

Avis d'expert  
Saint-Ouen, le 29 novembre 2016

***Règlement e-IDAS, une avancée juridique majeure en matière de signature électronique et de gestion de documents numériques***



*Par Hervé STREIFF – Responsable Conformité et Sécurité de l'Information chez LOCARCHIVES*

Quelques mois après l'entrée en vigueur d'e-IDAS, comment décrypter ce qui se cache concrètement derrière cet acronyme et comprendre ses impacts sur la gestion des documents numériques ? Hervé Streiff délivre ici les clés pour appréhender cette évolution juridique en toute confiance.

**e-IDAS : qu'est-ce que ça signifie?**

e-IDAS signifie Electronic **Identification and Services**. Ce règlement européen (\*) vise à promouvoir les services de confiance relatifs à l'identité numérique : horodatage, signature et cachet électroniques, lettre recommandée... afin de favoriser la dématérialisation des échanges dans toute l'Europe.

**Le dispositif repose principalement sur des « prestataires de service de confiance » (Trust Service Provider - TSP), qui s'engagent à proposer des produits qualifiés par e-IDAS, gage de reconnaissance dans l'Union Européenne.** L'adoption de ce règlement confirme l'engagement des dirigeants européens en faveur de **la dématérialisation des dispositifs de reconnaissance et d'identification**, dans une économie toujours plus numérique.

Hier encore, pour signer un contrat par exemple, il suffisait d'une feuille de papier et d'un stylo. Comment faire aujourd'hui, quand la majorité des documents sont générés directement par des systèmes informatiques ? Dans les faits, les documents électroniques sont imprimés, signés à la main puis numérisés pour retrouver leur format initial... la boucle est bouclée ! En effet, le citoyen ne dispose d'aucune technique fiable de signature électronique. C'est donc bien **l'identité numérique** qui est donc au cœur du règlement e-IDAS.

(\*) Règlement UE n° 910-2014 du 23 juillet 2014 entré en vigueur en juillet 2016

### Quels sont les impacts sur les documents numériques et leur archivage ?

Dans 20 ou 30 ans, comment **démontrer la conformité d'un consentement signé électroniquement** en 2016 ?

Dans le monde numérique, **c'est la validité du certificat d'identité du signataire** qui permet de vérifier la signature. Un certificat numérique doit être renouvelé tous les 2 ou 3 ans. Quant au dispositif technique qui permet de générer une signature, il doit être renouvelé tous les 5 à 10 ans.

On le voit, les moyens techniques seuls ne permettent pas de gérer tout le cycle de vie d'un document. C'est le rôle de l'archivage, qui permet de conserver à très long terme non seulement le document lui-même, mais aussi sa signature et les preuves de validité du certificat lors de la signature.

Le système de signature à la volée permet de valider un document sans certificat d'identité numérique. Il suffit au signataire de s'identifier et de donner l'ordre à une machine de signer le document à sa place. Pour vérifier la validité de la signature, il est indispensable de conserver l'ensemble des éléments de la transaction afin de prouver les points suivants : qui ? quoi ? quand ?

### Préserver la signature sans le document a-t-elle du sens ?

Théoriquement il est possible de conserver le document et sa signature dans deux systèmes distincts. Dans ce cas, les deux éléments seront exigés pour vérifier l'intégrité du document archivé.

Les normes d'application e-IDAS **préconisent plutôt de conserver un « objet d'archives » regroupant le document et sa signature**. Ce dispositif simple offre une meilleure maîtrise du risque à long terme. Aussi, il est recommandé de réfléchir simultanément aux processus de signature et d'archivage, afin de constituer un « objet d'archives » intégrant les éléments de preuve.

Que se passe-t-il entre le moment de la signature et le moment du versement en archivage :

L'intégrité d'un document numérique est gérée par le Système d'Archivage Electronique qui l'exploite, et non par le support du document.

