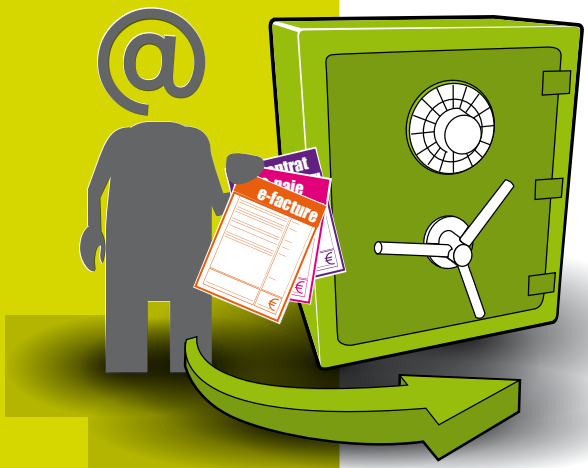
Fédération Nationale des
Tiers de Confiance

GUIDE DE L'ARCHIVAGE ELECTRONIQUE ET DU COFFRE-FORT ELECTRONIQUE



COLLECTION
LES GUIDES DE LA CONFIANCE
DE LA FNTC

Par le groupe de travail «archivage électronique»
de la Fédération Nationale des Tiers de Confiance

DANS LA COLLECTION LES GUIDES DE LA CONFIANCE DE LA FNTC :

• **Guide de l'archivage électronique et du coffre-fort électronique** (novembre 2010)

• **Au-delà de la migration ETEBAC** (septembre 2010)

• **Vade-mecum juridique de la dématérialisation des documents** (3ème édition, avril 2010)

• **Guide de la facture électronique** (janvier 2010)

• **Du mandat …… au mandat électronique** (décembre 2009)

• **Guide du vote électronique** (avril 2009)

• **Guide de la signature électronique** (septembre 2008)

• **Guide de la dématérialisation des marchés publics** (édition déc. 2006)

• **Guide de l'horodatage** (édition oct. 2004)

DANS LA COLLECTION LES GUIDES DE LA FORMATION DE LA FNTC :

• **MoReq2 et archivage sécurisé** (avril 2009)

SOMMAIRE

1 - PRÉFACE

Nous vivons désormais dans une société numérique, dans laquelle une grande partie des informations et des documents concernant notre vie privée et professionnelle sont dématérialisés. Pour les administrations et pour les entreprises, ce sont aussi bien les dossiers et les fichiers des clients et des fournisseurs que les stocks, la comptabilité, les procédés de fabrication, ou les documents administratifs, qui sont concernés. Que nous en soyons conscients ou non, les dossiers qui nous concernent ou qui concernent notre travail n'existent désormais souvent plus que sous forme électronique.

Parce qu'une information numérique se conserve et se duplique sans aucune altération, nous avons conçu l'illusion que nos données électroniques étaient éternelles. Funeste erreur ! Un rapport récent de l'Académie des sciences et de l'Académie des technologies[1] vient de révéler que les supports numériques couramment utilisés (disques durs, bandes magnétiques, disques optiques, etc.) ne garantissent pas une conservation au-delà de quelques années, car ils se dégradent rapidement. Se pose d'autre part la question de l'intégrité des informations conservées : comment pouvons-nous garantir que des données probantes ou contractuelles n'ont pas été frauduleusement modifiées depuis leur création ?

L'art de l'archivage électronique constitue la réponse à ces questions. Conserver pendant plusieurs décennies des documents médicaux ou des bulletins de paie dématérialisés ne s'improvise pas ; archiver même sur des périodes plus courtes les documents intéressant la vie de l'entreprise non plus. Dans ce petit guide, la Fédération Nationale des Tiers de Confiance fait le point sur cette question. Je ne doute pas que ce manuel sera d'un secours inestimable à nombre de responsables dans les années à venir.

Nathalie Kosciusko-Morizet
Secrétaire d'État chargée de la Prospective
et du Développement de l'économie numérique,
auprès du Premier ministre

1/.Jean-Charles Hourcade, Franck Laloë et Erich Spitz, Longévité de l'information numérique – les données que nous voulons garder vont-elles s'effacer ?, mars 2010.

2 - INTRODUCTION

L'archivage doit faire partie de la politique de maîtrise des risques de l'entreprise. Dans la continuité des pratiques de l'archivage des documents papier, et pour les mêmes raisons, l'entreprise doit maintenant archiver des documents immatériels ou dématérialisés, ceux-ci remplaçant progressivement les documents sous forme matérielle.

Ce guide a pour objectif d'aider les entreprises et leurs responsables à mettre en œuvre des solutions pertinentes d'archivage électronique de documents ou de données informatiques.

Il s'adresse aux chefs d'entreprises et également à leurs conseils, en particulier les experts-comptables et les commissaires aux comptes, en raison notamment de leur rôle accru en matière de prévention des risques de l'entreprise.

3 - L'ARCHIVAGE ÉLECTRONIQUE ET SES FAUX AMIS

L'archivage est à la fois une obligation et une nécessité pour l'entreprise :

- Obligation au regard des différentes lois, règlements et directives qui constituent le cadre dans lequel opère l'entreprise : code de commerce, code général des impôts, code du travail, codes et règlements spécifiques par activité ;
- Nécessité de se protéger en réduisant ses risques et préserver son patrimoine technique, commercial, informationnel au sens large.

L'archivage répond aux règles fondamentales de l'archivistique, qui restent applicables pour l'archivage électronique des documents (voir ci-dessous). Par ailleurs, il existe une définition des archives :

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.
(art. L 211-1 du Livre II du Code du patrimoine).

Archiver c'est donc conserver (des informations, des documents, des objets, etc.) dans le but de les retrouver, pour des raisons identifiées, sur des durées définies.

L'archivage électronique recouvre les mêmes fonctions appliquées aux documents sous forme numérique (on dira aussi dématérialisée ou électronique).

Il ne doit pas être confondu avec le stockage ou la sauvegarde :

- Le stockage est l'enregistrement de données sur un support informatique en vue d'une utilisation courante ou immédiate ;
- La sauvegarde est une copie de données d'un support sur un autre pour permettre la restauration de celles-ci à un état antérieur, en cas de panne matérielle ou logicielle.

L'archivage électronique tend à maintenir une valeur juridique aux documents, de leur établissement jusqu'au terme du délai de conservation.

L'archivage se distingue donc de la sauvegarde et du stockage du fait de son caractère pérenne et juridique[2].

Selon les fondamentaux de l'archivistique, les fonctions de l'archivage électronique se résument à :

- Sélectionner, identifier et préparer les documents qui constituent les archives ;
- Conditionner et verser les informations descriptives et les documents dans le Système d'Archivage Électronique ;
- Assurer la pérennité, l'intégrité et la conservation sur les périodes requises et donc « gérer » les archives, c'est-à-dire organiser leur enregistrement, leur classement, mettre en œuvre les dispositions de sécurisation, les prendre en charge, contrôler leurs accès ;
- Communiquer les archives, les restituer et les détruire en fin de durée de conservation.

2/.Eric Caprioli, « L'archivage électronique », JCP éd. G 2009 n°38.

4 - LES DOCUMENTS CONCERNÉS

Dans ce qui suit, on emploie le mot « document » dans son sens le plus large ; s'agissant de document sous forme numérique, on rencontrera des formes et des contenus très variés : fichier d'édition, document bureautique, fichier de données (base de données informatique, fichier structuré selon une norme ou une convention, fichier audio et/ou vidéo, etc.).

Les documents visés par l'archivage électronique sont ceux qui traduisent sous forme dématérialisée les relations de l'entreprise avec des tiers (clients, fournisseurs, administrations, organismes sociaux, salariés, actionnaires, etc.) au titre de ses activités, qu'ils soient reçus ou produits et émis.

A titre d'exemple :

- Pour les relations commerciales :
  - Copies des factures clients ;
  - Factures dématérialisées ;
  - Commandes ;
  - Bons de livraison ;
  - Tickets de caisse ;
  - Etc.

- Pour les relations avec les administrations et les organismes sociaux :
  - Les déclarations fiscales (TVA, liasse fiscale, etc.) ;
  - Les déclarations sociales (DUCS, DAS, etc.) ;
  - Etc.

- Pour la tenue des comptes :
  - Pièces comptables ;
  - Journaux, grand livre ;
  - Tableaux de calcul des provisions ;
  - Etc.

- Pour la gestion du personnel :
  - Les copies de bulletins de paie ;
  - Les relevés d'heures ;
  - Etc.

- Pour le système d'information (notamment la partie qui relève du contrôle des comptabilités informatisées) :
  - La documentation des logiciels ;
  - Etc.

Les courriers électroniques doivent eux aussi être archivés par l'entreprise. Mais, au vu de la multitude de courriers envoyés par chaque salarié chaque jour, on comprend bien que leur archivage total serait d'un coût prohibitif et de surcroît, serait inutile (certains messages étant sans réel intérêt professionnel). C'est pourquoi il est pertinent de gérer en amont l'archivage des courriers électroniques en mettant en place une Politique d'Archivage et des procédures pour déterminer quels courriers doivent être archivés (des correspondances professionnelles disposant d'un pouvoir engageant l'entreprise, le plus souvent).

Les courriers électroniques sont souvent utilisés devant les tribunaux en tant que commencement de preuve pour étayer un raisonnement juridique. En outre, ils peuvent servir de pièce justificative pour une transaction donnée ou un contrat.

On attachera beaucoup de soins à la détermination des documents qui doivent être archivés, avec l'objectif prioritaire de ne considérer que les documents dans leur forme d'origine ou originale, caractérisés par leur valeur. Tout changement de forme du document préalablement à son archivage risque de remettre en cause la valeur du document archivé.

Exemple :

- L'impression sur papier d'un écrit électronique au sens de l'article 1316-1 du Code Civil, par exemple un contrat, a la valeur de copie et non d'original ;
- L'impression sur papier d'une facture dématérialisée au sens de l'article 289 bis ou 289 V 1er alinéa du Code Général des Impôts n'a pas la valeur d'un original ;
- La numérisation avec destruction d'un document papier et la conservation de son image électronique peuvent affaiblir la valeur probatoire du document et avoir des conséquences pour l'entreprise, car le document numérisé n'est qu'une copie.

5 - LES ENJEUX PRINCIPAUX

Les enjeux principaux de l'archivage électronique sont d'ordre légal, fiscal ou réglementaire.

