LA DEMATERIALISATION DES PROCEDURES DE MARCHES PUBLICS

Institut d'études politiques de Bordeaux

DESS « Management des organisations et entreprises de service public »
Philippe Ruiz - Année 2002-2003
Sous la direction du Professeur H.G. Hubrecht et de M. Henri Perrier

«Le véritable voyage de découverte
ne consiste pas à chercher de nouveaux paysages,
mais à avoir de nouveaux yeux.»

Marcel Proust

"J'ai montré sans cesse la technique comme étant autonome, je n'ai jamais dit qu'elle ne pouvait pas être maîtrisée."

Jacques Ellul

SOMMAIRE

1. comment penser la dématérialisation ?

1.1 Le sens des mots : étymologie de la dématérialisation

Les définitions reprises ci-dessous proviennent du site d'analyse et traitement informatique de la langue française[1], relié au « trésor de la langue française informatisé (TLFi) »

DÉMATÉRIALISATION, subst. fém.
Action de dématérialiser, résultat de cette action.
Action ou fait de rendre immatériel, d'ôter la matière concrète, les éléments matériels (…)

IMMATÉRIEL, **-ELLE**, adj.
Qui n'a pas de consistance matérielle, qui n'est pas formé de matière. Monde, produit immatériel; chose, forme, image, richesse immatérielle.

Il ressort de ces définitions que ne peut être dématérialiser que ce qui existe matériellement. Le procédé utilisé en matière informatique est la numérisation. Cela consiste en une transformation de donnée matérielle (ici un support écrit) en une suite de chiffres dit binaire car composé de deux valeurs : 0 ou 1. La numération binaire est à la base de toute l'informatique. Ce chiffre est appelé « bit » (de « binary digit » ou chiffre binaire) et est regroupé en une suite de 8 bits, formant un octet. Cette conversion en valeurs ou signaux numériques, équivalents du point de vue de l'information transmise au support matériel, permet un traitement informatique des données.

[1] http://atilf.atilf.fr/tlf.htm

1.2 Le droit interne

1.2.1 Code des marchés publics (CMP)[1].

D'après l'article 56, « Les échanges d'informations intervenant en application du présent code peuvent faire l'objet d'une transmission par voie électronique ». Cela concerne bien évidemment toutes les pièces mises à disposition des entreprises par l'administration (« *Le règlement de la consultation, la lettre de consultation, le cahier des charges, les documents et les renseignements complémentaires* » : art.56 §1) mais aussi les candidatures et les offres (art. 56 §2). De la même manière des enchères électroniques pourront être réalisées pour l'achat de fournitures courantes (art. 56 §3). Il est remarquable que le principe d'échanges d'information par voie électronique peut s'appliquer de la diffusion du DCE à la réception des offres, ainsi qu'à l'organisation des enchères électroniques.

1.2.2 Décrets d'application de l'article 56[2] du CMP

Le décret 2001-846 (cf. annexe 5.2), pris en application du 3° de ce même article, s'applique à encadrer la procédure d'enchères électroniques. S'il rappelle les obligations qui incombent à la personne publique en matière de sécurité (des transactions et des informations), il pose que l'organisation des enchères « *sur un réseau informatique accessible à tous les candidats de façon non discriminatoire* » est de son ressort. Le *décret 2002-692 (cf. annexe 5.3)* est pris en application des 1° et 2° de l'article 56 du CMP. Outre l'énoncé des pièces consultables et archivables par « *les personnes intéressées* » selon le type de procédure, ce décret en son article 5 impose aux candidats de choisir « *entre, d'une part, la transmission électronique de leurs candidatures et de leurs offres et, d'autre part, leur envoi sur un support papier ou, le cas échéant, sur un support physique électronique*. », la prise de connaissance préalable des différents documents par voie électronique ne les engageant pas à utiliser la même voie en retour (art 2). Enfin, la personne publique assure la sécurité des transactions sur un réseau

[1] **Décret 2001-210** du 7 mars 2001 portant code des marchés publics (JO du 8 mars 2001), puis d**écret 2004-15** du 15 janvier 2005 portant code des marchés publics (JO du 8 mars 2001) : rédaction identique de l'article 56

[2] **Décret n°2002-692** du 30 avril 2002 pris en application du 1° et du 2° de l'article 56 du code des marchés publics et relatif à la dématérialisation des procédures de passation des marchés publics et **décret n°2001-846** du 18 septembre 2001 pris en application du 3° de l'article 56 du code des marchés publics et relatif aux enchères électroniques

informatique accessible à tous les candidats de façon non discriminatoire (art.7) (principes de liberté d'accès à la commande publique et d'égalité de traitement des candidats). De même, la personne publique prend les mesures propres à garantir la sécurité des informations portant sur les candidatures et les offres (art. 8).

Ces décrets[1] permettent de distinguer deux types de support : le support électronique (via un réseau informatique) et le support physique (papier ou électronique). La dématérialisation est pensée jusqu'à la réception des offres (uniquement dans le cadre des relations entreprises-acheteurs), voire le choix d'une offre dans le cas des enchères électroniques.

La personne publique est responsable de la sécurité des transactions et des informations. Enfin, il est précisé que les pièces « dématérialisées » doivent être consultables et archivables.

La dématérialisation vise explicitement les rapports de la puissance publique avec les entreprises candidates. Les autres flux de documents ne sont pas traités, hormis l'envoi des avis d'appel public à la concurrence qui sont « adressés à l'organe de publication par tout moyen permettant de donner date certaine à l'envoi »

1.3 Le droit communautaire

1.3.1 Proposition de directive du Parlement européen et du Conseil

Relative à la coordination des procédures de passation des marchés publics de fournitures, de services et de travaux[2], une proposition de directive est en cours d'adoption. Dans l'exposé des motifs, les institutions européennes affichent leur soucis de modernisation, de simplification et de flexibilité : « *modernisation pour tenir compte de nouvelles technologies et des modifications de l'environnement technologique* ». Dès 1998[3], la Commission affichait l'objectif ambitieux de conclure 25% des marchés par l'intermédiaire de support électronique en 2003. Cette position relative aux achats électroniques était affirmée de nouveau en 2000[4].

[1] consultable sur le site www.legifrance.fr
[2] proposition devenue la directive 2004/18 CE
[3] « **communication sur les marchés publics dans l'Union Européenne** » du 11 mars 1998
[4] conclusions de la présidence du Conseil Européen de Lisbonne des 23 et 24 mars 2000

L'utilisation de la dématérialisation doit permettre d'atteindre un objectif d'efficacité (par la réduction des délais de passation) et de transparence des procédures de passation.

La mise en place d'un tel dispositif légal de dématérialisation permet d'aborder d'autres questions, en particulier celle du droit de la preuve et de la fiabilité d'une signature électronique.

1.4 questions liées à la dématérialisation

1.4.1 Droit de la preuve

Dès 2000[1], les dispositions légales d'adaptation du droit de la preuve aux technologies de l'information étaient prises : « La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission ».

A une seule condition : la fiabilité du procédé d'identification de la signature électronique. Cette fiabilité est présumée dès lors que « la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie . ». Toutefois, même si ces dispositions ne concerne que le code civil, et malgré une absence de renvoi explicite à cette loi dans le code des marchés publics, l'obligation d'assurer « par tout moyen » le principe de la mise en concurrence ainsi que l'affirmation selon laquelle « les dispositions du présent code qui font référence à des écrits ne font pas obstacles au remplacement de ceux-ci par un support ou échange électronique » (art. 56-4) permettent d'affirmer une identité de vue entre code civil (art 1316-1 : « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, (…). ») et code des marchés publics.

1.4.2 Signature électronique

1.4.2.1 Définition

Article 1316-4 du code civil

« Lorsqu'elle est électronique (la signature : NdR), elle consiste en l'usage d'un procédé

fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. »

Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique

Art. 1er. - Au sens du présent décret, on entend par :

1. « Signature électronique » : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil ;

2. « Signature électronique sécurisée » : une signature électronique qui satisfait, en outre, aux exigences suivantes :

- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable ;

(..) »

Une signature électronique est donc une donnée présumée fiable dans la mesure où elle est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie. Elle sera qualifiée de sécurisée si, de plus, elle est propre au signataire, créée par des moyens que le signataire puisse garder sous son contrôle exclusif, et que toute modification ultérieure de l'acte auquel elle se rattache soit détectable.

Ces définitions imposent d'encadrer la création d'une signature électronique, la vérification de celle-ci (authentification de l'origine des données, non répudiation de la source) ainsi que l'intégrité du document chiffré (objets des chapitres 1^{er,} , 2ème et 3ème du décret sus-visé). En ce sens, la signature électronique est à distinguer du scellement qui ne permet que l'authentification de l'origine des données et la vérification de l'intégrité des données, la non répudiation étant une qualité de la signature électronique.

A ce stade de notre propos, il paraît nécessaire de définir plus précisément les notions, générale, de cryptologie, et plus particulièrement celles de chiffrement, d'empreinte et de

[1] loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de

certificat électroniques. Nous aborderons ensuite l'aspect technique de la transmission de document.

1.4.3 Sécurité des transactions : cryptologie et transmission de document.

Le groupe de travail 6 de la mission économie numérique affirme dans son « Rapport des travaux conduits en 2002 »[1] que « l'utilisation de clés asymétriques et de leurs certificats associés permet de répondre aux besoins communs en matière de sécurité et de confiance des échanges :

- identifier l'utilisateur ;
- authentifier l'utilisateur, c'est à dire garantir que l'utilisateur est bien celui qu'il prétend être (même s'il n'est pas pour autant identifie), voire permettre l'authentification réciproque serveur/utilisateur ;
- signer, c'est à dire manifester son accord et s'engager sur le contenu d'une transaction, sans pouvoir ensuite la « répudier » ;
- assurer l'intégrité, c'est à dire s'assurer que le document signé, transmis et reçu n'a pas subi d'altération au cours de ces trois phases ;
- éventuellement, assurer la confidentialité par la possibilité offerte à l'utilisateur de chiffrer les documents signés, via une clé spécifique ou une session sécurisée d transmission. ».

L'utilisation de moyens cryptographiques est donc présenté comme la solution technique permettant de garantir « sécurité et confiance des échanges ». Après avoir défini plus précisément les notions mises en œuvre par la cryptographie, nous aborderons la question du vecteur de transmission de ces données cryptées.

1.4.3.1 Définitions

- **Cryptographie** n. f. XVIIe siècle. Composé à l'aide du grec kruptos, «caché », et graphein, « écrire ».Art d'écrire en langage codé, secret, chiffré. (*Dictionnaire de l'académie française, 9° édition*). Écriture secrète qui consiste généralement à transposer les lettres de l'alphabet ou à les représenter par des signes convenus, de manière à ce que le sens de l'écrit ne soit accessible qu'au destinataire en possession du code. (*TLFi*). La transformation du texte clair en texte chiffré (ou cryptogramme) est appelé chiffrement,

