Délégation Générale pour l'Armement
Direction des Centre d'Expertises et d'Essais

C.E.L.A.R
Centre d'Electronique de l'Armement
Service informatique
BP 7 419
35 174 BRUZ Cedex
Tel : +33 (0) 2 99 42 90 11
Fax : +33 (0) 2 99 42 91 01

Institut Universitaire de Technologie de LAVAL
Département Service et Réseaux de Communication
52 Rue des Docteurs Calmette et Guérin
53 000 LAVAL
Tel : 02 43 59 49 20
Tel : 02 43 59 49 28

La dématérialisation de formulaires

Mémoire de fin de cursus

Réalisé par
Danilo Jacques

Du 1 Septembre 2004 au 31 Mai 2005

Soutenu le 23 Juin 2005

Tuteur professionnel
M. Lambert

Tuteur enseignant
Mme Puizillout

Je tiens à remercier tout particulièrement Madame Puizillout pour l'aide qu'elle m'a apportée tout le long de cette année en entreprise, mais aussi pour m'avoir accepté dans la formation Service et Réseaux de Communication de l'Institut Universitaire de Technologie de LAVAL, ainsi que toute l'équipe pédagogique.

Je remercie aussi le CELAR de m'avoir pris en contrat d'apprentissage mais surtout mon tuteur professionnel Yves Lambert pour le savoir qu'il m'a transmis.

Puis, je remercie aussi tout le service informatique pour le temps qu'il a consacré à ma formation.

SOMMAIRE

TABLE DES ILLUSTRATIONS

INTRODUCTION

Depuis quelques années, l'informatique a pris un rôle important dans notre société et dans l'administration. Avec l'aide d'Internet, le passage d'informations pose désormais moins de problèmes, ce qui est vu comme un avantage pour le monde administratif. La signature électronique, la mise à disposition d'outils de certification et de cryptographie, la standardisation des formats d'échanges basés sur la technologie XML, toutes ces avancées ont permis de réaliser une étape majeure vers l'administration électronique. La dématérialisation de formulaire a vu le jour.

Mais qu'est-ce que la dématérialisation de formulaire ? La dématérialisation de formulaire se résume à la transposition sous format électronique des échanges traditionnels réalisés au quotidien (contrats, courriers, factures, formulaires administratifs,…) mais avant tout un moyen de fluidifier les processus métier.

Amorcés dans les années 1990, notamment au travers de projets de l'administration autour de la volonté de simplification des procédures, les projets de dématérialisation couvrent principalement le transfert de résultats comptables, la déclaration de données sociales et plus récemment la déclaration et le paiement en ligne de la TVA pour les grandes entreprises ou la déclaration de revenus pour les contribuables français.

Imaginez les avantages d'une dématérialisation : au lieu d'avoir des archives énormes sur des comptes clients pour une grande société, un seul poste informatique suffit à y stocker une masse d'informations équivalente. De plus, cette entreprise gagnera un temps considérable lors d'une recherche d'un ancien client par exemple. Mais cette arrivée n'est pas sans contraintes : il faut passer le cap du stockage papier et retranscrire ces informations en un standard électronique, s'assurer de la sécurité des informations, etc. C'est ce que nous allons voir par la suite.

1. PRESENTATION DE L'ENTREPRISE

1.1 Situation géographique

Le CELAR, établissement récent, a ouvert ses portes en septembre 1968.

Son implantation, décidée par décret en 1964, s'est orientée hors de la région parisienne, dans le cadre de la politique de décentralisation et pour accompagner la volonté de développer en Bretagne un pôle électronique et informatique. Le choix final s'est porté sur la commune de Bruz, à proximité de Rennes. En effet, le CELAR est situé à 15 km de Rennes et donc à 350 km de Paris soit à 2 H de TGV plus 20 minutes de voiture. Cette situation bénéficie de nombreuses liaisons aériennes avec les métropoles européennes. Le CELAR est situé au sud-est de Rennes entre Bruz et Laillé, en pleine campagne pour permettre une grande infrastructure de 110 hectares.

Figure 1. Situation géographique du CELAR

Figure 2. Vue aérienne du CELAR

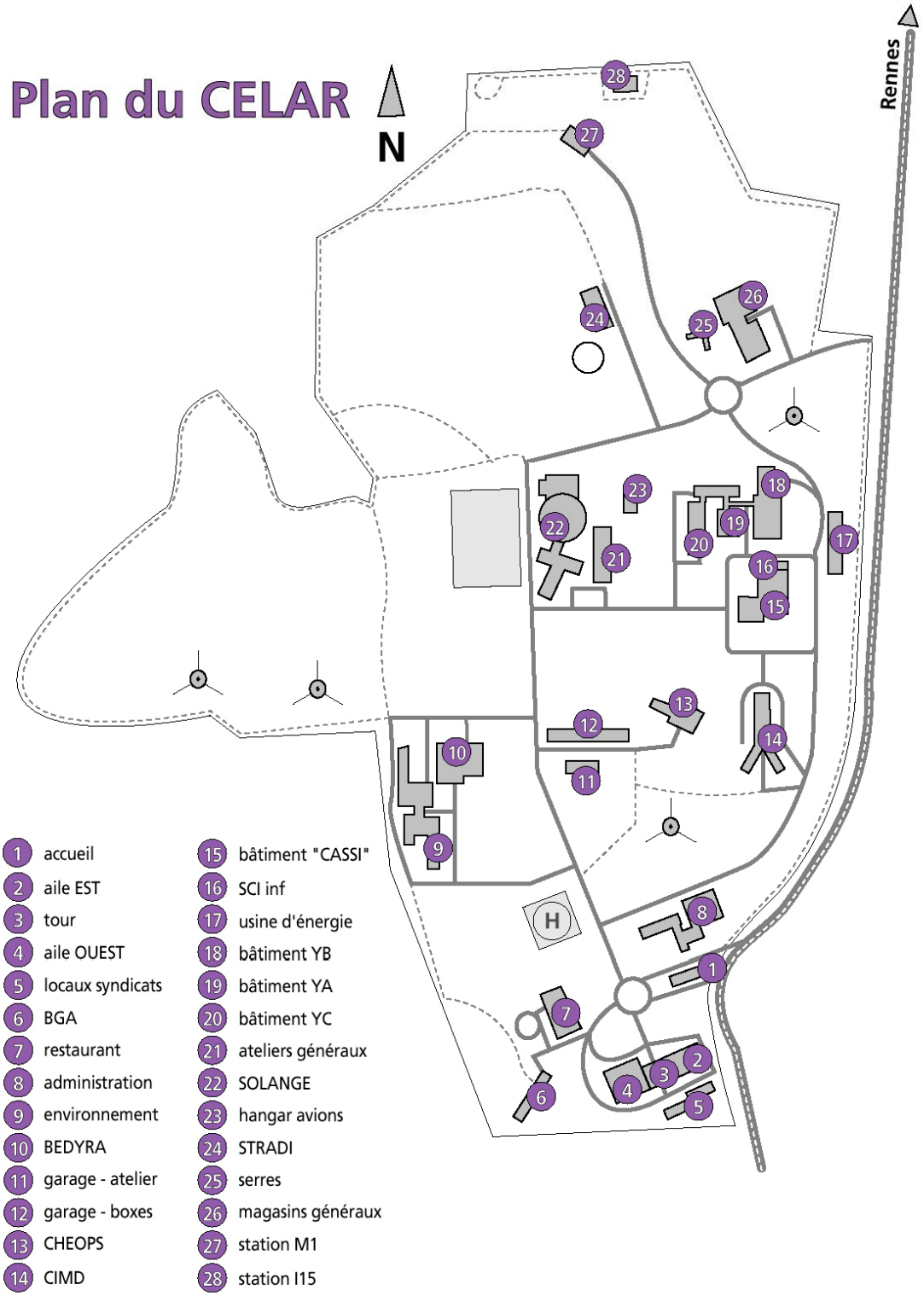

Figure 3. Plan du CELAR

1.2 Historique

- **1966 :** La première pierre est posée le 21 novembre par Pierre MESMER, ministre des Armées.
- **1968 :** ouverture du Centre d'ELectronique de l'ARmement (CELAR) le 2 septembre.
- **1972 :** mise en service de la chambre anéchoïque. C'est la plus grande chambre anéchoïque de France.
- **1974 :** mise en service de la station stradivarius, la surveillance de l'espace se développe au CELAR.
- **1975 :** le centre de calcul scientifique de l'armement (CCSA), décentralisé de la région parisienne, est implanté sur le site.
- **1976 :** création du GAFCEM (Gestion Automatisée des Fréquences et de Compatibilité Electromagnétique). Ce centre est implanté au CELAR.
- **Années 80 :** Essor des simulations numériques et hybrides. Renforcement compétences d'analyses technologiques des composants électroniques. Après la Guerre du Golfe en 1991 : le CELAR est désigné par la DGA comme étant le centre technique de la guerre électronique des systèmes d'armes.
- **1996 :** Reconnaissance officielle des compétences du CELAR en matière de sécurité des systèmes d'informations.
- **Depuis 1996 :** Grâce à la synergie entre ses activités, le CELAR a l'ambition de devenir le centre technique de la guerre de l'information.

1.3 Les Activitées

Le **CELAR** (**C**entre **EL**ectronique de l'**AR**mement) apporte son soutien aux directions de programmes d'armement nationaux ou en coopération internationale en conduisant des études d'essais des expertises dans les domaines suivants :

- **Guerre électronique des systèmes d'armes** : analyse technique de la menace électronique, systèmes d'observation et de renseignement, système d'autoprotection.
- **Systèmes d'information** : interopérabilité et maintien en condition opérationnelle, intégration des systèmes.
- **Télécommunication** : guerre électronique (brouillage et durcissement des transmissions), interopérabilité des systèmes.
- **Composants électroniques** : évaluation fonctionnelle, analyses technologiques.
- **Activité de recherche et de développement**

  Recherches spécifiques dans les domaines de :

  - la sécurité des systèmes d'information.
  - la technologie des composants électroniques
  - la guerre électronique et les satellites d'observation
  - les systèmes d'information.
- **Activité à l'international** : coopération en matière de recherche de défense et pour la réalisation de grands programmes d'armement.

1.4 L'évolution économique

Le CELAR n'étant pas une société privée, il ne réalise pas de bénéfice ou de perte. C'est pour cette raison que je dispose de peu de chiffres.

Les dépenses du CELAR sont de 116 millions d'euros répartis entre les rémunérations et les charges sociales (38.4 million d'euros), les programmes d'investissement annuel (15.5 millions d'euros), les études, le développement et les achats (42.2 millions d'euros) et la sous-traitance avec qui le CELAR travaille beaucoup (20.5 millions d'euros).

Voici les chiffres que je peux communiquer sur l'économie du CELAR.