Depuis l'an 2000, tous les textes légaux ou réglementaires produits vont dans le même sens : la reconnaissance de la valeur légale des formes électroniques et le formalisme ou les exigences qui sont attachés à leur valeur. Il est désormais impossible d'ignorer ces textes :

- 2000 : Loi du 13 mars 2000 qui introduit l'écrit électronique dans le Code Civil ;
- 2004 : Loi sur la Confiance dans l'Économie Numérique (LCEN) qui complète les dispositions apportées par la Loi du 13 mars 2000 en autorisant les écrits sous forme électronique chaque fois qu'un écrit est requis pour la validité d'un acte ;
- 2006 : Instruction fiscale relative au contrôle des comptabilités informatisées (récapitulant l'ensemble des exigences depuis la loi de finances récapitulative pour 1990) ;
- 2007 : Instruction fiscale relative à la conservation sous forme électronique des copies de factures produites sur support papier ;
- 2009 : Loi autorisant la dématérialisation du bulletin de paie qui en fixe le cadre et arrêté du 4 décembre 2009 rendant réglementaire pour l'archivage électronique des collectivités la norme d'archivage électronique AFNOR NF Z42-013.

Qu'ils émanent du législateur, de la Cour de Cassation, ou de l'Administration fiscale, tous ces textes vont dans le même sens et mettent en avant, à des degrés divers, les mêmes exigences :

- Imputabilité ;
- Intégrité ;
- Traçabilité ;
- Authenticité (notamment : garantie d'origine et date fiable).

Pour faciliter la compréhension, nous avons regroupé ces différents textes par nature.

5.1 La preuve électronique et les litiges faisant intervenir un document électronique

Plusieurs jurisprudences, notamment des arrêts de la Cour de Cassation, confirment les conditions de validité des écrits électroniques telles que définies par la loi du 13 mars 2000 modifiant le Code Civil.

À titre d'exemple, on cite l'arrêt du 4 décembre 2008 qui rejette la reconstitution *a posteriori* d'un document électronique présenté à titre de preuve.

Extraits de l'arrêt de la Cour de Cassation du 4 Décembre 2008 :

« […]
lorsqu'une partie n'a pas conservé l'original d'un document, la preuve de l'existence de ce document peut être rapportée par la présentation d'une copie qui doit en être la reproduction non seulement fidèle mais durable ; que la Cour d'Appel a constaté que le document litigieux présenté par la Caisse, qui ne comportait pas la signature de son auteur, comme la copie d'un courrier d'information prétendument envoyé par la CPAM de la MARNE le 20 janvier 2003 avait été «édité sur un papier à en-tête revêtu d'un logo diffusé en 2004» ; qu'en ne tirant pas les conséquences de cette constatation dont il résultait que le document n'était pas une copie fidèle du prétendu courrier d'information original, la Cour d'Appel a violé les articles 1334 et 1348 du Code civil ;

[…]
qu'en considérant le document produit par la CPAM de la MARNE comme la «copie informatique du courrier en date du 20 janvier 2003», sans rechercher si le fichier informatique litigieux avait bien été établi le 20 janvier 2003 et conservé dans des conditions interdisant à la Caisse de modifier le contenu de ce document, la Cour d'Appel a privé sa décision de toute base légale au regard de l'article 1316-1 du Code civil ;

ALORS, ENFIN ET EN TOUT ETAT DE CAUSE, QUE l'admission par le juge judiciaire d'une prétendue copie informatique qui ne présente aucune garantie de fidélité, d'inaltérabilité et d'intégrité n'est pas conforme aux exigences du procès équitable ; de sorte qu'en admettant que la preuve de l'exécution de son obligation d'information par la CPAM de la MARNE serait rapportée par la seule production d'un document informatique dont rien ne permettait de garantir qu'il n'avait pas été établi par la Caisse pour les besoins du litige, la Cour d'Appel a violé l'article 6-1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. »

Cet arrêt expose clairement les conditions de validité d'une copie électronique présentée à titre de preuve devant une juridiction :

- Fidélité au document original ;
- Authenticité ;
- Pérennité.

5.2 La tenue de la comptabilité et la conservation des informations comptables

Après une période de « laisser-faire », le Plan Comptable Général et le Code Général des Impôts rappellent aujourd'hui qu'une comptabilité informatisée doit respecter certaines conditions et que, en particulier, l'archivage des données et des éditions doit respecter certaines règles.

De plus, l'Instruction fiscale relative au contrôle des comptabilités informatisées précise que le périmètre du contrôle comprend toutes les informations et les traitements qui concourent directement ou indirectement à la formation des résultats comptables et fiscaux. Ainsi, c'est une partie très importante du système d'information qui, pour des raisons réglementaires, doit être archivée.

Extraits du Plan Comptable Général :

Art. 410-4. L'organisation de la comptabilité tenue au moyen de systèmes informatisés implique l'accès à la documentation relative aux analyses, à la programmation et à l'exécution des traitements, en vue, notamment, de procéder aux tests nécessaires à la vérification des conditions d'enregistrement et de conservation des écritures. Toute donnée comptable entrée dans le système de traitement est enregistrée, sous une forme directement intelligible, sur papier ou éventuellement sur tout support offrant toute garantie en matière de preuve.

Art. 410-6. Toute entité tient un livre-journal, un grand livre et un livre d'inventaire. Le livre-journal et le livre d'inventaire sont cotés et paraphés. Des documents informatiques écrits peuvent tenir lieu de livre-journal et de livre d'inventaire s'ils sont identifiés, numérotés et datés dès leur établissement par des moyens offrant toute garantie en matière de preuve.

Extrait de l'introduction de l'Instruction fiscale 13L-1-06 de janvier 2006 :

L'Instruction expose la teneur des obligations de présentation des documents comptables et de conservation des données concourant directement ou indirectement à la détermination du résultat fiscal posées respectivement par les articles 54 du code général des impôts et L. 102 B du livre des procédures fiscales.

A cet égard, la réalisation par les contribuables d'une procédure périodique de « figement » des données dans un fichier « archives », la mise en place de la traçabilité d'éventuelles modifications de ces données, ainsi que le recours à la signature électronique pour renforcer le caractère incontestable de l'archivage effectué, sont de nature à garantir aux entreprises qu'elles se conforment à leurs obligations de conservation.

Enfin, en ce qui concerne les conséquences du contrôle d'une comptabilité informatisée, l'Instruction décrit les manquements aux obligations de conservation et de présentation (tels que, par exemple, la non validation des écritures comptables, le défaut de traçabilité des modifications, l'insuffisance des données archivées) susceptibles de conduire au rejet d'une comptabilité informatisée car lui conférant un caractère non régulier et non probant, et leur éventuelle conséquence, la reconstitution des résultats.

La possibilité de sanctions est donc associée à une insuffisance d'archivage.

L'enjeu principal lié à la bonne tenue de la comptabilité et à son bon archivage est naturellement d'ordre fiscal. Mais au-delà, elle revêt une importance particulière dans tous les cas où la valeur de l'entreprise doit être évaluée, notamment en cas de vente ou d'achat d'une société (garantie de passif).

5.3 Les enjeux de l'archivage dans le cadre de système comptable intégré dans un ERP

La mise en place d'un ERP (*Enterprise Resource Planning*) ou Progiciel de Gestion Intégré (PGI) a prioritairement un objectif de rationalisation des processus métiers de l'entreprise. La comptabilité, intégrée, devient, dans un tel environnement, la résultante de processus métiers largement dématérialisés.

Aux obligations de traçabilité, de clôture des exercices, de conservation des données et de la documentation à vocation probatoire, l'ERP répond par dématérialisation des traitements et des données, référentiel unique, mise à jour en temps réel, adaptation du paramétrage. Ce qui n'est pas sans poser des difficultés de compatibilité d'objectifs entre les vérificateurs externes et les gestionnaires internes.

Comment allier souplesse de paramétrage et de gestion des données avec le respect des obligations de traçabilité et de conservation des données à vocation probatoire ? Une gageure pas toujours clairement appréhendée dans les projets de mise en place d'ERP.

Les obligations, édictées par le Plan Comptable Général (PCG) et par le Code Général des Impôts (CGI), ne font que transposer au monde informatique les obligations attachées à toute comptabilité et s'appliquent *a fortiori* aux comptabilités intégrées dans un ERP.

Les points clés de vigilance dans le cadre d'un ERP sont principalement les suivants :

1. ***Intangibilité des enregistrements, ce qui interdit toute modification ou suppression après validation des écritures (art. 410-5 du PCG) :***
   - *Cela implique de mettre en œuvre un verrouillage des écritures et des justificatifs amonts (facturation, calculs de provisions, etc.) avant que les états financiers définitifs soient établis, même si la comptabilité reste « en ligne » ;*
   - *Les états produits et les justificatifs attachés doivent alors faire l'objet d'un archivage à date avec vocation probatoire dans un format non propriétaire et non modifiable.*

2. ***Existence de clôtures comptables destinées à figer la chronologie des opérations :***
   - *Mise en place d'un blocage à l'ouverture d'un exercice, si l'exercice N-2 n'est pas clôturé, et de toutes les applications auxiliaires qui l'alimentent ;*
   - *Le processus de clôture d'exercice doit générer la production des archives comptables légales : livre-journal, journaux centralisateurs, grands livres auxiliaires et généraux, balances auxiliaires et générales, bilan, compte de résultat, annexes, etc. dans un format non propriétaire et non modifiable.*

3. ***Traçabilité de la Piste d'Audit Comptable avec association des justificatifs aux pièces comptables, l'élément de justification étant directement ou indirectement lié à l'écriture comptable générée :***
   - *La Piste d'Audit Comptable sera d'autant plus vulnérable si d'autres applications interviennent dans le système d'information. La conservation des fichiers d'interfaces est un élément majeur de l'archivage encore mal appréhendé (gestion des volumes), mais incontournable ;*
   - *La permanence de la Piste d'Audit Comptable s'effectue à deux niveaux. La piste d'audit statique qui permet la justification des informations contenues dans les comptes et dans les états financiers (y compris les retraitements extracomptables et informations hors bilan) et la piste d'audit dynamique qui permet de justifier l'évolution d'une donnée comptable ou d'un état financier, d'une date à une autre.*

4. ***Documentation des progiciels et des paramétrages avec historisation et conservation des différentes versions et leurs dates d'application :***
   - *Base de connaissance à disposition des vérificateurs, la documentation de l'ERP et ses mises à jour sont essentielles. Chaque version de la documentation doit par ailleurs être validée et archivée afin d'en assurer sa valeur probante. Elle est grandement liée à l'organisation du projet ERP et à sa maintenance ;*
   - *Trop souvent négligée après mise en œuvre de l'ERP, elle doit s'intégrer à la documentation du contrôle interne en général et faire l'objet d'audit régulier de conformité ;*
   - *Concrètement, la cartographie des processus et du système d'information doit mentionner les procédures d'archivage prévues pour chaque table ou fichier susceptible d'être contrôlé fiscalement.*

5. ***Conservation et traçabilité des référentiels par dates d'application, comme les tarifs de vente par exemple, lorsqu'ils concourent directement ou indirectement à la détermination du résultat fiscal :***
   - *La gestion des dates d'application des référentiels est un élément essentiel à la maîtrise de leur traçabilité. L'archivage des versions successives doit donc en tenir compte ;*
   - *La dématérialisation des opérations au sein de l'ERP renforce la gestion des référentiels et leur mise à jour ainsi que la nécessité d'une conservation à vocation probatoire des versions successives.*

Le cas de la facturation client dans un ERP permet d'illustrer l'impact à haut risque d'un non respect des points clés abordés ci-dessus. Des tables tarifaires (données indirectement liées à la détermination du résultat), dont les valeurs ne sont pas associées à une période de validité, et des factures clients (traitement directement lié à la détermination du résultat) non conservées dans un format indépendant et non modifiable, entraînent, lors d'un contrôle, la nécessité de générer un nouveau calcul de la facture. Ce nouveau calcul est, de fait, basé sur le nouveau tarif (puisque non borné par des dates de validité), même si la facture est recalculée à une date de réalisation antérieure.