---

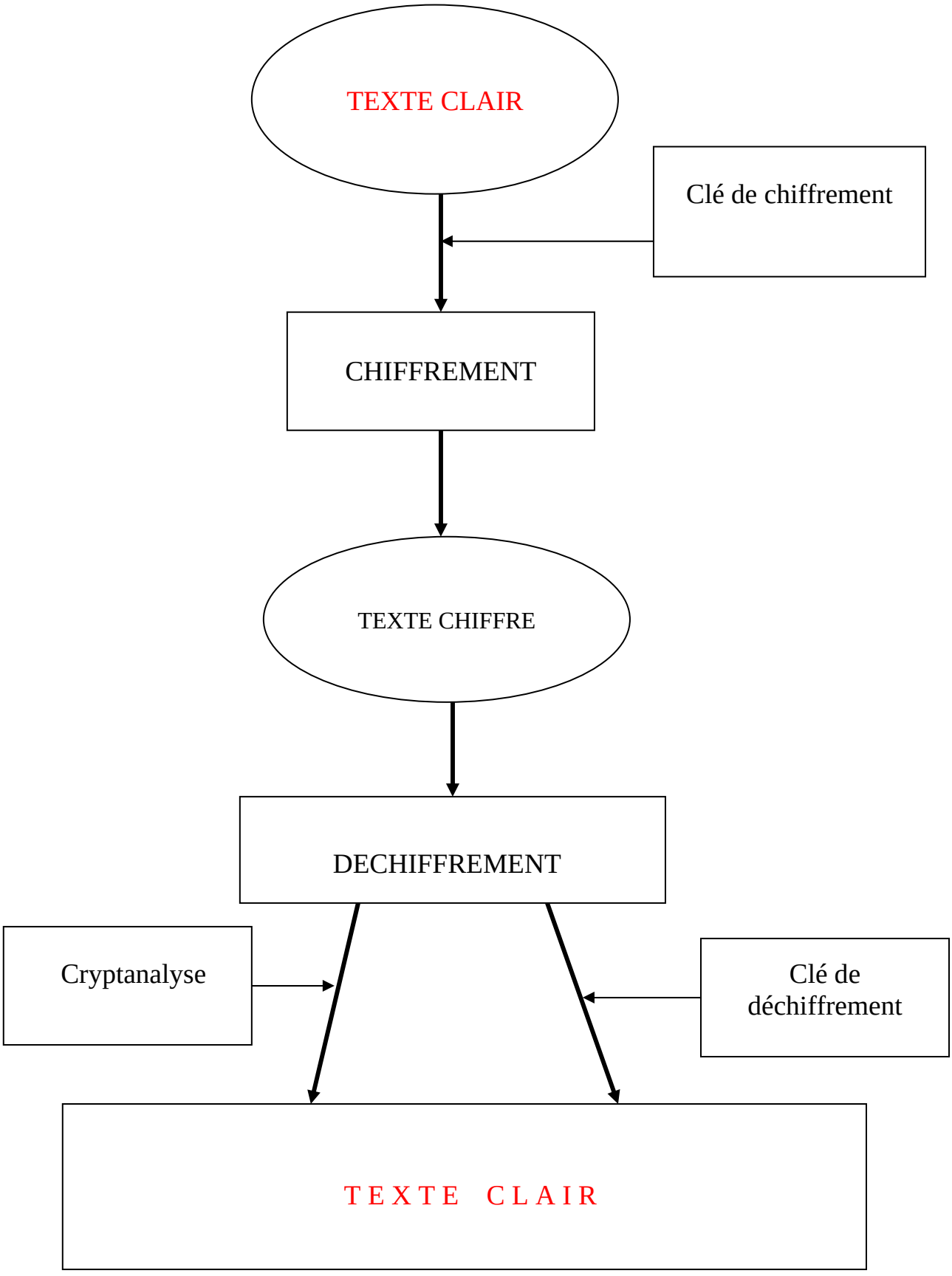
l'information et relative à la signature électronique (JORF n°62 du 14/03/2000, p.3968)
[1] http://www.men.minefi.gouv.fr/

l'opération inverse (du texte chiffré vers le texte clair) déchiffrement (cf. illustration page suivante).

- **Cryptanalyse**. La cryptanalyse est le déchiffrement de messages chiffrés dont on ne connaît pas le code.(*TLFi*)
- **Cryptologie**. Littéralement « science du secret ». Elle regroupe deux branches : cryptographie et cryptanalyse. Dans le projet de loi relatif à la confiance dans l'économie numérique[1], l'article 17 définit la prestation de cryptologie comme une « opération visant à la mise en oeuvre, (…), de moyens de cryptologie. » , sachant que « on entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité. ». Le but est donc de fournir une assurance de sécurité des échanges en utilisant des moyens de cryptologie garantissant une confidentialité, une authentification et une intégrité des données transmises ou stockées.

[1] http://www.assembleenationale.fr/12/dossiers/economie_numerique.asp Devenue la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, article 29. JORF du 22 juin 2004.

Schéma du déroulement des opérations de chiffrement et de déchiffrement d'un texte



Actuellement, l'utilisation, la fourniture, le transfert, l'importation et l'exportation de **moyens de cryptologie** sont régis par la loi du 26 juillet 1996, ses décrets d'application du 24 février 1998 (n° 98-101 et 98-102), les arrêtés du 13 mars 1998 ainsi que les décrets n° 99-199 et 99-200 du 17 mars 1999 et l'arrêté du même jour.

Il convient de distinguer au sein de ce régime, l'utilisation d'une part, la fourniture d'autre part, de moyens et prestations de cryptologie.

* L'utilisation de moyens et prestations de cryptologie

Lorsque les moyens ou prestations de cryptologie ne permettent que d'assurer des fonctions d'authentification ou de contrôle d'intégrité, l'utilisateur de ces produits est dispensée de toute formalité préalable.

Lorsque les moyens ou prestations de cryptologie assurent des fonctions de confidentialité, l'utilisation et l'importation de ces moyens sont fonction de la longueur de la clé utilisée (inférieure à 40 bits, comprises entre 40 et 128 bits, supérieure à 128 bits) et de l'utilisateur (usage privé par personne physique ou usage professionnel)

* La fourniture de moyens et prestations de cryptologie

La fourniture, l'utilisation, l'exportation ou l'importation (en provenance d'un Etat n'appartenant pas à la Communauté européenne ou n'étant pas partie à l'accord instituant l'Espace économique européen) sont dispensée de toute formalité préalable si ces techniques visent des moyens mettant en œuvre la cryptologie à titre accessoire (fonctionnement téléphone portable par exemple).

Une déclaration préalable est nécessaire si ces mêmes moyens assurent des fonctions d'authentification et de confidentialité par clés inférieures à 128 bits.

Une autorisation préalable est obligatoire dans les cas où les précédentes procédures ne s'appliquent pas.

Ces dispositions, somme toute assez complexes, se voient simplifiées dans le projet de loi cité ci-dessus qui prévoit

- une utilisation libre des moyens de cryptologie (article 18-I),
- la fourniture, le transfert, l'importation, l'exportation libres si seule une fonction d'authentification ou d'intégrité est assurée, (article 18-II)
- dans le cas où le moyen utilisé n'assure pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité, la sortie du territoire de ce moyen (transfert vers un Etat membre de la Communauté européenne ou exportation) est

soumis à autorisation du premier ministre (article 18-IV). L'introduction sur le territoire (la fourniture, le transfert depuis un Etat membre de la Communauté européenne ou l'importation) est soumise elle à une déclaration préalable auprès du premier ministre, « le fournisseur ou la personne procédant au transfert ou à l'importation (tenant) à la disposition du Premier ministre une description des caractéristiques techniques de ce moyen de cryptologie, ainsi que le code source des logiciels utilisés. » (article 18-III). De même, la fourniture de prestations de cryptologie doit être déclarée auprès du Premier ministre (article 19).

Il n'est donc plus question ici de longueur de clé. Les différents éléments ci-dessus peuvent être résumés ainsi :

Réglementation en vigueur au 4/06/2003

FINALITES		**FONCTIONS**	**OFFERTES**	
	Authentification intégrité		*Confidentialité*	
		Clé <= 40 bits	**40<clé<= 128 bits**	**Clé>128 bits**
Utilisation	Libre	Libre	Libre ou déclaration	Autorisation
Fourniture de moyens	Déclaration simplifiée	Déclaration	Déclaration	Autorisation
Importation	Libre	Libre	Libre ou déclaration	Autorisation
Exportation	Libre	Autorisation	Autorisation	Autorisation

Loi 2004-575 pour la confiance dans l'économie numérique *(mise à jour 2004)*

FINALITES	**FONCTIONS**	**OFFERTES**
	Authentification Intégrité	*Confidentialité ou autres fonctionnalités*
Utilisation	Libre	Libre
Fourniture de moyens	Libre	Déclaration préalable
Fourniture de prestations	Déclaration préalable	Déclaration préalable
Importation	Libre	Déclaration préalable
Exportation	Libre	Autorisation
Transfert		
Depuis un Etat membre CE	Libre	Déclaration préalable
Vers un Etat membre CE	Libre	Autorisation

- Le **chiffrement** est un processus qui applique un algorithme à un message afin d'en coder la signification. Cette transformation mathématique systématique est indépendante du contenu. Cette notion est à distinguer de l'encodage qui repose sur des conventions de langage (par exemple, les messages radio-diffusés destinés à la résistance française durant le deuxième guerre mondiale). L'algorithme, permettant cette transformation mathématique, utilise une clé de chiffrement qui empêche de décrypter le message. La qualité du chiffrement dépend de plusieurs facteurs : la qualité de l'algorithme, la taille de la clé (mesurée en bits) ainsi que la gestion des clés (différentes selon que l'on utilise un chiffrement symétrique ou asymétrique)

Il faut savoir que le terme de cryptage n'est qu'un anglicisme : l'emploi en est donc incorrect.

- **l'empreinte** ("hash" en anglais) ou condensé. L'empreinte d'un texte est la forme abrégée de ce texte obtenue à l'aide d'une fonction de hachage à sens unique (ou « one-way hash function »). Elle est dite à sens unique, car s'il est facile de calculer l'empreinte, il est très difficile d'effectuer l'opération inverse afin de déduire le texte initial. C'est donc une version synthétique et unique du document d'origine. L'intérêt est que les différences entre deux textes sont immédiatement décelées en comparant leurs empreintes. La caractéristique principale d'une empreinte est donc son unicité. Cette propriété[1] peut être mise à mal, en théorie[2], si le condensé est inférieur, dans l'état de l'art actuel, à 160 bits. C'est la raison pour laquelle les fonctions de hachage utilisées actuellement tendent à atteindre (RIPEMD-160 pour Ripe Message Digest 160 bits) voire dépasser (SHA-2 pour Secure Hash Algorithm 2 qui propose des tailles de 256, 384 ou 512 bits) ce seuil de 160 bits.

- **certificat** électronique (ou passeport électronique). C'est un petit fichier de 8 à 10 Ko qui voyage avec tous les envois certifiés et qui est public. Il identifie l'émetteur en fournissant le nom de la personne (physique, morale), la date de validité du certificat, …,

[1] Source : http://www.securiteinfo.com/crypto/hash.shtml

[2] Théorème ou paradoxe des anniversaires : sachant qu'un bit n'a que deux valeurs possibles (0 ou 1), il n'existe que 2^n empreintes possibles n représentant la longueur de celle-ci. Il faut effectuer $2^{n/2}$ essais pour trouver par hasard une empreinte identique qui pourrait correspondre à un autre texte original (phénomène de collision).

et est associé à une clé publique (authentification). Toute modification de ce certificat pourra être aisément détectée (intégrité). Ce certificat est émis par une autorité de certification (« certificate authority » ou CA) qui garantit la véracité des données d'authentification en signant avec sa clé privée. Le mécanisme légal de l'élaboration d'un certificat qualifié fait l'objet de l'article 6 du décret du 30 mars 2001. Le format informatique X.509v3 est actuellement utilisé pour la rédaction de ces certificats.

- **Le certificateur**[1]. L'acteur central est le prestataire de service de certification (PSC). Aux termes de la directive européenne sur la signature électronique, article 2, est PSC « toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques. ». On peut distinguer des fonctions différentes : l'opérateur de certification (OC), l'autorité de certification (AC), l'autorité d'enregistrement (AE).

  L'OC est un prestataire technique qui crée le certificat et le diffuse sur un support. Les plus connus sont Certplus, Certinomis, Omnicertis, Cashware.
  L'AC a pour fonction de signer les certificats à l'aide d'une clé qui lui est propre, sur demande d'une autorité d'enregistrement. Les certificats ainsi signés sont communiqués au centre de publication. L'AC garantit donc que la clé publique de certificat est bien celle du porteur. Des opérateurs de certification peuvent être AC (comme Certplus ou Certinomis), mais aussi des banques, des entreprises pour leurs salariés, ...
  L'AE est l'autorité qui vérifie qu'une personne est bien habilitée à demander un certificat. Après avoir collecté les informations nécessaires à cette identification et procédé à la vérification, la demande est transmise à une autorité de certification. Des organismes de proximité peuvent assumer ce rôle, comme les chambres de commerce par exemple.

1.4.3.2 Les systèmes cryptographiques symétriques et asymétriques

1.4.3.2.1 les systèmes cryptographiques symétriques ou à clé secrète (ou chiffrement conventionnel)

Ces systèmes utilisent la même clé au chiffrement et au déchiffrement. La clé doit donc être connue de l'expéditeur et du destinataire. Il est impératif que les différents

[1] Source : « Innovation et administration » n°22, 29 mai 2002

protagonistes se soient au préalable entendu sur cette clé (symétrique) et que celle-ci reste effectivement secrète (ce qui suppose un canal sûr pour l'échanger).

