archiveurs

Compte tenu de la complexité de mise en œuvre de la conservation sécurisée de données, la tendance est plutôt de se tourner vers un service externe mais encore faut-il en maîtriser les niveaux de services.

Ainsi le Cloud, apporte une bonne réponse en matière de service, sous réserve bien entendu que les opérateurs soient à même de garantir la sécurité adaptée et de prendre les engagements correspondants, ce qui malheureusement est encore loin d'être le cas, en ce qui concerne le niveau de sécurisation des données et la réponse aux contraintes légales et réglementaires, en particulier en matière de confidentialité.

En ce qui concerne l'archivage électronique à vocation probatoire, la logique de service est beaucoup plus engageante pour le tiers archiveur. En effet il ne suffira plus seulement de satisfaire à des temps de réponse ou à des volumes de stockage mais également à la pérennité des documents ainsi qu'à leur intégrité, intelligibilité, traçabilité, confidentialité et origine, sans oublier la localisation proprement dite des données.

Afin de s'assurer de la qualité du service, le principe de la certification représente sans doute le meilleur moyen actuel afin également de consolider l'environnement de confiance dont l'économie numérique a absolument besoin.

2. LES SOLUTIONS PROPOSEES

2.1. Les solutions actuelles :

Plusieurs options sont ainsi offertes aux entreprises pour préserver leur information :

- Stocker sans précaution particulière et sans vraiment faire attention au cadre réglementaire ! Comme évoqué, les risques encourus peuvent être très importants avec des conséquences désastreuses.
- Utiliser des services d'hébergement en mode « cloud » mais en ayant toutefois conscience de leurs limites (pérennité, localisation des données, nationalité du prestataire, engagements quant au respect de la confidentialité, de l'intégrité et de la non-perte des documents etc.).
- Avoir recours aux tiers archiveurs dans le respect strict de la réglementation et avec des engagements forts quant aux garanties proposées.

2.2. La solution de demain avec Pineappli :

Aujourd'hui arrive dans le monde de la conservation et de l'archivage une véritable révolution avec la solution Pineappli.

En rupture avec les systèmes traditionnels Pineappli apporte à la fois la souplesse du mode cloud et la sécurité d'un tiers archiveur ! Plutôt que de chercher à sécuriser le cloud en utilisant les techniques de chiffrement très contraignante quant à la gestion des clés, surtout sur du moyen, long terme il existe une nouvelle technologie basée sur le découpage des fichiers en blocs gérés de façon totalement indépendante, qui permet :

- de répondre concomitamment aux **quatre critères** sécuritaires (disponibilité, intégrité, confidentialité et traçabilité).
- de **conserver** de façon sécurisée les données ad vitam aeternam
- de choisir le **niveau** de sécurité adapté à la criticité des données concernées
- de **partager** efficacement et en toute sécurité l'informations entre utilisateurs identifiés

Nul doute que ce type d'architecture est amené à se répandre dans la mesure où il apporte souplesse, simplicité, efficacité, sécurité et confidentialité absolue.

C'est l'un des plus sûrs, si ce n'est le plus sûr au monde, pour conserver de la donnée numérique.

Au-delà de cette sécurité extrême, Pineappli s'est enrichi de nombreux services afin de répondre parfaitement aux enjeux induits par la transition numérique des entreprises.

En effet, afin d'affronter ce défi, les entreprises ont certes besoin, d'une sécurité maximale de leurs données, mais souhaitent également simplifier à l'extrême ces technologies nouvelles pour l'utilisateur final, tout en respectant parfaitement le cadre réglementaire de plus en plus exigeant et le tout à prix raisonnable, pouvant ainsi s'adresser aux entreprises de toute taille.

2.3. Le bureau numérique du futur :

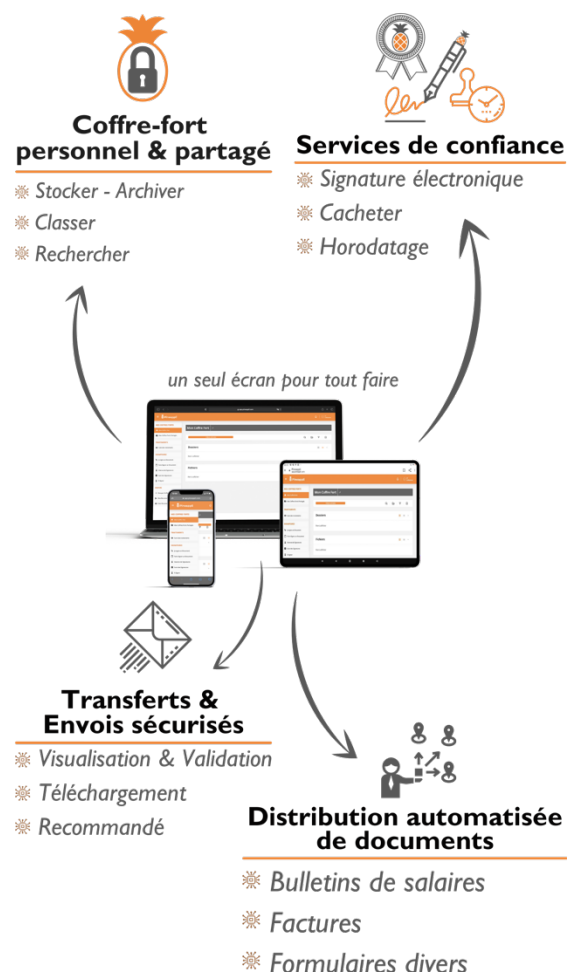
A partir d'un seul et même écran très intuitif, le bureau Pineappli, l'utilisateur peut gérer très facilement toutes les étapes de la vie d'un document.

Il peut ainsi conserver, archiver, classer, rechercher, partager, signer, cacheter, horodater, transférer un document, depuis son PC, sa tablette ou son smartphone.

Facile à utiliser et à installer en mode Cloud ou sur site, la solution Pineappli garantit une conformité légale et réglementaire et ce à prix très attractif.

En plus la solution Pineappli propose également une solution de numérisation à valeur probante permettant de supprimer les documents papier après les avoir scannés.

Le bureau numérique du futur



3. REPRESENTATION D'UN SYSTEME D'ARCHIVAGE ELECTRONIQUE



Tout ce que vous ne voyez pas

- Les supports physiques de conservation, les baies de stockage
- Les procédures entourant l'ensemble du service
- La charge d'exploitation du service
- La double administration à la fois sous l'angle technique et archivistique
- La maintenance de l'ensemble des composants employés tant matériels que logiciels
- La gestion de la sécurité, nous parlerons plutôt de gestion des risques
- La couverture en matière d'assurance, à prendre comme le transfert des risques que l'on ne peut ni accepter, ni réduire suffisamment
- Les migrations de supports dues à l'obsolescence rapide des matériels
- La conversion des formats afin de maintenir l'intelligibilité des donnée/documents conservés
- Les audits, internes et externes, destinés à vérifier le bon niveau de conformité du service tant d'un point de vue fonctionnel que légal et réglementaire
- La prise en compte de la signature électronique, en particulier afin de s'assurer de sa pérennité dans le temps
- L'utilisation d'un système d'horodatage fiable et plus précisément veiller à la synchronisation du temps pour l'ensemble des composantes matérielles et logicielles utilisées
- La veille à la fois légale, réglementaire et technique permettant de garantir la conformité requise