Conclusion : le montant de la facture ne correspond plus à la facture initialement enregistrée et le contrôleur est à même de rejeter la comptabilité !

Par ces points clés de vigilance de l'organisation de l'ERP, il est certain que l'archivage est un enjeu central de la matérialisation de la preuve. Il devient, dès lors, partie intégrante du système d'information et porte sur l'ensemble des opérations réalisées (collecte, saisie, traitement, etc.).

Dans cette optique, il faut bien repréciser que l'archivage (au sens fiscal) des données et traitements est absolument réalisé dans un format indépendant de celui de l'ERP et qu'il n'équivaut en aucun cas à la sauvegarde classique des données.

5.4 La conservation des copies de factures clients

La facture client est l'un des documents les plus importants de l'entreprise ; elle revêt en effet un triple rôle :

- Rôle comptable, puisqu'elle est la base de la comptabilisation du chiffre d'affaires ;
- Rôle fiscal, puisqu'elle est le support de la collecte de la TVA ;
- Rôle légal, puisque la facture peut être produite comme preuve devant un tribunal.

Nous avons rappelé précédemment les exigences en matière de comptabilité et de preuve. Concernant la TVA, l'Instruction fiscale 3-1-07 de janvier 2007 a décrit en 3 pages les pratiques à respecter pour la conservation du double de la facture émise sur support papier et résume en 3 lignes ce qu'il ne faut pas faire à l'article 19 :

Extrait de l'Instruction fiscale 3-1-07 (janvier 2007) :

Art.19. Ainsi, ne présentent pas une garantie suffisante les fichiers contenant le « double électronique » de la facture conservés sous un format qui peut faire l'objet de modification après sa constitution ou qui seraient enregistrés sur un support physique réinscriptible.

Cette pratique insuffisante est malheureusement encore majoritaire dans les entreprises, grandes ou petites. Le risque encouru est particulièrement important, l'impôt en jeu étant la TVA, premier impôt par le montant.

5.5 Le contrôle de l'URSSAF et l'Inspection du Travail

Le contrôle URSSAF fait peser sur les entreprises des contraintes d'archivage très proches de celles du contrôle fiscal.

L'URSSAF à l'obligation de mettre à disposition du cotisant une « charte du cotisant contrôlé » qui fixe les modalités de contrôle (article R.243-59 du code de la sécurité sociale).

En conséquence de l'article R.243-59-1 relatif aux investigations en milieu dématérialisé, la charte précise que :

Les investigations en milieu dématérialisé :

Dans l'hypothèse où vos systèmes de paie et votre comptabilité sont informatisés, le contrôle porte sur l'ensemble des informations, données et traitements qui servent de base directement ou indirectement à l'établissement des déclarations sociales obligatoires et des états sociaux, ainsi que sur la documentation relative aux analyses, à la programmation et à l'exécution des traitements.

L'inspecteur peut, si vous l'acceptez, effectuer lui-même la vérification sur l'équipement logiciel et matériel que vous utilisez. Si vous refusez que le contrôle soit effectué sur votre équipement, vous devez l'indiquer par écrit et mettre à sa disposition les copies des documents, des données et des traitements nécessaires au contrôle sur un support informatique répondant à des normes préalablement acceptées par écrit par l'inspecteur. Ces copies doivent vous être rendues avant l'envoi de la mise en demeure.

Vous pouvez demander à effectuer vous-même ou à faire effectuer par votre prestataire de service tout ou partie des traitements nécessaires au contrôle. Dans ce cas, l'inspecteur vous précise par écrit les travaux à réaliser ainsi que le délai accordé pour les effectuer.

En vue de faire face à un contrôle de l'URSSAF (sur place ou sur pièces), les entreprises doivent produire des documents qui sont, pour partie, archivés sous forme papier et, pour partie, sous forme dématérialisée (ces derniers remplaçant progressivement les documents sous forme papier).

Par exemple, le contrôle sur pièces de l'URSSAF peut porter sur les documents suivants :

- LIVRES LEGAUX :
  - Livre de paie ;
  - Registre du personnel.

- JURIDIQUE :
  - Statuts et registres juridiques des CA et AG ;
  - Extraits KBIS de la société.

- CONTRATS DE TRAVAIL :
  - Contrats de travail du personnel CDI/CDD/Apprentis/Autres ;
  - Contrats d'intéressements ou article 82 ou 83 ;
  - Dossiers administratifs spécifiquement liés aux abattements et exonérations.

- DECLARATIONS SOCIALES :
  - Déclarations URSSAF (bordereaux mensuels ou trimestriels) ;
  - Déclarations DADS et DAS 2 ;
  - Notification de taux accident du travail.

- DOCUMENTS DE TRAVAIL POUR LE CONTRÔLE :
  - Détail des avances et acomptes accordés ;
  - Détail des remboursements des frais professionnels ;
  - Détail des allocations forfaitaires de frais.

- PIECES JUSTIFICATIVES :
  - Bulletins de paie ;
  - Justificatifs des horaires de travail effectués ;
  - Fiches nominatives annuelles des salaires ;
  - Notes de frais professionnels (partiellement non dématérialisables) ;
  - Relevés détaillés des frais kilométriques ;
  - Détail et valorisation des avantages en nature.

Mais comme le souligne la charte :

Cette liste n'est pas exhaustive, l'inspecteur adaptant les modalités de sa vérification et ses demandes à l'organisation et au système d'information de votre entreprise. Il peut donc être amené à vous demander tout document et support d'information supplémentaires.

Concernant l'Inspection du Travail (Ministère de l'Emploi et de la Solidarité), la circulaire 98/9 du 2 novembre 1998 est obsolète s'agissant des mesures de simplification du bulletin de paie (modifiées par décret n° 2005-239 du 14 mars 2005). En revanche, elle demeure pertinente sur la conservation du bulletin de paie et notamment :

- Elle précise les modalités de communication aux services de contrôle des doubles des bulletins de paie lorsqu'ils ne sont pas conservés sur support matérialisé de type papier ;
- Elle fait un rappel de la jurisprudence relative au lieu de conservation des doubles des bulletins de paie (en cas d'externalisation des opérations liées à la paie ou cas d'entreprises à établissements multiples).

En matière d'archivage et de présentation de l'exemplaire employeur du bulletin de paie, les principales obligations de ce dernier vis-à-vis de l'Inspection du Travail peuvent donc être résumées comme suit :

- Les entreprises peuvent utiliser des supports informatiques pour la conservation des bulletins de paie, dès lors que « des garanties de contrôle équivalentes sont maintenues ». C'est ainsi notamment que les employeurs doivent mettre à disposition des agents de contrôle un moyen leur permettant d'accéder directement aux informations stockées et de les éditer sans délai. Pour mémoire, ce droit de communication est immédiat ;
- En cas d'externalisation des opérations liées à la paie, les doubles des bulletins doivent être détenus dans l'entreprise ;
- Dans le cas d'entreprises à établissements multiples, les bulletins de paie doivent être présents dans les entreprises ainsi que dans les établissements distincts comportant un représentant de l'employeur ayant le pouvoir de recruter du personnel.

L'archivage électronique apporte une réponse à la fois performante et économique ; il permet en effet de définir des profils de consultation limités à un établissement et évite ainsi d'envoyer une copie papier des bulletins dans chaque établissement (en plus parfois d'une autre copie envoyée à la DRH siège).

6 - LES SOLUTIONS ET LES BONNES PRATIQUES : MISE EN PLACE D'UN SYSTÈME D'ARCHIVAGE ÉLECTRONIQUE

Un Système d'Archivage Électronique (SAE) est un ensemble de moyens techniques, administratifs et humains, permettant de conserver dans de bonnes conditions les documents numériques qui lui sont donnés et ce pendant une période requise.

Les moyens techniques peuvent être assurés soit par l'utilisation d'un Coffre-fort Électronique, soit par la mise en œuvre d'une solution informatique développée en interne et répondant aux exigences de la norme NF Z42-013.

Il constitue l'un des composants de la Politique d'Archivage de l'entreprise qui a pour but d'organiser et de prévoir les responsabilités, les dispositifs et les pratiques pour l'ensemble des archives quels que soient leurs supports selon les exigences associées.

La période de conservation peut aller de quelques mois à plusieurs dizaines d'années, voire *ad vitam* (comme les documents patrimoniaux, par exemple).

Afin d'être un outil de confiance, un SAE se doit d'apporter et garantir :

- **La pérennité :** en utilisant des formats de conservation standardisés ou normalisés afin que le document puisse être relu pendant sa période de conservation ;
- **L'intégrité :** en disposant de moyens permettant de vérifier qu'aucune modification n'a été apportée au document ;
- **La sécurité :** en archivant sur plusieurs sites et en protégeant les accès contre tout système ou personne non autorisé ;
- **La traçabilité :** en enregistrant dans des journaux toutes les opérations relatives aux documents et en archivant ces journaux eux-mêmes ;
- **L'exhaustivité :** en disposant de moyens permettant de vérifier que la liste des documents (inventaire) est bien conforme à ce qui a été déposé et non retiré de l'archivage.

En archivage électronique, les principes ne changent pas mais sont adaptés pour les raisons suivantes :

- Modalités induites par les caractéristiques intrinsèques des objets numériques (dissociation information/support, contenu informationnel et métadonnées, format de structuration et de présentation du contenu informationnel) ;
- Nécessité de prendre en compte la totalité de l'espace temporel des objets numériques (c'est-à-dire depuis leur origine jusqu'à leur destruction) ;
- Modalités induites par les technologies de traitement de l'information.