Ce type de cryptographie, très utilisé pour le chiffrement des données, se caractérise par sa grande rapidité car il met en œuvre un cryptage dit « à la volée » (« on the fly »). On peut distinguer deux procédés différents : le chiffrement en continu (« stream cipher »).et le chiffrement par blocs (« block cipher »)

Le chiffrement en continu permet de chiffrer des données bit par bit sans attendre la réception complète des données à crypter. L'algorithme le plus couramment utilisé aujourd'hui est le RC4.

Le chiffrement par blocs, plus utilisé et permettant une meilleure sécurité, s'applique à des blocs de données et non à des flux. La taille des blocs (généralement 64 bits), la taille de la clé varient selon l'algorithme utilisé et donc le niveau de sécurité recherché. Les algorithmes les plus utilisés sont DES (« data encryption standard », qui utilise des clés de 56 bits) ou AES (« advanced encryption standard », qui utilise des clés de 112 à 256 bits).

L'évolution de la technologie est telle[1] que la sécurité offerte par la cryptologie symétrique est plus relative qu'absolue. En ce qui concerne le DES, l'utilisation d'un triple chiffrage (Triple-DES) est encore considéré comme sûr par les experts.

1.4.3.2.2 les algorithmes asymétriques ou à clé publique

Le problème de la confidentialité de la clé, inhérent au système de cryptologie symétrique, a été résolu avec l'utilisation de la cryptographie asymétrique. Chaque utilisateur dispose de deux clés liées mathématiquement. La première est la clé "privée", qui n'est jamais révélée, et la seconde est la clé "publique" qui est divulguée à tous les correspondants (elle est contenu dans le certificat ou accessible sur Internet par exemple).

Ces deux clés peuvent être utilisées de différentes manières :

- la clé publique sert au chiffrement. Tout un chacun peut chiffrer un message, mais seul le propriétaire de la clé privée pourra le déchiffrer : la confidentialité est préservée.
- La clé privée sert au chiffrement. N'importe qui peut déchiffrer un message, mais seul le propriétaire de la clé privée peut chiffrer : la signature est authentifiée.
- Clés publique et privée sont utilisées pour le chiffrement. Le document est d'abord chiffré avec la clé privée, puis de nouveau avec la clé publique. Pour déchiffrer, le

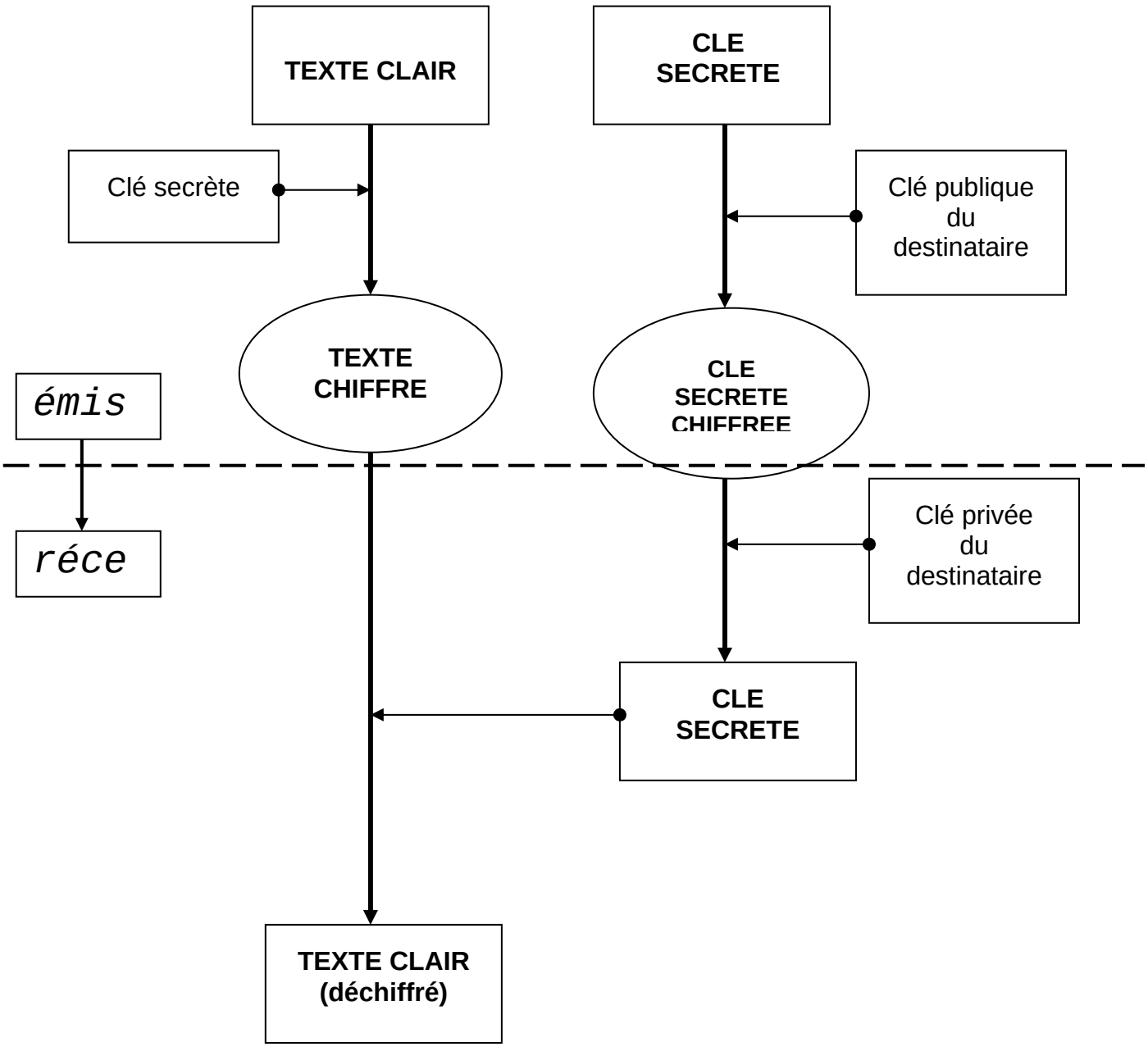
[1] cf. la loi de Moore qui prévoit le doublement de la puissance de calcul des processeurs tous les 18 mois. Jusqu'à aujourd'hui, cette loi a toujours été vérifiée.

destinataire utilisera tout d'abord sa clé privée (confidentialité), puis la clé publique de l'expéditeur (authentification de la signature).

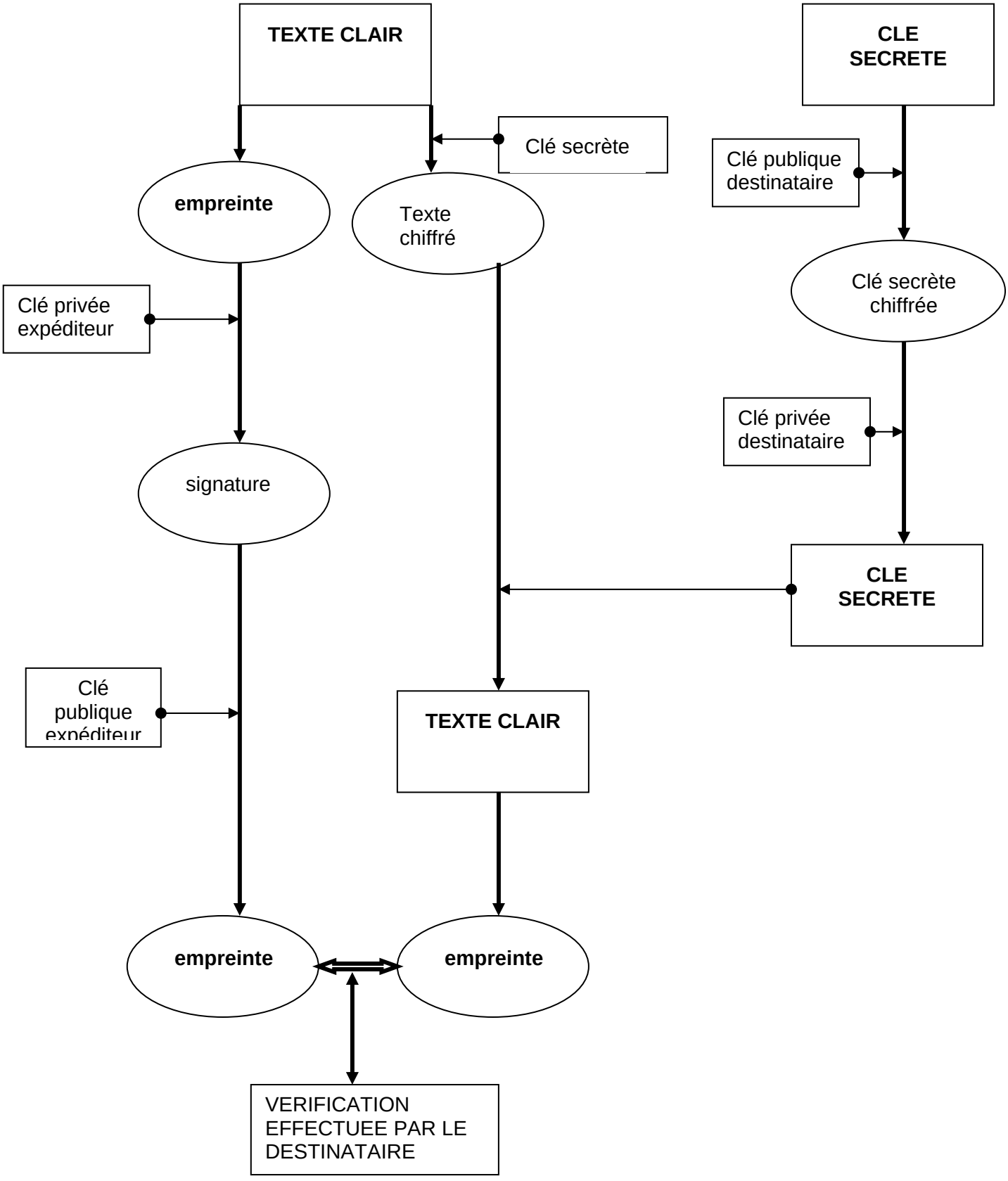
C'est donc le fait que les deux clés (privée et publique) d'une même personne soient liées entre elles, qui va permettre de vérifier l'authenticité de la signature.
Ce concept, inventé en 1976 (Whitfield Diffie et Martin Hellman), repose sur l'utilisation d'opérations mathématiques que l'on ne sait pas inverser efficacement. De nombreux algorithmes utilisent ce principe. Le plus connu est RSA (de Ronald Rivest, Adi Shamir et Leonard Adleman) : il met en œuvre le principe de la factorisation. On peut citer aussi les algorithmes ElGamal et Rabin.

Ces algorithmes sont plus lents que les algorithmes à clés secrètes, ce qui explique qu'ils sont souvent utilisés pour échanger une clé symétrique servant à chiffrer les communications de manière conventionnelle (cf. illustration page suivante).
Les conditions de création d'une signature électronique (alliant authentification de l'origine des données, intégrité des données et non répudiation de la source) implique l'utilisation d'un système cryptographique à clé publique.

Utilisation possible simultanée de clés secrète et publique



Exemple de chiffrement utilisant clés secrètes, publiques et fonction de hachage



1.4.3.3. Transmissions de documents

Transmettre des documents confidentiels en utilisant un média aussi universel et ouvert qu'Internet paraît simple tant l'utilisation de cet outil est désormais répandu. Néanmoins, dans le domaine de la dématérialisation des procédures, deux écueils sont à éviter : le choix d'un moyen technique de transmission inadapté, une sécurité informatique insuffisante.

1.4.3.3.1 le choix d'un moyen technique de transmission : format d'échange de document, moyen de transmission.

Une expérience de mise en œuvre de standard de transmission de l'information (XML, transmission en large bande) est actuellement en cours au Royaume Uni. Le but est d'évaluer l'utilisation de XML.

