



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DIRECTION GÉNÉRALE DE LA COMPTABILITÉ PUBLIQUE

PROGRAMME HELIOS

Pôle national de dématérialisation

pour le secteur public local

Immeuble Maille Nord bat.3

9-10 Porte de Neuilly

93192 Noisy-le-Grand

Cadre National d'Acceptation de la Dématérialisation dans le Secteur Public Local

Normes et principales solutions de dématérialisation référencées de la chaîne comptable et financière

Table des Matières

| | |
|---|-----------|
| 1. INTRODUCTION | 3 |
| 1.1 OBJET DU CADRE NATIONAL D'ACCEPTATION..... | 3 |
| 1.2 ÉVOLUTION DU CADRE NATIONAL D'ACCEPTATION..... | 3 |
| 1.3 CADRE GÉNÉRAL DES NORMES | 4 |
| 1.4 RAPPELS DES BESOINS, CONTRAINTES ET ENJEUX..... | 4 |
| 1.5 ÉCHANGES, DONNÉES ET DOCUMENTS | 4 |
| 1.6 DÉFINITIONS..... | 5 |
| 2. PRINCIPES FÉDÉRATEURS DE LA DÉMATÉRIALISATION | 5 |
| 2.1 PÉRIMÈTRE DE LA DÉMATÉRIALISATION..... | 5 |
| 2.2 UNICITÉ DES FICHIERS PARTAGÉS..... | 6 |
| 2.3 PORTABILITÉ ET EXPLOITABILITÉ DES DONNÉES & DOCUMENTS | 6 |
| 2.4 ÉCHANGE DE DONNÉES..... | 6 |
| 2.5 SÉCURITÉ DES DOCUMENTS..... | 6 |
| 2.6 PRINCIPES TRANSVERSES..... | 6 |
| 2.6.1 Cycle de vie des documents..... | 6 |
| 2.6.2 Génération | 7 |
| 2.6.3 Identifiant Unique | 7 |
| Référencement & Métadonnées..... | 8 |
| 2.6.4 Indexation et recherches | 9 |
| 2.6.5 Exemple..... | 9 |
| 2.6.6 Réflexions à engager..... | 10 |
| 2.7 CARACTÉRISTIQUES PHYSIQUES..... | 10 |
| 2.7.1 Format de fichier..... | 10 |
| 2.7.2 Support..... | 12 |
| 2.7.3 Transmission (Protocole)..... | 12 |
| 2.7.4 Stockage | 13 |
| 2.7.5 Sécurité..... | 13 |
| 2.7.6 Recherche..... | 15 |
| 2.7.7 Archivage | 15 |
| 2.7.8 Destruction..... | 16 |
| 3. PRINCIPES SPÉCIFIQUES PAR SUPPORT D'ÉCHANGE | 16 |
| 3.1 LE SUPPORT PAPIER | 16 |
| 3.1.1 Caractéristiques générales..... | 16 |
| 3.1.2 Solutions globales identifiées..... | 16 |
| 3.2 LE SUPPORT CD-ROM | 17 |
| 3.2.1 Caractéristiques générales..... | 17 |
| 3.2.2 Solutions globales identifiées..... | 17 |
| 3.3 LE SUPPORT « ELECTRONIQUE »..... | 18 |
| 3.3.1 Les systèmes de fichier..... | 18 |
| 3.3.2 Les systèmes de transfert et d'accès distant | 18 |
| 3.3.3 Les messageries électroniques | 18 |
| 3.3.4 Principes communs | 19 |
| 3.3.5 Les solutions de GED ou gestion de contenu..... | 19 |
| 4. LES PROJETS MAJEURS DE LA DÉMATÉRIALISATION | 20 |
| 4.1 INTÉGRATION DE LA DÉMATÉRIALISATION AU PES HÉLIOS | 20 |
| 4.1.1 Modèle de stock..... | 21 |
| 4.1.2 Modèle de flux..... | 21 |
| 4.1.3 Modèle transitoire à flux parallèle..... | 22 |
| 4.1.4 Principe de référencement des pièces justificatives dans Hélios | 22 |
| 4.2 LE PROJET « ACTES » DE LA DGCL..... | 22 |
| 4.3 LES PROJETS DE « PARAPHEUR ÉLECTRONIQUE » | 23 |
| 4.4 LE PROJET GEIDE DE LA DGCP (AMIENS) | 23 |
| 4.5 LES PRINCIPALES EXPÉRIENCES DE DÉMATÉRIALISATION..... | 24 |
| 4.5.1 Les expérimentations de dématérialisation..... | 24 |
| 4.5.2 Procédures à mettre en œuvre pour le lancement d'expériences de dématérialisation | 24 |
| 5. ANNEXE : RÉFÉRENCES DES SOURCES D'INFORMATIONS | 26 |

La Direction Générale de la Comptabilité Publique (DGCP) a initié, sous l'impulsion du plan d'action du Trésor Public relatif à la gestion publique, une réflexion en matière de dématérialisation.

Faisant suite au schéma directeur pour la dématérialisation dans le secteur public local, le présent document précise les principes fédérateurs, les normes et solutions auxquelles tout projet de dématérialisation doit se référer afin de mettre en œuvre une solution qui satisfasse l'ensemble des acteurs de la chaîne comptable et financière.

La dématérialisation en cause porte sur les échanges de données et de documents entre les trois acteurs de la chaîne comptable et financière que sont l'ordonnateur, le comptable et le juge des comptes, à l'exclusion des procédures de règlement des titres de recettes et de paiement des mandats de dépenses.

Ce Cadre national d'acceptation est susceptible d'évoluer à raison notamment des expérimentations en cours et à venir de solutions de dématérialisation.

1. Introduction

Ce document pose tout d'abord le périmètre et le champ d'application du Cadre National d'Acceptation de la dématérialisation dans le secteur public local, en ce qui concerne la chaîne comptable et financière. Ce cadre a pour objet de préciser les principales normes techniques et solutions de dématérialisations référencées.

Dans un deuxième temps, l'ensemble des recommandations de définition et de mise en œuvre de la dématérialisation est présenté par type d'échange.

Les projets en cours pour la dématérialisation entre la DGCP et ses partenaires sont listés en fin de document.

1.1 Objet du Cadre National d'Acceptation

Le Cadre National d'Acceptation a pour objet de :

- Préciser le périmètre de la dématérialisation dans le secteur public local,
- Présenter les principes fédérateurs généraux de la dématérialisation,
- Proposer pour chaque type de support d'échanges identifiés les principes fédérateurs spécifiques,
- Présenter les projets en cours,
- Identifier les points particuliers restant à traiter.

1.2 Évolution du Cadre National d'Acceptation

Le présent Cadre évoluera parallèlement à la mise en place des premières expérimentations pour intégrer les mises à jour et compléments résultant :

- de l'évolution des besoins,
- des retours d'expérience sur les expérimentations dans le secteur public local,
- et de l'intégration de l'évolution des normes et standards et de leur implémentation (« open source » ou solutions d'éditeur).

Le cadre d'acceptation prend en compte les préconisations du Cadre Commun d'Interopérabilité de l'administration de l'ADE et évoluera donc aussi au fur et à mesure des publications de l'ADAE.

La prise en compte des demandes d'évolution de ce document sera assurée par la structure partenariale prévue par la Charte de la dématérialisation dans le secteur public local.

1.3 Cadre général des normes

Ce Cadre National d'Acceptation s'inscrit en premier lieu dans une démarche de dématérialisation de la chaîne comptable et financière. A ce titre, elle fait partie intégrante de la Charte de la dématérialisation dans le secteur public local dont elle constitue le volet technique.

En second lieu, l'initiative de la DGCP autour de la dématérialisation est à rapprocher des travaux menés par d'autres administrations et organismes inter-ministériels sur ce même sujet ou dans un cadre élargi autour de l'administration électronique :

- Protocole d'Echange Standard du programme Hélios de la DGCP,
- Projet « Actes » de la Direction Générale pour les Collectivités Locales (DGCL),
- Les projets de Parapheur Électronique,
- Projet de GEIDE de la DGCP (solution développée au Département Informatique d'Amiens).

Ces projets à caractère générique sont considérés comme autant de voies d'exploration et de convergence pour la dématérialisation et sont présentés dans cette note en complément d'une analyse par type de support.

1.4 Rappels des besoins, contraintes et enjeux

Si les échanges de données entre les trois partenaires de la chaîne comptable et financière représentent un besoin commun, les solutions potentielles peuvent être multiples. En outre, ces échanges sont fortement contraints par les besoins « métiers » de chaque partenaire ainsi que par le cadre réglementaire et juridique régissant leurs relations. Les facteurs principaux influençant ces échanges sont :

- les contraintes « métiers » et juridiques propres à chaque partenaire,
- les contraintes « métiers » et juridiques liées aux échanges (exemple : portabilité),
- l'hétérogénéité liée à la taille et aux moyens disponibles (humains, techniques,...),
- les spécificités liées à certains types de données (signature électronique).

1.5 Échanges, données et documents

Si l'échange d'information recouvre pour l'ensemble des acteurs la notion de partage d'un certain nombre de données, les caractéristiques de ces échanges peuvent considérablement varier, notamment dans un contexte de dématérialisation. En effet, avec la généralisation des moyens informatiques l'échange d'informations :

- n'implique plus nécessairement la transmission systématique des données (accès partagé) notamment entre l'ordonnateur et le comptable ;
- peut se faire sous des formats divers (ASCII, texte, bureautiques) ;
- avoir des supports multiples (CD-Rom, disque, bases de données, fichiers,...) ;
- s'appuyer sur une structuration des données de plus ou moins haut niveau (données brutes, Word, XML).