La réglementation impose que les documents à vocation probatoire soient conservés dans un Système d'Archivage Electronique répondant aux exigences **de la norme NF Z 42-013**. La révision de cette norme, qui devrait être publiée au printemps 2017, devrait permettre de détruire les documents originaux une fois numérisés selon un processus encadré. Cette conformité offre un haut niveau de traçabilité, intégrant des journaux chaînés, horodatés et eux-mêmes archivés afin de préserver l'ensemble des preuves d'intégrité.

### Comment garantir la vocation probatoire des documents ?

Ce sont **ces éléments de preuve** (générés par et conservés dans le SAE) qui confèrent leur vocation probatoire aux documents, et non le SAE lui-même.

Préserver l'intégrité impose de réduire au strict minimum la conservation des documents dans un environnement peu ou pas sécurisé, et de les verser dans un SAE au plus vite après leur signature.

Une entreprise qui utilise une GED (Gestion Electronique des Documents) avec des processus de validation aura donc intérêt à mettre en œuvre **un connecteur d'archivage associé au workflow de signature**, plutôt que d'attendre plusieurs années avant de verser les documents en masse, comme on l'observe encore trop souvent.

Développer son propre système d'archivage en interne nécessite des investissements importants à long terme : infrastructures informatiques et logicielles, moyens humains, procédures, certifications...

En cas d'externalisation de ces solutions, il est toutefois recommandé de s'assurer du respect de certaines normes : à minima **la certification NF Z 42-013, gage de confiance**. Lorsqu'il s'agit **d'archives publiques**, l'agrément du **SIAF** (Service Interministériel des Archives de France) est nécessaire.

Enfin, **l'agrément HDS** (Hébergeur de Données de Santé) est indispensable lorsque les documents contiennent **des données de santé à caractère personnel**

Le règlement e-IDAS est une véritable progression juridique. La signature électronique représente un levier conséquent **pour la digitalisation des entreprises dans une économie numérique où les process se dématérialisent**. C'est un gage de fiabilité et de sécurité accrue pour les entreprises ou utilisateurs qui y recourent. La signature électronique deviendra, à terme, **un gage de confiance aussi sécurisé que la signature manuelle**.

## A propos de LOCARCHIVES

LOCARCHIVES organise, gère et conserve les documents et archives sur supports numériques et physiques pour le compte de ses 6 000 entreprises et organisations clientes.

Avec un chiffre d'affaires de 45,5 M€ en 2015, LOCARCHIVES se positionne en leader dans le secteur de la gestion documentaire. LOCARCHIVES accompagne les entreprises dans leur transition numérique et met en œuvre des solutions externalisées dans une optique d'efficacité, de conformité et d'optimisation des coûts

Les chiffres 2015 :

- 450 salariés - 50 consultants et experts en traitement documentaire - 35 ingénieurs informatiques - 10 sites de conservation - 2 centres de numérisation – 2 datacenters internes - 1 Po de capacité de stockage - 10 millions de pages numérisées par an - 4 000 km de rayonnages - Plus de 7 millions d'ordres traités par an.

LOCARCHIVES est certifiée NF Z 42-013, NF Service Z40-350 et ISO 9001 ; agréée archives publiques sur supports papier et électroniques et hébergeur de données de santé ; labellisée FNTC-TA et France Cybersecurity

*Save the date : prochain rendez-vous LOCARCHIVES le mardi 6 décembre à Lyon pour le petit-déjeuner santé sur la dématérialisation des dossiers médicaux.*

Pour plus d'informations sur [LOCARCHIVES](#)

**Retrouvez les aussi sur les réseaux sociaux :**

[LinkedIn](#) [Twitter](#) [Google+](#) [Facebook](#)



**LOGARCHIVES**

**Contact presse**

Vanessa Marlier/Tatiana Graffeuil

01 41 11 37 70

[vanessa@oxygen-rp.com](mailto:vanessa@oxygen-rp.com)

\*\*\*