En France, depuis janvier 2002 pour les administrations de l'Etat, l'utilisation du cadre commun d'interopérabilité (CCI) est obligatoire[1]. Ce CCI, œuvre de l'agence pour les technologies de l'information et de la communication dans l'administration (ATICA)

- « fixe les standards relatifs aux infrastructures réseaux, aux services d'annuaires, et aux services d'interconnexion de messagerie et de transport de protocole sur lesquels s'appuient les échanges entre les systèmes d'information gouvernementaux, ainsi que les relations entre ces systèmes et avec les usagers des services en ligne ;
- énonce des recommandations relatives aux standards concernant les systèmes d'information géographiques, les cartes et les catalogues électroniques. »

Ces dispositions sont propres aux administrations de l'Etat mais les collectivités territoriales « sont invitées à participer à la définition des évolutions du cadre commun d'interopérabilité. Elles sont également invitées à mettre en oeuvre l'ensemble des dispositions figurant dans la deuxième version du cadre commun d'interopérabilité, de leur propre initiative, sous leur propre responsabilité et sous une forme adaptée à leurs besoins. » (in circulaire du 4 décembre 2002). Il existe donc une volonté politique d'uniformisation des systèmes d'information publics.

Le CCI distingue 6 formats d'échanges inter-applicatif :

[1] Circulaire du premier ministre du 21 janvier 2002 relative à la mise en œuvre d'un cadre commun d'interopérabilité pour les échanges et la compatibilité des systèmes d'information des administrations, circulaire du premier ministre du 4 décembre 2002 relative à la mise en œuvre de la deuxième version du cadre commun d'interopérabilité des systèmes d'informations publics.

Standard	Utilisation	Etat du standard
TXT	Possible, - pérenne, - ouvert, - très utilisé	Les fichiers textes sont pérennes car très simples, mais ils induisent une perte d'information sensible. D'autre part le codages des fins de lignes n'est pas standardisé. Il est conseillé de les migrer vers XML.
XML	Recommandé, - pérenne, - ouvert, - utilisé	XML (Extensible Mark-Up Language) est basé sur SGML. Il a été conçu et promu par l'association W3C (World Wide Web Consortium) qui est le référent dans le domaine Internet.
SGML	Possible, - pérenne, - ouvert, - faiblement utilisé	SGML (Structured General Mark-Up Language) est un langage de description de documents. L'utilisation de XML, de préférence à SGML, est recommandée.
HTML	Possible, - pérenne, - ouvert, - très utilisé	HTML (Hyper Text Mark-up Language) est à la base des applications Internet. Il peut être utilisé en tant que format d'échange, bien que le format recommandé soit XML. Il est recommandé de faire figurer le numéro de version ainsi que les feuilles de style
RTF	Possible, - pérenne, - propriétaire, - très utilisé	Le format RTF (ou Rich Text Format) est un format propriétaire de Microsoft, destiné à l'échange de documents.
PDF	Possible, - pérenne, - propriétaire, - très utilisé	Le format PDF, ou Portable Document Format, est un format propriétaire de la société Adobe, lié au logiciel Acrobat. Son usage est très répandu. Adobe diffuse actuellement gratuitement le logiciel de lecture Acrobat Reader, sous réserve de l'acceptation de la licence

Il apparaît clairement que pour l'Etat français, le format d'échange de document recommandé est le format XML.

Une fois déterminé ce format, (à savoir XML), reste à déterminer le moyen de transmission. La transmission de documents volumineux (comme un DCE par exemple) en utilisant une ligne téléphonique couplé à un modem de 56 Kbits/s serait trop lent pour

que la mise en œuvre de la dématérialisation soit d'un réel avantage. De plus, la commission européenne a fait de la technologie haut débit un des deux thèmes prioritaires de son plan d'action « e-europe 2005 » : 3,8 milliards d'euros sont mobilisés pour son développement depuis 4 ans. Ces arguments techniques et politiques font que le haut débit est le moyen privilégié pour la transmission des documents.

Ce que l'on appelle le haut débit est la transmission ultrarapide d'un grand volume de données numérisées. Plusieurs technologies peuvent mettre en œuvre ce principe[1] :

- **l'ADSL** (asymetric digital subscriber line). Cette technologie permet de transmettre des données à haut débit (plusieurs centaines de kilobits par seconde) sur les lignes téléphoniques. ADSL est dit " asymétrique " car il privilégie un sens de transmission par rapport à l'autre : le débit peut aller de 256 kbit/s à 9 Mbit/s du réseau vers l'abonné, c'est-à-dire dans le sens " descendant ", mais seulement de 16 à 640 kbit/s de l'abonné vers le Réseau (sens " montant "). Il n'est efficace que si la distance qui sépare le central téléphonique de l'abonné ne dépasse pas 4 km. L'Union internationale des télécommunications (UIT) vient tout juste d'officialiser la norme ADSL2 Plus. Comparée à l'ADSL actuel, il est possible d'augmenter le débit sans changer ni les lignes ni les centraux ADSL déjà mis en place par les opérateurs en augmentant la tension électrique des lignes téléphoniques, pour y faire passer plus de données à la fois. Le débit maximal est porté à 16 Mbit/s. En voie montante (de l'abonné vers le fournisseur d'accès Internet), le débit ne dépassera pas 800 kbits/s pour une distance maximale du central allant de 1 400 à 2500 mètres**.** Chez France Télécom, on affirme que cette technologie pourrait être déployée dès le courant de l'année prochaine.
- La **boucle locale radio (BLR**) ou Wireless Local Loop (WLL) . Raccordement par voie hertzienne de l'abonné au réseau d'un opérateur de télécommunications.
- La **fibre optique.** Support conducteur de lumière, de plus en plus utilisé dans les réseaux pour les débits très élevés qu'il autorise. La fibre optique permet de transmettre des données sous forme d'impulsions lumineuses modulées, à des débits supérieurs à ceux du fil de cuivre. Elle se compose d'un " coeur " de quelques dizaines de microns, qui transporte les impulsions lumineuses, d'une gaine plus ou moins opaque qui peut réfléchir ces impulsions pour leur permettre de poursuivre leur trajet, et d'un revêtement protecteur.

[1] Définitions obtenues sur http://www.01net.com/

- Le **satellite**
- Le **câble**
- Les **CPL** (courants porteurs en ligne). Cette technologie , utilisant les cables électriques, offre des débits allant de 1 à 2 Mbit/s, sachant que le débit maximal d'un câble électrique est de 168 Mbit/s.

Des expériences de développement des réseaux hauts débits sont menés en Europe. Illustrons notre propos avec le Royaume-Uni, l'Allemagne et la France.

Le **Royaume-Uni** était en décembre 2001 le pays européen où la population connectée au haut débit était la moins nombreuse (0,03%)[1]. Pour autant, l'objectif de **devenir le plus grand marché du haut débit du G7 en 2005** a entraîné la mise en œuvre d'une politique volontariste. Baisse des prix (réduction de 41% des tarifs de location des lignes haut débit de British Telecom pour les fournisseurs d'accès à Internet (FAI) en février 2002 par exemple), développement de la demande (stimulation destinée aux entreprises, aux particuliers, raccordement des immeubles en construction au câble, …), stimuler la fourniture d'accès au haut débit, toutes ces mesures tendent vers cet objectif. Le soucis principal est d'éviter un isolement grandissant des zones rurales. Pour ce faire, le développement du satellite (dans les Highlands et les îles) et du câble (Nord de l'Ecosse, avec le concours financier de l'Union Européenne), semble pouvoir permettre un développement harmonieux des structures de transmission du Royaume-Uni.

L'Allemagne, en juin 2001, était au 11° rang des pays de l'OCDE en terme de pénétration haut débit. La volonté, comme au Royaume-Uni est de développer ce moyen de transmission sans isoler les zones rurales. Développement d'accès haut débit par satellite (offre T-DSL de Deutsche Telekom) pour les zones rurales ou isolées, mise en place d'un programme d'action pour le haut débit, tout est mis en œuvre pour atteindre l'objectif du gouvernement allemand : un **passage au tout fibre optique d'ici 2010**.

La **France**, au début de l'année 2002, se situait à l'avant-dernier rang des onze pays où les particuliers utilisent intensivement internet. « Dans le domaine professionnel, la France se positionne derrière la Suède, l'Allemagne ou le Canada, avec 85 % d'entreprises connectées. Le nombre de micro-ordinateurs connectés par entreprise se situe dans une moyenne basse, avec cinq en France, pour huit en Espagne, par exemple.

[1] Source : http://www.telecom.gouv.fr/

Encore faut-il prendre en compte les disparités régionales : en Ile-de-France, 55 % des PME sont connectées sur le haut débit, alors que 44 % des entreprises du Nord et de l'Ouest de la France disposent d'un simple modem. On constate par ailleurs que plus de 40 % des entreprises françaises disposent d'un site web propre, contre près de 80 % en Grande-Bretagne. Mais la France comble très rapidement son retard en matière d'ADSL : elle a conquis la deuxième place européenne pour le nombre d'abonnés (1,4 millions fin 2002) »[1].

La volonté de combler ce retard « numérique » a été formalisé par la mise en œuvre du plan « RE/SO 2007 » (pour une République numérique de la société de l'information). Lors d'une intervention en novembre 2002, le Premier ministre a rappelé les projets engagés par le Gouvernement et précisé les trois axes de réflexion suivants :
- une simplification et une clarification des règles en vigueur sur internet;
- une démocratisation de l'accès à internet pour le plus grand nombre;
- une définition du rôle de l'Etat, notamment en matière d'administration électronique.

La politique ainsi définie est assortie d'objectifs liés aux trois acteurs de ce développement : les entreprises, les particuliers, les collectivités territoriales.
- les entreprises : "*faire en sorte que **toutes nos entreprises soient connectées à Internet à l'horizon 2007***".
- les particuliers : "*atteindre **10 millions d'abonnés(à l'internet haut débit) dans les cinq prochaines années***".
- les collectivités territoriales : « *le souhait exprimé par le Président de la République de **voir toutes les communes de France équipées de l'internet haut débit d'ici 2007***. »

Des expériences de transfert de données à haut débit ont été menées par des collectivités territoriales[1]. Il ressort, entre autres constatations, que ces collectivités ont mis en œuvre des technologies diverses : ADSL, mais aussi fibre optique, BLR, satellite. On peut noter avec intérêt de nouvelles expérimentations, en région parisienne, de la technologie CPL entreprises par une filiale d'EDF et des sociétés telles que Télé-2 ou Aéroport de Paris. Ces expérimentations visent pour l'instant les particuliers (citadins) et les entreprises. Cette nouvelle activité permettrait à EDF de se diversifier dans les télécommunications, même si cela lui est normalement interdit au nom du principe de « spécialité ».

[1] annexe 3 du rapport d'orientation **pour l'achat public de services de télécommunications (transfert de données à haut débit)**, élaboré dans le courant des troisième et quatrième trimestres 2002.

1.4.3.3.2 Sécurité informatique[1]

Chiffrer les données transmises, pour autant que cela soit indispensable, n'est pas suffisant pour assurer une sécurité optimale des transmissions. La sécurité du système informatique lui-même nécessite d'autres précautions, ne serait-ce que pour éviter :

- la divulgation de données,
- la modification de données,
- l'utilisation de ressources réseau.

Des vérifications doivent être assurées, au niveau de l'architecture du système, des éléments logiciels du système, ou encore des éléments matériels du système.

1.4.4 conservation et mise à disposition des documents archivés[2]

1.4.4.1 Qu'est-ce qu'un document ?

Un travail collectif de réflexion, actuellement en cours au sein du réseau thématique pluridisciplinaire 33 du département STIC du CNRS, a pour but de préciser la notion de document dans son passage au numérique.[3]

Sont distingués trois dimensions :

- la forme (comme un objet matériel ou immatériel, dont on étudie la structure, à dissocier du contenu, pour mieux l'utiliser ou le manipuler),
- le signe (comme un porteur de sens, indissociable du sujet qui le construit ou le reconstruit et lui donne sens)
- la relation (comme un vecteur de communication, qui s'est affranchie de l'espace et du temps ; en même temps, il est un élément de systèmes identitaires et un vecteur de pouvoir.).

La dimension qui nous intéresse ici est celle de la forme, puisque en matière informatique, et d'autant plus dans le cadre de la dématérialisation des procédures, il s'agit de numériser des objets matériels, c'est à dire manipuler la structure sans modifier le contenu.