Dans ce qui suit, le terme « document » est utilisé au sens large, dans la mesure où il concerne des données ayant des niveaux de structuration, des formats et des supports variables. L'ISO fournit une définition du document électronique : « Un document est l'ensemble constitué d'un support d'information et des données enregistrées sur celui-ci sous une forme en général permanente et lisible par l'homme ou par une machine dans le cadre de dispositifs de traitements d'information ».

Le document est donc porteur d'informations sur le fond - ce sont les données (le contenu) - et sur la forme - c'est la présentation (structuration, feuilles de style).

Dans le cadre d'une chaîne de dématérialisation, le document ou la donnée peuvent être ainsi les vecteurs de l'échange. L'échange doit, autant que faire se peut, privilégier l'échange de données structurées.

1.6 Définitions

Les concepts utilisés ci-après sont précisés afin de lever toute ambiguïté :

Nommage : On entend par nommage, le nom donné au fichier du document sur le système d'information (*exemple : 01_999843_20043103_001.xml pour un document de type xml*)

Identifiant : On entend par identifiant, un libellé numérique ou « chaîne de caractères » permettant d'identifier un document. Cet identifiant peut être lié ou déconnecté du nommage du fichier (*exemple : 01_999843_20043103_001*)

Référence : La référence permet de véhiculer un pointeur sur le document sans avoir à transmettre celui-ci. Elle inclue souvent l'identifiant du document. Par extension, la référence peut être utilisée pour localiser un document et y accéder au moyen d'un lien actif.

Métadonnées : Les métadonnées sont un ensemble de données dérivant les caractéristiques d'un document et éventuellement son contenu (par exemple nom du fichier, auteur, date de création, date de modification, type de document, etc). Les **métadonnées du document** servent à identifier le document et le retrouver aisément, à assurer sa traçabilité tout au long de son cycle de vie. Elles sont en particulier utiles dans la perspective d'un archivage.

Indexation : L'indexation est l'ensemble des mots clés extraits de son contenu et des caractéristiques (nom du fichier, auteur, date de création, date de modification, type de document, etc) permettant d'identifier un document à partir de ses éléments constituant son index. L'index est exploité par un outil de recherche permettant de retrouver les documents correspondant aux caractéristiques souhaitées. **L'indexation peut par définition prendre en compte tout ou partie des métadonnées d'un document.**

| Principe | Objet |
|-------------|---|
| Nommage | Identification des documents par le nom du fichier. Le plan de nommage évite les fichiers doublons par l'adoption d'un identifiant unique national |
| Identifiant | Libellé numérique ou « chaîne de caractères » permettant d'identifier un document. |
| Référence | Pointeur sur le document afin d'en éviter la copie ou le transport systématique. La référence permet d'identifier – localiser et accéder au document. |
| Métadonnées | Ensemble de données servant à identifier le document et le retrouver aisément, à assurer sa traçabilité tout au long de son cycle de vie. |
| Indexation | Ensemble de critères et mots clés permettant d'identifier le document en vue d'une recherche à l'aide d'un outil logiciel. |

2. Principes fédérateurs de la dématérialisation

2.1 Périmètre de la dématérialisation

L'intérêt de la dématérialisation est d'autant plus important que celle-ci peut s'effectuer de bout en bout de la chaîne comptable et financière. La dématérialisation doit être pensée pour l'ensemble des intervenants et privilégier les démarches concertées entre tous les acteurs impliqués dans ces échanges.

La démarche de dématérialisation concerne les échanges de données indépendamment des applications. Il n'est pas admis d'échanges directs entre deux applicatifs. Les échanges sont effectués sur la base de documents structurés en fichiers et échangés sur un mode asynchrone.

2.2 Unicité des fichiers partagés

Tout document partagé sur un système accessible par plusieurs acteurs doit être unique. Si plusieurs versions d'un fichier co-existent, elles doivent être clairement identifiées. Par ailleurs, si la duplication ne peut être évitée dans le cas d'une transmission de copie, le document de référence doit être identifié et reconnu comme tel par l'ensemble des acteurs.

2.3 Portabilité et exploitabilité des données & documents

Toute donnée ou document transmis ou partagé doit être exploitable. Le format est un élément fondamental de la portabilité, mais aussi de son exploitabilité (notamment au travers de l'accès aux informations qu'il contient). Le support utilisé pour la transmission des données doit également garantir l'exploitabilité du document.

2.4 Echange de données

Dans la mesure des possibilités techniques, il convient de favoriser les solutions d'échanges de fichiers de données, permettant pour l'ensemble des acteurs une exploitation plus performante des données numériques. Cette approche est particulièrement recommandée pour les documents à forte structuration et en nombre important (exemple : états de paye, titres, mandats...). Dans le cadre du déploiement du progiciel Helios, l'utilisation des objets comptables XML conformes au Protocole d'Echange Standard (PES) sera recommandé, afin d'accélérer la dématérialisation par échange de données.

2.5 Sécurité des documents

Bien que la technologie permette la signature électronique des documents, et la mise en œuvre d'un niveau fort de sécurisation, la délivrance des certificats matériels et l'authentification des signataires restent peu répandues (cf. PC-Type du Minefi et PRIS de l'ADAE). De ce fait, il convient dans la perspective de la mise en place des certificats pour les agents publics de privilégier les mécanismes rapidement utilisables au coût limité.

Les certificats logiciels sont recommandés pour un niveau de sécurité élevé (cf. 2.7.5), ils permettent d'assurer l'identification des partenaires de l'échange, l'intégrité et la confidentialité des échanges et la non répudiation des éléments transmis.

En complément pour une sécurisation standard les mécanismes suivants sont recommandés :

- Utilisation d'identifiant & mot de passe pour les accès aux systèmes ou dossiers partagés,
- Restriction de l'accès aux Documents en mode lecture pour garantir l'intégrité des documents, le tout éventuellement complétés par une protection par mot de passe.

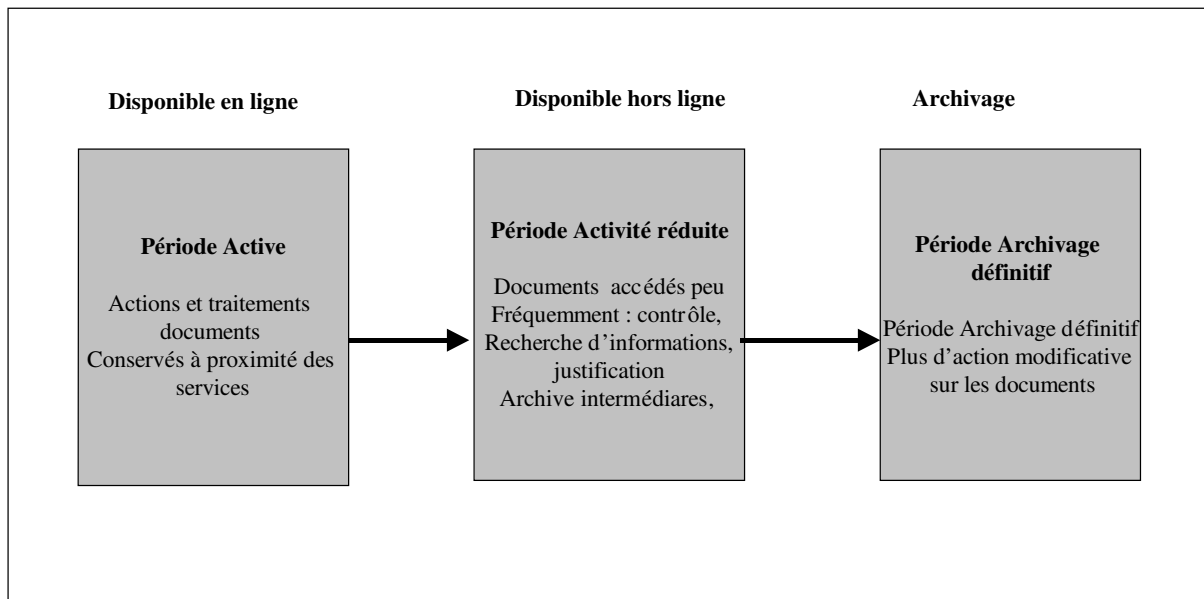
2.6 Principes transverses

2.6.1 Cycle de vie des documents

Les documents échangés entre les collectivités locales ou établissements publics locaux, les comptables du Trésor et les Chambres Régionales des Comptes s'inscrivent dans un cycle de vie dont il convient de distinguer les différentes phases et les caractéristiques qui leur sont associées (format, nom du document, stockage, transmission, utilisation) :

- Une phase « court terme » recouvrant la production des documents et leur utilisation locale par le producteur dans le cadre de ses fonctions ;
- Une phase « intermédiaire » durant laquelle le document est transmis et stockée pour des tiers en vue d'une utilisation potentiellement différente de celle effectuée par le producteur (document accessible en ligne) ;
- Une phase « long terme » durant laquelle le document est archivé pour répondre aux exigences légales et réglementaires (document hors ligne).

Notamment il convient de prendre en considération la possibilité pour un document d'avoir des caractéristiques différentes selon la phase dans laquelle il se trouve et d'avoir ainsi plusieurs formes potentielles au cours de son cycle.



Cycle de vie des documents

2.6.2 Génération

Les gains de la dématérialisation étant directement liés à son extension à l'ensemble des partenaires conformément aux principes de la Charte de dématérialisation, plusieurs principes doivent être respectés :

- Chaque partenaire doit être en mesure d'accepter les documents dématérialisés lui parvenant et respectant les présentes recommandations ;
- Tout document dématérialisé ne doit pas être « re-matérialisé » (autant que faire se peut) ;
- La génération des documents dématérialisés doit être effectuée au plus tôt, c'est à dire à la source de production des documents pour l'ensemble des partenaires ;
- Les documents dématérialisés doivent être prioritairement produits à partir des applicatifs et progiciels métiers et des outils de bureautiques.