La finalité de l'archivage conduit à définir les critères fondamentaux d'une solution d'archivage. Le tableau ci-après dresse la liste de ces critères en comparant les deux types d'archivage (traditionnel et électronique) :

Critères	Archivage traditionnel	Archivage Électronique
Pérennité	Qualité des supports et conservation d'un exemplaire unique.	Écritures en multiples exemplaires, utilisation de formats informatiques non propriétaires, etc.
Intégrité	Méthodes de protection des objets (en limitant leurs sorties).	Catalogue des objets conservés, outils permettant de détecter toute modification des objets conservés.
Sécurité	Contrôle des accès, protection des locaux et de leur contenu (contre l'incendie, les dégâts des eaux, les nuisibles, etc.).	Contrôle des accès physiques, protection des locaux (contre l'incendie, les dégâts des eaux, etc.), gestion des droits d'accès informatiques, administration du système, réplications, sauvegardes des systèmes, etc.
Traçabilité	Journal des évènements.	Journal des évènements.
Authenticité	Signature et date.	Signature électronique, horodatage, calcul et gestion d'empreintes, etc.
Lisibilité / Intelligibilité	Implicite. Attention, certains documents peuvent s'estomper avec le temps (carbone, papiers chimiques, etc.).	Dispositifs matériels (lecteurs), formats de stockage, métadonnées spécifiques.
Disponibilité	Organisation des moyens et des ressources.	Organisation des ressources, plan de continuité, solutions de *back-up*, Plan de Reprise d'Activité.

Pour mettre en œuvre un SAE, un choix double s'offre à l'entreprise :

- Soit elle décide de s'équiper en interne d'un Système d'Archivage Électronique ;
- Soit elle décide de confier son archivage électronique à un tiers, comme cela est souvent le cas pour l'archivage papier. Ces tiers s'appellent des Tiers Archiveurs.

Afin de sécuriser son choix, l'entreprise pourra retenir une solution ou un service bénéficiant d'un label attribué par la Fédération Nationale des Tiers de Confiance (FNTC) (*Cf. 12 - Les Labels FNTC*).

Labels FNTC spécifiques à l'archivage électronique

Avec l'essor de la dématérialisation et la substitution de pièces numériques aux originaux papiers, l'archivage électronique est devenu une composante essentielle de la politique de maîtrise des risques des organisations.
Qu'il s'agisse de disposer de preuves numériques pouvant s'avérer indispensables dans les cas de contentieux, de contrôles ou de veiller à la préservation et à la disponibilité du patrimoine informationnel, l'enjeu est important.

C'est pourquoi la FNTC a fait de l'archivage électronique une des priorités de son programme de labellisation destiné à sécuriser le marché et à promouvoir la confiance. La FNTC a ainsi élaboré deux labels spécifiques à l'archivage électronique, qu'il s'appuie en interne sur un progiciel de type Coffre-fort Électronique (CFE) ou qu'il soit confié à un Tiers Archiveur (TA).

Le label FNTC-TA est un label « service » dédié au tiers archivage

Le schéma d'évaluation a été élaboré à partir du « CoBIT » (Control OBjectives for Information and related Technology), une méthode internationale d'audit des systèmes d'information mise au point par l'ISACA (Information Systems Audit and Control Association) aux États-Unis et dont l'AFAI (Association Française de l'Audit et du Conseil Informatiques) est le promoteur en France.

Ce schéma, le CoBIT-TA, qui prend en compte les points essentiels d'analyse des systèmes d'information, a été complété par les spécifications techniques de la norme NF Z42-013, les spécifications relatives à la réversibilité des archives électroniques ainsi que les aspects juridiques et contractuels élaborés par la FNTC, définissant notamment la responsabilité du Tiers Archiveur envers son client.

Le label FNTC-CFE est un label « solution » dédié aux progiciels de type Coffre-fort Électronique

Il garantit le respect des exigences du référentiel élaboré par la FNTC, dans le respect de la norme NF Z42-013, en termes de fonctionnalités et de supports de la part de l'éditeur.

Le besoin de conservation des objets numériques, à plus ou moins long terme, est lié à diverses considérations d'ordre réglementaire, juridique, patrimonial, historique, etc.

La conservation de ces objets doit prendre en compte les exigences d'authenticité, d'intégrité et de traçabilité. Le Coffre-fort Électronique ou numérique a pour but d'y répondre afin d'assurer la conservation des objets numériques et leur valeur probatoire.

Le référentiel FNTC-CFE définit les fonctions minimales garantissant la conservation sécurisée, l'intégrité et l'interopérabilité entre des coffres-forts électroniques d'éditeurs différents.

7 - LES PRINCIPALES DURÉES DE CONSERVATION

Les durées légales de conservation sont déterminées par les lois et règlements concernés. Les durées réelles de conservation peuvent être supérieures à ces durées, notamment pour tenir compte de besoins spécifiques (patrimoniaux notamment et règles relatives aux durées de prescription).

Pour un même document, l'application des textes peut fournir des durées différentes. En pratique, on choisira la durée la plus importante[3].

Type de documents	Délai de conservation	Délai de prescription
Contrats	Délai particulier : 10 ans pour les contrats conclus avec les consommateurs d'un montant supérieur à 120 euros et en ligne (art. L. 134-2 du Code de la consommation).	5 ans (pour les contrats établis après le 18 juin 2008) sauf si les obligations sont soumises à des exigences particulières (art. L. 110-4 du Code de commerce) (ex : délai de prescription fondée sur un contrat d'assurance : 2 ans à compter de la survenance de l'événement – art. L. 114-1 du Code des assurances).
Factures	Délai commercial : 10 ans (art. L. 123-22 Code de commerce). Délai fiscal : 6 ans (art. L. 102-B LPF).	5 ans (pour les factures émises après le 18 juin 2008) – 10 ans (avant le 18 juin 2008 et dans un cadre commercial). Début du délai : date de la dernière opération mentionnée sur les livres ou registres ou date à laquelle les factures ou pièces ont été établies.
Livres et registres comptables Bons de commande	Délai commercial : 10 ans (art. L. 123-22 Code de commerce). Délai fiscal : 6 ans (art. L. 102-B LPF) dont les trois premières années sous forme électronique.	5 ans (pour les documents comptables émis après le 18 juin 2008) – 10 ans (avant le 18 juin 2008 et dans un cadre commercial). Début du délai : date de la dernière opération mentionnée sur les livres ou registres ou date à laquelle les documents ou pièces ont été établis.
Justificatifs comptables (ex. : notes de frais)	Délai commercial : 10 ans (art. L. 123-22 Code de commerce). Délai fiscal : 6 ans (art. L. 102-B LPF) dont les trois premières années sous forme électronique.	5 ans (pour les documents comptables émis après le 18 juin 2008) – 10 ans (avant le 18 juin 2008 et dans un cadre commercial). Début du délai : date de la dernière opération mentionnée sur les livres ou registres ou date à laquelle les documents ou pièces ont été établis.
Correspondances commerciales liées à une opération comptable	Délai commercial : 10 ans (art. L. 123-22 du Code de commerce).	5 ans (pour les correspondances émises après le 18 juin 2008) – 10 ans (avant le 18 juin 2008 et dans un cadre commercial).

3/.Extrait du Guide FNTC « Vade-mecum Juridique de la Dématérialisation des Documents » en date du 31 mars 2010.

Type de documents	Délai de conservation	Délai de prescription
Relevés de comptes		5 ans (pour les documents établis après le 18 juin 2008) sauf si les obligations sont soumises à des exigences particulières (art. L. 110-4 du Code de commerce) (ex. : Cf. convention de comptes bancaires).
Comptes annuels	Délai commercial : 10 ans (art. L. 123-22 Code de commerce). Délai fiscal : 6 ans (art. L. 102-B LPF) dont les 3 premières années sous forme électronique.	5 ans (pour les documents comptables émis après le 18 juin 2008) – 10 ans (avant le 18 juin 2008 et dans un cadre commercial). Début du délai : date de la dernière opération mentionnée sur les livres ou registres ou date à laquelle les documents ou pièces ont été établis.
Statuts, annexes, pièces modificatives		5 ans à compter de la radiation du RCS (pour les statuts établis après le 18 juin 2008).
Bulletins de paie	Pour l'employeur : 5 ans (art. L. 3243-4 du Code du travail). 10 ans en tant que pièce comptable (art. L. 123-22 Code de commerce). 6 ans en tant que pièce fiscale (art. L. 102-B LPF) dont les 3 premières années sous forme électronique. Pour le salarié : durée illimitée (art. R. 3243-5 du Code du travail).	
Contrats de travail		5 ans à compter de la fin du contrat (pour les documents émis après le 18 juin 2008) – 10 ans (avant le 18 juin 2008 et dans un cadre commercial).
Déclarations URSSAF	3 ans suivant l'année de l'envoi litigieux. 5 ans en cas de travail illégal. 2 ans concernant le paiement des majorations de retard. (art. L. 244-3 du Code de la sécurité sociale).	

8 - FOIRE AUX QUESTIONS

Ce chapitre présente les diverses questions qui reviennent le plus souvent et les réponses que l'on peut leur apporter.

Qu'est-ce que l'archivage électronique ?
La norme NF Z42-013 définit l'archivage électronique comme suit :

> *Ensemble des actions visant à identifier, recueillir, classer, conserver, communiquer et restituer des documents électroniques, pour la durée nécessaire à la satisfaction des obligations légales ou pour des besoins d'informations ou à des fins patrimoniales.*

L'archivage électronique consiste donc, notamment, en la conservation de documents d'origine électronique de façon durable et sécurisée au moyen d'un Système d'Archivage Électronique (SAE).

Qu'est-ce qu'un coffre-fort électronique ?
Un coffre-fort électronique, également dénommé coffre-fort numérique ou coffre-fort virtuel, est un dispositif informatique, matériel et/ou logiciel, permettant de réaliser la conservation sécurisée des documents ou données versés, de façon à garantir leur intégrité et leur pérennité. Ce composant essentiel du SAE, à vocation probatoire, trace toutes les opérations effectuées afin de pouvoir démontrer ce qu'il a réalisé.

Je possède déjà une solution de Gestion Électronique de Documents (GED) ou d'archivage en interne. Est-ce suffisant ?
Une solution d'archivage interne, comme une solution de GED, n'est pas obligatoirement un Système d'Archivage Électronique. Il est nécessaire d'assurer, en plus du stockage du document, le stockage d'attributs et de métadonnées garantissant son origine, son authenticité et son intégrité, ainsi que tous les éléments de traçabilité des opérations faites depuis la réception/création jusqu'au sort final (destruction) comme le requiert la norme NF Z42-013.

De plus, ces solutions liées au système d'information contenant des données d'identification ne garantissent pas la permanence du lien. Une archive électronique doit, pour être valide, remplir plusieurs conditions, en particulier être indépendante du système qui l'a créé, ce qui n'est souvent pas le cas avec les solutions de GED intégrées dans les activités opérationnelles des entreprises.

Pour résumer, une GED ou un Workflow a pour objectif de faire « vivre » un document, tandis qu'en complément, un Système d'Archivage Électronique met en œuvre plusieurs dispositifs pour le conserver sous une forme non modifiable.