[1] Source www.ssi.gouv.fr/
[2] source « guide pour la conservation des informations et des documents numériques pour les télé procédures les intranets et les sites internet » Agence pour le développement de l'administration électronique (ADAE), et plus généralement le site de l'ADAE (http://www.adae.pm.gouv.fr/)
[3] www.cnrs.fr/stic/

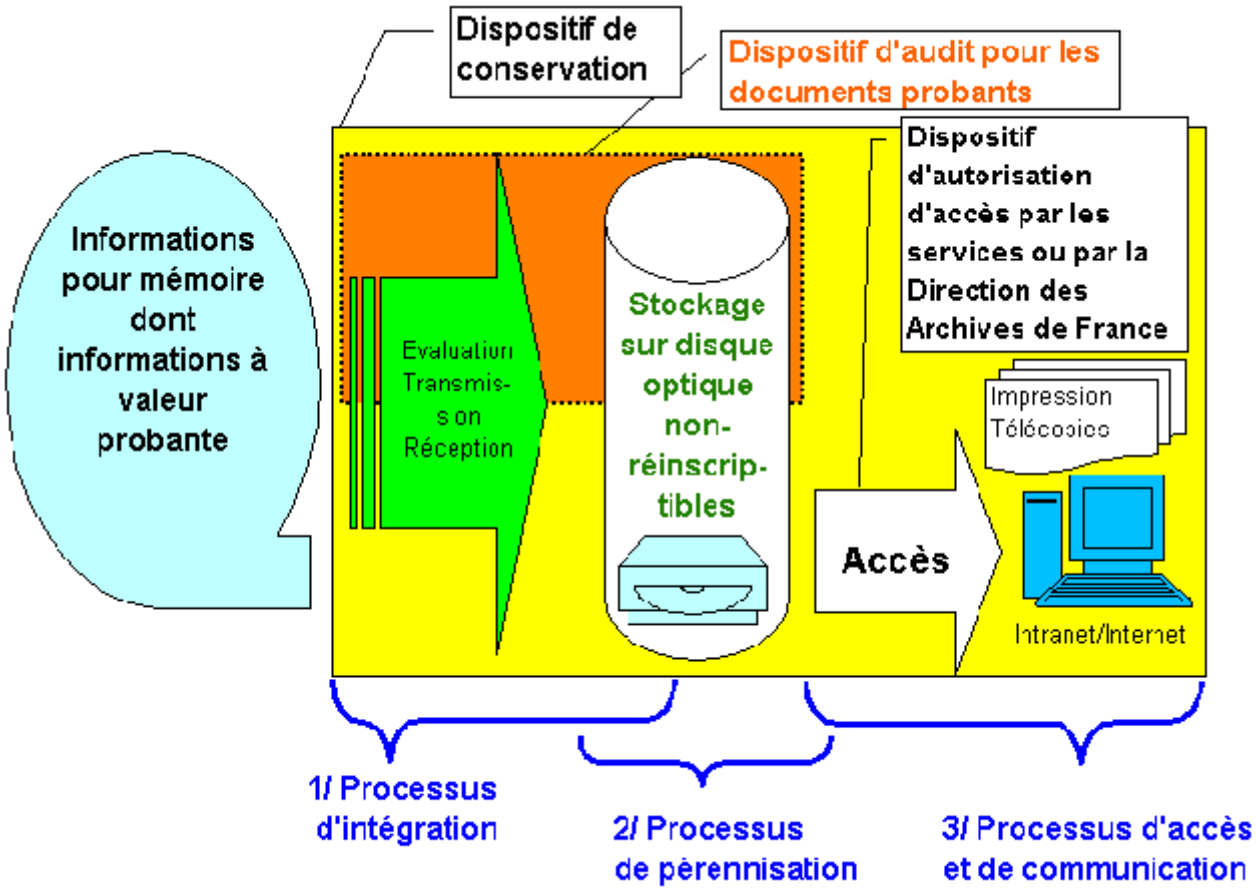
1.4.4.2 le principe de conservation

Le Conseil d'Etat dans le chapitre II de son rapport « Internet et réseaux numériques » énonce que « le document doit être assorti d'une signature fiable, et être conservé de façon durable sous le contrôle des signataires ou d'un tiers à qui ces derniers souhaitent confier cette fonction. ». Le Conseil assimile la signature électronique à la force probante d'un écrit sous signatures privées.

Pour être admise, la conservation doit remplir le critère de durabilité. Ce critère est définit à l'article 1348-2 du Code civil : « Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support. »

L'agence pour le développement de l'administration électronique (ADAE), dans son « guide pour la conservation des informations et des documents numériques pour les télé procédures les intranets et les sites internet – version 3 » édité en février 2001, définit la conservation des informations et documents électroniques comme une fonction autorisant « l'accès et la restitution des informations et des documents dans le temps ». La notion de conservation s'inscrit donc la durée, durée utile à un service ou durée réglementaire. Après avoir précisé que cette fonction peut être externalisée, elle y distingue trois processus : l'intégration, la pérennisation et l'accès. Ces processus peuvent être représentés ainsi[1]

[1] « Guide pour la conservation des informations et des documents numériques pour les téléprocédures, les intranets et les sites internet » ADAE, partie 1/5.



, le tout étant sous-tendu par le processus de gestion et d'audit.

L'ADAE définit ainsi les trois processus de la fonction de conservation :

- intégration : identification des documents numériques à conserver, formats recommandés, méta-données à associer ;
- pérennisation : stockage et supports recommandés ;
- accès et communication : gestion des droits d'accès (deux types devant être prévus : accès par les services administratifs producteurs, accès par d'autres services et par les usagers et chercheurs), conservation et auditabilité de cette fonction.

Ce guide prend appui sur la norme NF Z 42-013 (validée en 1999) d'une part et les standards XML d'autre part.

1.4.4.3 Norme NF Z 42-013

« la présente norme fournit un ensemble de spécifications concernant les mesures à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents

électroniques afin d'assurer la conservation et l'intégrité de ceux-ci ». Le but de la norme est de « parer aux risques d'obsolescence des systèmes, de parer aux risques de contentieux et de créer un état de l'art en matière d'archivage électronique »[1] elle définit ainsi ce qu'est un document fidèle : (fidélité) « au document d'origine s'il permet de reconstituer toute l'information nécessaire aux usages auxquels est destiné le document d'origine ».

1.4.4.4 XML

eXtensible Markup Language, traduisez *Langage à balises étendu* ou *Langage à balises extensible*, est en quelque sorte un langage HTML amélioré. Mis au point par le XML Working Group sous l'égide du world wide web consortium (W3C) dès 1996, il est un langage reconnu depuis 1998, les spécifications *XML 1.0* étant reconnues à cette date comme recommandations par le W3C.

XML décrit le contenu plutôt que la présentation (contrairement à HTML) : il permet de séparer le contenu de la présentation. Il est possible, par exemple d'afficher un même document sur des applications ou des périphériques différents sans pour autant nécessiter de créer autant de versions du document que de représentations possibles.

Cela permet de créer une unité de conservation, unité dans laquelle sont regroupés :

- le(s) document(s) numérique(s) à conserver,
- le fichier XML : méta-données propre au document (date du document et identifiant unique, organisme producteur, créateur, règle de conservation, format et logiciel d'origine, mot clé, …), liste des documents, migrations effectuées, …
- le schéma : structure du fichier XML

Pour extraire les données du document ainsi créé, il est nécessaire d'utiliser un outil, appelé analyseur (ou *parseur*). Cet outil permet d'une part d'extraire les données d'un document XML (on parle d'*analyse* du document ou de *parsing*), de vérifier éventuellement la validité du document d'autre part.

Une polémique s'est développé au sujet de la préférence donnée au disque optique numérique WORM[2] dans la norme NF Z 42-013 (position reprise par le guide de l'ADAE) par rapport à la micrographie informatique (ou microformes COM), arguant du

[1] http://www.adae.pm.gouv.fr/upload/documents/NORMENFZ.PDF
[2] DON-WORM : disque optique numérique (c'est à dire utilisant la technologie laser) non-réinscriptible (ou write once read many : écrit une fois, lit plusieurs)

fait que le support informatique proposé, utilisant la technologie WORM, ne garantit pas l'irréversibilité de l'information.

Si l'on se reporte à la « Note d'information de la Direction des Archives de France - Année 1996 - Note n° 1 », les deux options pouvaient être envisageables pour l'archivage de document, toutes deux offrant « une rapidité d'accès à l'information incontestable ». Cependant, la solution numérique présentait l'avantage de « (permettre) un accès simultané à l'information par plusieurs utilisateurs » et assurait « les meilleures garanties d'irréversibilité ».

De plus, les arguments liés à l'irréversibilité du document stricto sensu, avantage prépondérant de la micrographie, tombent d'eux-mêmes quand l'on connaît la structure d'un document archivé suivant les standards XML (cf. ci-dessus), telle qu'elle est préconisée aussi bien dans la norme que dans le guide de l'ADAE. De plus, ce format de document est celui que recommande le cadre commun d'interopérabilité pour les échanges et la compatibilité des systèmes d'information des administrations, édité par l'ATICA (cf. § 1.4.3.3.1).

1.4.4.5 la norme ISO 15-489 : le « records management » (RM)

Aucun équivalent français de l'expression « records management » n'a été pour le moment déterminée (le fascicule édité par l'association française de normalisation reprend le terme anglophone, n'ayant pas trouvé d'équivalent satisfaisant). En se référant à la proposition de définition du terme « document » (cf. §1.4.4.1 ci-dessus) par le CNRS privilégiant la forme, l'expression « gestion des documents administratifs »ne pourrait-elle pas offrir un équivalent sémantique satisfaisant ?

Avant de définir ce qu'est le « records management », il paraît utile de rappeler les étapes du cycle de vie d'un document.

L'évolution d'un document suit trois étapes importantes[1] :

- *création et utilisation* : le document est utilisé pendant un laps de temps variable. Il s'agit d'un document actif.
- *conservation* : la durée de cette étape est soumise aux délais légaux de conservation, ou propres à l'entité créatrice.
- *conservation définitive* : là aussi, cette étape est soumise aux délais légaux (archives historiques par exemple)

[1] on pourra se reporter utilement au site voir le site www.archivesdefrance.culture.gouv.fr/fr/archivistique/DAFrecords.html

Toutes ces étapes ne s'enchaînent pas automatiquement, chacune pouvant se conclure par une opération de tri et de destruction.

Le RM est la gestion de cet ensemble. Il permet donc :

- « le contrôle des documents dès leur création ;
- d'en détruire sans crainte. ».

Le RM recouvre par conséquent des domaines très variés

Il apparaît donc clairement que la norme NF Z 42-013 ne couvre qu'une partie du « records management » puisqu'elle ne vise que les mesures à mettre en œuvre « pour l'enregistrement, le stockage et la restitution de documents électroniques », occultant la phase de création et d'utilisation du document.

1.5 Mise en œuvre des principes de la responsabilité[1]

La responsabilité d'une personne est subordonnée à trois conditions :

- l'existence d'un préjudice certain,
- l'existence d'une faute. Dans le cadre qui nous intéresse, ie celui de l'administration, la règle de droit commun est que la personne publique commet la faute hormis les cas de faute détachable du service (intérêt personnel, excès de comportement, faute d'une gravité exceptionnelle),
- l'existence d'un lien entre la faute et le préjudice.

Dans son rapport 2002, le groupe de travail 8 « Aspects juridiques, » de la mission économie numérique (MEN), après avoir élaboré dans un premier temps un tableau déterminant la localisation de la responsabilité première selon les domaines de risques majeurs en matière d'échange électronique, propose dans un deuxième temps deux grilles d'analyse, l'une permettant de déterminer les besoins de sécurité, l'autre formalisant les responsabilités par rapport aux risques.

Les domaines de risques majeurs mis en avant par ce groupe sont :

- défauts d'intégrité de l'information échangée,
- défauts d'intégrité de l'information publiée,
- défauts d'intégrité de l'information conservée.
- authentification des acteurs,

[1] Source : rapport 2002 du groupe de travail 8 de la mission pour l'économie numérique

- authentification des auteurs,
- authentification de l'acte.
- Date de création du document,
- Date d'envoi,
- Date de réception.

Un groupe de risques majeurs ne se voit pas associé de localisation de responsabilité première : ce sont les risques majeurs liés aux lieux de création, d'émission et de réception de l'acte.