NB : La scannérisation des documents papiers constitue une solution alternative à la production directe de pièces justificatives sous forme numérique. Dans le cas où l'un des partenaires souhaite mettre en œuvre une solution de scannérisation en raison de sa viabilité économique pour ses besoins propres, les documents produits devront être compatibles avec les recommandations présentées dans ce document à commencer par le principe de l'identifiant « unique » et l'indexation.

2.6.3 Identifiant Unique

L'identifiant unique permet d'identifier sans ambiguïté un document tout au long de son cycle de vie et sur l'ensemble de la chaîne comptable et financière. Cet identifiant peut être un code ou un libellé véhiculé, avec le document ou les données, lors des échanges et lors de l'exploitation des pièces. Toutefois, une première solution consiste pour les documents ou données existants sous forme de fichier électronique, à leur donner un nom reprenant les principes de l'identifiant. Dans le cas où le nom de fichier constitue l'identifiant, le système d'identification s'apparente à un plan de nommage des fichiers.

2.6.3.1 Principes de l'Identifiant Unique

Les principes préconisés pour l'identification des pièces sont les suivants :

- Tout acteur de la chaîne comptable et financière doit affecter **obligatoirement** au document dématérialisé qu'il produit, **un identifiant unique** valable tout au long de la vie du document.
- L'unicité de l'identifiant peut être générée selon une règle propre au seul organisme « émetteur », le couple émetteur et identifiant constituant **obligatoirement** un identifiant unique pour l'ensemble des acteurs de la chaîne comptable.
- L'adoption d'un système d'identification homogène à l'échelle nationale est préférable : l'identifiant unique national devra être mis en œuvre autant que faire se peut.

L'identifiant unique pourra utilement intégrer, un certain nombre d'éléments communs dont, à minima :

- un identifiant de l'émetteur du document (en d'autres termes son producteur) ;
- une référence - de type date ou numéro - permettant pour son producteur de garantir l'unicité du nom du document.

Ainsi, l'identifiant de l'émetteur (codes SIRET, SIREN, FINESS,...) associé à une numérotation propre à chaque organisme permet de garantir l'unicité du document et d'en identifier la source. Afin que le numéro d'identification soit unique au sein de l'entité émettrice du document, il est nécessaire d'y associer une logique ne permettant pas de retrouver deux fois le même numéro.

Dans le cas où l'identifiant unique est associé au nommage du fichier, le nombre de caractères utilisé doit permettre la portabilité ; aussi le nombre de caractères du nom de fichier sera limité à 64.

A défaut d'être explicite pour tous les partenaires ; l'identifiant unique sera secondé par un système de référencement ou d'indexation. Dans ce cas, c'est la référence qui portera les informations sur le contenu du fichier permettant d'en identifier le contenu (type de pièces, période couverte, etc...). Un système d'indexation pourra compléter le référencement pour identifier le document à partir de mots clés utilisés par un moteur de recherche. Le référencement peut ainsi être spécialisé selon la catégorie d'utilisateurs (référence « métier ») bien que le nom de l'identifiant reste unique.

En tout état de cause, pour être utilisé, l'identifiant de chaque document créé devra être transmis aux applications tierces (notamment Hélios) avec sa référence active et, le cas échéant, ses informations complémentaires (indexation, référencement, métier...), si l'on souhaite un référencement et un accès par ces applications.

Afin d'éviter la multiplication des nomenclatures de nommage, la définition d'un identifiant unique sur les actes échangés entre les collectivités et les administrations de l'Etat, pourra être favorisée dans le cadre commun d'interopérabilité de l'ADAE.

Référencement & Métadonnées

Chaque document doit avoir un identifiant unique mais doit également faire l'objet systématique d'un référencement. Le référencement des pièces justificatives et plus généralement des documents dématérialisés permet :

- d'identifier l'existence des documents,
- de servir de déclaration de transmission,
- de localiser ou d'accéder directement au document (référence active de type URL).

La référence doit à minima inclure le nom de fichier. En complément, la référence peut être enrichie par :

- des données « métier » permettant d'accroître l'identification du document, lorsque le nom ne suffit pas.
- la localisation du fichier pour y accéder par un système tiers ;
- une référence active permettant d'y accéder automatiquement depuis le système sur lequel se situe la référence.

Dans le cas de la mise en œuvre d'une référence active, il est essentiel que les documents soient couplés à un système de visualisation permettant leur accès à distance.

Le référencement doit aussi permettre de caractériser les **métadonnées associé au document** qui serviront à l'identifier et à assurer sa traçabilité tout au long de son cycle de vie. Certaines de ces métadonnées pourront déjà être présentes dans l'identifiant unique du document mais devront également être enregistrées en tant que métadonnées, comme par exemple :

- le nom du producteur du document (N° SIREN, SIRET, FINESS pour l'organisme),
- la date de création et le type du document,
- les éléments métiers définis en accord avec l'ensemble des partenaires.
- le format du document et le cas échéant, la nature de la signature utilisée,
- la date d'archivage, sa durée de conservation,
- ses références à d'autres documents,
- des informations techniques sur le support utilisé...

Ces éléments peuvent servir à l'indexation mais seront aussi particulièrement utiles dans la perspective d'un archivage.

2.6.4 Indexation et recherches

L'indexation permet d'accéder rapidement à des documents ou certaines informations qu'ils contiennent par l'utilisation de mots clés ou de caractéristiques distinctives. L'index permet d'identifier plus finement un corpus de documents et autorise des recherches multicritères. L'index peut-être constitué manuellement ou par l'examen automatique des fichiers.

L'indexation associe à chaque document l'ensemble des éléments (noms de fichiers, date de création, nom du rédacteur, mots clés) permettant de le caractériser et de le retrouver lors d'une recherche ultérieure. **L'indexation peut par définition prendre en compte tout ou partie des métadonnées d'un document.**

La qualité de l'index est un facteur principal de succès pour la recherche des documents. L'adéquation des critères d'indexation avec les données est donc primordiale.

Un seul index regroupant les critères communs et particuliers de l'ensemble des partenaires est préférable à la cohabitation de plusieurs indexes spécialisés (sous réserve de la maîtrise de la volumétrie et des performances pour la mise à jour de l'index et la recherche). Parmi les critères d'indexation à retenir, figurent notamment :

- le nom du producteur du document (N° SIREN, SIRET, FINESS pour l'organisme),
- la date de création et le type du document,
- les éléments métiers à définir en concertation avec l'ensemble des partenaires.

L'indexation doit privilégier les aspects métiers par rapport à l'identifiant qui a vocation à être général. Le pôle dématérialisation devra préciser avec ses partenaires les informations d'indexation préconisées ou obligatoires dans les conventions par type de flux (feuilles de paye, titres de recettes, mandats...).

Par ailleurs, certains flux de documents à forte structuration pourront nécessiter de mettre en place un système de recherche étendue, permettant de réaliser des requêtes en vue de trouver le ou les documents répondant aux critères souhaités (exemple : feuille de paye).

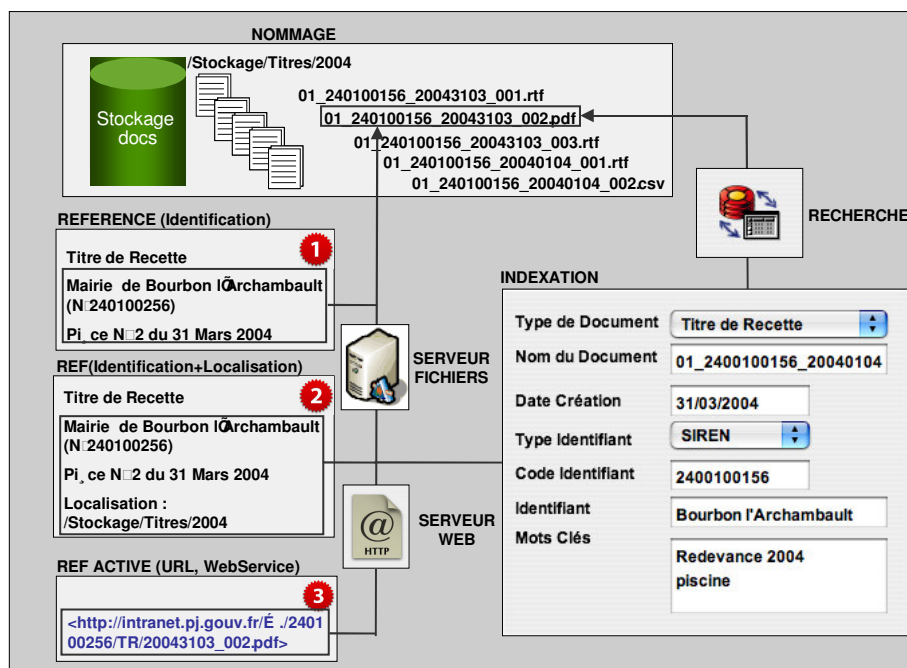
2.6.5 Exemple

Le schéma ci-après (cf *Principes de nommage, référence et indexation*) permet d'illustrer les principes de l'identifiant unique, du référencement et de l'indexation.