Année	2000	2001	2002	2003
Chiffre d'affaire	58	88	109	91
Prise de commande	113	141	71	76

Tous les chiffres sont en millions d'euros

Figure 4a. Evolution économique de l'entreprise (tableau)

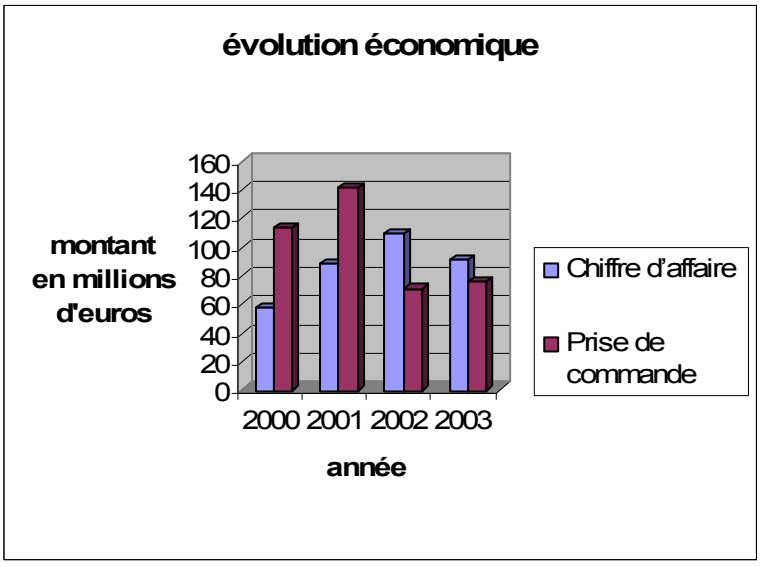

Figure 4b. Evolution économique de l'entreprise (graphique)

1.5 Les aspects juridiques

```
Centre d'électronique de l'armement
Route de Laillé
35174 Bruz

N° SIRET: 15200046900014
Tel: 02.99.42.90.11
Fax: 02.99.42.91.01

Structure juridique : Etablissement étatique
Effectif Rennes : 713
Chiffre d'affaire : 91 millions d'euros
Effectif global : 18000
Adresse siège :   DGA
            26, Boulevard Victor
            Paris 00460 Armées
```

Le CELAR est un établissement sous la tutelle de l'état. Il fait partie du ministère de la défense. Il est sous contrôle de la DGA (direction générale des armées). Les personnes y travaillant sont des fonctionnaires. Leurs avantages sont d'avoir une sécurité de l'emploi.

1.6 L'organisation

1.61 Le CELAR dans le ministère

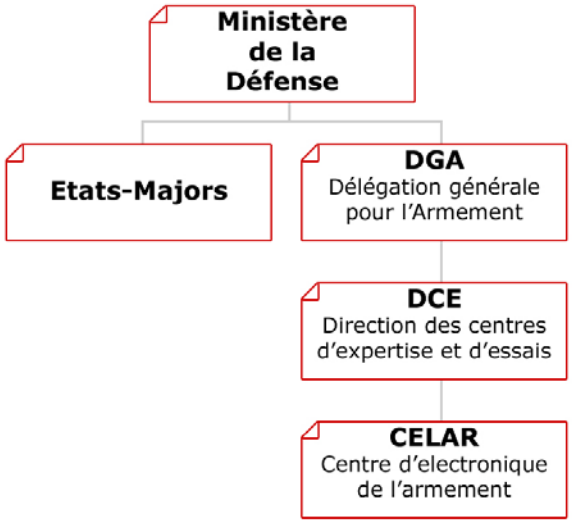

Figure 5. Organigramme du ministère de la défense

La délégation générale pour l'armement (DGA) a créé en janvier 1997, à l'occasion de la réforme de son organisation, la direction des centres d'expertise et d'essais (DCE).

Pour une efficacité accrue et une meilleure complémentarité la DCE regroupe ses 7900 personnes et ses 20 centres autour d'objectifs communs :

- Amélioration de la qualité du service à un prix toujours plus compétitif,
- Maintien des équipements et des savoir-faire à la pointe de la technologie,
- Fourniture de prestations globales.

La DCE, dont la vocation principale est d'assurer les expertises, les évaluations et les essais au profit de la défense française réalise pour ses clients des prestations comme des études, des expertises techniques, des évaluations de systèmes, des simulations, etc. Dans le cadre d'une stratégie d'ouverture vers la clientèle externe à la défense française, la DCE met à disposition le savoir-faire et les moyens de ses centres pour éprouver et qualifier les systèmes.

Les 20 centres de la DCE sont répartis en 5 ETC (établissement technique central) en fonction de leurs activités.

1.62 Au sein du CELAR

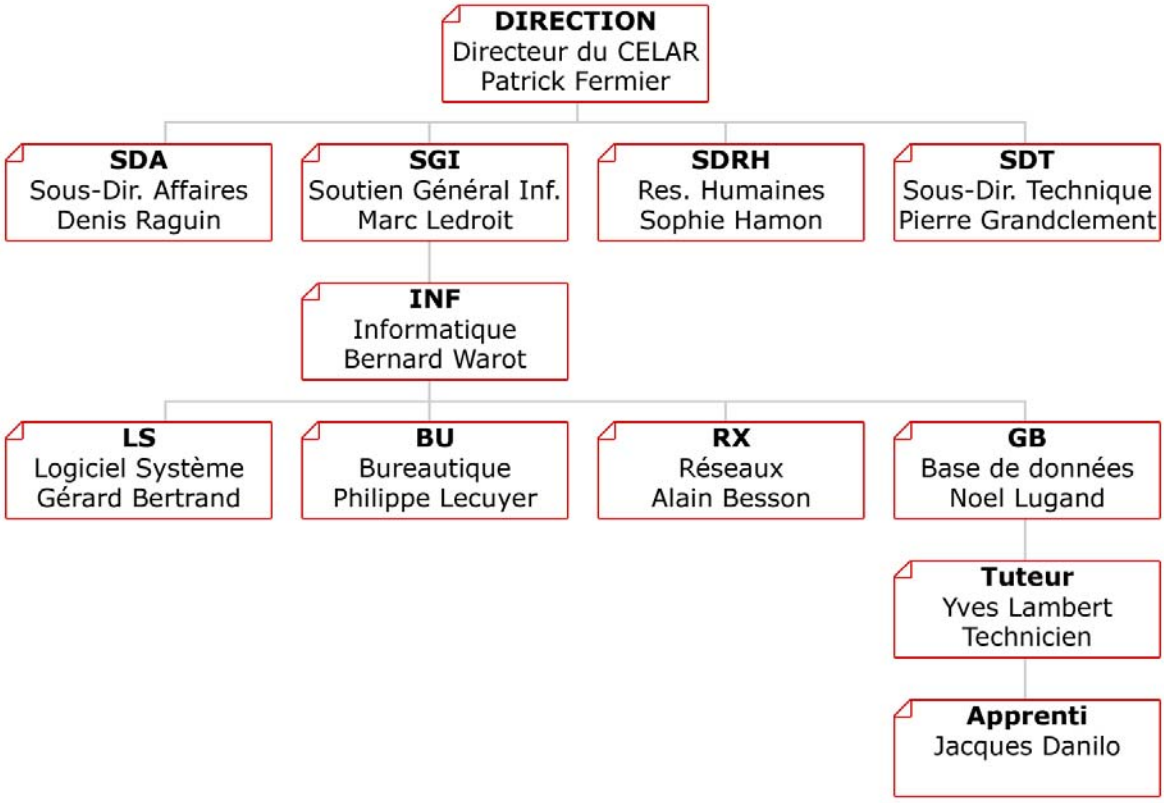

Figure 6. Organigramme interne

L'organisation générale du CELAR est composée de la façon suivante :

- La direction
- La sous direction technique
- La sous direction affaires
- Les services administratifs
- Le soutien

Sont rattachés à la direction : le bureau contrôle de gestion, le bureau sécurité, le service communication et le bureau qualité.

La sous direction technique est composée d'une équipe de direction responsable de l'animation, du pilotage des activités, du suivi des différents indicateurs de réalisation, de l'évolution des compétences ainsi que de la mise en œuvre de la politique de sous-traitance.

Elle assure la production des prestations d'expertises et d'essais organisée autour de 17 départements regroupés en deux divisions (IRIS et DIRAC) qui intègrent compétences et outils permettant d'effectuer les prestations demandées par la sous direction affaires. Elle assure aussi le management technique incluant le court terme (élaboration d'éléments propres à la SDT permettant au comité affaires de prendre ses décisions, adéquation de l'emploi des ressources et de la qualité technique des prestations) et la préparation de l'avenir à moyen et long terme c'est-à-dire le positionnement futur de la SDT. La sous direction technique effectue également le fonctionnement quotidien de la SDT, centre de responsabilité de coût, soutenu par une équipe dont le chef est l'adjoint gestion/production.

La division intégration de réseaux d'information sécurisés (IRIS) traite tous les problèmes de sécurité (cryptographie, sécurité informatique) qui concernent les systèmes d'information ainsi que l'évaluation des réseaux et systèmes de transit et de transmission mis en œuvre par les télécommunications militaires.

La division détection, interception, radar, autoprotection, composant (DIRAC) intervient dans les domaines de la guerre électronique des systèmes d'armes, de l'observation et de l'écoute spatiales, des analyses de signatures électromagnétiques. Elle a également la charge des essais, des évaluations et de la normalisation des composants. Elle centralise les questions de métrologie au sein du CELAR et assure les essais mécaniques et climatiques sur les matériels des systèmes d'armes.

La sous direction affaires vise à maîtriser l'activité productive du CELAR dans sa dimension économique (prix, coûts, plan de charges, délais,…) et à l'inscrire dans la stratégie de l'établissement.

Les services administratifs comprennent la sous direction ressources humaines – SDRH (y compris le service médico-social et le service hygiène et sécurité), la division achats/marchés – DAM, la division finance – DF.

Le soutien est assuré par la division soutien général et informatique (SGI) qui fournit la logistique nécessaire à la vie de l'établissement (dont les ateliers, les bureaux d'études et de préparation, les transports, l'édition, le bureau courrier, le gardiennage, la documentation,…). Il assure aussi le soutien du CELAR pour son domaine informatique.

Le département informatique (INF) est dirigé par Bernard WAROT. Son rôle est de superviser toutes les opérations. Ce service est divisé en plusieurs équipes :

- La section « RéseauX » (RX) qui est dirigée par Alain BESSON. Il a sous sa tutelle quatre techniciens qui sont Pierrick BUDOR, Patrick GUEZILLE, Christian BOISEAU, Philippe MARIE. L'équipe RX s'occupe de maintenir le réseau Intranet et Ethernet en état. De plus il y a trois personnes qui s'occupent du réseau PABX (réseau téléphonique).
- La section « Logiciels Systèmes » (LS) est dirigée par Gérard BERTRAND qui a sous sa tutelle quatre personnes qui sont Yves TROCHU, Pascale KERDRAON, Thierry LE SANN, Patrick AUBRY. Leurs rôles est de gérer le parc Linux et Unix mais aussi les accès à Internet.
- La section « Gestion et Bases de données » (GB) est dirigée par Noël LUGAND. Il encadre une équipe de quatre personnes qui sont Michel VANDEPUTTE, René EVENO, Denis DEFFAY, Yves LAMBERT. Leurs rôles sont de gérer les bases des données du CELAR.
- La section « BUreautique » (BU) est dirigée par Philippe LECUYER. Il a pour rôle de gérer les PC bureautique et les serveurs NT (dépannage et installation) sur tout le parc informatique du CELAR.

De plus quatre sous traitants sont à la disposition du département INF.

2. ENJEUX ECONOMIQUES

Si 30% des entreprises sont séduites par la dématérialisation des documents, c'est que derrière il y a un réel enjeu économique. En effet, les avantages sont nombreux. Le format papier demande de la place, un entretien particulier, une organisation particulière, des postes de gestion de ces documents, etc. L'informatique a résolu tous ces problèmes : La place ? un disque dur. Un entretien ? Aucun, si ce n'est une sauvegarde régulière et automatisée. Une organisation ? Un système d'arborescence, de multi-partages et de divisions… Des postes de gestion de ces documents ? Aucun ou alors une charte de bon fonctionnement ! Cela ressemblerait presque à un rêve économique ce qui permettrait un gain de temps pour tout le monde et donc une productivité accrue. Mais à l'heure actuelle, plus de la moitié des informations d'une entreprise est stockée dans des documents papiers. Les dématérialiser et les intégrer au système d'information permet d'accroître la réactivité, tout en abaissant le coût de traitement de l'information. C'est du moins ce que montre l'analyse d'IDC France dans une récente étude portant sur 200 entreprises françaises.