Quelles sont les principales différences entre une solution de GED et un SAE ?
Le tableau suivant présente les différences existant entre une solution de GED et un SAE :

GED	SAE
Permet la modification des documents et l'existence de plusieurs versions (documents « vivants »).	Empêche le document d'être modifié (documents « figés » ou « morts »).
Peut permettre la suppression des documents par leur propriétaire.	Empêche le document d'être supprimé sauf dans des circonstances strictement contrôlées.
Peut inclure quelques règles de rétention.	Doit comprendre des règles de rétention strictes.
Permet la mise en place d'une structure de répertoires qui peut être sous le contrôle de l'utilisateur.	Doit comprendre une structure rigoureuse de classement maintenue par un administrateur.
Supporte une utilisation quotidienne des documents dans le cadre de l'activité de l'entreprise.	Peut supporter une utilisation quotidienne, mais l'objectif principal est le maintien d'un référentiel sécurisé et contrôlé pour des documents à valeur probatoire.
Permet d'accéder au document à l'identique sans objectif de préservation au-delà de la durée de vie du logiciel de GED dans l'entreprise. La pérennisation est de la responsabilité de l'utilisateur (formats obsolètes).	Doit permettre d'accéder et de restituer un document authentique, intègre et lisible. La pérennisation est de la responsabilité du SAE (sélection des formats pérennes, capacité du SAE à adapter les formats le cas échéant). La réversibilité doit être assurée pour permettre un changement de SAE.
Permet de fournir un historique des opérations sur les documents.	Doit apporter la preuve de la conservation de l'intégrité des documents au moyen de traces sécurisées (non modifiables) de l'historique des opérations.

Mon ERP/logiciel de comptabilité a une fonction d'archivage électronique. Ai-je besoin d'autre chose ?
OUI. En plus de la réponse précédente, on ajoutera qu'en général de telles solutions sont « propriétaires », avec notamment des formats ou des modes d'accès que seul l'éditeur de l'ERP maîtrise. C'est donc en contradiction avec les principes énoncés dans ce guide sur au moins trois aspects :

- L'indépendance par rapport au système créateur ;
- L'absence de métadonnées ;
- L'absence de garanties sur l'intégrité.

De plus, des éditeurs d'ERP proposent des solutions qui permettent de recréer les documents à la demande à partir de la base de données. Pour répondre aux besoins d'archivage, cette procédure doit être prohibée, car très risquée, dans la mesure où il n'y a aucune garantie de fidélité sur l'ensemble des informations requises, par exemple évolution d'un fond de page contenant le capital social (*Cf. 5.1 - La preuve électronique et les litiges faisant intervenir un document électronique*).

Est-ce qu'utiliser la fonction « Archiver » d'Outlook est de l'archivage électronique ?
NON. Pour les mêmes raisons que celles de l'ERP à la question précédente.

Pourquoi utiliser les services d'un Tiers Archiveur labellisé FNTC-TA ?
La mise en œuvre et l'exploitation d'un système d'archivage en interne dans les entreprises ou organisations peut représenter un investissement important, difficile à justifier (architecture sécurisée, procédures spécifiques, audits).

Si les documents à archiver présentent un caractère de valeur probante, le SAE doit garantir la conservation de cette valeur dans le temps.
Le recours à un Tiers Archiveur permet de bénéficier de services répondant aux besoins avec des coûts maîtrisés et proportionnels aux volumes ou aux fonctionnalités recherchées, sans investissements lourds de mise en œuvre.

De par la détention du Label FNTC-TA, ce Tiers Archiveur apporte toutes les garanties de fiabilité, de sécurité, de pérennité et de conseil au client qui fait appel à lui. Le client peut avoir toute « CONFIANCE » dans les services qui lui sont proposés, sans avoir à recourir à des audits complémentaires.

L'évolution du contexte légal renforce cette approche, par exemple, dernièrement, la possibilité pour les services d'archives publiques, administrations et collectivités, d'externaliser leur archivage chez un tiers (décret n° 2009-1124 du 17 septembre 2009).

Comment faire évaluer mon propre système d'archivage ?
Deux cas sont possibles :

- Vous possédez une solution labellisée FNTC-CFE ou vous faites appel aux services d'un Tiers Archiveur labellisé FNTC-TA : dans ce cas, seules vos procédures (sélection, identification, préparation, conditionnement et versement ou échange avec le Tiers Archiveur) doivent être évaluées ;
- Vous ne possédez aucun label et vous ne faites pas appel aux services d'un Tiers Archiveur labellisé : vous devez faire analyser vos processus et vos solutions par une expertise sur l'ensemble du dispositif d'archivage : juridique (*Legal opinion*), onctionnel, organisationnel et technique.

Remarque :
Les solutions globales propriétaires émanant de constructeurs de systèmes de stockage présentent l'inconvénient de l'opacité de ces systèmes et de leur éventuelle absence de conformité à des lois ou normes françaises.

Je grave des CD et DVD. Quelles précautions dois-je prendre ?
Le CD est un support d'archivage éprouvé qui donne un bon résultat, à condition de réaliser une gravure de qualité et de prendre des précautions pour sa conservation. Le référentiel FNTC-TA précise ces recommandations.

Dans tous les cas, il est indispensable de conserver au minimum deux exemplaires en deux lieux distincts.

Un professionnel de l'archivage, notamment ceux labellisés FNTC-TA, prend le maximum de précautions : il sélectionne une marque de CD à vocation d'archivage, dispose d'un analyseur pour vérifier régulièrement la qualité de sa production, grave toujours en deux exemplaires minimum issus de lots de fabrication distincts.

La valeur probante de mes archives est-elle mieux garantie chez moi que chez un tiers ?
Il faut considérer l'archivage électronique comme un processus qui combine plusieurs techniques (traçabilité, signature électronique, horodatage, etc.). Vous pouvez, bien évidemment, traiter votre

archivage chez vous avec une solution labellisée FNTC-CFE ou en passant par un Tiers Archiveur labellisé FNTC-TA.

De surcroît, un Tiers Archiveur effectue une veille réglementaire constante et fait évoluer ses solutions au rythme des évolutions légales, fiscales ou sociales.

Quels sont les avantages que l'on peut attendre d'un archivage électronique ?
Un Système d'Archivage Électronique permet de diminuer de façon importante les espaces de stockage nécessaires à la conservation des documents papier.

L'accès à l'information est accéléré grâce aux outils de recherche et de consultation.

Dans une logique de prévention du risque, il est beaucoup plus facile et moins onéreux de dupliquer et de conserver en plusieurs endroits des documents numériques.

Puis-je me passer d'un SAE ? En quoi un SAE est-il nécessaire ?
Aujourd'hui, du fait de l'origine électronique de la plupart des documents, ceux-ci, pour des raisons légales, fiscales ou autres, doivent être conservés dans leur format d'origine au même titre que les documents papiers. Une entreprise ne peut plus se passer d'un SAE.

Comment se passe un versement dans un Système d'Archivage Électronique ?
Chaque document versé dans un Système d'Archivage Électronique (SAE) doit répondre aux deux critères suivants :

- Après conversion éventuelle, le document doit être versé dans un format pérenne prévu pour l'archivage à long terme, c'est-à-dire dans un format normalisé ou standardisé dont les spécifications sont librement accessibles pendant toute la durée de conservation (NF Z42-013) ;
- Le document doit être accompagné d'informations permettant au SAE de vérifier l'intégrité du document depuis sa création ou sa réception jusqu'a son dépôt et après son dépôt (utilisation d'empreintes, voire de signatures).

Lors d'un dépôt massifié, les documents sont d'abord regroupés au sein d'un même ensemble avant d'être envoyés au SAE. Cet ensemble doit disposer d'une fiche descriptive fournissant les informations sur chaque document à archiver, à savoir :

- Nom du document ;
- Information permettant au SAE de vérifier l'intégrité du document (empreinte ou signature) ;
- Informations complémentaires appelées métadonnées.

À réception, le SAE parcourt la fiche descriptive et vérifie que chaque document décrit est bien présent et intègre. Le SAE alloue un identifiant unique à chaque archive avant de l'enregistrer définitivement avec ses métadonnées éventuellement fournies. Ces dernières, si elles existent, permettent au propriétaire des archives d'effectuer plus facilement des recherches via un système de consultation en ligne.

À qui s'adresse l'archivage électronique ?

Tout professionnel gérant son activité avec des moyens informatiques est aujourd'hui doublement concerné :

- Tout d'abord à titre fiscal : le cadre fiscal du contrôle des comptabilités informatisées et les modalités de conservation du double électronique de la facture émise font l'objet de deux instructions fiscales spécifiques (*Cf. 5.2 - La tenue de la comptabilité et la conservation des informations comptables* et *5.4 - La conservation des copies de factures clients*) ; tous les contribuables ne sont pas encore en conformité, mais l'administration fiscale considère de son côté que la période de « pédagogie » est terminée ;
- Ensuite, le professionnel doit envisager le problème de l'archivage pour les documents créés par des moyens informatiques et qui pourraient avoir une valeur de preuve à l'occasion d'un litige. Cela ne signifie pas qu'il doit tout archiver, mais que la question du risque et des enjeux doit être posée pour les documents concernés. (*Cf. 5.1 - La preuve électronique et les litiges faisant intervenir un document électronique*).

L'archivage électronique est-il obligatoire ?

OUI. En particulier pour tous les documents originaux électroniques sur lesquels portent des exigences. À l'heure de la dématérialisation des données, de nombreuses activités ou actions dans les entreprises et les échanges qu'elles ont avec leurs partenaires (clients, fournisseurs, banques, Administration, etc.) se font selon des modalités de dématérialisation complète des documents dont certains doivent être conservés à titre de justification ou de preuve. On peut citer :

- Les travaux d'inventaire de fin d'exercice pour fixer certaines provisions qui sont réalisés à partir d'export de fichiers vers des outils autonomes, tels que des feuilles de calcul. La conservation de la feuille de calcul (avec ses règles et paramètres) est une obligation au sens du contrôle fiscal des comptabilités informatisées ;
- Les entreprises qui échangent avec leurs donneurs d'ordre des messages structurés (commandes par exemple) doivent conserver les messages dans leur forme d'origine surtout en fin d'exercice (évaluation des engagements) ; c'est une obligation comptable et une obligation fiscale ;
- On peut citer également les différentes déclarations sociales ou fiscales dématérialisées.

Au vu de ces différents éléments, et afin d'éviter tout risque avec un tiers (risques légaux et fiscaux), l'archivage électronique apparaît aujourd'hui comme un élément essentiel de la politique des risques de l'entreprise : une entreprise qui ne prendrait pas de dispositions en matière d'archivage électronique ferait un choix qui pourrait être comparé à la décision de ne pas souscrire de police d'assurance.

Quelles sont les précautions à prendre ?