- L'identifiant unique, éventuellement associé au nommage, permet de désigner de manière unique un fichier grâce à un identifiant dont l'unicité est garanti.
- Le référencement est destiné à véhiculer un lien vers le document (pointeur) sans avoir à recopier l'information contenue dans celui-ci, à dupliquer ou transmettre le document en

chacun des lieux où l'information qu'il contient doit être stipulée. L'accès au document référencé est réalisé :

- indépendamment de la référence, si celle-ci n'est pas active, (cf. schéma 1 & 2)
 - ou en l'utilisant si elle est bien active (cf. 3) au travers d'un serveur d'accès distant (serveur web pour un lien HTTP, serveur de fichier pour une adresse SMB, AFP ou NFS, serveur SOAP-XML pour un service web).
- L'indexation permet d'extraire du document des caractéristiques et mots clés qui pourront être exploités ultérieurement par un moteur de recherche comme critères de recherche. Le moteur de recherche pourra donner comme résultat une référence active de type URL pour accéder dans un deuxième temps au document. L'indexation est réalisée au moyen d'un moteur d'exploration ou par une saisie manuelle.



Principes d'identification, nommage, référence et indexation

2.6.6 Réflexions à engager

Des groupes de travail permettront de préciser les propositions de ce Cadre National d'Acceptation, pour chaque type de flux « métier » (feuilles de paye, titres de recettes, mandats...).

2.7 Caractéristiques Physiques

2.7.1 Format de fichier

Différents formats sont envisageables pour les données selon le type l'utilisation. Parmi les principes communs retenus, il est nécessaire de privilégier la compatibilité du format sur l'ensemble de la chaîne de diffusion de celui-ci et donc vis-à-vis des outils et sur la durée de vie de ce dernier.

Certains formats employés lors de la production des documents ne sont pas ou peu utilisables en dehors de ce contexte ; c'est le cas pour la plupart des formats d'impression.

Par ailleurs, les opérations de changement de format lors de l'acquisition de documents ou plus en aval dans leur cycle de vie, constituent des points de fragilité qui doivent être particulièrement maîtrisés et sont donc à éviter.

Les formats de fichier recommandés sont les formats permettant d'être exploités sur tous les systèmes (hétérogènes) des acteurs de la chaîne comptable et financière. A ce titre, la portabilité et l'exploitabilité du document est un élément prépondérant. Pour les documents nécessitant une reprise des données, le stockage dans le format original est recommandé sous réserve de compatibilité entre partenaires.

A des fins de clarifications, deux principaux types de formats de fichier sont distingués :

- des formats dits orientés « données » : dans ce cas, les données sont indépendantes d'une éventuelle présentation d'un ensemble de documents.
- des formats dits orientés « document » : dans ces formats, les données sont étroitement associées à une présentation figée

2.7.1.1 *Les formats orientés « données »*

Lorsque c'est possible, la dématérialisation doit consister en la communication des données, éventuellement associé à des outils d'exploitation (visualisation et recherches). Dans le cas contraire, l'utilisation de fichier « index » permettant d'associer des données structurées aux documents (visualisables) doit être conseillée.

Dans ces deux cas, l'usage des formats « données » suivants est recommandé :

- Le format XML,
- Le format CSV (« comma separated value »),
- Les formats ASCII ou Unicode avec séparateurs.

Le choix de ces formats permet de garantir une certaine pérennité d'accès dans le temps, corollaire des besoins de stockage et d'archivage.

Les données échangées selon un tel format résulteront la plupart du temps d'un traitement réalisé à partir de la base de données originale du progiciel des gestion (extraction).

L'utilisation de formats de fichier « données » non recommandés est déconseillée, car leur pérennité d'exploitation n'est pas assurée. En tout état de cause, dans une telle situation, il est conseillé de produire parallèlement une copie des données sous un des formats préconisés.

Outil d'exploitation

L'utilisation de fichiers de données peut nécessiter l'association avec un outil d'exploitation, afin d'assurer les fonctions de visualisation et de recherche. Les fichiers associés à l'outil d'exploitation, en particulier de fichiers décrivant des masques de recherche et ou de visualisation, devront dans la mesure du possible, relever des formats préconisés au précédent paragraphe.

2.7.1.2 *Les formats orientés « document »*

Parmi les formats orientés « document » recommandés, le format « image » dans ces différentes formes n'est pas la solution préférentielle. En revanche, les formats permettant de conserver l'accès aux informations structurées du document et donc son exploitabilité devront être privilégiés. Ainsi, les formats recommandés sont :

- Le format XML pour tous les documents de type texte destinés à être intégrés dans un applicatif « partenaire », éventuellement associé à un fichier de présentation au format XSL,
- Le format HTML, sans référence externe, et pouvant être fournis avec d'autres fichiers référencés placés dans un container,
- Le format « texte » (ASCII ou Unicode) particulièrement adapté au fichier « full-text » n'ayant pas de besoin de présentation,
- Le format bureautique usuel Word RTF, seul format généré par MS Word compatible avec toutes les versions en prenant compte de ses limitations,

- Le PDF (Portable Document Format) pour les documents étant initialement dans ce format (Versions 3, 4 et 5),
- Le format TIFF, PNG et JPG pour les documents de type image.

2.7.1.3 Les formats « container »

Dans le cas de document « composite » comportant plusieurs fichiers, comme par exemple dans le cas d'un fichier de données et d'un fichier de présentation, il est conseillé d'utiliser les formats TAR ou GTAR, ou leurs versions avec compression pour tous les documents compactés. Ces formats garantissent que les noms des fichiers inclus dans l'archive seront préservés durant leur acheminement au travers de système hétérogènes (nombre de caractères, caractères accentués, etc...).

2.7.2 Support

Différents supports peuvent être utilisés tout au long du cycle de vie d'un document : on distingue essentiellement les supports de stockage, de partage et d'échange. Les supports spécifiques tels que ceux pour l'archivage sont abordés au § 2.7.7.

1- Les supports utilisables pour le stockage et le partage des documents dématérialisés sont :

- Les disques durs des systèmes informatiques (serveur de fichiers, système GED, NAS, SAN)
- Les CD-ROM aux normes ISO 9660 avec extension Joliet (64 caractères) et ISO 10149.
- Les disquettes de capacité 1,44 Mo au format FAT en dernier ressort du fait de leur faible fiabilité.

2- Les supports utilisables pour l'échange des documents dématérialisés sont :

- Les systèmes de transmission électronique servant aux réseaux, messagerie et transfert de fichiers (se reporter à la section transmission pour compléments).
- Les CD-ROM aux normes ISO 9660 avec extension Joliet (64 caractères) et ISO 10149.

Pour les CD-ROM, les fichiers gravés devront être complétés :

- De la liste au format texte (ASCII) ou XML des fichiers présents sur le disque et de leur localisation si le contenu est organisé en arborescence.
- De l'index ou des références permettant leur intégration dans un système tiers.

2.7.3 Transmission (Protocole)

Lors de l'échange de documents dématérialisés, le mode de transmission fait intervenir un « médium » ainsi qu'un protocole de transmission. Dans le cas d'un échange utilisant un support matériel de type CD-ROM ou disquette, la transmission s'effectue par voie postale ou dédiée. Dans le cas d'une transmission électronique, plusieurs types de protocoles sont disponibles selon les outils sélectionnés

Pour une transmission locale s'effectuant sur un système d'information partagé la transmission pourra s'effectuer :

- par déplacement ou copie du fichier dans un répertoire du système de fichier prévu à cet effet,
- par attachement du document dans un mèl.

Pour une transmission sur un réseau étendu la transmission peut utiliser :

- le canal de la messagerie électronique et des pièces jointes (MIME et S/MIME),
- la transmission sur mode fichier au travers de protocoles de type FTP ou HTTP.

Afin de protéger les documents échangés, la mise en œuvre d'une signature électronique est possible au travers des outils de messagerie ou du navigateur Web pour l'ensemble de ces modes.

Pour les transmissions impliquant un engagement des parties, l'implication d'un « tiers de confiance » assurant la vérification des identités, l'horodatage des échanges et la non répudiation sera nécessaire.

Une alternative consiste à intégrer ces fonctions au sein des réseaux d'échange de la DGCP, la DGCP jouant le rôle de postier électronique.

Quelque soit le mode de transmission choisi (messagerie, fichier, « upload » sur serveur web), il conviendra de mettre en œuvre les standards normalisés :

- HTTP pour les échanges au travers d'un serveur web,
- SMTP pour les échanges entre messageries électroniques,
- MIME pour les pièces jointes aux messages,
- FTP pour les échanges au travers d'un serveur de fichier.

Les versions sécurisées de ces protocoles sont recommandées pour assurer l'intégrité et la confidentialité des échanges, à l'exception du FTPS qui n'est pas encore normalisé.

2.7.4 Stockage

La notion de stockage correspond à la nécessité de conserver pour la durée d'exploitation du document, une copie électronique sur un support offrant toutes garanties d'accessibilité durant cette période spécifique. Il convient également de différencier cette notion de stockage, liée à la période « active » du document, de la notion d'archivage (cf. § 2.6.7) liée à la période d'archivage définitif du document. Le stockage privilégie l'exploitation en ligne du document alors que l'archivage en assure la pérennité.

2.7.5 Sécurité

2.7.5.1 Définition des concepts de sécurité

Rappel des principaux concepts essentiels en matière de sécurité et de leur définition :

- **Identification** : Nom unique attribué à chaque élément du processus de communication
- **Authentification** : Preuve de l'identification fournie
- **Intégrité** : Garantie que le contenu ne peut pas être altéré de quelque manière que ce soit
- **Confidentialité** : Garantie que seul le destinataire du contenu est apte à lire et exploiter le dit contenu
- **Non répudiation** : Garantie que le contenu d'un message ne peut pas être réfuté, ni par l'émetteur, ni par le destinataire (principe de l'accusé de réception).

2.7.5.2 de la sécurité

Objectifs globaux :

- La sécurité doit demeurer **transparente à l'utilisateur** en termes de mise en œuvre et de facilité de service.
- L'administration de la sécurité doit être réalisée sans délai préjudiciable à la **qualité du service fourni** (création, modification ou suppression de droits, ...).