Selon le cabinet d'études, 94% des entreprises interrogées anticipent un accroissement important de la part des documents électroniques dans les années à venir. La majorité estime que plus de la moitié de leurs documents pourrait être dématérialisée à terme. « *Le discours autour de la dématérialisation a évolué. Les responsables informatiques ne recherchent plus le zéro papier à tout prix* » explique Karim Bahloul qui a mené l'enquête chez IDC. L'objectif actuellement est d'accélérer le traitement de l'information, la recherche et le stockage, tout en diminuant les coûts. Les entreprises souhaitent surtout dématérialiser leurs documents et les intégrer dans leurs processus métiers pour accélérer le traitement de l'information (82%) et diminuer les coûts des processus documentaires (62%) par une plus grande automatisation. 54% des entreprises cherchent également à améliorer la qualité des informations. Mais les deux principaux freins à l'automatisation des processus documentaires sont une législation contraignante (43%) et une résistance au changement (59%), juste avant le coût des investissements (38%). L'implication de la direction générale est donc indispensable pour réussir un projet de ce type. « L'automatisation des processus documentaires touche les relations internes entre collaborateurs, mais aussi de plus en plus les clients, prospects et partenaires au travers de

la dématérialisation des flux commerciaux. La sécurité des formulaires comme des documents est donc un enjeu croissant » précise Karim Bahloul.

30% des entreprises possèdent déjà une solution technique dédiée et opérationnelle et 54% prévoient de mettre en place une solution informatique d'ici un à deux ans. Les principales fonctionnalités attendues des outils sont l'indexation et la recherche d'informations au sein des documents (88%), un bon niveau de sécurité (68%), et une intégration au système d'information (67%). La présence d'un moteur de workflow n'arrive qu'en sixième position (54%) après la possibilité d'annoter et de formater automatiquement les documents. L'étude relève aussi que deux entreprises sur trois (64%) manipulent déjà des formulaires électroniques. Elles les utilisent majoritairement sur leur site web pour récolter des informations (80%) et dématérialiser des dossiers (60%), le dossier client par exemple. La majorité des entreprises estiment que XML et le format PDF d'Adobe sont complémentaires : PDF pour présenter et stocker les documents (89%) et XML pour intégrer et manipuler les données (81%).

Mais cette vision économique n'est pas sans risque. En effet, même si une majorité d'entreprises se voit intéressée par le passage en numérique de leurs papiers, elles restent pour la plupart peu confiantes dans le système informatique : peur de plantages, peur de pertes des documents et une certaine crainte des employés à l'utilisation d'un ordinateur. Car même si dans notre milieu cela devient plus que banal d'utiliser un ordinateur au quotidien, chez les plus de 40 ans il existe encore une certaine crainte sur le monde informatique. C'est pourquoi les entreprises hésitent longuement sur le passage du papier en version numérique. L'utilisation d'un ordinateur au quotidien au sein d'une entreprise nécessite un minimum de connaissances pour l'utilisateur de la machine ainsi que le plus souvent d'une formation spéciale orientée vers la GED, Gestion Electronique de Documents, pour l'utilisation d'un logiciel spécialisé dans la recherche, gestion et organisation des documents numériques.

Le passage vers le numérique réalise donc à terme une économie importante, même si le passage du format papier au format numérique coûte cher. Il existe cependant des entreprises de services qui proposent de venir structurer les documents papiers et proposer un système de gestion particulier pour chaque entreprise. Ces entreprises vendent un système complet, de la numérisation à la formation des employés sur un logiciel spécifique à la gestion de ces documents numériques.

L'économie est un facteur important dans une entreprise. Le passage vers le numérique, même s'il est long et souvent difficile à mettre en place, permet au fil des ans de gagner en productivité. C'est pourquoi les entreprises se mettent peu à peu à une dématérialisation de formulaires…

3. LA LEGISLATION

La réglementation en ce qui concerne les échanges électroniques est en rapide évolution. Depuis plusieurs années, le gouvernement et les administrations ont mis en place une réflexion pour réagir rapidement aux avancées des techniques et des pratiques. Cette réflexion est toujours en cours. S'inscrivant dans une double stratégie de simplification des relations entre les administrations et la société et de développement de la société de l'information, elle est aussi liée aux négociations sur le commerce et le commerce électronique, sur la protection de la vie privée, sur la preuve et la signature.

Le développement des échanges électroniques doit s'effectuer en respectant à la fois la réglementation générale en vigueur et les nouvelles règles qui se mettent en place pour le fonctionnement d'Internet et des réseaux.

Dans la plupart des cas, il s'agit de transposer à l'espace électronique les règles édictées pour les transmissions papier. En fait, il est en général possible d'effectuer les échanges en respectant la réglementation, à condition que celle-ci ne précise pas qu'elle traite d'un document papier. Une généralisation sémantique est alors possible pour étendre des notions comme document. C'est surtout dans le domaine de la preuve et de la signature que des apports nouveaux doivent être réalisés. Ils sont en cours d'élaboration à la fois en France (textes législatifs) et en Europe (préparation de directives).

Une série de textes importants a marqué l'attention constante des gouvernements aux développements des EDI dans l'administration. Dans ces textes, il a été fait systématiquement référence à l'utilisation de normes et des standards de l'Internet. Dans certains d'entre eux, la norme EDIFACT était citée, car elle était alors la seule solution pour les échanges électroniques automatiques. La démarche XML peut tout à fait se situer dans le prolongement de la démarche EDIFACT. La problématique de cette évolution dans la continuité est l'objet de la présente étude.

Le rôle de l'Etat dans la crédibilisation des échanges électronisés est doublement important, puisqu'il est à la fois un opérateur très présent et une référence, et ceci très fortement dans la société française en général. Il est d'autant plus important dans l'espace socio-sanitaire, dont les organismes sont tous liés de façon plus ou moins étroite à l'administration et sont en tout état de cause sous tutelle publique pour l'essentiel.

Dans l'évolution qui a accompagné les nouveaux réseaux autour de l'EDI et d'Internet, une première pierre a été posée par la loi n° 94.126 du 11 février 1994 relative à l'initiative et à l'entreprise individuelle (dite "Loi MADELIN"). Dans le titre 1, *"Simplification de formalités administratives imposées aux entreprises",* l'article 4 stipulait que *"Toute déclaration d'une entreprise destinée à une administration, personne ou organisme ... peut être faite par voie électronique, dans les conditions fixées par voie contractuelle."* . L'orientation EDI était reprise et détaillée dans la circulaire du 31 janvier 1994 relative à l'établissement d'un cadre coordonné de gestion de l'informatique dans l'administration En 1996, la circulaire du 16 septembre du Premier ministre (dite "Circulaire Juppé") intégrait *"les échanges de données informatisées avec les entreprises et les particuliers"* dans les schémas directeurs ministériels des systèmes d'information et de communication. Enfin, la circulaire du Premier ministre recommandait le 16 janvier 1997 *"l'emploi de la norme EDIFACT-ONU par les administrations"*. Le texte précisait : *"Dans tous les nouveaux projets de dématérialisation des échanges avec leurs partenaires et usagers, elles utiliseront, lorsqu'ils existent, les messages édictés en tant que normes européennes et françaises correspondant à leurs besoins".* La seule norme existant à ce moment étant EDIFACT, le texte recommandait donc la migration des formats propriétaires. L'important est que l'Etat faisait référence à une norme, ce qui représente un choix important, jamais remis en cause depuis lors (cf. infra Normalisation). En 1997, le rapport confié par le ministre de l'Economie à Francis Lorentz sur le commerce électronique soulignait le caractère exemplaire du rôle de l'Etat. Un groupe de travail particulier, animé par Jean Paul Baquiast, auteur d'un premier rapport sur le sujet, insistait sur l'intérêt réciproque des entreprises, de l'Etat et des organismes sociaux à développer les téléprocédures.

La normalisation proprement dite est le fait d'une organisation internationale hiérarchisée. Il faut seulement rappeler que, pour tout domaine - et il en sera ainsi pour les échanges électroniques dans le secteur social - un très grand nombre de groupes spécialisés est concerné. En effet, la normalisation va porter aussi bien sur les protocoles de télécommunications que sur les structures des échanges ou sur les données elles-mêmes. Il existe des groupes qui travaillent sur les échanges et d'autres qui définissent les structures d'adresses, d'autres la nomenclature pour les pays,… L'organisation générale et officielle de la normalisation est simple. L'ISO, International Organization for Standardization (http://www.iso.ch) est le regroupement au niveau international des

organismes nationaux de normalisation, en France l'AFNOR (http://www.afnor.fr). Au niveau européen, des accords particuliers ont mis en place un système de coopération et de règles communes, dans le cadre du CEN, Comité Européen de Normalisation (http://www.cenorm.be). L'accord européen prévoit que les normes CEN s'appliquent obligatoirement comme normes nationales après un délai (trois ans).

3.1 L'ISO

Le comité technique en charge des technologies de l'information est le JTC1, et certains de ses comités (SC) concernent plus directement le développement des EDI. Il faut cependant noter que ce développement lui-même fait l'objet d'une procédure spéciale, évoquée ci-après. Ce sont notamment le SC17 (cartes, l'AFNOR étant le convenor pour les cartes à micro-circuit), et surtout le SC32 (Gestion et échange de données – Working Group 1 pour Open EDI, WG2 pour les meta données entre autres), le SC34, qui a publié SGML (ISO 8879;1986) et continue depuis de publier les normes d'application et de développement à l'exclusion, actuellement, du volet XML qui relève du monde Internet, lequel a un statut particulier dans la normalisation (cf. infra).

3.2 Le CEN

Une action particulière a été lancée en 1997 pour faciliter l'évolution vers la société de l'information en promouvant des produits et services visant à la normalisation et donc à l'interopérabilité. C'est le programme ISSS – Information Society Standardization System, sous l'égide duquel ont été placés les différents comités concernés par les technologies d'information, y compris l'EBES (cf. infra). C'est dans le cadre de ce programme que se place le soutien européen à des projets facilitant le commerce électronique par la standardisation – Electronic Commerce Open Marketplace for Industry Sectors (ECOM-IS). Un programme de sensibilisation vers les PME est aussi en place. Le CEN comprend un certain nombre d'ateliers particuliers (workshops) dont certains sont particulièrement importants pour le développement des EDI. A côté de l'European Board for EDI Standards (EBES – cf. l'organisation particulière de l'EDI), ce sont entre autres les groupes sur les annuaires, les cartes à microprocesseur, les différents groupes spécialisés du commerce électronique. Le CEN ISSS a considéré qu'XML EDI était un thème particulièrement important et lui a consacré un atelier spécial. Ce groupe

du CEN suit donc l'évolution des travaux initiés entre les industriels américains (pour la plupart) d'OASIS et le monde EDIFACT (cf. infra). Le business plan de ce groupe indique clairement les orientations. Il affirme que XML formera la base pour les échanges de la prochaine génération de systèmes, rendant ainsi l'EDI beaucoup plus facile et moins coûteux, tout en préservant les acquis actuels. Les objectifs du groupe sont d'identifier les besoins des utilisateurs, étudier les outils XML et recommander des règles pour la migration des applications EDI, participer à la normalisation internationale, concentrer des efforts particuliers vers les PME.