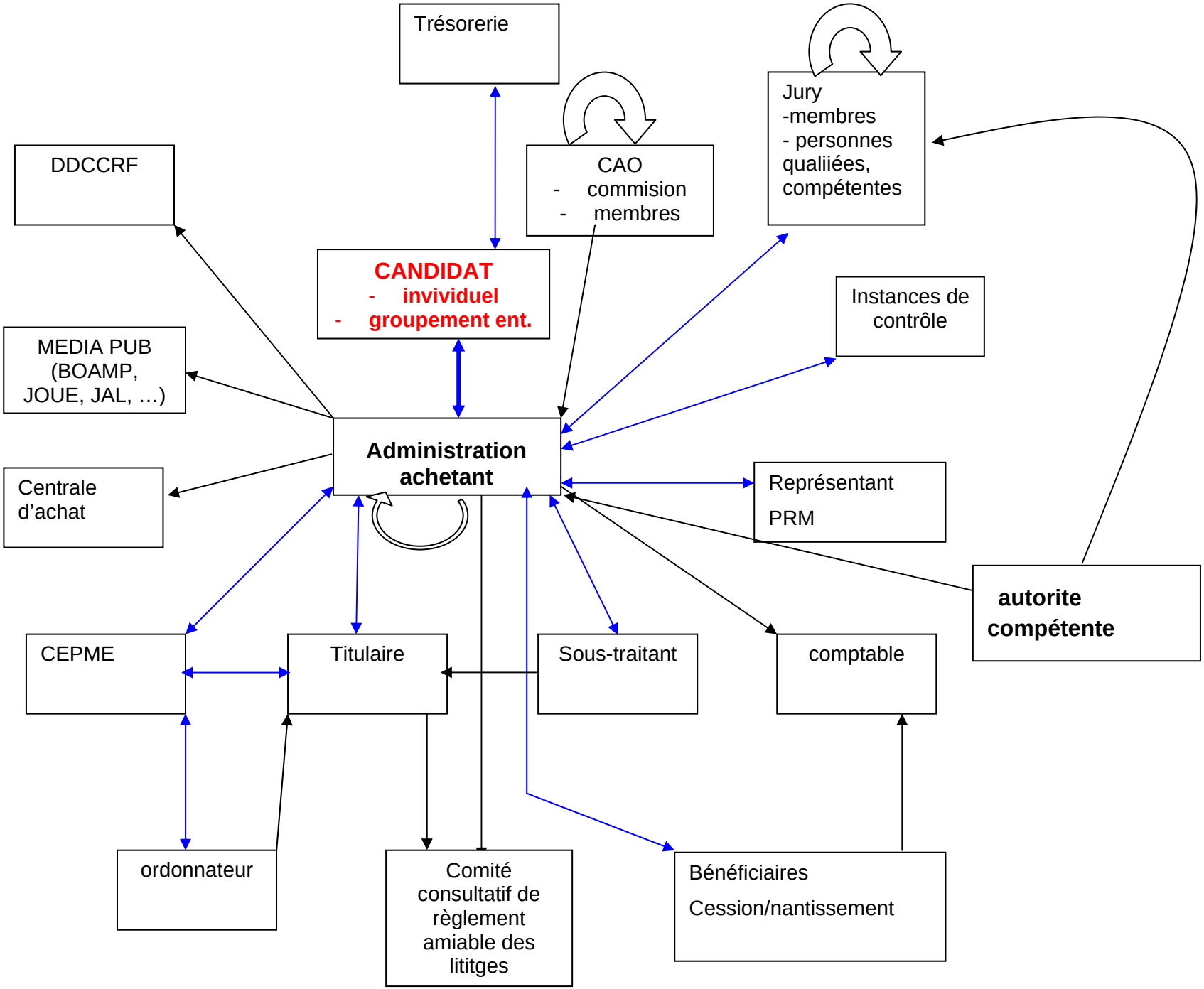
Il n'en demeure pas moins qu'aux termes du décret 2002-692, « la personne publique assure la sécurité des transactions sur un réseau informatique accessible à tous les candidats » (article 7) et que, de même, cette même « personne publique prend les mesures propres à garantir la sécurité des informations portant sur les candidatures et les offres. Elle s'assure que ces informations demeurent confidentielles. »

En sa conclusion, ce groupe met en avant deux impératifs, facteurs clés du succès de mise en œuvre de téléprocédure ou téléservice : « l'efficacité technique et la sécurité juridique du dispositif ».

1.6 Que pourrait-on dématérialiser ?

2. Que pourrait-on dématérialiser ?

Après exploitation du code des marchés publics, les flux d'informations entre l'entité « Administration achetant » (regroupant les termes personne publique, personne publique contractante, personne responsable des marchés, assemblée délibérante utilisés dans le code des marchés publics) et les entités « extérieures » pourraient être représentés ainsi :



Mis à jour février 2005

CEPME : crédit d'équipement des petites et moyennes entreprises

BOAMP : bulletin officiel des annonces des marchés publics

JOUE : journal officiel de l'union européenne

DDCCRF : direction départementale de la concurrence, la consommation et de la répression des fraudes

CAO : commission d'appel d'offres

JAL : journal d'annonces légales

 : relation à sens unique, dans le cadre du CMP

 : relation bilatérale

Les intervenants sont donc multiples. Pourtant, le CMP, en son article 56, ne traite explicitement que des relations entre l'Administration et le candidat. La dématérialisation ne concerne pas directement (même si l'article 56§4[1] ouvre la possibilité de remplacer tout écrit « par un support ou un échange électronique ») le titulaire ou toute autre personne que ce soit. Elle ne vise donc qu'à faciliter l'accès des entreprises (les candidats) aux marchés publics et à diminuer les coûts de gestion matérielle des document. En détaillant cette relation (Administration achetant-candidat) à travers le prisme du CMP dans son ensemble, nous obtenons les informations suivantes, que l'on pourrait assimiler à un dictionnaire des données :

+ documents émis par le candidat au profit de la personne publique :

- Acte d'engagement,
- attestation sur l'honneur,
- demande de renseignements complémentaires,
- candidature,
- déclaration sur l'honneur datée et signée (satisfait aux obligations fiscales et sociales),
- demande de cahier des charges et de documents complémentaires,
- dossiers (candidature+offre),
- offre modifiée,

[1] « 4° Les dispositions du présent code qui font référence à des écrits ne font pas obstacle au remplacement de ceux-ci par un support ou échange électronique. »

- demande écrite des motifs de rejet,
- demande écrite des motifs d'arrêt de la procédure,
- offre,
- certificats délivrés par les administrations et organismes compétents.

+ documents reçus par le candidat (il s'avère que le flux d'informations reçu par celui-ci provient exclusivement de l'administration) :
- Dossier de Consultation des Entreprises,
- cahier des charges,
- Cahier des Clauses Administratives Particulières,
- Cahier des Clauses Techniques Particulières,
- documents complémentaires,
- Offres en retour si la candidature n'est pas retenue,
- renseignements Complémentaires Éventuels,
- lettre de consultation,
- mise au point du marché,
- négociations,
- demande de précision de l'offre,
- Décision d'attribution du marché (concours),
- décision de déclarer sans suite la procédure,
- avis de rejet des candidatures,
- avis de rejet des offres,
- Décision de choix d'un ou plusieurs lauréat(s) (concours),
- réponse écrite sur les motifs de rejet,
- réponse écrite sur les motifs d'arrêt de la procédure.

Une fois éliminés les flux relatifs à la transmission des documents constituant le dossier de consultation des entreprises d'une part, les candidatures et les offres d'autre part, nous constatons qu'en ce qui concerne le flux généré par les candidats, seules les demandes « écrites » des motifs de rejet de candidature ou d'arrêt de procédure ainsi que les certificats délivrés par les administrations et organismes compétents pourraient être visés par l'article 56§4. Si pour les demandes écrites, le passage au numérique paraît chose aisée, l'expédition des divers certificats fait intervenir d'autres administrations : le succès

de cette dématérialisation est suspendu à la démarche suivie par celles-ci en matière de dématérialisation des documents.
Au contraire, en ce qui concerne l'administration achetant, il serait possible d'utiliser l'article 56§4 pour de nombreuses pièces : lettre de consultation, demande de précision de l'offre, avis de rejet de candidature ou d'offre, décision de choix du lauréat ou d'attribution du marché, réponse « écrite » sur les motifs de rejet ou d'arrêt de procédure.

La dématérialisation des procédures, telle qu'elle est prévue dans le code des marchés publics, couvre de manière explicite une partie conséquente des flux d'information entre l'administration achetant et le candidat, laissant toute latitude aux différents acteurs pour les autres flux.
Cette latitude pourrait se révéler bien vite être un « cadeau » empoisonné. A titre d'illustration, prenons le cas du contrôle de légalité exercé par les préfectures auprès des collectivités (l'exemple consistant à prendre la transmission des dossiers en commission spécialisée des marchés serait tout aussi instructif). Ce contrôle consiste en une validation des projets de marché (ces projets devenant marché une fois la notification effectuée). Un exemplaire original du projet (donc signé du futur titulaire), une copie de ce même projet, le DCE ainsi que l'offre sont donc expédiés par l'administration achetant à la Préfecture. Dans le cas où cette administration aurait passé un marché dématérialisé, quid de la transmission du dossier si le contrôle de légalité n'en est pas arrivé au même niveau de dématérialisation (et d'utilisation de la signature électronique) ? Faudra-t-il en passer par une « re-matérialisation » des documents ? Mais alors, le document électronique signé puis imprimé ne sera pas pour autant un document papier signé : quelle sera alors la valeur juridique de ce document ? Cette question du contrôle de légalité est jugé suffisamment sensible pour être abordé dans l'article 28 du projet de loi habilitant le gouvernement à simplifier le droit, adopté le 10 juin 2003 :
« *Dans les conditions prévues par l'article 38 de la Constitution, le Gouvernement est autorisé à prendre par ordonnance toutes mesures nécessaires pour développer l'utilisation des technologies de l'information afin de simplifier :*
1° Les conditions de fonctionnement des collectivités territoriales et des autorités administratives ;
2° Les procédures de transmission des actes des collectivités territoriales et des autorités administratives soumis au contrôle du représentant de l'Etat dans le département. »

Le gouvernement, plutôt qu'imposer une mise à niveau des infrastructures électroniques des préfectures (la formation du personnel et d'éventuelles réorganisations structurelles allant de pair), préfère se ménager la possibilité d'aménager le droit applicable en matière de contrôle.

L'utilisation d'une carte électronique d'achat (projet carte d'achat, mené par la direction générale de la comptabilité publique au sein du ministère de l'économie, des finances et de l'industrie) entre Administration et titulaire est souvent présentée comme un exemple de dématérialisation. Mais il serait ici plus exact de parler de dématérialisation de l'exécution de la dépense publique plutôt que de dématérialisation des procédures de marchés publics. C'est la raison pour laquelle cette expérience, indiscutablement prometteuse, ne sera pas abordé dans le cadre que nous avons défini.

Appliquant le principe selon lequel on ne peut dématérialiser que ce qui existe matériellement aux marchés publics, la matière juridique de ce principe est vaste. Vaste car, outre le code des marchés publics (plus particulièrement l'article 56) et les décrets d'application (décret 2001-846 et 2002-692), un projet de directive européenne relative à la coordination des procédures de passation des marchés publics de fournitures, de services et de travaux traite de la dématérialisation des procédures.

Cette idée d'utiliser la voie électronique pour transmettre des documents entraîne inévitablement vers les domaines

+ du droit de la preuve et de son adaptation aux technologies de l'information,
+ de la signature électronique et de sa fiabilité mettant en œuvre les trois qualités primordiales que sont l'intégrité des données, authentification de l'origine de ces mêmes données ainsi que la non-répudiation de la source,
+ de la sécurité des transactions, aussi bien des données (cryptologie) que des moyens utilisés (format de document, technique de document)
+ de la conservation et de la mise à disposition des documents archivés
+ de la mise en œuvre de la responsabilité.

Tous les éléments, aussi bien techniques que juridiques, semblent réunis pour mettre en oeuvre une dématérialisation des procédures. La seule question restant en suspend est la suivante : tous les acteurs de la dématérialisation avanceront-ils en même temps sur cette voie (cf. exemple du contrôle de régularité) ? Les problèmes, si problèmes il y a, proviendront plus de la maîtrise d'une mise en œuvre coordonnée de la dématérialisation que de la dématérialisation elle-même.
Une fois prise la mesure de ce qu'est et entraîne en théorie cette dématérialisation, il convenait de comprendre concrètement ce que pouvait représenter cette opération dans l'application du code des marchés publics.