Elles sont de deux sortes :

- Au niveau des bonnes pratiques par l'utilisation, pour les documents d'archives, de formats pérennes (formats standardisés ou normalisés comme XML, PDF/a, TIFF ; Cf. NF Z42-013) et par la mise en place de procédures et de moyens de traçabilité assurant le respect des principes de l'archivistique ;
- Au niveau des scénarii de mise en œuvre par l'utilisation d'un Coffre-fort Électronique ou en faisant appel à un Tiers Archiveur labellisé.

Suis-je couvert par mon assurance ?
Les assurances, pour les risques liés aux pertes de données, ne sont pas nombreuses et souvent inadaptées. On peut penser à :

- L'assurance responsabilité civile professionnelle couvrant les dommages que peut subir le client dans le cadre de l'exécution d'un contrat de prestations de services à la suite d'une faute commise par une personne. À ce titre, les fautes liées à des pertes de données par le Tiers Archiveur seraient prises en compte ;
- L'assurance de responsabilité du Syntec informatique permettant de garantir les conséquences financières supportées par un client de l'assuré à la suite de dommages dont il serait responsable. Elle est plus adaptée, là encore, aux Tiers Archiveurs.

Quid de mes documents scannés ?
Dans certains cas, la décision de destruction doit s'apprécier en fonction de l'utilisation de ces documents et du risque éventuel en cas de désaccord sur leur contenu.

Puis-je archiver tous types de fichiers (PDF ; Word ; Vidéos, …) ?
OUI. Toutefois, une attention particulière doit être portée sur les formats de fichiers utilisés pour la conservation à long terme. La FNTC a publié, au travers de son Référentiel FNTC-TA, la liste des formats retenus.

9 - CONCLUSION : ARCHIVAGE ET DÉMATÉRIALISATION

Qu'il soit physique (papier) ou électronique, l'archivage est vécu comme une contrainte alors qu'il est une source de sécurité juridique, fiscale et donc financière pour l'entreprise. Il doit donc être mis en place dans le cadre de la politique de maîtrise des risques de l'entreprise, au même titre que les assurances ou les protections d'intrusion ou d'incendie.

L'archivage est une brique essentielle de la dématérialisation. En définissant une Politique d'Archivage, l'entreprise construit les règles fondamentales qui lui permettront de réussir une dématérialisation de ses documents et de ses processus. La dématérialisation et l'archivage sont source d'efficacité, de sécurité, de satisfaction client et d'économies.

10 - ANNEXE 1 : RÉFÉRENCES DES DOCUMENTS

ISO :

- **ISO 15489-1 : 2001 :** Information et documentation - « *Records management* » - Partie 1 : Principes directeurs ;
- **ISO/TR 15489-2 : 2001 :** Information et documentation - « *Records Management* » - Partie 2 : Guide pratique ;
- **ISO 14721 : 2003 :** Systèmes de transfert des informations et données spatiales - Système ouvert d'archivage d'information - Modèle de référence (OAIS : *Open Archival Information System*).

AFNOR :

- **NF Z42-013 mars 2009** : Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes.

FNTC :

- Référentiel Technique Label Tiers Archiveur Version 2.0 ;
- Référentiel définissant un Coffre-fort Électronique pour l'archivage à vocation probatoire d'objets numériques Version 2009 ;
- Guide de la Signature électronique - Collection « Les Guides de la Confiance » ;
- Vade-mecum Juridique de la Dématérialisation des Documents - 3ème édition - Collection « Les Guides de la Confiance » ;
- « MoReq2 et archivage sécurisé » de la collection « Les Formations de la FNTC ».

Autres :

- **MoReq2 :** Exigences types pour la maîtrise de l'Archivage Électronique - Mise à jour et extension 2008 - Direction des Archives de France ;
- **Bulletin Officiel des Impôts** - DGI - Numéro spécial 3 C.A. N° 136 du 7 août 2003 - Taxe sur la Valeur ajoutée. Obligations des Assujettis. Obligations relatives à l'établissement des factures ;
- **Délibération CNIL n°2005-213 du 11 octobre 2005** portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel ;
- **Bulletin Officiel des Impôts - DGI 13L-1-06 N°12 du 24 janvier 2006** - Contrôle des Comptabilités Informatisées ;
- **Bulletin Officiel des Impôts - DGI 3E-1-07 N°4 du 11 janvier 2007** - Taxe sur la Valeur Ajoutée : Obligations relatives à la conservation des factures. Mesures d'assouplissement ;
- **Loi n° 2009-526 du 12 mai 2009** de simplification et de clarification du droit et d'allègement des procédures (article 26 concernant les bulletins de paie) ;
- **Décret n°2009-1124** relatif à la compétence et aux coopérations entre services d'archives (J.O. du 18 septembre 2009) ;
- **Arrêté du 4 décembre 2009** précisant les normes relatives aux prestations en archivage et gestions externalisées (J.O. du 12 décembre 2009, p. 21505).

11 - ANNEXE 2 : EMPREINTE, SIGNATURE ET HORODATAGE EXPLIQUÉS

Ce paragraphe explique ce que sont une empreinte, une signature, un horodatage, comment ces objets sont calculés et ce qu'ils apportent en terme de garantie.

Le lecteur pourra toujours se reporter aux guides FNTC suivants :

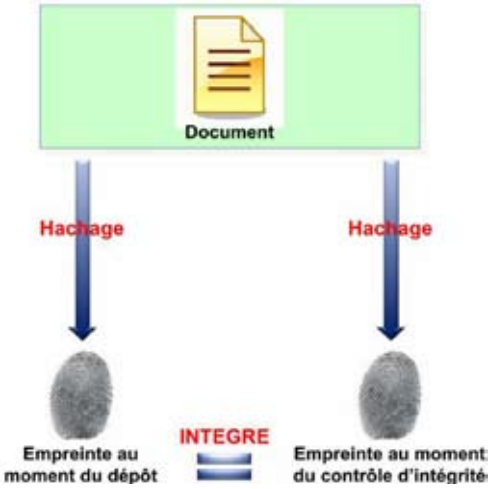
- Guide de la signature électronique ;
- Guide de l'horodatage.

11.1 Qu'est-ce qu'une empreinte ?

Une empreinte électronique est le résultat du calcul informatique effectué par une *fonction de hachage* (fonction surjective) sur un fichier informatique. Ce résultat (l'empreinte) est une chaîne de caractères représentant de façon unique le fichier informatique.

Les fonctions de hachage sont des fonctions mathématiques dont les intérêts sont multiples :

- À un fichier informatique correspond une seule et unique empreinte (fonction surjective) ;
- Le fait que deux fichiers informatiques aient la même empreinte s'appelle *une collision*. Les algorithmes actuellement utilisés ont des risques de collision infinitésimaux (10^{-48}) Les nouveaux algorithmes (SHA256, SHA512) ont des taux de collision encore plus faibles ;
- La fonction de hachage fournit toujours une empreinte de même longueur quelle que soit la taille du fichier informatique *haché* ;
- La moindre modification sur le fichier informatique se reflète par une empreinte différente ;
- Il n'est pas possible de déduire le fichier informatique d'origine à partir de son empreinte (le processus de calcul d'empreinte est irréversible, c'est-à-dire à sens unique).

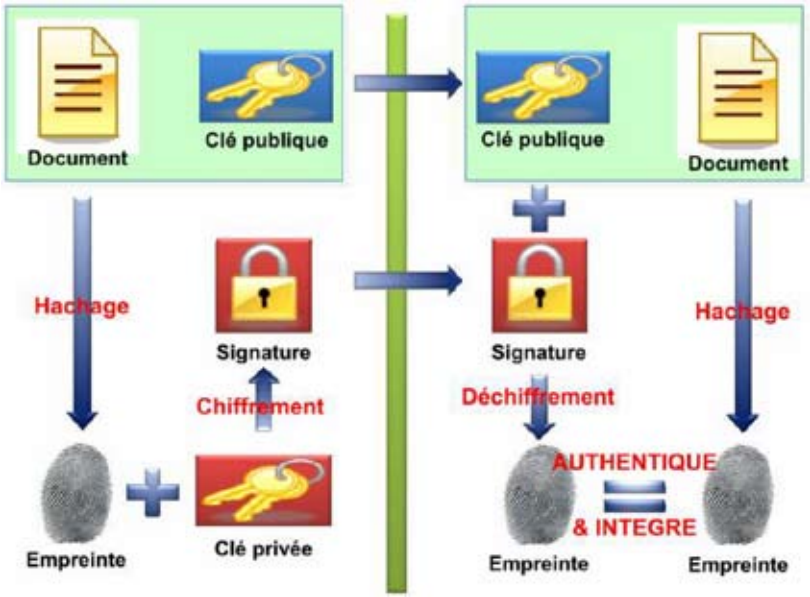


11.2 Qu'est-ce qu'une signature ?

La signature électronique est le résultat du calcul informatique effectué par une f*onction de chiffrement* à laquelle sont passés les deux éléments suivants :

- L'empreinte du fichier informatique à signer (calculée au préalable par une *fonction de hachage*) ;
- Une *clé* permettant d'initialiser la fonction de chiffrement (ainsi, la même empreinte sera chiffrée différemment avec une *clé* différente).

Les fonctions de chiffrement utilisées dans le cadre de signatures électroniques sont des fonctions mathématiques possédant la particularité d'être *asymétriques*, c'est-à-dire qu'elles servent à la fois au chiffrement et au déchiffrement.



Leur principe de fonctionnement est simple et peut se résumer dans le tableau suivant :

	La fonction de chiffrement nécessite	Le résultat est
Chiffrement	L'empreinte en clair du fichier ; Une clé *CLE1* de chiffrement.	L'empreinte chiffrée.
Déchiffrement	L'empreinte chiffrée. Une clé *CLE2* de déchiffrement.	L'empreinte en clair (déchiffrée).

Les deux clés *CLE1* et *CLE2* jouent des rôles très spécifiques et ne sont pas choisies au hasard. Ces deux clés sont dites *asymétriques* (d'où le nom de la fonction de chiffrement) : **ce que l'on chiffre avec l'une, on le déchiffre avec l'autre et réciproquement.**

Il est clair que la clé servant au chiffrement doit être protégée afin d'empêcher quiconque (une personne malveillante) de recalculer l'empreinte chiffrée. Par convention, on appelle *clé privée* la clé servant au chiffrement et *clé publique* la clé servant au déchiffrement.

Dans le tableau ci-dessus, la clé *CLE1*, servant au chiffrement, est la *clé privée* et la clé *CLE2* est la *clé publique*.

Ces deux clés sont fournies par un organisme appelé Autorité de Certification (*Certificate Authority* ou *CA* en anglais) au travers d'un certificat (*Cf. 11.3 - Qu'est-ce qu'un certificat ?*) qui peut avoir deux formes :

- **La forme privée** : seul le propriétaire du certificat possède cette forme, car il contient les deux clés ;
- **La forme publique** : tout le monde peut obtenir une copie de cette forme de certificat (délivrée par l'Autorité de Certification ou par son propriétaire) car il ne contient que la clé publique.