3.3 L'AFNOR

En France, l'AFNOR est essentiellement organisée en groupes miroir de ceux créés au CEN et à l'ISO, où elle est le représentant national. Plusieurs comités intéressent directement le développement des EDI en dehors des relations directes avec EDIFRANCE : le Comité d'orientation stratégique "Technologies de l'information et de la communication", la Commission de normalisation "CN données".

La CN données suit en particulier "les travaux récents en matière de méthodologie concentrés sur le partage et l'enregistrement des données dans des répertoires directement accessibles" et donc les travaux sur le BSR.

3.4 Le BSR (Basic Semantic Register)

Le BSR est une initiative de l'ISO TC154 pour proposer un répertoire de références universel de la société de l'information afin de remédier à la prolifération des dictionnaires et des définitions de données souvent sémantiquement ambiguës ou contradictoires. L'idée, vieille de plus de dix ans, est de développer un glossaire multilingue des concepts d'informations élémentaires, permettant de garantir une interopérabilité sémantique entre les différentes langues et ne pas imposer l'anglais comme seule référence universelle. Le BSR doit pouvoir accueillir la définition d'informations propre aux métiers des différents secteurs d'activité avec des liens vers des répertoires de données sectoriels, nationaux ou internationaux. Un consortium français, regroupant l'AFNOR, l'INSEE, EDIFRANCE et d'ARVA, a pour objectif de développer

un outil de gestion du BSR. Le BSR est aujourd'hui au centre de débats souvent vifs car il peut être une réponse à la difficulté de préciser et partager les sémantiques du commerce électronique, notamment exprimées dans des schémas XML. Le principe du BSR est de définir une classe de données puis de préciser progressivement les différentes variantes de la donnée par des attributs situés pratiquement à droite de la définition de classe. Une codification neutre permet de traiter symétriquement les différentes langues.

Les principales sources pratiques pour nourrir le BSR aujourd'hui sont les dictionnaires EDIFACT. Cependant, les critiques sont nombreuses, la principale ayant trait en fait à la légitimité même de la démarche, qui suppose bien qu'il existe une sémantique vraiment commune à tous les secteurs et tous les pays ou tout au moins que la définition d'un dictionnaire commun est plus efficiente que la mise en relation de dictionnaires multiples. La démarche EDIFACT avait permis d'établir un tel dictionnaire unique, le TDED (cf. infra) mais il faut reconnaître aussi que les interprétations concrètes variaient souvent d'un pays à l'autre ou d'un secteur à l'autre pour une même entité. La référence à une autorité unique est aussi difficile à assurer mondialement. Le succès du BSR dépendra sans doute de sa faculté à s'intégrer dans la notion de "Namespace" et plus généralement aussi dans la capacité de ses promoteurs à suivre le développement rapide des outils XML. Il dépendra aussi de la souplesse et de la flexibilité de la démarche, et aussi de sa rapidité, parce que la mise en place des échanges du commerce électronique exige des solutions à relativement court terme.

3.5 La signature électronique

De nombreux documents demandent l'apposition d'une signature. Cette signature atteste que son auteur laisse une marque personnelle sur le document et qu'il manifeste son accord sur le contenu et se l'approprie.

La loi du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, apporte d'importantes modifications au code civil en ce qui concerne la notion de signature et l'écrit pour preuve. Pour la première fois, le code civil dans l'article 1316-4 énonce une définition de la signature qui montre deux caractéristiques présentées par toutes les signatures : la signature identifie le signataire et manifeste son consentement au contenu du document signé.

Article 1316-4 – La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte (…)

Cette définition est valable pour tout type de signature. Par analogie avec l'écrit défini dans un autre article de la loi, la signature, jusqu'ici uniquement manuscrite, pourra adopter la forme électronique. La signature électronique répondra naturellement à la même définition mais des précisions seront apportées sur la façon dont elle est réalisée. En effet, toute signature répond ainsi pour la création à un véritable processus. Si la signature manuscrite est le résultat d'un procédé manuel, qui n'a généralement pas besoin d'être organisé, la signature électronique est produite par un procédé informatique d'identification fiable.

Lorsqu'elle est électronique [la signature], 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 du 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.

La loi française en application de la directive 1999/93/CE du parlement européen a donné une reconnaissance juridique à la signature numérique. La signature électronique des techniciens s'est vue imposée par le droit des exigences techniques et juridiques pour devenir une signature électronique sécurisée.

La signature électronique se présente sous une forme numérique qui est fonction, à la fois, de l'identité du signataire mais encore du contenu du document signé. Instrument de sécurité, elle présente les caractéristiques suivantes :

- elle met en œuvre des moyens cryptographiques (clé privée et clé publique)…
- attestée par un prestataire de services spécialisés (le prestataire de service de certification électronique)…
- au moyen d'un message électronique spécialisé appelé « certificat ».

Le décret numéro 2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du Code Civil et relatif à la signature électronique explicite les termes de l'article qui annoncent les conditions dans lesquelles « la fiabilité de ce procédé est présumé, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie ». La signature qui respecte les impératifs techniques du décret prend alors le nom de signature électronique sécurisée (SES). Seul ce type de signature permet de bénéficier de la présomption de fiabilité instaurée par le code civil, ce qui lui permet de jouer sur un message électronique le même rôle qu'une signature manuscrite sur papier.

La fin du premier alinéa de l'article 1316 apporte une précision importante. En visant le support et les modalités de transmission, le texte ouvre la voie à deux variétés d'écrit : l'écrit traditionnel sur support papier et l'écrit sous forme électronique. La nouvelle modalité, l'écrit sous forme électronique, peut comme l'écrit papier traditionnel, être porteur de force probante. Le principe est stipulé par l'article 1316-1 :

Article 1316-1. – L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

L'écrit de forme électronique doit être accompagné de certaines caractéristiques qui vont de soi dans l'écrit papier traditionnel, mais qui devront être intégrées, maintenues et vérifiées dans le contexte électronique. Selon l'article 1316-1, il faut que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. Pour l'écrit traditionnel, il peut être simple de déterminer son origine : papier à en-tête, indication de l'auteur en toutes lettres, éléments postaux etc. La chose est plus délicate en électronique surtout s'il y a télétransmission. Il y a aussi la question de la pérennité du support : malgré une apparente fragilité, le papier peut se conserver plusieurs siècles. Quant à l'écrit électronique, il ne possède pas de support et n'est constitué que d'informations élémentaires qui peuvent cheminer par des voies différentes et donc se perdre pendant les télétransmissions. D'où

une exigence d'intégrité à respecter. Cet article est une étape notable dans l'histoire de la dématérialisation de l'écrit.

3.6 L'échange électronique

La situation juridique peut s'analyser aussi simplement que possible lorsque les personnes qui échangent un document sont face à face. Les relations juridiques peuvent se dérouler dans un environnement sûr et la transmission d'un document de l'un à l'autre ne vient pas ajouter des éléments d'incertitudes juridiques. Ce n'est pas le cas avec les échanges électroniques. Les personnes y sont absentes. Le contrôle du bon déroulement et de la régularité des opérations repose généralement sur le contrôle visuel. La présence physique des utilisateurs permet à chacun de contrôler l'identité de l'autre, la date et de l'heure de l'échange. On peut contrôler que l'échange est fait volontairement. Cette présence physique et les possibilités de contrôles visuels garantissent de nombreux concepts juridiques, comme :

- la capacité et la compétence de chacun des acteurs contrôlés par l'autre,
- l'échange des consentements, parce que simultanément l'un offre et l'autre accepte,
- la datation des actes et documents,
- la pré-constitution de la preuve,
- la localisation et la datation des actes et documents,
- la formalisation de l'ensemble des éléments précédents par la signature.

Au contraire, l'échange de messages électroniques s'analyse comme une situation juridique entre personnes absentes. L'absence physique rend les garanties citées incertaines :

- il est impossible de vérifier visuellement la capacité et la compétence des personnes.
- l'échange des consentements est douteux car il n'est plus simultané ; il y a un délai entre l'offre de l'un et l'acceptation de l'autre.

- la datation de l'acte est problématique : un contrat existe d'abord pleinement pour l'un (l'offreur) alors que l'autre n'est pas encore lié (acceptant).
- la pré-constitution de la preuve doit être contrôlée puisque l'acte ou le document n'est plus échangé de la main à la main.
- la localisation de l'acte n'est plus unique mais double entre le lieu de l'émetteur et le lieu du destinataire ;
- l'apposition des signatures n'est plus simultanée.

Lorsqu'on considère les échanges électroniques au niveau technique, on s'aperçoit que les utilisateurs ont des préoccupations techniques proches des préoccupations juridiques. Les utilisateurs des systèmes informatiques sont à la recherche de sécurité pour ce qu'ils confient aux télécommunications : échanges électroniques privés, commerce électronique ou relations électroniques entre entreprises et administrations. Quelle que soit la méthode, viser la sécurité des échanges consiste à s'assurer de la réalisation d'un certain nombre de garanties techniques. Ces garanties visent à apporter autant de certitudes dans les conditions des échanges électroniques ainsi que dans les acteurs qui sont aux deux bouts de la ligne, à l'émission comme à la réception.

Les garanties les plus recherchées sont les suivantes :

- l'authentification permet d'indiquer avec précision l'origine d'un message électronique expédié par télécommunications,
- l'intégrité garantit que le message électronique reçu par le destinataire lui est parvenu dans l'état où il a été émis,
- la confidentialité est obtenue lorsque le message n'est compréhensible que par le destinataire ou par les personnes autorisées,
- l'horodatage garantit avec exactitude le moment, en date et heure, où un quelconque événement a pu survenir.

Ces garanties de sécurité sont concrètement obtenues par des moyens divers : équipements et terminaux, logiciels spécialisés, réseaux et/ou services ou par un mélange des uns et des autres.

Mais il existe peu de textes législatifs dans le droit interne qui donnent des indices sur le cadre juridique de la transmission électronique. L'article 1316 du code civil précise dorénavant que l'écrit, surtout sous sa forme électronique, est destiné à être transmis. Cependant la loi numéro 94-126 du 11 février 1994 relative à l'initiative et à l'entreprise individuelle (dite Loi Madelin) fixe un cadre général pour les déclarations faites par voie électronique. En effet, l'article 4 de cette loi fournit le cadre légal pour la transmission de télé procédures.

Article 4-I – Toute déclaration d'une entreprise destinée à une administration, personne ou organisme visés à l'article premier peut être fait par voie électronique, dans les conditions fixées par voie contractuelle.

Article 4-II – Ce contrat précise notamment pour chaque formalité, les règles relatives à l'identification de l'auteur de l'acte, à l'intégrité, à la lisibilité et à la fiabilité de la transmission, à sa date et à son heure, à l'assurance de sa réception ainsi qu'à sa conservation. La réception d'un message transmis conformément aux dispositions du présent article tient lieu de la production d'une déclaration écrite ayant le même objet.

Article 4-III – Lorsque la transmission d'une déclaration écrite entre une entreprise et une administration, personne ou organisme visés à l'article premier est soumise à une date limite d'envoi, le cachet de la poste fait foi de la date de cet envoi.

L'article 4-II de la loi Madelin liste une série de garanties de sécurité à prendre en compte dans le contrat à passer entre le déclarant et l'administration. Parmi ces garanties figurent l'identification et l'intégrité qui sont particulièrement à l'honneur avec la loi numéro 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique. Mais les autres peuvent être envisagées quelques instants dans la mesure où elles auraient un rôle à jouer en matière de conversation des déclarations.