Conditions de mise en œuvre :

- La mise en place de mécanismes de sécurité entre partenaires ne peut être réalisée sans la définition préalable d'une politique de sécurité commune aux partenaires dans le cadre de leurs échanges.

Authentification mutuelle Utilisateur / Service :

- Le Service doit être capable de s'identifier de manière **irréfutable**, auprès de **l'utilisateur**.
- L'utilisateur doit être capable de s'identifier de manière **irréfutable**, auprès du **Service**.
- Tout **usurpateur d'identité** ne doit pas être en mesure de s'identifier sous une fausse identité, que ce soit dans le cadre d'une machine volée ou d'une machine dont l'accès a été forcé.

- Le **contenu** véhiculé durant la phase d'authentification ne doit être **ni détourné** par un serveur tiers, **ni lu ou altéré**.

2.7.5.3 *Transcription de ces principes sur la chaîne comptable et financière*

La sécurité des échanges sur la chaîne comptable et financière du secteur public local peut se décliner ainsi :

Fiabilité des échanges

La fiabilité des échanges repose en premier lieu sur la qualité des infrastructures qui en ont la charge. Dans ce contexte, la dématérialisation des échanges impose de recourir à des infrastructures d'échanges fiables permettant notamment de détecter les incidents et de reprendre automatiquement les échanges temporisés ou interrompus après rétablissement du service.

Confidentialité des échanges lors des échanges

La confidentialité des échanges, qui peut être assurée par le cryptage des documents échangés et/ou le cryptage des données échangées sur le canal d'échange, est quant à elle basée sur un protocole sécurisé. Le cryptage des documents est souhaitable lorsque les documents transitent sur des systèmes de stockage dont l'accès n'est pas protégé. Le cryptage des échanges est recommandé pour assurer que les documents ne seront pas interceptés et consultés par des tiers au delà de la durée de l'échange.

Intégrité des documents durant les transmissions

L'intégrité des documents peut à l'instar de la confidentialité être garantie par la protection du document ou du canal de l'échange selon les mêmes mécanismes. A cette fin, la mise en œuvre de protocoles de transfert sécurisé est souhaitable (cf. §.2.7.3 Transmission).

Identification vérifiée des personnes et rôles

La vérification de l'identité des personnes, ou des systèmes a pour objectif de garantir que la transaction d'échange s'est effectuée selon des modalités pré-établies quant à l'identité des personnes devant participer à l'échange. Lorsque l'échange est soumis à certaines obligations sur le contenu ou la date de l'échange, l'enregistrement de l'identité des personnes permet de garder une trace de l'échange engageant la responsabilité des parties. Cet enregistrement ou trace pourra être utilisé en cas de conflit.

Afin de vérifier l'identité des personnes, la signature électronique basée sur un certificat matériel ou logiciel pourra être utilisée.

Authenticité des documents transmis (vérification de la signature électronique)

Garantir qu'un document dématérialisé est authentique consiste à vérifier que la signature apposée sur le document est valide. Dans cette perspective, le signataire appose une signature électronique sur le document. La validité de la signature est dans un deuxième temps vérifiée pour attester que la signature électronique est toujours valide (le certificat n'ayant pas été répudié). A contrario, la vérification consistant à valider que le signataire a bien les droits lui permettant de signer le document ne peut pas être réalisée sans la mise en place d'un référentiel des personnes, de leur rôles et des pièces échangées. Cette vérification impose de facto la modélisation de l'ensemble des procédures d'échanges impliquant la vérification de l'authenticité de la signature.

Afin d'assurer la sécurité des échanges il est recommandé :

- de s'appuyer sur les protocoles sécurisés pour la confidentialité et l'intégrité des échanges,
- d'utiliser les certificats logiciels pour la signature électronique des documents,
- de mettre en place un système d'horodatage et de séquestre pour les échanges de documents engageant la responsabilité des parties à défaut d'une convention entre les partenaires éliminant cette obligation.

Afin de garantir l'intégrité des documents indépendamment de l'échange il sera nécessaire :

- de protéger les documents en modification, éventuellement complétés par un mot de passe,
- d'assurer une gestion des accès sur les systèmes de stockage de ces documents.

Les certificats sélectionnés devront être référencés dans le cadre de la Politique de Certificat-Type du MINEFI, qui correspond au niveau « fort » de la Politique de Référencement Intersectorielle de la Sécurité (PRI) de l'ADAE.

La liste des certificats effectivement référencés par le MINEFI est publiée à l'adresse suivante :

http://www.minefi.gouv.fr/dematerialisation_icp/dematerialisation_declar.htm

La PRI de l'ADAE est publiée :

http://www.adae.gouv.fr/article.php3?id_article=220

La signature de document ou tout autre procédé issu d'autres certificats ne pourra être reconnue comme ayant une valeur probante.

2.7.6 Recherche

Les documents dématérialisés sont susceptibles d'être recherchés en vue de leur utilisation (contrôle, modification,...). La recherche s'appuie d'abord sur le système d'identifiant unique, de référencement et d'indexation qui identifie tout document dématérialisé. Toutefois, lorsque le référencement ne permet pas de retrouver l'information recherchée (référence inexistante ou erronée, contenu non référencé), un outil de recherche s'appuyant sur l'indexation pourra être mis en oeuvre. Cet outil de recherche s'appuiera dans l'ordre sur :

- le nom du fichier,
- un ensemble de mots-clefs ou champs statiques défini lors de l'enregistrement du fichier,
- le contenu du document basé sur une indexation réalisée en amont de la recherche (indexation statique) ou lors de la recherche.

Lorsque l'outil de recherche est en charge d'explorer les documents, le choix des formats de fichiers est primordial pour garantir qu'il saura les exploiter.

La recherche peut s'effectuer à distance (interface Web) mais impose que les indexes et le moteur soient localisés sur un même site. Dans ce cas l'unification des moyens d'indexation et de recherche des pièces dématérialisées est donc un pré requis.

La constitution d'une cible commune pour les règles d'indexation, les critères retenus et le corpus des mots clés est à privilégier. La réalisation d'indexes particuliers pour la recherche d'informations spécifiques (à un métier) sera précisée dans les conventions par type de flux, et pourra être complétée à l'initiative des partenaires en ayant l'utilité.

2.7.7 Archivage

Les supports pour l'archivage des documents peut être différent de celui utilisé pour le stockage durant leur période d'activité. Le choix du support doit se faire en fonction de plusieurs critères : capacité de stockage du dit support, facilité et/ou vitesse de la restitution, coût du média, irréversibilité du support...

Ainsi, un support de type bande peut être envisagé pour des raisons de coûts. Quelque soit le support choisi, il convient de s'assurer que les données pourront être extraites de leur support et exploitées sur une durée de 10 ans à compter de la fin de l'exercice auquel les opérations comptables et les pièces dématérialisées associées, se rapportent.

Pour répondre à ce besoin, le système d'archivage doit également assurer la compatibilité des documents archivés avec les applications permettant de les exploiter. A cette fin, deux stratégies principales sont envisageables :

- faire évoluer les documents sur les versions ultérieures compatibles,
- archiver les applicatifs permettant d'exploiter les documents dans leur version initiale.

Concernant cette dernière option, il convient néanmoins de noter que l'évolution rapide du matériel et des systèmes d'exploitation rend sa mise en oeuvre difficile sur de longue durée.

La nécessité de stocker des objets comptables et d'en garantir la conservation sur de longue durée, conduit aujourd'hui à privilégier l'archivage sur une composante optique. Dans le cadre d'une conformité avec la norme NF Z42-013, « *Seul des supports WORM, tels que définis au paragraphe 3.7 de la norme Z42-013, sont admis pour réaliser les opérations de stockage des documents électroniques. Ces documents doivent comporter d'origine un numéro d'identification unique introduit par le fabricant.* », on se limitera aux disques non réinscriptibles.

Quelque soit le support d'archivage choisi, il est aussi nécessaire de se conformer aux recommandations techniques concernant les conditions de sa conservation, **en se référant aux documents suivants** : norme ISO FDIS 11799 Information et documentation – Prescriptions pour les magasins d'archives et de bibliothèques, 2003 ; norme AFNOR NZ 42011-2 sur les CD-R .

2.7.8 Destruction

Tout document ayant achevé son cycle de vie et n'ayant donc plus d'utilité en tant que justificatif, peut être détruit. A l'issue du cycle de vie du document déterminée par la fin du délai d'archivage, le document pourra être détruit ainsi que toutes les copies, références et indexes qui lui sont associés.

Dans le cas de certains documents considérées comme des archives publiques leurs destructions peuvent être conditionnées par un visa accordé par l'administration des archives (services des archives nationales, services des archives territoriales en région, département, dans les villes...).

3. Principes spécifiques par support d'échange

Les échanges dans le secteur public local sont multiples et recouvrent de ce fait différentes formes. L'analyse proposée pour la dématérialisation s'appuie une typologie des flux fondée sur le type de support d'échange des informations : le papier, le CD-Rom ou le flux électronique.

L'ensemble des principes énoncés précédemment s'applique aux flux présentés ci-après sauf mention explicite.

3.1 Le support papier

3.1.1 Caractéristiques générales

Les documents papiers actuellement utilisés continueront d'exister pour partie en raison du délai nécessaire à la mise en place d'une dématérialisation concertée et généralisée. Par ailleurs certaines pièces ne pourront pas être dématérialisées pour des raisons de coût ou de faisabilité. Aussi, la cohabitation des documents sous les formes papier et électronique reste inéluctable à moyen terme.

3.1.2 Solutions globales identifiées

Peu d'éléments communs seront partagés par les documents dématérialisés et les versions papiers ne serait-ce qu'au regard du compte de gestion. Il est ainsi nécessaire de maintenir un lien entre les systèmes informatiques et les documents papier. La mise en œuvre d'un référencement des documents papier et leur intégration dans les systèmes de gestion des documents dématérialisés est à prévoir.