Au final, une signature électronique est composée des éléments suivants :

- L'empreinte chiffrée ;
- La forme publique du certificat (ceci, afin de permettre la vérification de la signature).

11.3 Qu'est-ce qu'un certificat ?

Un certificat est un simple fichier informatique contenant, entre autres choses, les informations suivantes :

- Le nom du propriétaire du certificat ;
- Le nom de l'Autorité émettrice du certificat ;
- Le numéro de série du certificat ;
- Les dates de début et de fin de validité du certificat ;
- L'objet de l'utilisation du certificat ;
- La clé publique du certificat ;
- La signature, par l'Autorité de Certification, du certificat délivré par cette même Autorité.

Si le certificat est dans sa forme privée alors il contient en plus la clé privée.

Comme indiqué, un certificat est un fichier signé par l'Autorité de Certification émettrice. Il est donc possible, en vérifiant la signature du certificat, de contrôler :

- S'il n'a pas été modifié (vérification de signature) ;
- La validité du certificat de l'Autorité de Certification (contenu dans sa propre signature).

Il s'agit d'un système pyramidal. Le certificat final d'un utilisateur émis par une Autorité de Certification est signé par cette Autorité. L'Autorité de Certification possède donc son propre certificat, lui-même signé et émis par une autorité supérieure.

L'Autorité la plus haute est appelée Autorité Racine (*Root Authority*). C'est l'Autorité qui fabrique le tout premier certificat (certificat racine) de cette chaîne de vérification ; elle génère et signe son propre certificat (on dit que ce certificat est auto-signé).

11.4 Différences entre empreinte et signature

Les fonctions de hachage et les fonctions de chiffrement sont connues du monde informatique et font partie du domaine public. Autant, il est possible de recalculer très facilement l'empreinte d'un document (il suffit seulement de connaître la fonction de hachage utilisée), autant il n'est pas possible de recalculer la signature d'un document si l'on ne possède pas la clé privée (ayant servi à initialiser la fonction de chiffrement).

Ainsi, si un document est émis uniquement avec une empreinte, il ne sera pas possible de détecter les modifications effectuées par une personne malveillante sur ce document, si celle-ci en recalcule l'empreinte. *A contrario*, si le document est émis avec une signature, la modification du document par une personne malveillante pourra être immédiatement détectée car il lui sera impossible de recalculer la signature (à moins de posséder le certificat dans sa forme privée).

Lorsque la forme privée d'un certificat a été subtilisée, le propriétaire se doit d'avertir au plus vite l'Autorité de Certification (révocation du certificat) afin que tout contrôle futur de celui-ci retourne une erreur.

11.5 Comment est vérifiée une signature ?

Comme vu au paragraphe *11.2 - Qu'est-ce qu'une signature ?*, la fonction de chiffrement est dite asymétrique car utilisant des clés (asymétriques) ayant la particularité de « défaire » ce que l'autre « fait » (ce que l'on chiffre avec l'une, on le déchiffre avec l'autre et réciproquement).

Une signature est un ensemble composé, entre autre, des éléments suivants :

- L'empreinte chiffrée (par la fonction de chiffrement) ;
- Le certificat public (ne contenant que la clé publique).

Pour vérifier que la signature d'un document est valide, il suffit :

- De déchiffrer l'empreinte chiffrée (grâce à la clé publique contenue dans le certificat) ;
- De calculer l'empreinte du document (avec la même fonction de hachage que celle utilisée par l'émetteur de la signature) ;
- De comparer l'empreinte calculée avec celle déchiffrée : si elles sont égales alors la signature est valide.

Il est conseillé, mais pas obligatoire, de vérifier la validité d'un certificat en interrogeant l'Autorité de Certification l'ayant délivré. Cette vérification est à effectuer lors de la réception du document (avec sa signature) et doit être conservée afin de prouver qu'elle a bien eu lieu. Cette vérification devient inutile pendant la conservation du document.

La durée de vie d'un certificat étant très courte (1 à 3 ans) comparée à la durée de conservation d'un document, la validité du certificat aura sans doute expirée avant la fin de conservation du document alors même que sa signature restera encore valide.

11.6 Qu'est-ce qu'un horodatage ?

Un horodatage est une signature électronique à laquelle est ajouté un *jeton d'horodatage*. Ce jeton est formé, entre autre chose, des informations suivantes :

- Date et heure de la demande d'horodatage ;
- Numéro de série de la demande d'horodatage.

Comme une signature, un horodatage s'appuie sur le chiffrement d'une empreinte (*Cf. 11.2 - Qu'est-ce qu'une signature ?*). Le système ou l'organisme délivrant un horodatage reçoit une empreinte (voire une signature dont il extrait l'empreinte) qu'il chiffre puis fabrique une signature électronique dans laquelle il adjoint des informations d'horodatage, c'est-à-dire la date et heure courante à laquelle cette signature est effectuée.

La difficulté d'un système d'horodatage n'est pas dans la délivrance d'une telle signature mais dans l'exactitude de la date et heure fournie. En effet, l'importance d'un horodatage est de permettre à l'entreprise qui le demande de garantir l'existence d'un document à partir d'un instant donné.

La précision de cet horodatage et son exactitude peuvent être cruciaux dans certaines activités, comme par exemple, la télé-déclaration des impôts.

Une entreprise peut disposer de son propre système d'horodatage dans la mesure où il respecte les exigences évoquées ci-dessus ou faire appel à un tiers appelé Tiers Horodateur.

Un Tiers Horodateur doit conserver pendant une durée de 10 ans les jetons qu'il a générés.

11.7 Qu'apporte une empreinte ? Une signature ? Un horodatage ?

a) Qu'apporte une empreinte ?

Une empreinte permet de vérifier l'intégrité du document auquel elle est associée, à la condition que celle-ci soit conservée sur un autre site de stockage, ou dans une base de données, ou encore rendue inviolable par son enregistrement sur un support WORM ou verrouillée au travers d'une signature électronique.

Lorsque de telles protections sont mises en place, le contrôle d'empreinte (recalcul de l'empreinte et comparaison avec celle stockée) est extrêmement rapide comparé au contrôle d'une signature.

b) Qu'apporte une signature ?

Une signature étant calculée à partir d'un certificat délivré par une Autorité de Certification et ce certificat contenant des informations relatives à la personne (morale ou physique), une signature électronique permet :

- De vérifier l'intégrité du document ;
- D'authentifier l'émetteur du document (non répudiation).

c) Qu'apporte un horodatage ?

Un horodatage permet, avant tout, d'apporter la preuve de l'existence d'un document (ou d'un acte ou d'un traitement) à partir d'une date et heure.

12 - LES LABELS FNTC

La Fédération Nationale des Tiers de Confiance (FNTC) a mis en place un programme de labellisation qui concernera à terme l'ensemble des services de confiance. Le premier à voir le jour a été, en 2004, le label FNTC-TA dédié aux services de tiers archivage.

12.1 Le label FNTC-TA « Tiers Archiveur »

Le label « Tiers Archiveur », issu des travaux de la FNTC, qualifie les entreprises qui offrent des services de tiers archivage. Il valide les aspects techniques et organisationnels des entreprises auditées.

Le processus d'attribution de ce label a été élaboré à partir d'une version simplifiée du CobiT. Ce schéma, le COBIT-TA, qui prend en compte les points essentiels d'analyse des systèmes d'information, a été complété par les spécifications techniques de la norme NF Z42-013 de 2009, des spécifications relatives à la réversibilité des archives électroniques ainsi que des aspects juridiques et contractuels élaborés par la FNTC définissant notamment la responsabilité du Tiers Archiveur envers son client.

12.2 Le label FNTC-CFE « Coffre-fort Électronique »

Le label « Coffre-fort Électronique », issu des travaux de la FNTC, qualifie les logiciels d'Archivage. Il valide les aspects techniques de la plate-forme logicielle auditée.

Le processus d'attribution de ce label a été élaboré à partir des spécifications techniques de la norme NF Z42-013 complétées par les recommandations de la FNTC.

12.3 Le label FNTC-PFFE « Plate-Forme de Facturation Électronique »

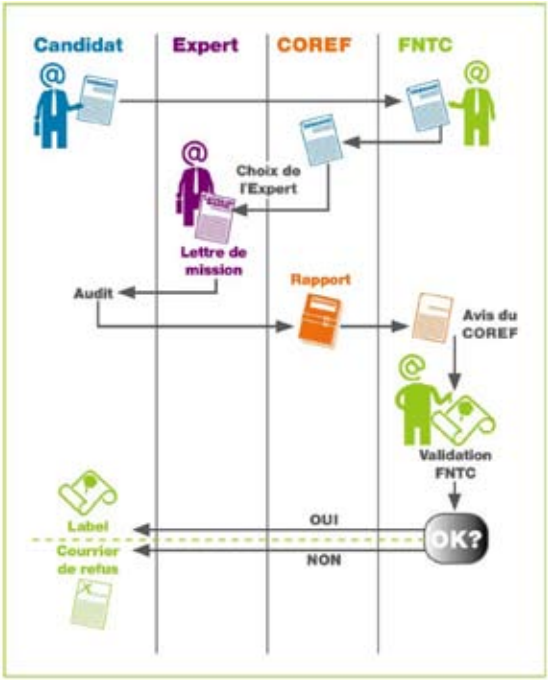
Le label « Plate-Forme de Facturation Électronique », issu des travaux de la FNTC, qualifie les entreprises qui offrent des services de dématérialisation de factures signées, conformes au paragraphe 289-V du code général des impôts. Il valide les aspects juridiques et techniques de la plate-forme auditée.

Le processus d'attribution de ce label a été élaboré à partir d'un référentiel émis par la FNTC.

12.4 Les différentes étapes de la procédure d'obtention des labels

- Les candidats à la labellisation font acte de candidature auprès de la FNTC qui transmet cette demande au COREF ;
- Le COREF sélectionne un expert par tirage au sort dans la liste tenue à jour par lui. Sous réserve de la non-existence de conflits d'intérêts entre cet expert et le candidat au label, le COREF établit une lettre de mission pour l'expert. Celui-ci audite le candidat et remet son rapport au COREF ;
- Le COREF, après vérification du respect des procédures par l'expert, fournit à la FNTC ce rapport d'audit qui synthétise les missions réalisées par l'expert ;
- Au vu de ce rapport, la décision finale est alors prise par le Conseil d'Administration de la FNTC ;
- Les labels sont attribués pour une période de deux ans renouvelable sous réserve d'audits de contrôles.