4. DE L'ETUDE A LA REALISATION

4.1 Mise en œuvre

La dématérialisation de formulaires est une étape importante pour une bonne gestion future. Il faut savoir ce qui peut être utile et inutile dans une conversion d'un formulaire papier vers un formulaire numérique. Les numéros de pages, la redondance de noms, les informations inutiles, etc. Un formulaire a été pensé pour tous les cas possibles, mais il s'avère qu'au bout d'un certain temps certaines informations ne sont jamais réutilisées.

Au sein du CELAR, si nous prenons l'exemple de la fiche de transport, certaines informations comme le nom, le prénom, l'âge, le numéro de téléphone et la fonction ne sont pas importantes si le matricule les remplace. Une simple coupure entre la table du personnel et la fiche de transport fera l'affaire. Nous gagnons donc de la place sur le disque ainsi qu'une rapidité d'exécution. Toujours avec cet exemple, la législation ne permet plus de transport à plus de 2 dans une voiture. Nous pouvons donc enlever lors de la dématérialisation les 3-4 lignes de la version papier.

Dans tous les cas de dématérialisation, il faut prévoir la gestion des données stockées. Certaines choses sont en trop, d'autres manquent, il faut savoir s'adapter. Une étude est donc à mener, en partant du fonctionnement actuel pour en créer un, ressemblant il est vrai, sur informatique. Le workflow est important aussi. Il faut connaître avant de matérialiser le processus de dématérialisation toutes les étapes qu'il y a après le remplissage de la fiche. Le formulaire est ensuite donné à la secrétaire qui va le faxer au département transport ; ce dernier remettra la fiche à l'un des employés pour qu'il réserve un véhicule et le prépare, fasse sa révision, etc. Si toutes ces informations ne sont pas transmises à la personne chargée de la mise en œuvre d'une dématérialisation, le travail sera bâclé, erroné. Dans notre cas, cela nous a permis de définir des moments : le formulaire est en attente, le document est envoyé puis ce document est traité. Nous avons donc réalisé un cahier des charges pour réaliser une application de dématérialisation de formulaires qui traite également le workflow.

4.2 Echange de données

Lors de la création d'une application mettant en œuvre un formulaire, il faut savoir que ces données seront généralement stockées dans une base de données.

Cela fonctionne généralement via une application client serveur. Le client, à l'aide de son navigateur web (Internet Explorer, Nescape, Mozilla ou autres) vient se connecter sur un serveur généralement en Intranet, afin de pouvoir remplir un formulaire. Cette conception est dite client léger : le client n'a rien à installer pour pouvoir remplir le formulaire.

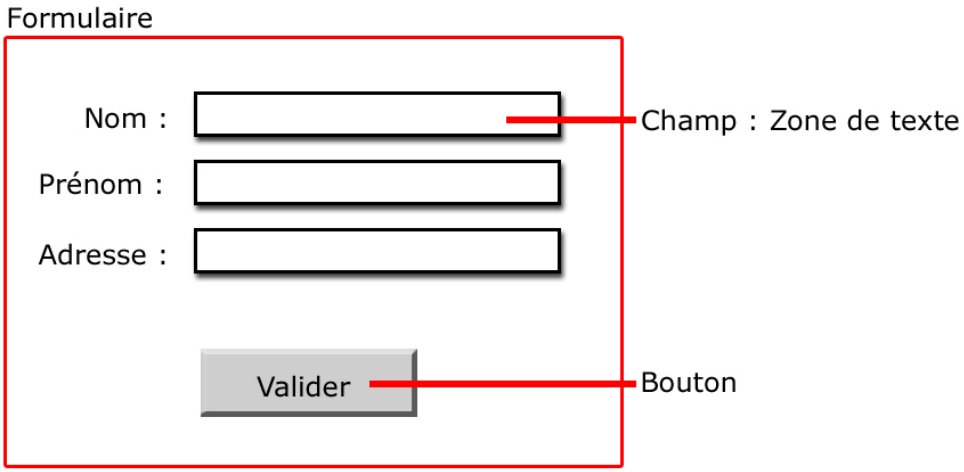

Figure 7. Exemple de Formulaire

Dans le formulaire se trouvent plein d'informations, contenues dans des champs. Ces informations vont être envoyées, suite à la validation du formulaire, au serveur afin d'y être traitées et stockées. Le voyage se fait via un réseau d'entreprise ou via internet. Ces données, acheminées sous forme de paquets sur le réseau, atteignent le serveur pour être analysées, traitées et stockées dans des bases de données.

Ces échanges de données se font donc avec un applicateur et une base de données. L'applicateur est un langage de programmation qui va interroger la base pour pouvoir retourner quelque chose à l'utilisateur. Les applicateurs (interpréteurs) sont, pour ne citer que les plus connus PHP, ASP, Java, JSP, HTMLDB,… Tous ces langages utilisent le même fonctionnement algorithmique : ils se connectent à la base, font une requête qui leur retourne un tableau de résultat, ils exploitent ce tableau en faisant de la mise en page

et du traitement puis se déconnectent de la base. Ce processus est le même pour tous ces langages mais leur écriture est différente.

L'échange de données informatiques (EDI) n'est qu'une forme de l'échange d'informations utilisant les réseaux. Il peut être défini comme l'échange entre applications hétérogènes, avec une automatisation des traitements. Dans un EDI, c'est le processus d'échange qui est informatisé. L'EDI met en relation des systèmes d'informations en ayant pour objectif des gains en efficacité et en productivité tout en automatisant certains aspects ou la totalité de ces processus. Ainsi, il s'agit d'échanges non seulement de machines mais de systèmes d'informations à systèmes d'informations, le tout sans qu'il y ait à modifier les applications amenées à fournir ou à recevoir des informations. Par ailleurs, il s'agit bien d'échanges automatisés, ce qui suppose un investissement et donc une certaine fréquence. En effet, l'EDI doit savoir s'adapter par rapport aux différentes applications distribuées au sein d'une entreprise et en externe : boite de messageries, applications web, applications réseaux, etc.

Les supports physiques permettent une première distinction. L'échange par bande ou disquette a joué un rôle important dans le développement de l'informatisation et l'amorce des EDI. Les échanges par réseaux de télécommunications se divisent eux-mêmes en de nombreuses techniques, dont la plus importante en France a été la télématique, à coté des réseaux professionnels spécialisés, support privilégié de l'EDI jusqu'ici. La caractéristique des techniques Internet/Intranet est de rendre les communications indépendantes du réseau physique sur le plan du contenu car les capacités du réseau vont se traduire par des contraintes de débit et de fiabilité.

L'autre caractéristique de l'EDI est l'échange d'information structurée. C'est aussi par-là qu'il faut le distinguer. Il ne suffit pas d'échanger des fichiers texte ou des images, même automatiquement, pour faire de l'EDI. Encore faut-il que ces documents soient suffisamment « auto-renseignés » et structurés ou au moins contenus dans des enveloppes permettant d'identifier clairement le contenu et les conditions de l'échange. Il faut en effet pouvoir adresser le document à l'application à laquelle il correspond et garder une trace analysable des échanges.

Enfin, l'EDI se caractérise par l'automaticité des traitements. C'est à dire qu'il doit être distingué, en particulier, de l'échange totalement contrôlé par messagerie, même si celui-ci consiste en l'envoi d'un formulaire structuré. Par ailleurs, l'EDI peut être plus ou

moins intégré aux applications qui dialoguent. L'évolution même des systèmes et des échanges va vers une prise en compte de l'échange.

Le développement d'XML est mené dans le W3C par un nombre croissant de groupes de sorte que le XML devient l'outil central sur internet. Le groupe le plus important est l'Architecture Working Group qui a en charge le XML lui-même. Il comprend 4 groupes de travail : sur le méta-langage (Core), sur les Schémas, le lien (Linking) et les requêtes (Query). Des perspectives portent sur les applications distribuées, les protocoles de réseaux et les systèmes de messagerie.

4.3 Stockage et gestion

Arrivées sur le serveur, les informations contenues dans les champs du formulaire sont ensuite traitées pour pouvoir être stockées dans une base de données, sorte de grands tableaux où se trouvent toutes les informations. Il existe actuellement plusieurs types de bases de données développées par différentes entreprises qui se disputent la première place du marché. Voici un tour d'horizon des différents systèmes de bases de données avec leurs avantages et inconvénients :

InterBase : ce système de gestion de bases de données (SGBD) possède beaucoup de qualités ; tout d'abord, l'administration d'InterBase est facile, et elle est auto-optimisée et auto-administrée. De nombreux outils sont disponibles pour gérer InterBase. Il est fiable et robuste. Il supporte de nombreuses instructions avancées. Enfin, l'un de ses principaux points forts est sa disponibilité dans sa version OpenSource. Il existe néanmoins une version payante, portant le nom de Desktop Edition, possédant des fonctions avancées… InterBase est optimisé pour être utilisé avec C++ et Delphi.

Filemaker : issue du monde Mac, c'est un SGBD de type bureautique. Sa simplicité et sa comptabilité Win/Mac l'on rendu très populaire auprès des Mac'iens et des transfuges Mac/PC. Il en existe toute une gamme : Pro, Developer, Serveur Advanced, Mobile. Comme MS-Acces, il permet de développer des solutions en utilisant un environnement interne et simpliste, ou par le biais de plugin en C. Comparativement aux autres SGBDR (Système de gestion de bases de données relationnelles), il est très limité en terme de montée en charge. Pour la création de liens plusieurs stratégies sont possibles (import export avec mise à jour, XML, etc.)

Microsoft SQL Server : Il a l'avantage de proposer un langage procédural facile et un langage SQL proche du standard. Son administration, sans être simple, n'atteint pas des sommets de complexité, étant très visuelle, grâce aux nombreux assistants dont Microsoft a le secret. Enfin, SQL Server propose des instructions avancées. An niveau du SQL, SQL Server possède un bon niveau avec la présence d'un SQL assez complet et assez normatif (le transact-SQL). Possibilité de faire des sous requêtes, système de procédures, gestion de l'indexation textuelle, SQL serveur possède des qualités certaines.

Access : Access est aussi bien un outil grand public que professionnel. Il est assez performant en tant que SGBD allié à un outil de développement intégré qui en facilite l'utilisation. Access peut, en tant qu'outil de développement, être utilisé conjointement avec un véritable serveur de base de données SQL pour bénéficier des avantages du Client/Serveur, sous certaines conditions. Un néophyte peut facilement utiliser Access et se créer une base de données complète, grâce à de nombreux assistants pour l'aider ; à remarquer, son intégration dans Office.

MySQL : C'est une version très courante en hébergement public, grâce à sa très bonne intégration dans l'environnement Apache/PHP. En revanche, MySQL ne supporte qu'une faible partie des standards SQL-92, ne supporte ni les sous-requêtes, ni les triggers, ni les procédures stockées. MySQL est un très bon choix si vous souhaitez l'utiliser en relation avec PHP avec des requêtes simples, mais manque cruellement de fonctions par rapport aux autres SGBD. Il existe plusieurs versions de ce produit : en version standard (licence GPL), MySQL Max (amélioration des performances), MySQL Pro (licences commerciales) et MySQL Classic (aucune intégrité référentielle, aucun trigger, … et seulement en licences commerciales).