3.1.2.1 Recommandations

Le principe de l'identifiant unique pour les documents dématérialisés devra être appliqué pour les pièces « papier ».

Le support papier limite les interactions possibles avec les systèmes informatiques. Le référencement de la pièce papier permet d'identifier et de localiser la pièce. La scannérisation n'étant pas

globalement recommandée, la référence de la pièce est le seul élément dématérialisé du document. Dans ce cas, l'indexation, la recherche ou l'accès à distance ne sont pas envisageables.

3.2 Le support CD-Rom

3.2.1 Caractéristiques générales

On entend par l'appellation "CD-ROM", un CD-R enregistré au format CD-ROM.

Bien que cette solution ne soit pas intrinsèquement la plus optimale du point de vue de la dématérialisation, car nécessitant une ou plusieurs interventions humaines, il convient néanmoins d'adopter une démarche pragmatique. En effet, intégrer l'ensemble des collectivités dans un écosystème de stockage et d'échange électronique, nécessitera du temps au regard de la quantité d'acteurs et de sites impactés. La production de CD-Rom, à partir d'outils bureautiques propres aux collectivités locales, est donc une alternative à recommander qui s'inscrit dans la démarche d'une dématérialisation de documents en tant que première approche. De plus, cette solution permet de répondre aux conditions strictes fixées par la réglementation afin de satisfaire à la présomption de fiabilité d'un document électronique dans la durée.

3.2.2 Solutions globales identifiées

3.2.2.1 Règles générales

Les moyens de transmission seront identiques à ceux utilisés pour les transmissions des documents papier actuels. Le CD-Rom devra comporter un identifiant unique non modifiable, numéro incluant l'identifiant de l'organisme « émetteur », la date de production, le numéro d'ordre de production chez l'émetteur. S'agissant de données comptables, il comportera aussi les mentions du nom de l'ordonnateur, du poste comptable assignataire, du budget et de l'exercice concernés, ainsi que de la date d'édition.

Comme indiqué au § 4.1, ces supports seront également susceptibles d'être référencés au travers du Protocole d'Echange Standard (PES) du progiciel Hélios, dès que l'implémentation de ce référencement sera effective au sein du PES.

Une fois édité, le CD-Rom ne devra être accessible qu'en lecture et toutes possibilités de réinscription et de modification des informations initialement gravées, devront être exclues. Les plages inutilisées du CD-Rom devront être neutralisées.

La validité CD-Rom devra être certifiée par l'émetteur au travers d'un des dispositifs suivants :

- une signature (indélébile) sur le support lui-même,
- une signature électronique présente sur le cdrom utilisant les certificats référencés,
- ou un bordereau signé certifiant la validité de son contenu, mentionnant l'identifiant unique et précisant le résultat d'une opération de checksum MD5 sur les données du cdrom.

3.2.2.2 Conditions

Les conditions d'utilisation sont liées au respect des principes de l'identifiant unique (cf. § 2.6.3). En particulier, les documents accessibles depuis le CD-Rom devront pouvoir être recherchés à minima à partir de leur identifiant unique.

Le CD-Rom peut être fourni avec son logiciel d'exploitation permettant la recherche de documents selon plusieurs critères de type « texte » ou « numérique », en particulier dans le cas où le volume de documents est important.

A l'issue de l'opération de gravage, il convient de réaliser systématiquement une vérification permettant de s'assurer que toutes les données ont bien été gravées et sont bien lisibles. Cette vérification est en général une fonctionnalité des logiciels de gravage, mais il convient donc de l'activer systématiquement.

3.2.2.3 Limitations

Elles sont essentiellement relatives à la capacité de stockage du support physique et à la mise en œuvre de système de classement de CD-Rom (jukebox) au sein des divers organismes de la chaîne de dématérialisation. De plus, ce type de flux nécessite tout comme le flux papier, un certain nombre d'interventions humaines (réception, stockage, ...) avant l'utilisation du contenu proprement dit.

3.3 Le support « Electronique »

Le support « électronique » constitue le support d'échange préférentiel car le mieux à même de permettre une automatisation de bout en bout du processus, entre les différents partenaires. En particulier, l'échanges de données selon des formats standards permettra une intégration complète et automatisée entre les systèmes d'information des différents partenaires.

Par support électronique, on entend toutes les solutions ne faisant pas appel à un support d'échange matériel et dédié tel que le papier et le CD-Rom. Ainsi, les supports électroniques servant à l'échange inter ou intra système d'information, sont :

- les systèmes de fichiers,
- les systèmes de transfert et d'accès distant,
- les systèmes de messagerie,
- les solutions de gestion électroniques de documents ou de gestion de contenu.

3.3.1 Les systèmes de fichier

Les systèmes de fichiers permettent pour les utilisateurs locaux d'un système d'information d'échanger et d'accéder à un certain nombre de documents classés et triés à l'aide d'une arborescence de dossiers, sous-dossiers. Ce type de solution est principalement accessible aux utilisateurs d'un même système d'information. Il permet donc de répondre au besoin d'un support pour la dématérialisation, uniquement dans le cas où les partenaires peuvent travailler sur un même système local. Par la mise en place d'un accès distant, ce système peut toutefois être ouvert à des partenaires.

3.3.2 Les systèmes de transfert et d'accès distant

Le système de transfert et d'accès distant, basés sur des technologies de type FTP, HTTP+WebDav pour les protocoles de transfert et type VPN pour les réseaux autorisent des partenaires à se connecter ponctuellement sur un système d'information pour y déposer ou récupérer des données ou documents. Dans ce cas, l'extension de transfert et d'accès distant permet d'étendre le système d'information - donc son système de fichier - vers des tiers. Par delà les passerelles de connexion et les protocoles de transfert, la logique de l'échange reste toutefois basée sur le système de fichier natif.

3.3.3 Les messageries électroniques

Les messageries électroniques peuvent être utilisées comme moyen d'échange par attachement des documents aux messages électroniques. Ce type de système, largement répandu, peut ainsi constituer un des vecteurs de l'échange. Les normes MIME et S/MIME garantissent un niveau d'interopérabilité pour les documents échangés au travers des messageries supportant ces normes. Toutefois dans la perspective de la mise en œuvre d'une messagerie pour le transfert de documents, il pourra être nécessaire de créer et gérer des boîtes aux lettres dédiées aux rôles et non aux personnes, afin :

- de réorienter les flux en cas de changement de personne ou pour une délégation temporaire,
- ou d'automatiser des actions sur les boîtes aux lettres telles que re-directions, réponses automatiques, multi-diffusion.

Une fois reçues ou transférées, les pièces devront être reversées sur le système de fichier afin de bénéficier de ses fonctionnalités natives et d'en assurer ainsi la pérennité (notamment pour bénéficier de la sauvegarde) et l'accès à plusieurs utilisateurs.

3.3.4 Principes communs

Les systèmes d'échange identifiés précédemment diffèrent par les modes de transfert des documents : copie locale, copie distante, pièce jointe. Néanmoins après transfert, les documents sont stockés sur système de fichier et s'appuient donc sur les fonctions natives de ce dernier. Dans ce contexte, les principes transverses évoqués en section 2.5 (Format, stockage, sécurité, recherche, etc) sont à mettre en œuvre de manière homogène pour l'ensemble des partenaires partageant un même système de fichier pour leurs échanges. A défaut, il est nécessaire de mettre en place des passerelles de transformation et d'adaptation entre systèmes non homogènes (identifiants, classification, etc).

Afin d'élargir les fonctionnalités offertes par les systèmes de fichiers sans avoir à en assurer la conception, le développement et la maintenance, les systèmes de Gestion Electronique de Documents peuvent être une voie à envisager.

3.3.5 Les solutions de GED ou gestion de contenu

Les systèmes de Gestion Electronique de Documents (GED) visent à gérer le cycle de vie complet des documents (ou données) au sein d'une entité. Pour y parvenir, ces systèmes autorisent la gestion de documents ou données sous différentes formes autour d'un référentiel ; ils permettent alors d'en assurer le suivi, la recherche, la manipulation et la transformation. Ainsi trois fonctionnalités principales peuvent être distinguées, ce sont :

- l'acquisition qui permet de créer ou d'intégrer des documents ou données sous différentes formes en entrée du système de GED,
- la gestion, bâtie autour d'un référentiel permettant de stocker, d'indexer, de gérer les versions, d'archiver et d'établir les recherches de toute donnée ou document,
- la restitution qui par le biais d'outils de transformation autorise la sortie d'un document sous un format différent de celui qu'il avait en entrée.

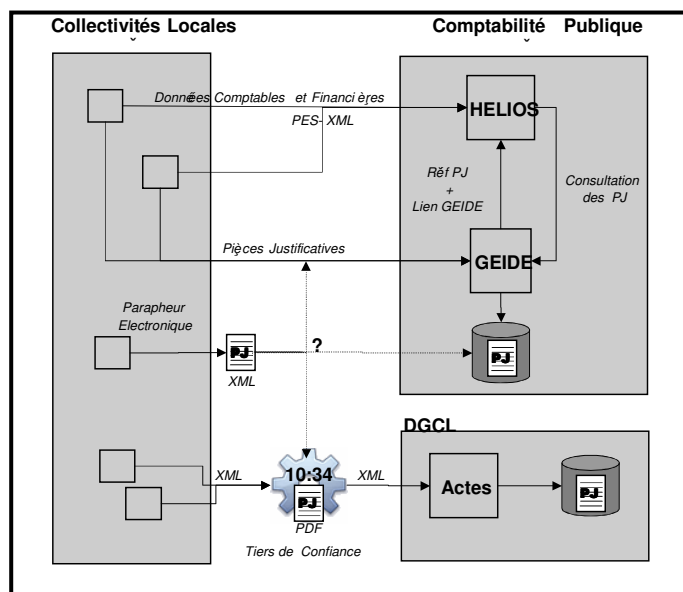
Par ailleurs, des fonctionnalités complémentaires telles que le workflow pour la prise en charge automatisée de certains traitements sur un lot de document ou une partie de la chaîne comptable et financière, peuvent venir enrichir ces fonctionnalités. En complément, des modules spécialisés répondent à des besoins spécifiques ou des solutions métiers.