A la lumière de ces éléments, nous allons pouvoir aborder les expériences menées aussi bien par une administration d'Etat que par une collectivité territoriale.

3 Expériences de dématérialisation des procédures

3.1 Expérience Etat : le portail achats.defense.gouv.fr du ministère de la défense

Les portails d'achats du ministère de la défense (www.ixarm.com et www.achats.defense.gouv.fr) sont en ligne depuis bientôt un an. Cet engagement dans la voie de la dématérialisation a nécessité une structure de projet, celle-ci précisant les choix techniques avant de proposer un produit fini aux utilisateurs : entreprises et administrations du ministère de la défense.

3.1.1 la structure de projet

Une équipe a été constituée : elle regroupe 5 personnes à temps plein, pour un budget financier global de 6 millions d'euros sur 3 ans. La prestation prévue englobait la création de 2 portails (un consacré aux achats d'armes et munitions, l'autre aux prestations relative au soutien, infrastructures, informatique, vivres, habillement, essences, santé), ainsi que la maintenance du produit (sachant que la maintenance de premier niveau est assurée en interne, la charge étant évaluée à ½ personne à temps plein).

Pour ce faire, un marché de maîtrise d'œuvre, d'une durée de 3 ans, poursuivi par un marché pluri-annuel pour assurer le fonctionnement ont été conclu. De plus, un marché d'assistance à maîtrise d'ouvrage, d'une durée de 2 ans et couvrant la période mi-2002 mi-2004 a été notifié.

Le projet à proprement parlé a débuté officiellement à la mi-2000. L'équipe de projet restera constitué au moins jusqu'en 2005.

L'aspect juridique de la dématérialisation a été pris en compte en amont du projet. La présence d'un avocat a faciliter l'étude des principales difficultés que la dématérialisation pouvait poser. A la suite de quoi, des choix de conception ont été effectué, les points « délicats » pour lesquels il était nécessaire d'imposer une réglementation identifié. La démarche adoptée consiste à comparer les risques de la procédure électronique avec ceux déjà existant en procédure « papier », l'objectif étant de diminuer ces derniers en préservant la simplicité d'utilisation. Cette démarche de veille juridique est un processus continu, mené en parallèle à la phase de conception du projet technique. Un audit juridique est prévu après quelques mois d'utilisation.

3.1.2 l'aspect technique

Les divers aspects de la dématérialisation abordés en première partie ont fait l'objet de choix techniques déterminants au niveau du fonctionnement des portails.

Aucun format de document n'a été imposé : seule obligation, les formats utilisés doivent être communément répandus (rtf, doc, xls, ppt, pdf, dgn, dxf, dwf), de telle sorte que l'administration puisse les lire ou qu'il existe une visionneuse gratuite.

Le cadre commun d'interopérabilité (obligatoire pour les administrations de l'Etat depuis janvier 2002) de l'ATICA (cf. § 1.4.3.3.) n'a pas servi de référence, il a été jugé trop restrictif. Quant au format d'échange inter-applicatif, à savoir XML pour le CCI, il s'agit d'un format de document structuré. Hors, actuellement, ni les DCE ni les plis ne sont des documents structurés. Leur normalisation éventuelle ne pourrait intervenir que dans plusieurs années. Néanmoins, pour l'échange de DCE entre applications (entre application productrice et la place de marché par exemple), les DCE sont encapsulés dans un message XML mais le document lui-même demeure dans un format bureautique.

En ce qui concerne les moyens de transmission, toutes les transactions sont possibles avec une connexion bas débit, même si les utilisateurs fréquents sont incités à utiliser une liaison haut débit, quelle qu'elle soit.

La sécurité informatique a été considéré dans son ensemble, le point le plus important (et donc le plus sensible) étant la sécurisation des offres afin de garantir leur confidentialité entre la réception et l'ouverture par la commission d'appel d'offres. En ce qui concerne la cryptographie, des certificats ont été achetés à un opérateur de certification (celui qui fabrique les certificats) puis délivré par l'administration, qui se pose ainsi en prestataire de service de certification (PSC). A court terme, certains PSC seront reconnus, les entreprises pourront alors acheter directement un certificat. Dans le domaine de la signature électronique, celle-ci est vérifiée dès réception des plis par la place de marché, puis les informations sont transmises avec le pli au service achat concerné pour d'éventuelles vérifications ultérieures.

3.1.3 Le produit proposé aux utilisateurs

Dès le départ du projet, le principe retenu était celui du portail d'achat, nœud central des procédures d'achat du ministère. Le gestionnaire de ce portail se comporte alors comme un prestataire de service, offrant un espace, vis à vis des autres administrations du ministère de la défense.

Le portail « achats.defense.gouv.fr », place de marché, est articulé autour de 3 pôles :

- un pôle de publication d'avis (avis officiels et non officiels, ie ceux dont la publicité n'est pas obligatoire) ;
- un pôle salle des consultations dématérialisées (SCDM). Dans ce lieu, les DCE sont publiés et peuvent être téléchargés, les entreprises peuvent transmettre leurs candidatures et offres.
- Un pôle « outils d'achats » regroupant une salle des enchères inversées (SEI), une salle de facturation (FAC), une salle d'acquisition sur catalogue (SAC).

L'équipe a tablé sur une montée progressive en puissance : mille clients (entreprises et administration) et cent cinquante DCE par an, puis trois mille utilisateurs (environ cinq cents pour l'administration et deux mille cinq cents entreprises) pour trois cents DCE, pour atteindre bientôt cinq mille utilisateurs (environ huit cents pour l'administration et quatre mille deux cents entreprises) pour deux mille DCE devant le succès grandissant de ce portail, aussi bien côté entreprise que administration.
Néanmoins, la lourdeur de la mise en œuvre de la signature électronique est le seul frein à un développement plus grand encore.

Il est encore trop tôt pour pouvoir évaluer les conséquences de l'application de ces nouveaux principes d'organisation des procédures pour les administrations, aussi bien dans les domaines financiers, humains que dans le management des équipes chargés des marchés publics. Si certaines sont attendues (meilleures transparence et concurrence, économie de moyens, efficacité de la commande publique accrue), d'autres ne sont que pressenties (évolution des modes de management des équipes par exemple).

3.2 Expérience collectivité territoriale : le conseil général de la Somme

Depuis le 20 mai 2003, une plate-forme est mise à disposition du conseil général de la Somme et de la communauté d'agglomération d'Amiens. Ce projet a été conduit par l'agence de développement des technologies de l'information et de la communication (TIC) en Picardie, syndicat mixte du conseil général de la Somme et d'Amiens Métropole (communauté d'agglomération rassemblant 21 communes) avec l'appui technique de Susinet, société d'économie mixte ayant pour objet de développer des applications d'intérêt général liées aux TIC. Les choix techniques effectués ont permis d'élaborer une plate-forme unique, intégrée sur le site internet de chaque collectivité.

3.2.1 la structure de projet

Avant d'élaborer le cahier des charges, toutes les directions des marchés des collectivités membres ont été consulté par l'agence de développement des TIC.

Il est à noter que la création et le fonctionnement de cette plate-forme n'ont entraîné aucune dépense particulière pour les collectivités membres de l'agence pour le développement des TIC : le montant de ces opérations est partie intégrante des cotisations annuelles versées par les parties prenantes (cotisations qui s'élèvent à 380 000 euro pour chaque entité).

3.2.2. L'aspect technique

Le choix s'est porté sur une plate-forme unique, à charge aux administrations de l'intégrer à leur propre site internet. La solution du portail d'achats a donc été écarté au bénéfice de cet outil qui pourra être répliqué autant de fois que nécessaire.

3.2.3 Le produit proposé aux utilisateurs

Le produit proposé permet actuellement de mettre en ligne les avis d'appel public à la concurrence, les dossiers de consultation des entreprises, les avis d'attribution des marchés ainsi que d'autres services parmi lesquels un forum aux questions (FAQ). Dans un deuxième temps, il est prévu de pouvoir recevoir les dossiers de candidature et les offres des soumissionnaires, mais aucun calendrier n'est encore défini.

Si cette plate-forme fonctionne sur le site du syndicat mixte, le département de la Somme en est encore à la phase d'expérimentation, le but étant un fonctionnement normal à compter du mois de septembre 2003. Pour Amiens Métropole, le degré d'avancement du projet est bien moindre, pour ne pas dire au point mort, faute de moyens humains.

4 Que faire au CRA ?

4.1 La situation actuelle

Actuellement aucune démarche structurée (type projet) n'est entamée au niveau des systèmes d'information du conseil régional en ce qui concerne la dématérialisation en général, et celle des marchés publics en particulier.

4.2 Préliminaire à une démarche technique

Avant d'entamer une démarche technique, l'accent devrait être mis sur l'unification des outils informatiques utilisés, de manière à réduire la diversité des formats de document alimentant une future plate-forme électronique (PFE). En matière de commande publique, la mise en œuvre du logiciel « MARCO » par tous les services concernés (et pas seulement l'unité des marchés publics) permettrait d'atteindre ce but d'unification. Mais attention à ne pas privilégier uniquement l'aspect marché public de la dématérialisation : les solutions retenues pourrait ne pas correspondre aux besoins d'autre cas de dématérialisation de document. Toutes les directions devraient être impliquées dans le processus de réflexion.

4.3 les acteurs du processus

Contrairement au passage des systèmes informatiques à l'an 2000 (le fameux « bug » de l'an 2000) où seuls les informaticiens étaient impliqués, ici, la dématérialisation des procédures de marché public concerne aussi bien les informaticiens que les acteurs, côté conseil régional, de la commande publique : c'est une affaire aussi bien informatique que technique (en ce qui concerne la définition des besoins) et juridique.

5 Conclusion.

Le principe de dématérialisation des procédures, mis en avant par l'article 56 du code des marchés publics, est en théorie applicable dans les meilleures conditions, aussi bien technique que juridique. Des solutions techniques différentes, adaptées aux besoins des différentes administrations, sont d'ores et déjà expérimentées. Les moyens mis en œuvre, tant financier qu'humain, diffèrent eux aussi selon les objectifs visés. Les conséquences de l'utilisation de ce nouveau mode de communication ne sont pas encore réellement déterminées, même si pour certaines le principe en est déjà connu.

Toutefois, cette dématérialisation des procédures de marché public a des limites, aussi bien d'ordre technique que juridique.

Au niveau technique, le risque est grand de confrontation d'administrations, certaines ayant suivi le processus de dématérialisation, d'autres non. Comment alors faire passer une information uniquement électronique entre deux correspondants ? Et plus les correspondants sont nombreux, plus la question des passerelles entre système d'information se pose avec acuité. On peut penser, par exemple, à un document élaboré par un mandataire, transmis au conseil régional qui lui-même le retransmet à la Préfecture : quel sera le format de document utilisé ? Sera-t-il commun à tous les intervenants ? tous les systèmes d'information seront-ils compatibles entre eux ?

Au niveau juridique, force reste à la preuve écrite. A en croire J.Grand d'Esnon**,** responsable de la direction des affaires juridiques (DAJ) du ministère des finances,[1] « Il paraît peu envisageable de considérer le média internet comme un vecteur unique de publicité. Cela dit, ce mode de diffusion paraît tout à fait complémentaire aux journaux d'annonces légales. »

Le papier a donc encore de beaux jours devant lui. Mais l'impulsion est donnée : de nouveaux modes opératoires sont en train de voir le jour, entraînant des évolutions dépassant largement le cadre des marchés publics.