Oracle : Oracle n'est pas un SGBDR optimisé pour les petites bases de données. Sur de petits volumes de traitements (2Go par exemple) et peu d'utilisateurs (une trentaine) vous pourriez trouver des benchmark ou MySQL offre des performances quasi comparables à Oracle. Si l'on monte à de plus importants volumes (supérieur à 200Go) et un grand nombre d'utilisateurs (supérieur à 300) les écarts de performance entre MySQL et Oracle seront très visibles.

PostGreSQL : C'est un très bon SGBD, fiable et relativement performant, tout en restant simple d'utilisation. PostGreSQL supporte la majorité du standard SQL-92 et possède en plus un certain nombre d'extensions. Enfin, de nombreux modules sont disponibles. Il est très performant pour des applications moyennes ou avec un volume de

données assez important, mais il n'est utilisable que sous Linux, ce qui implique un certain nombre de connaissances techniques de ce côté-là ! Il est possible de l'installer sous Windows, mais cela doit se faire par l'intermédiaire de CygWin, qui requiert également ces connaissances. Il est gratuit, mais ne prend pas en compte le XML et les services Web.

Adaptive Server Enterprise (ASE) : anciennement nommé SyBase SQL Server, c'est un moteur SGBDR qui se comporte extrêmement bien en environnement OLTP ou mixte. En deux mots : puissance et simplicité. Bien que semblables au niveau architectural, MS-SQL et ASE suivent des stratégies différentes : Microsoft vise l'administration zéro, tandis que SyBase tend à améliorer la stabilité, les performances et les fonctionnalités de son moteur. Preuve en est l'évolution du nombre de paramètres de configuration (37 sous MS-SQL 2000, 228 sous ASE 12.5). Dans sa version 15 (fin 2004), ASE se comporte comme un système nerveux, capable de gérer dynamiquement ses paramètres de configuration selon la demande des clients connectés et les ressources disponibles, via un optimiseur couplé à un système expert. En comparaison avec Oracle, il demande moins de ressources et son administration est simpliste.

4.4 Automatisation des processus métiers

La dématérialisation permet également une automatisation des processus métiers, c'est-à-dire qu'elle permet une traçabilité du document depuis l'envoi d'un formulaire jusqu'à sa validation. En effet, la dématérialisation permet de gagner du temps, donc d'automatiser les échanges. Le formulaire ne passe plus par des dizaines de mains avant de finir sur le bureau de la personne compétente. Désormais, le formulaire peut lui être envoyé par mail directement après la validation du formulaire par le client.

Auparavant, lorsqu'un client envoyait un formulaire par la poste à une entreprise, cette entreprise le recevait en un jour, puis le triait en une ou plusieurs journées avant d'être envoyé vers une personne qualifiée pour utiliser ce formulaire… Il fallait donc, en général, un jour et demi pour que le formulaire passe du client au destinataire. Maintenant, il est possible d'envoyer par mail un formulaire ou bien encore de l'inscrire dans une base de données qui pourra être lue et utilisée par le destinataire dans l'heure qui suit… Ce gain de temps coïncide avec ce qui s'appelle les processus métiers. En effet, le formulaire ne passe plus par un facteur, une secrétaire, un trieur de courrier, un

coursier, une autre secrétaire,..., mais passe tout simplement par un réseau public (Internet) ou privé (Intranet) pour être remis au destinataire. Ce gain en ressources humaines permet une meilleure gestion du personnel et donc une meilleure rentabilité à une entreprise.

Jean Claude La Haye, gérant de Synphonat, explique *« nous commercialisons des compléments nutritionnels par correspondance avec 400 commandes par jour, dont 150 par courrier. Avec 25 employés, nous voulions éliminer la tâche fastidieuse que représente leur traitement en l'automatisant. Cela nous a permis d'avoir un gain de traitement de l'ordre de 30 à 40 %, ce qui nous permet de ne plus craindre les pics d'activité. Cette amélioration contribue beaucoup à la qualité de notre travail. Nous avons pu également former les opérateurs pour les redéployer sur des fonctions d'accueil client, plus lucratives et valorisantes. Ensuite notre prochain objectif sera de dématérialisé le dossier client pour le passé vers un dossier client électronique. Nous envisageons de numériser tous les documents entrants, y compris les courriers, pour les indexer et les stocker dans une GED. Nous accéderons ainsi en temps réel au dossier numérique d'un client. Cette approche nous parait fondamentale quand on parle de qualité de service client ».*

5. UTILISATION ET ERGONOMIE

5.1 Aisance d'accès

Le monde Internet nous a ouvert un nouveau moyen de communication, qui, utilisé d'une bonne façon nous aide énormément. Dans le domaine de la dématérialisation, le but ne consistait pas seulement à réduire au sein d'une entreprise (ou administration) l'utilisation du papier), mais également de fournir via Internet des informations, devis ou facture aux clients. Les factures et/ou devis n'arrivent plus au client par la poste mais par mail la plupart du temps, ce qui fait une économie importante pour l'entreprise. En plus de cela, certaines entreprises proposent un devis en ligne ou encore une inscription, etc. Mais la réelle nouveauté a été réalisée par l'administration française. En effet, le Trésor Public, la Sécurité Sociale, l'Etat et les Impôts proposent actuellement un lot de formulaires à remplir en ligne. Que ce soit la déclaration de nos revenus ou d'autres papiers pour la Sécurité Sociale, presque tout se fait en ligne de nos jours. Cela permet un gain de temps pour tout le monde.

Pourquoi alors se déplacer à la mairie pour récupérer un formulaire s'il est également disponible en ligne ? Actuellement 7 foyers sur 10 sont équipés d'une connexion à haut débit et quasiment toutes les entreprises dans le milieu tertiaire possèdent au moins un poste informatique relié au réseau Internet. C'est pourquoi il est extrêmement simple de se procurer un formulaire administratif via Internet.

L'état français souhaite arriver avant 2010 à une totalité des formulaires administratifs en ligne. Actuellement il y a environ 80% d'entres eux disponibles par une simple connexion, que ce soit en les téléchargeant (imprimable donc) ou en les remplissant en ligne directement. Dans ce dernier cas, tout se fait de façon électronique et il s'agit alors d'une complète dématérialisation de formulaires administratifs.

Toutes les personnes sont donc aidées par Internet dans ces cas. Plus besoin de se rendre dans un centre administratif (Sécurité Sociale, ANPE, Trésor Public, mairie, etc.) pour tenter de récupérer un formulaire entre midi et deux ou encore prendre une demi-journée de congé car un service administratif est prit d'assaut…

Internet a ses qualités : Ouvert 24h sur 24, 7 jours sur 7, sans attente… Il est alors possible de récupérer et remplir des formulaires de son domicile et ce, à n'importe quelle

heure ! Cela permet donc d'améliorer la qualité du service rendu pour une entreprise ou administration tout en simplifiant les procédures en respectant le cadre légal.

5.2 Simplification

Le fait qu'une entreprise ou une administration passe ses formulaires sur Internet a permis une amélioration visuelle de ceux-ci. La version papier d'un formulaire est généralement sobre, monochrome, entassée et le plus souvent peu intuitive. Internet a su résoudre certains problèmes.

Une feuille papier possède un format, le plus souvent 21 cm de largeur sur 29,7 cm de longueur (Format A4). Il fallait donc pouvoir mettre un maximum de choses sur un minimum de feuilles pour qu'un formulaire devienne le plus économique possible. L'informatique et surtout le monde Internet proposent une mise en page quelque peu différente. En effet, Internet reste virtuel, il n'existe rien de concret mis à part le matériel de l'utilisateur. C'est pourquoi Internet possède sa mise en page propre : plus de largeurs, hauteurs, etc. La notion de page fait alors référence à un groupement d'informations, textes ou médias, dans un même espace d'affiche. Cet espace d'affiche se nomme page et se retrouve via une adresse (comme un numéro de pages). Dans un espace Web (page) il n'y a donc pas de fond, la largeur étant le plus souvent considérée par la largeur de l'écran de l'utilisateur. Ces pages sans fond, donc, peuvent contenir énormément d'informations, c'est pourquoi il n'est pas rare de retrouver des formulaires papiers de 15 pages (sondages par exemple) en une seule et même page web.

Internet permet donc une mise en page différente. Le formulaire est donc plus lisible et plus simple car on y voit apparaître de la couleur, une mise en page espacée qui respire, ainsi que des regroupements d'informations par catégories le plus souvent (informations personnelles, informations professionnelles, etc.). Les choses paraissent alors plus claires pour l'utilisateur, ce qui permet un meilleur rendement.

Ces aspects bien que visuels influent énormément sur l'utilisateur qui se sent moins agressé qu'une version papier.

Le fonctionnement d'Internet, par sa mise en page et sa souplesse, évite également d'indiquer, contrairement à la version papier, certaines informations comme des numéros de pages, des reports d'informations, etc. Combien de fois a-t-il fallu indiquer le numéro de page ou encore reporter un numéro de dossier sur toutes les pages, etc. La mise en

forme d'un formulaire Internet facilite ainsi le travail de l'utilisateur en supprimant des numéros de pages ou toutes autres formes de redondance… Une certaine forme d'automatisation du travail se met alors en place aidant au mieux l'utilisateur. Par exemple, lorsque le nom de la personne est rentré, il apparaît alors aussitôt dans tous les champs du formulaire où il devra l'indiquer. Cela est utile lors d'une commande notamment où généralement l'adresse du client est la même que l'adresse du destinataire du colis.

Cette automatisation de remplissage de formulaire s'accompagne le plus souvent d'un système de reconnaissance, permettant alors une grande facilité d'utilisation. Certains systèmes d'exploitation (Windows, Mac Os ou encore Linux) peuvent garder en mémoire le nom de l'utilisateur de la machine, ce qui, dans certain cas, évite le remplissage de certaines cases. En effet, l'utilisateur de la machine se voit alors reconnu par une page Internet ce qui lui permet de ne pas avoir à taper son adresse email, son nom ou bien encore le nom de sa société car le système d'exploitation possède déjà ses informations.

Au sein même d'un formulaire dans sa version Internet, il existe le plus souvent une aide ou des exemples qui lui sont associé. Il n'est donc pas rare de voir une case date avec l'aide associé : ex. 13-02-05. Pour que l'utilisateur soit le moins perdu possible, le formulaire est généralement d'aide.

5.3 Fonctionnalité

Comme il a été évoqué plus haut, un formulaire en ligne est généralement lié avec une aide, le plus souvent réalisée par des utilisateurs (foire aux questions, forums) qui renseignent l'utilisateur actuel le plus simplement du monde avec des exemples, des commentaires associés aux champs à remplir. Plus besoin de retourner faire la queue pendant de longues minutes pour redemander au guichet ce que veut dire telle ou telle abréviation, pourquoi il n'y a pas assez de place pour le nom, etc. Ce temps est fini où l'on passait une demi -journée à remplir une fiche administrative avec une cinquantaine de personnes toutes énervées par la rapidité exemplaire du service entier. Ici tout est plus simple, une aide directement accessible en cliquant sur l'icône avec un point d'interrogation suivant le champ en question pour lire les quelques lignes de commentaires ou d'exemples situés juste en dessous.

Le système de mise en page, avec des couleurs, des regroupements intelligents entre les informations personnelles et le reste ou encore une simplification du remplissage, a permis une meilleure production. Le temps passé sur un formulaire Internet est de moitié comparé au même formulaire en version papier. Pour un particulier, ce temps gagné ne se voit pas énormément mais pour une entreprise qui fonctionne aussi bien en interne qu'en externe, ce temps gagné par les télé procédures est considérable.