Ainsi les systèmes de type GED proposent un cadre technique général capable de gérer des échanges de documents sur la base d'outils intégrés. Ce type de système constitue donc une solution globale pour les échanges multiformes entre partenaires. Toutefois les principes transverses (formats, identifiant, indexation, critères de recherche, etc) régissant les échanges restent à définir, le système GED assurant la flexibilité nécessaire et l'homogénéité d'ensemble pour la cohabitation simultanée de plusieurs de ces principes.

4. Les projets majeurs de la dématérialisation

Plusieurs projets sont menés par les collectivités locales, les établissements publics locaux (EPL) et la DGCP pour la dématérialisation partielle et progressive de catégories de pièces ou d'échanges. Parmi ces projets, **certains partagent la caractéristique commune d'offrir des solutions génériques présentant des perspectives de convergence et de complémentarité**. Les principaux projets identifiés à ce jour, sont présentés dans les pages suivantes :

- Le Projet PES Hélios,
- Le Projets Actes de la DGCL,
- Le Projet Parapheur Électronique (AMF),
- Le Projet GEIDE-DGCP Amiens.



Présentation des Projets de Référence pour la Dématérialisation

Une liste complémentaire des expérimentations en cours dans le secteur public local est présentée dans la section suivante. D'autres expériences génériques pourront à l'avenir abonder les solutions préférentielles recommandées dans ce Cadre national d'acceptation. Le schéma ci-après présente les champs d'investigation de chaque projet

4.1 Intégration de la dématérialisation au PES Hélios

Dans le cadre du programme Hélios, les données comptables et financières générées par les applicatifs des collectivités locales et des établissements publics locaux sont structurées selon le Protocole d'Échange Standard (PES) et transférées dans le système Hélios au travers de différents canaux de communication (CFT, disquette, ...). Les données échangées entre ordinateurs et Hélios sont structurées en fichiers XML qui sont, après transmission et contrôle, intégrées dans le progiciel Hélios.

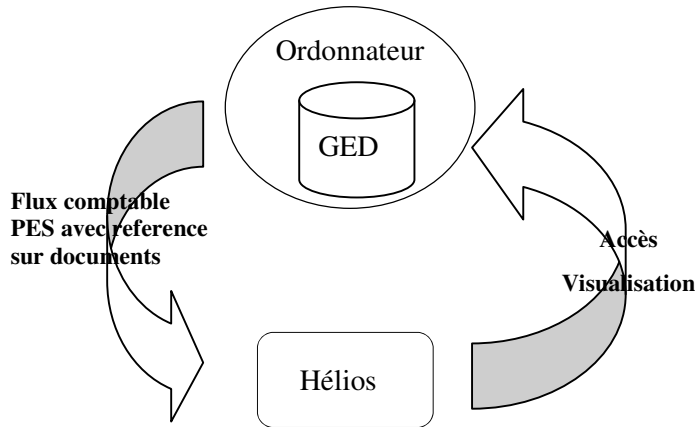
Dans sa première version, le PES ne prévoit pas le transfert de documents justificatifs dématérialisés.

Dans la perspective d'un attachement des documents justificatifs à des fins de contrôle, la prise en compte des pièces justificatives dans le flux comptable est prévue dans la version 2.0 du PES. Cet attachement aura d'autant plus d'intérêt que les pièces justificatives seront dématérialisées.

Hélios constituera donc un accélérateur de la dématérialisation des pièces justificatives, au fur et à mesure que les collectivités et établissements adopteront le PES pour leurs échanges. Cette dématérialisation pourra être réalisée autour deux principaux modèles :

4.1.1 Modèle de stock

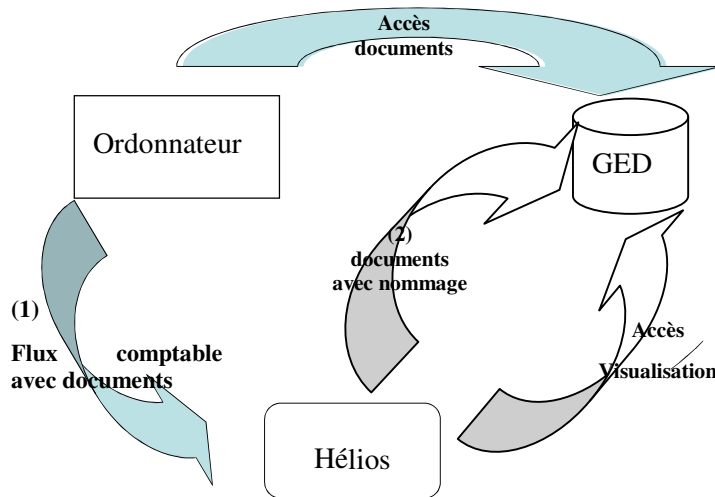
L'ordonnateur ayant la responsabilité du stockage (puis de l'archivage) de ses pièces, il paraît plus pertinent de privilégier l'intégration dans le PES d'une référence de la pièce justificative plutôt que du contenu du document lui-même. Il s'agit alors d'un modèle où le document est stocké chez l'ordonnateur, ce qui implique la mise en œuvre d'un accès sécurisé de la DGCP-Hélios au document de l'ordonnateur via une authentification partagée. Les échanges de ce modèle sont représentés dans le schéma ci-dessous.



Cette approche « simple » nécessite de prévoir la production par l'ordonnateur d'un CD-Rom pour la remise du compte de gestion au comptable pour la CRC.

Une variante de ce modèle, dit de « stock par tiers », consiste en la sous-traitance du stockage à un tiers (prestataire ou plateforme de collectivité locale telle celle du projet de la Région Bourgogne).

4.1.2 Modèle de flux



Dans le cas où l'ordonnateur ne fournit pas un accès cohérent et uniforme à ses pièces justificatives dématérialisées, il est nécessaire que les pièces justificatives soient transmises simultanément au flux comptable PES. Il s'agit alors d'un modèle « de flux ».

Ce modèle permet à l'ordonnateur de transmettre, une fois pour toute, le document avec le flux comptable, sans se préoccuper par la suite de ses modalités d'accès et de stockage. Il convient cependant de noter que ce modèle a un impact significatif sur la volumétrie « réseau » échangée entre Hélios et l'ordonnateur et sur les besoins de stockage associé à Hélios.

4.1.3 Modèle transitoire à flux parallèle

Dans l'attente de la version 2.0 du PES, le document dématérialisé pourra être transmis et stocké indépendamment des données comptables et financières transmises via le PES (flux parallèle).

Quelle que soit la nature de l'hébergeur des pièces justificatives, cette situation oblige néanmoins à la communication de fichiers « indexés » à Hélios permettant de rapprocher les objets « comptables » Hélios avec les pièces dématérialisées. Ce modèle correspond à la solution « type » GED du DI Amiens (cf. § 4.4).

4.1.4 Principe de référencement des pièces justificatives dans Hélios

La référence entre les données comptables et financières transmises par le PES et les pièces justificatives doit permettre d'établir un lien figé et non modifiable, garant de la sincérité des informations échangées au travers des deux fichiers.

Cette référence sera fondée sur l'identifiant unique de la pièce justificative dématérialisée, associé à l'identifiant de la collectivité et/ou de l'hébergeur.

Si le lien entre les données Hélios et les pièces justificatives, établi par un référencement, est un pré-requis, l'exploitation de ces pièces pour un contrôle n'en est pas pour autant garantie.

Quelque soit le système choisi pour transmettre et stocker ces documents, il est aussi nécessaire d'établir un lien entre le fichier référencé et sa localisation physique. Pour exploiter la référence sur la pièce dématérialisée, l'hébergeur devra stocker les pièces sur un système unifié permettant d'activer un lien actif entre la référence Hélios et la localisation physique de la pièce dématérialisée (serveur local de fichier, http, système GED, Juke-box...)

Après modification du PES afin d'y inclure une référence active vers le document, il sera possible de visualiser depuis Hélios la pièce justificative, par l'intermédiaire d'outils adéquats (Reader PDF, navigateur Web,...).

4.2 Le Projet « Actes » de la DGCL

L'objectif du projet mené par la Direction Générale des Collectivités Locales (DGCL) consiste à dématérialiser la transmission des actes de délibération des collectivités vers leur préfecture de rattachement en utilisant une infrastructure d'échange sécurisée.

L'infrastructure d'échange sécurisée se charge des opérations d'authentification, de réception, de validation, d'horodatage et d'archivage des pièces avant leur transmission sécurisée vers le serveur de la préfecture. Un workflow assure, en interne du serveur de preuve, l'enchaînement des opérations pour chaque pièce transmise. Chaque pièce est accompagnée d'un bordereau de télétransmission au format XML. Les transmissions sont cryptées par le protocole SSL (Secure Socket Layer). Le serveur assure la garantie de transmission vers le serveur du Ministère de l'Intérieur (support des notifications et remontée des anomalies).

La solution mise en œuvre dans le cadre du projet « Actes » permet la transmission de documents dématérialisés dans des conditions sécurisées. L'utilisation des certificats électroniques permet de garantir l'identité des parties impliquées, la confidentialité et l'intégrité des documents échangés. Par ailleurs le service d'horodatage permet la trace sécurisée des échanges pour authentifier le respect de certains délais, la signature revêtant un caractère exécutoire.