[1] Dans le cadre d'une interview parue sur Localmundi du 23 juin 2003 (devenu localjuris.com.fr)

6. Glossaire

MOT	DEFINITION
ATICA	Crée en août 2001, l'Agence pour les technologies de l'information et de la communication dans l'administration (ATICA) est placée sous l'autorité du Premier ministre. Supprimée et remplacée par l'agence pour le développement de l'administration électronique (ADAE).
Autorité de certification (AC)	A pour fonction de signer les certificats à l'aide d'une clé qui lui est propre, sur demande d'une autorité d'enregistrement. Les certificats ainsi signés sont communiqués au centre de publication. L'AC garantit donc que la clé publique de certificat est bien celle du porteur. Des opérateurs de certification peuvent être AC (comme Certplus ou Certinomis), mais aussi des banques, des entreprises pour leurs salariés, ...
ADAE	Agence pour le développement de l'administration électronique. est un service interministériel placé auprès du Premier ministre, mis à la disposition du ministre chargé de la réforme de l'Etat. Elle a été créée par le décret du 21 février 2003, publié au JO du 22 février. • L'ADAE favorise le développement de systèmes d'information permettant de moderniser le fonctionnement de l'administration et de mieux répondre aux besoins du public ; • Elle propose au Premier ministre les mesures tendant à la dématérialisation des procédures administratives, à l'interopérabilité des systèmes d'information, ainsi qu'au développement de standards et de référentiels communs ; • Elle assure, pour le compte du Premier ministre, la maîtrise d'ouvrage des services opérationnels d'interconnexion et de partage des ressources, notamment en matière de transport, de gestion des noms de domaine, de messagerie, d'annuaire, d'accès à des applications informatiques et de registres des ressources numériques.

ADSL	Asymetric digital subscriber line. Cette technologie permet de transmettre des données à haut débit (plusieurs centaines de kilobits par seconde) sur les lignes téléphoniques. ADSL est dit " asymétrique " car il privilégie un sens de transmission par rapport à l'autre.
AE	Autorité d'enregistrement. Est l'autorité qui vérifie qu'une personne est bien habilitée à demander un certificat. Après avoir collecté les informations nécessaires à cette identification et procédé à la vérification, la demande est transmise à une autorité de certification. Des organismes de proximité peuvent assumer ce rôle, comme les chambres de commerce par exemple.
bit	De « binary digit » ou chiffre binaire. Le système de numération binaire est à la base de toute l'informatique et le " bit " est son unité fondamentale. Un bit ne peut prendre que deux valeurs, 0 ou 1. Il est nécessaire de les combiner pour obtenir une plage de valeurs distinctes suffisante pour définir un sous-système de codage . Différents codages sont nécessaires sur un ordinateur, celui des lettres, chiffres et signes typographiques, mais aussi celui des codes de commandes du microprocesseur ou celui des adresses de stockage en mémoire. Les bits ont généralement été regroupés par huit pour former un octet pouvant prendre 256 (2 puissance 8) valeurs.
Bit par seconde	Unité de débit de données (de vitesse de transmission). L'abréviation correspondante est bit/s, mais on trouve aussi dans la littérature spécialisée le sigle anglais « bps » (bits per second). Le bit étant l'unité de compte des données en informatique, il est naturel que, pour exprimer combien de données on peut transmettre en un temps donné, on utilise le bit/s. Utilisés avec le bit (ou d'autres unités), des préfixes multiplicateurs représentent un coefficient légèrement différent du coefficient décimal habituel, cette fois-ci fondé sur les puissances de 2 les plus proches. Ainsi, le préfixe kilo ne représente pas un coefficient de 1000 (10 puissance 3), mais de 1024 (2 puissance 8). Le préfixe méga ne multiplie pas par 1 000 000, mais par 1 048 576 (2 puissance 16). Le préfixe giga correspond à un coefficient de 1 073 741 824 (2 puissance 24), …

BOAMP	Bulletin officiel des annonces des marchés publics.
boucle locale radio (BLR)	Wireless Local Loop (WLL). Raccordement par voie hertzienne de l'abonné au réseau d'un opérateur de télécommunications
cadre commun d'interopérabilité (CCI)	D'utilisation obligatoire pour l'administration d'Etat, le CCI, œuvre de l'agence pour les technologies de l'information et de la communication dans l'administration (ATICA). Le but est la mise en œuvre d'un cadre commun d'interopérabilité pour les échanges et la compatibilité des systèmes d'information des administrations, dont la deuxième version est parue en décembre 2002 (circulaire du premier ministre du 4 décembre 2002)
CAO	Commission d'appel d'offres
CDC	Caisse des dépôts et consignation
CEPME	Crédit d'équipement des petites et moyennes entreprises. Dans le cadre des marchés publics, il peut procéder à des paiements à titre d'avances et à des crédits de trésorerie au bénéfice des titulaires des marchés, travaux sur mémoire et achats sur factures ou au bénéfice de leurs sous-traitants ayant droit au paiement direct.
certificat électronique	Ou passeport électronique. C'est un petit fichier de 8 à 10 Ko qui voyage avec tous les envois certifiés et qui est public. Il identifie l'émetteur en fournissant le nom de la personne (physique, morale), la date de validité du certificat, …, et est associé à une clé publique (authentification). Toute modification de ce certificat pourra être aisément détectée (intégrité)
chiffrement	Processus qui applique un algorithme à un message afin d'en coder la signification. Cette transformation mathématique systématique est indépendante du contenu. Cette notion est à distinguer de l'encodage qui repose sur des conventions de langage (par exemple, les messages radio-diffusés destinés à la résistance française durant le deuxième guerre mondiale). L'algorithme, permettant cette transformation mathématique, utilise une clé de chiffrement qui empêche de décrypter le message
conservation des informations et documents électroniques	Fonction autorisant « l'accès et la restitution des informations et des documents dans le temps ». La notion de conservation s'inscrit donc dans la durée, durée utile à un service ou durée réglementaire.

CPL	Courants porteurs en ligne. Cette technologie , utilisant les câbles électriques, offre des débits allant de 1 à 2 Mbit/s, sachant que le débit maximal d'un câble électrique est de 168 Mbit/s.
Cryptanalyse.	La cryptanalyse est le déchiffrement de messages chiffrés dont on ne connaît pas le code.
Cryptographie	n. f. XVIIe siècle. Composé à l'aide du grec kruptos, «caché », et graphein, « écrire ».Art d'écrire en langage codé, secret, chiffré. (*Dictionnaire de l'académie française, 9° édition*). Écriture secrète qui consiste généralement à transposer les lettres de l'alphabet ou à les représenter par des signes convenus, de manière à ce que le sens de l'écrit ne soit accessible qu'au destinataire en possession du code. (*TLFi*). La transformation du texte clair en texte chiffré (ou cryptogramme) est appelé chiffrement, l'opération inverse (du texte chiffré vers le texte clair) déchiffrement (cf. illustration page suivante).
cryptologie	Action de transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète.
CSM	Commissions spécialisées des marchés
DCE	Dossier de consultation d'entreprises
DDCCRF	direction départementale de la concurrence, la consommation et de la répression des fraudes.
DÉMATÉRIALISATION,	subst. fém. : Action de dématérialiser, résultat de cette action. Action ou fait de rendre immatériel, d'ôter la matière concrète, les éléments matériels (…).
disque optique numérique (DON) WORM	Disque optique numérique (c'est à dire utilisant la technologie laser) non-réinscriptible (ou write once read many : écrit une fois, lit plusieurs).
e-award	Ouverture des plis, dépouillement, sélection des fournisseurs, avis d'attribution
e-contract	Contractualisation, notification de contrat, catalogue électronique
e-invoice	Facturation électronique, paiement, comptabilisation

empreinte	"Hash" en anglais ou condensé. L'empreinte d'un texte est la forme abrégée de ce texte obtenue à l'aide d'une fonction de hachage à sens unique (ou « one-way hash function »). Elle est dite à sens unique, car s'il est facile de calculer l'empreinte, il est très difficile d'effectuer l'opération inverse afin de déduire le texte initial. C'est donc une version synthétique et unique du document d'origine.
e-notice	Publication électronique des avis d'appel public à la concurrence, information des fournisseurs sur appel d'offre.
e-order	Commande électronique sur catalogue, suivi logistique de la commande.
e-tender	Publication des cahiers des charges, réception et archivage des réponses avec horodatage.
fibre optique.	Support conducteur de lumière, de plus en plus utilisé dans les réseaux pour les débits très élevés qu'il autorise. La fibre optique permet de transmettre des données sous forme d'impulsions lumineuses modulées, à des débits supérieurs à ceux du fil de cuivre. Elle se compose d'un " coeur " de quelques dizaines de microns, qui transporte les impulsions lumineuses, d'une gaine plus ou moins opaque qui peut réfléchir ces impulsions pour leur permettre de poursuivre leur trajet, et d'un revêtement protecteur.
JOUE	Journal officiel de l'union européenne
Certificateur	En matière de certification, l'acteur central est le prestataire de service de certification (PSC). Aux termes de la directive européenne sur la signature électronique, article 2, est PSC « toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques. ». On peut distinguer des fonctions différentes : l'opérateur de certification (OC), l'autorité de certification (AC), l'autorité d'enregistrement (AE).
Algorithme asymétrique ou à clé publique	Le problème de la confidentialité de la clé, inhérent au système de cryptologie symétrique, a été résolu avec l'utilisation de la cryptographie asymétrique. Chaque utilisateur dispose de deux clés liées mathématiquement. La première est la clé "privée", qui n'est jamais révélée, et la seconde est la clé "publique" qui est divulguée à tous les correspondants (elle est contenu dans le certificat ou accessible sur Internet par exemple).

Mission pour l'économie numérique	Rattachée au ministre de l'économie, des finances et de l'industrie, elle est chargée de favoriser le développement de l'économie numérique en assurant la coordination des travaux conduits à cet effet au niveau du ministère de l'économie, des finances et de l'industrie et en animant une réflexion prospective sur le développement et l'impact de l'économie numérique.
Norme NF Z 42-013	La présente norme fournit un ensemble de spécifications concernant les mesures à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques afin d'assurer la conservation et l'intégrité de ceux-ci.
Numérisation.	Cela consiste en une transformation de donnée matérielle (un support écrit par exemple) en une suite de chiffres dit binaires car composés de deux valeurs : 0 ou 1.
OC	Opérateur de certification. Prestataire technique qui crée le certificat et le diffuse sur un support. Les plus connus sont Certplus, Certinomis, Omnicertis, Cashware.
PFE	plate-forme électronique
records management	Aucun équivalent français de cette expression n'a été pour le moment déterminée (le fascicule édité par l'association française de normalisation reprend le terme anglophone, n'ayant pas trouvé d'équivalent satisfaisant). Le rédacteur propose, en se référant à la proposition de définition du terme « document » du CNRS (cf. §1.4.4.1) privilégiant la forme, l'expression « gestion des documents administratifs ».
système cryptographique symétrique ou à clé secrète (ou chiffrement conventionnel)	Ces systèmes utilisent la même clé au chiffrement et au déchiffrement. La clé doit donc être connue de l'expéditeur et du destinataire.
UGAP	Union générale des achats publics
signature électronique	Ce terme est générique et désigne tous les systèmes permettant de retrouver pour les documents électroniques le même gage (voire un gage plus puissant) d'identité de son émetteur que la signature manuelle l'a été pour les documents papier pendant des siècles. Pour être validé, un système de signature

	électronique doit également pouvoir vérifier que le document électronique signé n'a pas été modifié entre son émission et sa réception. Cette signature sera qualifiée de sécurisée si, de plus, elle est propre au signataire, créée par des moyens que le signataire puisse garder sous son contrôle exclusif, et que toute modification ultérieure de l'acte auquel elle se rattache soit détectable.
www.achats.defense.gouv.fr	le portail "achats.defense.gouv.fr"est un des deux portails du ministère de la défense en France. Il est consacré à la totalité des achats du ministère de la défense autres que ceux relatif aux armes, munitions et matériels de guerre (soutien, infrastructures, informatique, vivres, habillement, essences, santé).
www.ixarm.com	le portail "ixarm.com" du ministère de la défense français est relatif au périmètre "armes, munitions et matériels de guerre" c'est-à-dire les contrats relatifs aux études amont, à l'acquisition et au maintien en condition opérationnelle des équipements de défense.
XML	Extensible Mark-Up Language , ie *Langage à balises étendu* ou *Langage à balises extensible*. Est en quelque sorte un langage HTML amélioré. Mis au point par le XML Working Group sous l'égide du world wide web consortium (W3C) dès 1996, il est un langage reconnu depuis 1998, les spécifications *XML 1.0* étant reconnues à cette date comme recommandations par le W3C. XML décrit le contenu plutôt que la présentation (contrairement à HTML) : il permet de séparer le contenu de la présentation. Il est possible, par exemple d'afficher un même document sur des applications ou des périphériques différents sans pour autant nécessiter de créer autant de versions du document que de représentations possibles.