Cependant, ces formulaires sont parfaits pour des utilisateurs réguliers d'Internet. Si un utilisateur régulier s'y retrouve, il existe cependant des personnes qui, pour plusieurs raisons, n'utilisent que très peu voire pas du tout Internet. En effet, un utilisateur habitué des discussions en ligne, des forums, des sites avec inscriptions, etc. ne sera pas dérangé par un formulaire administratif. Mais certaines personnes, par le niveau social, leur domaine d'activité ou leur âge ne peuvent utiliser un ordinateur.

Un utilisateur d'Internet, d'après une étude menée par 01.NET, a entre 15 et 35 ans, vient d'un milieu social moyen ou plus, et exerce une profession dans le domaine tertiaire (informatique, vente, etc.). Seulement 5% des plus de 50 ans utilisent un ordinateur à la maison ou au travail de façon régulière et 17% de ces personnes possèdent une connexion à Internet. Dans les domaines d'activités comme la pêche, l'agriculture ou encore les métiers manuels (maçonnerie, ébénisterie, etc.) seul 1 français sur 10 possède une connexion internet. Tous ces paramètres sont alors à prendre en compte lors d'une dématérialisation. C'est pourquoi il n'existe pas ou peu de formulaires en ligne pour une demande de retraite par exemple. La cible des formulaires en ligne concerne avant tout les grandes sociétés, comme pour le cas de la déclaration de revenus.

Le service sur Internet serait-il la mort de l'accueil client ? Si tout se passe bien sur Internet, il existe encore quelques cas où l'utilisateur peut avoir besoin d'une aide de l'organisme proposant le formulaire. C'est pourquoi il est encore utile de voir des guichets et des bureaux de renseignements dans les administrations françaises (ou entreprises). Sur le plan du rapport humain, Internet ne permet pas de discussions, de contacts avec d'autres personnes.

6. LA SECURITE

6.1 Risques

La sécurité des informations est très importante, que ce soit en version papier ou sur informatique. Mais l'heure de l'Internet a fait comprendre à bien des gens le rôle d'une bonne sécurité. Avant cette ère, les documents importants étaient stockés dans un coffre-fort pour une grande société. Mais maintenant, l'ère de l'informatique, encore à ses débuts, fait peur à beaucoup de monde mais fascine en même temps. Seule une élite de personnes, administrateurs par exemple, peuvent parler de sécurité ou de risque. Dans le cas d'une entreprise, il y a généralement 2 réseaux, un libre et un sécurisé, avec un système d'authentification avec un login et un mot de passe. Pour la dématérialisation, plusieurs systèmes de contrôle de l'information et donc de sécurité peuvent se mettre en place au sein du système : le contrôle intégré qui vérifie les informations contenues dans des champs, les certificats et signatures électroniques qui contrôlent l'identification et la non-répudiation du document et le cryptage permettant une confidentialité du document ainsi que le procédé.

L'informatique a ses failles, comme les systèmes de sécurité. Le fait d'avoir un système complet de sécurité, au niveau du document, du réseau et de l'échange, diminue les risques d'un éventuel piratage et augmente considérablement la sûreté du système.

Mais les risques sont là… Lorsque l'on fait de l'échange de données entre ordinateurs, une sécurité s'applique. Sur un ordinateur il est possible par de simples logiciels gratuits d'espionner ce que fait quelqu'un, ce qu'il tape sur son clavier ou bien encore quelles pages internet il visite, etc. Au sein du réseau lui-même il est possible d'écouter entre différents ordinateurs et de lire tout ce qui part d'un ordinateur vers le réseau. L'exemple même de ce genre de piratage est le fait d'avoir plusieurs postes téléphoniques pour un même numéro. A la maison, si quelqu'un décroche un des postes alors que la ligne est déjà utilisée, cette personne pourra entendre la discussion… D'un point de vue réseau c'est strictement la même chose. Il est donc possible de savoir dans un réseau interne ce qui s'y passe… Mais ces risques peuvent être contrôlés car s'il existe des logiciels permettant une écoute d'un ordinateur sur le réseau, il en existe aussi qui bloquent ces espions ou les trompent. L'un des moyens les plus utilisés est d'envoyer des informations inutiles sur le réseau afin de tromper l'espion. Sur le réseau ce n'est pas la voix qui est

transmise comme au téléphone, mais des bits (chiffres 1 ou 0) qui correspondent à des caractères (lettres, chiffres, caractères spéciaux). Si un message sur 10 est vrai et que les 9 autres sont tout simplement là pour tromper l'espion, comment l'espion saura-t-il faire le tri ?

Le piratage industriel devient de plus en plus important. Les attaques de pirates ont été multipliées par mille dans les 5 dernières années et ce chiffre ne cesse d'augmenter. C'est pourquoi il est intéressant de se mettre tout le temps à jour sur les derniers moyens de se protéger des attaques ainsi que de protéger les données sensibles.

Ces risques peuvent donc être contrôlés au maximum, c'est pourquoi une bonne gestion du réseau est importante. Hélas, une sécurité mise en œuvre n'évite jamais complètement la faille aussi, il est utile de même en œuvre une farandole de sécurités les plus diverses afin de limiter la casse. Il existe donc des contrôles intégrés, un système de signature virtuelle ainsi que le cryptage du message envoyé.

6.2 Contrôles intégrés

Les formulaires disponibles sur le web procèdent de deux façons : l'une permet le remplissage en ligne puis une impression du formulaire (qui sera à envoyer plus tard par la poste), l'autre permet de l'envoyer directement via le site web (stockage dans une base de données sur le serveur distant).

Dans ces deux cas pratiques, il existe certains outils de contrôles intégrés comme le javascript par exemple qui permet de vérifier les valeurs de champ. Qu'il s'agisse d'une date, un numéro ou un nom en majuscule, un système de contrôles intégrés vérifiera les informations entrées afin de vous prévenir si la taille du numéro entré dépasse la taille autorisée, si le texte est en majuscule, etc. Ce contrôle intégré permet une validation du document sur la machine cliente avant de l'envoyer sur la machine distante (pour un stockage dans une base de données généralement).

Internet fonctionne de la façon suivante : lorsque vous tapez une adresse, vous demandez à un serveur de vous envoyer des informations (des pages Internet). Vous recevez donc un fichier HTML affiché dans le navigateur. Avec ce fichier HTML qui contient le formulaire, un fichier JS (JavaScript) est attaché (ou inclus dans le HTML) afin de réaliser une vérification des champs du formulaire. Cette vérification se fait en interne, c'est à dire uniquement sur la machine client. Aucune information n'est envoyée

sur Internet à ce moment là. Après avoir complété le formulaire d'une façon correcte, lorsque vous cliquez sur « Valider » (ou Suivant, accepter, etc.), les informations sont envoyées.

Avec ces contrôles intégrés, une certaine sécurité est appliquée avant l'envoi des informations. Cela permet d'envoyer des informations correctes, de ne pas prévoir un contrôle des informations sur la machine distante ainsi d'éviter les risques de bugs.

6.3 Signature virtuelle

Avec la généralisation du courrier électronique et du commerce électronique, la sécurisation des échanges paraît de plus en plus nécessaire. Plusieurs systèmes existent.

Les Chambres de Commerce et d'Industrie proposent un certificat de signature électronique baptisé « CHAMBERSIGN ». C'est un outil électronique, matérialisé sous la forme d'une clé logicielle à installer sur son ordinateur, qui va en quelque sorte jouer le rôle d'une « carte d'identité Internet » en permettant ainsi à l'expéditeur de signer son document et en permettant aussi au destinataire d'être sûr de l'identité de son correspondant tout en assurant, tant à l'expéditeur qu'au destinataire, que le message n'aura pas été modifié au cours du transfert. Comme nous l'expliquent les Chambres de Commerce et d'Industrie, ce procédé est facile à mettre en œuvre : « Il faut au moins posséder un ordinateur et être connecté à Internet. Attention, cependant : renseignez-vous avant d'acquérir un certificat numérique afin qu'il corresponde bien à l'usage que vous voulez en faire. Si le Chiffre d'Affaires de votre entreprise dépasse 15 244 901,72 euros, votre entreprise est soumise à l'obligation d'utiliser les télé-procédures en matière de déclaration de TVA. Le certificat que vous devez acquérir doit être référencé par le ministère de l'Economie et des Finances.

Actuellement, la détention d'un certificat de signature électronique n'est pas obligatoire, mais elle devient un préalable indispensable à la déclaration de TVA pour toutes les entreprises soumises à cette obligation fiscale. Depuis le premier janvier 2002, des sanctions pécuniaires sont appliquées par l'administration fiscale aux entreprises qui, réalisant un Chiffre d'Affaires supérieur à 15 244 901,72 euros, n'auront pas utilisé les télé-procédures pour déclarer et régler leur TVA.

Ce système de certificat de signature électronique s'adresse à toutes les entreprises en général. Mais à terme, avec la généralisation des télé-procédures, la dématérialisation des

formulaires administratifs et l'accroissement des échanges sur Internet, elle pourra s'adresser à tout professionnel et même à tout particulier désirant utiliser le web en toute sécurité.

Les signatures électroniques offrent des fonctions telles que l'authentification, la confidentialité, l'intégrité des données et la non répudiation.

L'authentification est la vérification de l'identité d'une personne. Cela garantit l'identité de la personne qui a signé les données. De cette façon le destinataire connaît celui qui a participé à la transaction et sait que celui-ci n'a pas été falsifié. Cela permet également de déterminer de façon irrévocable l'utilisateur qui tente d'accéder à un système grâce à la confirmation de son identité.

La signature électronique protège aussi l'intégrité des données. Cela signifie que le message envoyé n'a pas été altéré, volontairement ou involontairement. D'un point de vue technique, la signature électronique contient un hash (empreinte numérique) de l'ensemble du message qui a été signé. Toute modification apportée à ce document après signature rend ce hash invalide.

L'auteur d'un message prouve son identité. La non-répudiation établit, plus tard, qui a participé à une transaction. L'expéditeur ne peut nier avoir envoyé le message et le destinataire ne peut nier l'avoir reçu. Simplement, la non-répudiation signifie qu'une information ne peut être rejetée, comme avec les signatures manuscrites.

6.4 Cryptage

Depuis longtemps, la transmission de données sensibles a nécessité l'utilisation d'un système de sécurisation performant.

Les services secrets des grandes puissances économiques et politiques, de tout temps très impliqués, ont développé, tout d'abord, des codages alphabétiques et numériques simples puis des techniques cryptographiques plus poussées, grâce à l'outil mathématique pour rendre inviolables et inexploitables directement leurs données sensibles.

La cryptologie, véritable science régissant le codage de l'information, a connu une réelle explosion avec le développement des systèmes informatiques, passant d'une ère artisanale et confidentielle à des systèmes de très hautes technologies nécessitant une importante puissance de calcul. Elle a connu un plus large essor encore avec l'arrivée des

systèmes de communications modernes (internet, etc.) où il y a une nécessité absolue de protéger les données échangées pour respecter les individus.

La cryptologie, science fondamentale qui régit la cryptographie, est essentiellement basée sur l'arithmétique.

Ainsi, dans le cas d'un texte, il s'agit de transformer les lettres qui composent le message en une succession de chiffres (sous forme de bits dans le cas de l'informatique pour permettre le fonctionnement binaire des ordinateurs), puis ensuite de faire des calculs sur ces chiffres pour:

- d'une part les modifier et les rendre incompréhensibles. Le résultat de cette modification (le message chiffré) est appelé cryptogramme
- d'autre part, faire en sorte que le destinataire sache les déchiffrer en utilisant les outils préétablis ou joints aux données.