Ceci peut être représenté par le schéma suivant :



12.5 La FNTC

La FNTC, la Fédération Nationale des Tiers de Confiance a pour mission :

- D'établir la confiance ;
- De promouvoir la sécurité et la qualité des services dans le monde de l'économie numérique ;
- De garantir les utilisateurs ;
- De défendre les droits et intérêts liés à la profession des Tiers de Confiance.

Créée en 2001, la Fédération Nationale des Tiers de Confiance compte aujourd'hui plus de quatre-vingts membres.

Les Tiers de Confiance (archiveurs, certificateurs, horodateurs, hébergeurs, etc.), membres de la FNTC, répondent aux besoins nés de la dématérialisation des documents et de la généralisation de la signature électronique et couvrent les domaines suivants :

- L'archivage électronique sécurisé (tiers archivage et/ou coffre-fort électronique) ;
- La signature électronique ;
- Le chiffrement des échanges et la cryptographie ;
- L'horodatage ;
- La « notarisation » électronique ;
- L'hébergement ;
- L'ASP (Application Service Provider) ou le SaaS (Software as a Service).

12.6 Le COREF

Le COREF (COnfiance et REFérencement) est une association qui a pour objet d'attribuer toute forme d'attestations de conformité à des règles définies (labels, certifications, etc.), de participer à la définition de ces règles et de valider des référentiels dans les domaines des services numériques de confiance, de l'expertise informatique ou tout autre domaine connexe.

Le COREF est né en 2006 à la suite d'un projet nommé CODIL, dont la FNTC a été, en 2003, l'initiateur et le fondateur. Début 2010, les associations adhérentes du COREF sont :

- La FNTC (Fédération Nationale des Tiers de Confiance) ;
- EESTEL (Association des Experts Européens en Systèmes de Transactions Électroniques) ;
- CONCERT International.

13 - GLOSSAIRE

Archive numérique : Ensemble composé d'un à plusieurs fichiers informatiques (formant un tout cohérent), d'éléments d'indexation (métadonnées) et, éventuellement, d'attributs de représentation afin d'en restituer l'intelligibilité pour l'homme.

Authenticité : Caractéristique d'un document dont on peut prouver qu'il est bien ce qu'il prétend être, qu'il a été effectivement produit ou reçu par la personne qui prétend l'avoir produit ou reçu, et qu'il a été produit ou reçu au moment où il prétend l'avoir été (ISO 15489).

Autorité de Certification : (voir Tiers Certificateur)

Certificat public : Issu du certificat privé, ce certificat ne contient pas la clé privée. Il peut donc être publiquement mis à disposition comme c'est le cas lors d'une signature.

Certificat privé : Fichier informatique délivré par une Autorité de Certification et contenant des informations sur son propriétaire ainsi que les clés publiques et privées.

Certificate Authority : (voir Tiers Certificateur)

Document numérique : (voir Archive numérique)

Empreinte : Résultat d'un calcul informatique effectué par une fonction de hachage sur un fichier informatique. Ce résultat se présente sous la forme d'une chaîne de caractères représentant de façon unique le fichier informatique. Toute modification du document numérique entraînera une empreinte différente qui révélera la modification par comparaison avec la première empreinte (NF Z42-013).

ERP : *Enterprise Resource Planning* ou Progiciel de Gestion Intégré (PGI).

Fidélité d'un document : Un document est considéré comme fidèle au document d'origine s'il permet de reconstituer toute l'information nécessaire aux usages auxquels le document d'origine était destiné. Ce concept est utilisé en cas de rupture incluant notamment une numérisation ou une conversion de format (NF Z42-013).

Fonction de chiffrement : Fonction servant dans le calcul de signatures et ayant la particularité d'être asymétrique, c'est-à-dire servant à la fois au chiffrement et au déchiffrement.

Fonction de hachage : Fonction qui fait subir une succession de traitements à une donnée quelconque fournie en entrée pour en produire une empreinte servant à identifier la donnée initiale (NF Z42-013).

Horodatage : Information permettant de démontrer qu'une donnée (par exemple, un document, un enregistrement d'audit, ou une signature électronique) existait à un instant donné (NF Z42-013).

Imputabilité : L'imputabilité est une notion juridique qui exprime la possibilité de faire porter la responsabilité d'une infraction à une personne (Wikipedia).

Intégrité : Caractéristique d'une information qui n'a subi aucune destruction, altération ou modification intentionnelle ou accidentelle (NF Z42-013).

Jeton d'horodatage : Délivré par un service d'horodatage ou un Tiers Horodateur, il contient, entre autre chose, l'empreinte à horodater, la date et heure de la demande d'horodatage et un numéro de série identifiant de façon unique cette demande.
Ce jeton fait partie d'une demande d'horodatage.

Métadonnées : Ensemble structuré d'informations techniques, de gestion et de description attaché à un document servant à décrire les caractéristiques de ce document en vue de faciliter son repérage, sa gestion, son usage ou sa préservation (NF Z42-013).

Pérennité : Aptitude que doit avoir l'information à traverser le temps durant tout son cycle de vie en préservant son intégrité (NF Z42-013).

Piste d'Audit Comptable : Aptitude, à partir d'une écriture comptable, à remonter au fait générateur ou à la pièce d'origine et réciproquement, pour retracer toutes les étapes d'un traitement comptable.

PCG : Plan Comptable Général.

PGI : Progiciel de Gestion Intégré ou *Enterprise Resource Planning* (ERP).

Politique d'Archivage : Une politique d'archivage a pour objet d'organiser et de prévoir les responsabilités, les règles et les moyens à mettre en œuvre pour assurer l'archivage des documents, quelles que soient leurs natures, selon les exigences associées.

Scellement numérique : Procédé permettant de garantir l'intégrité d'un document par l'utilisation conjointe de fonctions de hachage, de signatures électroniques et optionnellement l'horodatage (NF Z42-013).

Signature électronique : Donnée ajoutée à une donnée ou à un ensemble de données permettant de garantir l'intégrité et d'authentifier l'origine de cette ou de ces données (NF Z42-013).

Système d'Archivage Électronique (SAE) : Système consistant à recevoir, conserver, communiquer et restituer des archives et qui s'appuie sur une plate-forme informatique (NF Z42-013).

Tiers Archiveur : Autorité de confiance offrant un service d'archivage à valeur probatoire sur des documents électroniques.

Tiers Certificateur : Autorité de confiance délivrant des certificats et maintenant les listes de révocations de ceux-ci.

Tiers Horodateur : Autorité de confiance délivrant des jetons d'horodatage.

Traçabilité : Faculté de pouvoir présenter l'historique des traitements opérés sur un document durant tout le cycle de vie (NF Z42-013).

14 - REMERCIEMENTS

Ont participé à l'élaboration de ce guide :

- Pascal Agosti (Cabinet Caprioli & Associés) ;
- Xavier Bordes (ACOSS) ;
- Alain Borghesi (Cecurity.com) ;
- Denis Bourdillon (Pitney Bowes Asterion) ;
- Christine Burriau-Natouri, associée Invicio ;
- Éric Caprioli (Cabinet Caprioli & Associés) ;
- Marc Chédru (Marc Chédru Conseil) ;
- Bruno Couderc (Bruno Couderc Conseil) ;
- Élise Debies (Direction de la Sécurité Sociale) ;
- Éric Descours (Docubase Systems – Groupe Tessi) ;
- Bernard Etchevers, associé Incivo ;
- Gabriel Gil (GLI Services) ;
- Olivier Glatigny (PF Numérique) ;
- Frédéric Juppet (Gdoc Lasercom) ;
- Jean-Jacques Milhem (Atos Worldline) ;
- Jean-Louis Mistral (Microlist) ;
- Jérôme Pailhé (ACOSS) ;
- Lucien Poulain (Docapost DPS) ;
- Guy Saignes (Opus Conseils).

A PROPOS DE LA FEDERATION NATIONALE DES TIERS DE CONFIANCE

La FNTC est aujourd'hui reconnue comme un acteur essentiel de la sécurisation des échanges électroniques et de la conservation des informations, maillons essentiels à la maîtrise de l'ensemble de la vie du document électronique.

Elle regroupe aujourd'hui les principaux professionnels de la dématérialisation répartis en 4 collèges en fonction de leur activité professionnelle, tous concernés directement ou indirectement par la sécurisation des échanges électroniques et la conservation des informations. Elle réunit les opérateurs et prestataires de services de confiance (acteurs de l'archivage électronique, de la certification, de l'horodatage et des échanges dématérialisés ; les éditeurs et intégrateurs de solutions de confiance ; les experts et les représentants des utilisateurs ainsi que les institutionnels et les professions réglementées). Elle a pour but d'établir la confiance, de promouvoir la sécurité et la qualité des services dans le monde de l'économie numérique, d'offrir une garantie aux utilisateurs et de défendre les droits et intérêts liés à la profession des Tiers de Confiance.

LES ADHÉRENTS FNTC* :

Accelya ; ACOSS ; AFCDP ; Alma Conseils et Services ; Almerys ; Alphacode ; APECA ; Argus DMS ; Aspheria ; Atos Worldline ; Bernard Starck ; Bruno Couderc Conseil ; Cabinet Caprioli & Associés ; Cecurity.com ; Celtipharm ; CertEurope ; ChamberSign ; Chambre Nationale des Huissiers de Justice ; CodaSystem ; Compagnie Nationale des Commissaires aux Comptes ; Conseil National des Greffiers de tribunaux de commerce ; Conseil Supérieur de l'Ordre des Experts-Comptables ; Corus ; DARVA ; Darwin Consulting & Finance ; Data One ; Data Syscom ; Demaeter ; Digimedia Interactivité ; Docapost DPS; Docubase Systems ; Document Channel ; Ecosix ; Edificas ; Edokial ; EESTEL ; ESI ; Esker ; Esopica ; Everial ; Explain ; Extelia ; Forum Atena ; G.L.I. Services ; Gdoc Lasercom ; Hervé Schauer Consultants ; Imprimerie Nationale ; Info Service Europe ; Interb@t ; Isilis ; jedeclare.com ; Khan & Associés ; Keynectis ; Lex Persona ; Locarchives ; Maileva ; MiaXys ; Micrographie Services ; Microlist ; MIPIH ; Neuflize OBC ; NPAI ; Odyssey Services ; OFSAD ; Omnikles ; OPUS Conseils ; PF Numérique ; Pitney Bowes Asterion ; PPI ; Primobox ; ResoCom ; Scala ; Société Générale d'Archives ; Sogelink/DICT.fr ; SR Développement ; Stocomest ; Syrtals ; TrustMission ; Valerian ; Voxaly Electionneur.

** Liste arrêtée au 15 octobre 2010*

FÉDÉRATION NATIONALE DES TIERS DE CONFIANCE
19, rue Cognacq-Jay
75007 – Paris
Tél. 01 47 50 00 50
info@fntc.org

www.fntc.org

Conception graphique et illustration : www.idsg.fr

www.fntc.org