La solution mise en œuvre sur le projet « Actes » permet de répondre aux besoins de transfert sécurisé des échanges entre les collectivités locales et leur préfecture. Ce canal de transmission permet d'acheminer ainsi par voie électronique des données depuis les collectivités.

Perspectives

Les documents soumis au contrôle de légalité de façon dématérialisée, et ceux d'entre eux qui doivent être joints aux mandats et titres de recette comme pièces justificatives, relèvent de circuits différents. Si les premiers sont transmis au Préfet, une partie seulement de ceux-ci constituent des pièces

justificatives à adresser au comptable du Trésor par l'ordonnateur. Dans ce dernier cas, l'ordonnateur certifie, sous sa propre responsabilité, le caractère exécutoire de l'acte conformément à l'article 2131-1 du CGCT. Ces pièces justificatives sont adressées au comptable indépendamment de leur réception par le Préfet concerné dans le cadre du contrôle de légalité.

Quant aux documents « budgétaires » transmis au préfet et au comptable, la convergence de la DGCP et la DGCL vers une même solution évitera aux collectivités de transmettre plusieurs fois un même document. Ceci nécessitera préalablement un accord sur le format des documents « budgétaires », format permettant leur exploitabilité, et sur le schéma de transit des documents.

Plus généralement, les infrastructures d'échange sécurisée constituent une solution rapidement disponible pour la télétransmission des documents sécurisés. La possibilité d'utiliser une telle infrastructure à des fins d'échanges des pièces justificatives entre la collectivité et le comptable, ou à des fins de stockage pour le compte de la collectivité devra être étudiée.

4.3 Les Projets de « parapheur électronique »

Un certain nombre de collectivités locales expérimentent actuellement des projets de parapheurs électroniques (Ville Metz, CG Val d'Oise, ...).

Notamment le projet expérimental mené par la communauté de communes des CHATAIGNIERS et le SYCTIAM en liaison avec l'Association des Maires de France (AMF) vise à fournir aux collectivités locales un outil de communication de documents dématérialisés : le « parapheur électronique ».

Cet outil permet l'échange de documents entre les représentants d'une même collectivité. A l'instar d'un parapheur, il permet de transmettre un ensemble de documents à différents destinataires pour traitement. Exportés dans leur format natif depuis les applicatifs, les documents sont ainsi véhiculés par le parapheur depuis leur production jusqu'à leur traitement final (envoi, stockage, ...). Comparable à une messagerie électronique doublée d'un workflow, le parapheur permet ainsi de gérer et contrôler les différentes étapes du traitement d'un document. Chaque membre de la collectivité est doté d'une boîte à lettre permettant l'envoi et la réception des documents. Le « parapheur électronique » autorise la signature des documents sur la base des certificats X509.

Le « parapheur électronique » permet d'une part, la production de documents dématérialisés depuis les progiciels des collectivités et d'autre part, d'assurer la gestion de leur cycle de vie au sein des collectivités.

De surcroît, le « parapheur électronique » prend en compte le besoin de signature électronique de certaines pièces et en assure le support par l'emploi de certificats.

Ce projet se présente, dans ses ambitions actuelles, comme **un complément des projets Hélios et Actes**. Il permet de générer les pièces éventuellement signées au sein des collectivités. Ces pièces peuvent être, après production, référencées voire transmises en même temps que les données transitant via le PES. Pour les documents signés ou protégés nécessitant un canal de transmission sécurisé, l'intervention d'un tiers de confiance (tel qu'il intervient dans « Actes ») assurant l'horodatage pourra être un canal de transmission complémentaire.

Afin d'assurer les échanges des documents issus du parapheur vers Hélios il est nécessaire :

- d'intégrer au projet « parapheur électronique » le principe de l'identifiant unique pour chaque document produit par l'ordonnateur ;
- de vérifier la faisabilité du référencement de la pièce dans Hélios ;
- de vérifier l'interopérabilité des formats générés, transmis et exploités.

4.4 Le Projet GEIDE de la DGCP (Amiens)

La GEIDE (Gestion Électronique d'Information et de Documents Existants) regroupe l'ensemble des outils et procédures simples de gestion électronique de documents : transmission, workflow attaché au document, archivage avec index, recherche et consultation, conservation des documents, extraction des documents.

La première expérimentation menée par la DGCP (département informatique d'Amiens) a porté sur la gestion du dossier des pensionnés de l'Etat en région Picardie. Le projet de GEIDE a ensuite été étudié pour la dématérialisation des titres de recettes de la ville du HAVRE (30 000 titres de recettes par an).

Ce service de GEIDE constitue une solution de dématérialisation de premier niveau (avec de très faibles impacts sur l'existant chez l'ordonnateur) et se caractérise par l'émission d'un flux « Cold », généré par la ville du HAVRE à partir des titres de recettes. Par ailleurs, le service de GEIDE permet l'édition et l'envoi à la CRC de CD-Rom contenant les titres de recettes, avec des fonctionnalités de consultation autonome et de recherche par critères. L'exploitation de l'application GEIDE est faite sur un site dédié identique à celui de l'application Hélios.

4.5 Les principales expériences de dématérialisation

4.5.1 Les expérimentations de dématérialisation

A ce jour, près de 150 conventions de dématérialisation ont été signées entre des ordonnateurs du secteur public local et leur comptable du Trésor, après visa de la Chambre Régionale des Comptes (CRC) compétente. Parmi ces expérimentations en cours dans le secteur public local, on peut citer quelques projets qui constituent des solutions « référencées », dans la mesure où ils ont largement anticipé la prise en compte des principales normes du présent Cadre national d'acceptation (ces expérimentations sont citées de façon non exhaustive) :

- Le Département des Yvelines a mis en œuvre une dématérialisation des bulletins de paye sous forme de fichier de données transmis au comptable mensuellement ; le Département de l'Aube et le Service Départemental d'Incendie et de Secours pour la dématérialisation de la paye, ont retenu une solution mixte associant fichier de données et reconstitution de fac-similés des bulletins de salaire, les données numérisées étant transmises au comptable mensuellement et à la CRC sur CD-Rom ; la Ville et le Département de PARIS, avec la Recette Générale des Finances de PARIS, ont mis en place une solution proche de la précédente pour la dématérialisation de la paye (solution de GED).
- Les CHU de MONTPELLIER, de NANTES, d'ANGERS, comme près d'une centaine de centres hospitaliers, ont mis en œuvre une dématérialisation des titres de recettes. Ces expérimentations s'inscrivent dans le cadre de l'instruction du 14 février 2002 de la DGCP qui, avec l'accord du juge des comptes, pose un cadre standard applicable aux collectivités et établissements publics locaux pour promouvoir un déploiement cohérent et accéléré de ce dispositif. La dématérialisation des titres de recettes a aussi été mise en œuvre par l'OPAC d'Indre et Loire, la ville et le Département de PARIS.
- Le Conseil Régional de Bourgogne, au delà de la dématérialisation des appels d'offres des marchés publics, va mettre en œuvre des solutions de dématérialisation des titres de recettes (CD-Rom ez-Php/MySQL) et des bulletins de paye et développer une plate-forme pour les collectivités locales et EPL de la région.

4.5.2 Procédures à mettre en œuvre pour le lancement d'expériences de dématérialisation

Afin de garantir le succès des nouvelles expérimentations de dématérialisation initiées dans le secteur public local, il est conseillé d'appliquer les règles suivantes :

- Le lancement d'une nouvelle expérimentation doit faire l'objet au préalable, d'un projet de convention entre les partenaires, après étude conjointe de la solution de dématérialisation envisagée ;
- Le périmètre du projet ainsi que les solutions techniques mises en œuvre devront, lorsque l'étude sera finalisée, être présentés au Pôle national de la Dématérialisation de la DGCP pour validation, notamment au regard du présent Cadre national d'acceptation ;
- Le Pôle national de la Dématérialisation apportera à cette occasion le soutien et l'accompagnement nécessaire, aux services de l'ordonnateur et au comptable ;

- Il est largement conseillé d'associer la CRC à la réflexion dès que le projet de dématérialisation est suffisamment défini ;
- La convention locale de dématérialisation est ensuite soumise à l'aval de la CRC et in fine signée par l'ordonnateur et le réseau du Trésor.

Rapidement, le Pôle national de la Dématérialisation va définir des conventions « type » pour chacun des grands flux de documents papier répétitifs (paye, titres de recettes, mandats, pièces justificatives des marchés publics, etc...), en concertation avec les représentations nationales des partenaires concernés (AMF, ADF, ARF, FHF, FOHLM, Cour des comptes). Ainsi, les projets de dématérialisation, respectant ces conventions nationales type, pourront être mis en œuvre plus rapidement.

5. Annexe : Références des sources d'informations

- Norme Afnor NF Z42-013, relatives à la conception et à l'exploitation de systèmes informatiques pour conservation et intégrité des documents.
- Norme ISO FDIS 11799 Information et documentation – Prescriptions pour les magasins d'archives et de bibliothèques, 2003
- Norme AFNOR NZ 42011-2 sur les CD-R
- ADAE, dans le cadre de son action dans le domaine de la dématérialisation. Domaine interministériel de l'administration électronique (Actions normatives)
- DGCP - GEIDE Amiens
- DGCP - 3ème sous direction
- DGCL - cadre de collaboration DGCP / DGCL - Charte fonctionnelle de service
- AMF - Parapheur Électronique (Microsoft)
- Diverses conventions de service comptables et financières (CSCF)
- Domaine hospitalier, Offices HLM
- Cour des comptes - Projet de stockage
- État de l'art du marché de la dématérialisation & mises en oeuvre