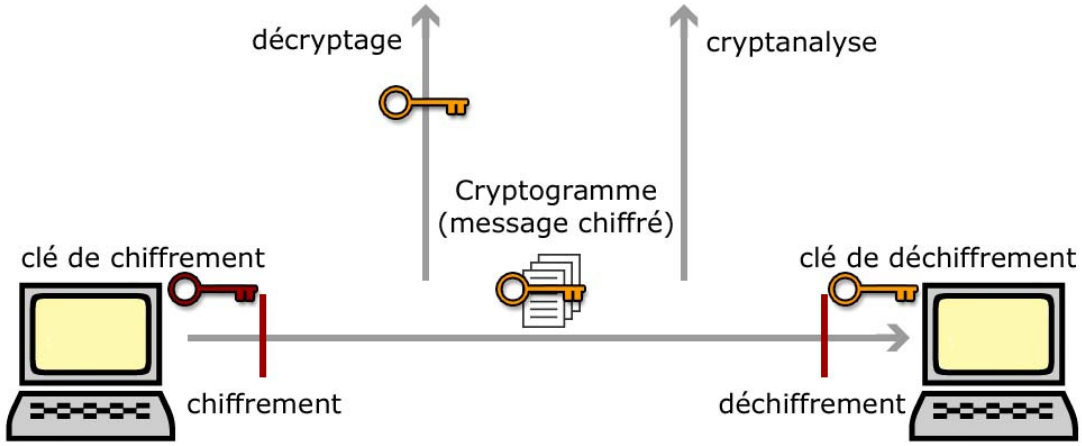

Figure 8. Exemple de Cryptage

Le fait de coder un message de façon à le rendre secret s'appelle *chiffrement*. La méthode inverse consistant à retrouver le message original, est appelée *déchiffrement*.

Le chiffrement se fait généralement à l'aide d'une *clé de chiffrement*, le déchiffrement avec une *clé de déchiffrement*. On distingue généralement deux types de clés :

- *Les clés symétriques*: on utilise des clés identiques à la fois pour le chiffrement et pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète. Il s'agit de la cryptographie à clé privée.

- *Les clés asymétriques*: on utilise de clés différentes pour le chiffrement et le déchiffrement. On parle alors de chiffrement asymétrique. Il s'agit de la cryptographie à clé publique.

Au cours des années soixante dix, un système de sécurisation basé sur la polarisation des photons est apparu : la cryptographie quantique. Cette technique est différente des autres cryptosystèmes à clé puisqu'elle fonctionne sur des propriétés physiques intrinsèques au système.

6.41 La cryptographie à clé privée

Figure 9. Cryptage à clé privée

Le chiffrement à clé privée, aussi appelé chiffrement symétrique ou chiffrement à clé secrète, consiste à utiliser la même clé pour le chiffrement et le déchiffrement.

Si A veut envoyer un message à B, tous deux doivent au préalable s'être transmis la clé. Celle-ci est identique chez l'émetteur et le destinataire du message. Les deux parties doivent se communiquer la clé à un moment ou à un autre, ce qui constitue un risque non négligeable d'interception. Elle peut servir pour plusieurs messages ou être modifiée à chaque échange. Dans le premier cas, elle repose sur la confiance en l'utilisateur. Les systèmes à clé privée posent un second problème. Si une clé différente est mise en oeuvre pour chaque paire d'utilisateurs du réseau, le nombre total des clés augmente beaucoup plus rapidement que celui de protagonistes.

Dans les années 20, Gilbert Vernam et Joseph Marlogne mettent au point la méthode du *one time pad* (méthode du masque jetable) , basée sur une clé privée générée aléatoirement, utilisée une et une seule fois puis détruite. Plus tard, le Kremlin et la

Maison Blanche sont reliés par le fameux *téléphone rouge*, dont les communications étaient cryptées par une clé privée selon la méthode du *masque jetable*. La clé était alors échangée au moyen de la valise diplomatique (jouant le rôle de canal sécurisé).

Dans les années 80, Claude Shannon démontra que pour être totalement sûr, les systèmes à clé privée doivent utiliser les clefs d'une longueur au moins égale à celle du message à chiffrer, ce qui pose problème. De plus, le chiffrement symétrique impose d'avoir un canal sécurisé pour l'échange de la clé, ce qui dégrade sérieusement l'intérêt d'un tel système de chiffrement.

6.42 La cryptographie à clé publique

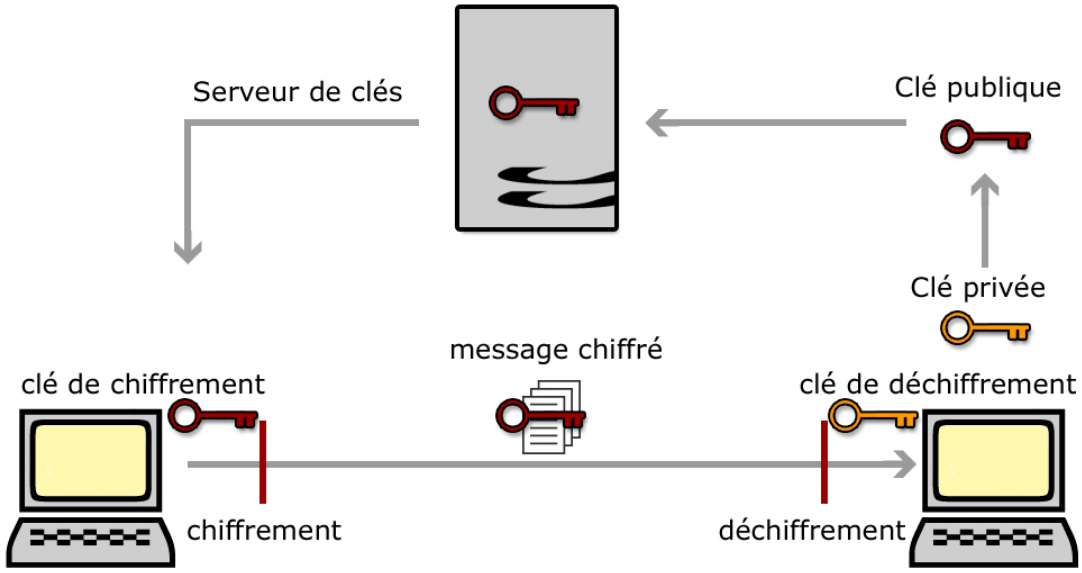

Figure 10. Cryptage à clé publique

La cryptologie moderne est née en 1976 avec l'introduction par deux chercheurs de l'Université de Stanford, Whitfield Diffie et Martin Hellman, du concept de clé publique.

Le principe émet que seule l'opération de déchiffrement doit être protégée par une clé gardée secrète. Le chiffrement peut parfaitement être exécuté à l'aide d'une clé connue publiquement, à condition, bien sûr, qu'il soit virtuellement impossible d'en déduire la valeur de la clé secrète. On parle alors de « cryptographie asymétrique ». Les deux inventeurs butent cependant sur la difficulté de proposer un véritable cryptosystème à clé

publique ; la solution vient du MIT en 1978, avec la publication d'un procédé de chiffrement mettant en œuvre les idées de Diffie et Hellman.

Ils constatent que la clé publique permet le transport des clés conventionnelles, qui ne repose pas sur l'existence d'une hiérarchie cloisonnée . C'est bien ainsi que fonctionne le système actuellement. Ils savent également qu'un système de chiffrement peut être utilisé comme mode d'authentification : c'est le principe de l'I.F.F. (Identification Friends and Foes), mis au point dans les années 1950 par l'Armée de l'Air Américaine, qui identifie les appareils amis par leur capacité à déchiffrer un message choisi au hasard et inclus dans le signal radar. Dans le contexte de la clé publique, pouvoir déchiffrer un message produit la preuve qu'on est en possession de la clé secrète. Contrairement au mode conventionnel, cette preuve est opposable aux tiers, puisque quiconque peut vérifier par chiffrement public qu'on restitue le message initial. On réalise l'analogue d'une signature manuscrite liant un document à son auteur. C'est précisément ce mécanisme de signature numérique qui se met en place aujourd'hui pour les besoins du commerce électronique.

Au-delà de l'invention de la clé publique, l'un des apports de la cryptologie moderne est d'avoir su fournir un cadre conceptuel cohérent pour analyser qualitativement les menaces potentielles contre un système cryptographique. La sécurité est algorithmique : elle fait l'hypothèse que l'adversaire éventuel dispose d'une puissance de calcul importante mais bornée; ceci est contraire à la théorie de Shannon qui attribue à l'ennemi une capacité infinie de calcul et conduit de ce fait à ce qu'on appelle la « sécurité inconditionnelle ». Cette dernière mène à des systèmes peu utilisés puisque la clé a nécessairement une longueur au moins égale au texte à chiffrer. Elle est toutefois parfaitement réalisable par combinaison du texte clair –supposé d'une suite de bits (c'est-à-dire 0 et 1) avec une autre suite constituant la clé, la combinaison étant réalisée par une addition de bits à bits, analogue à l'addition ordinaire, à ceci près que 1+1 vaut 0. Ce mécanisme, connu sous le nom de « chiffrement de Vernam », est parfaitement sûr lorsque chaque clé n'est utilisée qu'une seule fois. On peut imaginer d'autres mécanismes de sécurité qui ne soient ni algorithmiques ni inconditionnels ; c'est ainsi qu'on envisage aujourd'hui la possibilité de procédés de cryptographie sur les lois de la physique quantique.

6.43 La cryptographie quantique

Sur le réseau Internet, les cryptographies à clé publique ou privée ne permettent pas de savoir si le message crypté émis a été intercepté par une personne autre que le destinataire. En revanche avec la cryptographie quantique, un espion est immédiatement repéré.

Née au début des années 70, cette méthode est liée au principe d'incertitude de Heisenberg selon lequel la mesure d'un système quantique perturbe ce système. Le texte du message codé sous la forme de bits classiques est ici représenté par un ensemble de photons dont l'état quantique correspond à la valeur de ses bits. Si un intrus agit sur un des photons, il en détruit la polarisation, si bien que l'émetteur et le récepteur s'en rendent immédiatement compte.

6.44 Quelques applications de la cryptographie

Les banques, mais aussi de nombreuses entreprises, échangent couramment des informations confidentielles sous la forme de données télématiques par l'intermédiaire d'ordinateurs. Ces données sont en général transmises par le réseau téléphonique ou par d'autres réseaux publics, si bien qu'il convient de mettre au point des cryptages efficaces pour les protéger. En combinant les systèmes de cryptographie évoqués ci-dessus, on peut ainsi créer des chiffres de complexité variée, avec la contrainte que les clés sont elles aussi amenées à être transmises sur ces réseaux.

Avec suffisamment de temps et de matériel, on peut résoudre la plupart des codes chiffrés et découvrir ainsi leurs clés. Aussi la complexité du code doit-elle être adaptée afin qu'il soit impossible de le découvrir en un temps raisonnable. Par exemple, des ordres militaires qui ne doivent rester secrets que pendant quelques heures peuvent être cryptés au moyen d'un chiffre qui ne conviendrait pas au codage de rapports diplomatiques exigeant une confidentialité à long terme.

Avec ses pages interactives, ses images, ses documents sonores, le réseau Internet a permis le développement d'une forme plus spectaculaire de commerce électronique que celui déjà connu par le minitel. Désormais, les entreprises de vente par correspondance peuvent concevoir des catalogues illustrés sous forme électronique et les achats peuvent s'effectuer au moyen d'une carte de crédit (les jeux téléchargés permettent de faire l'économie du prix de l'emballage).Il existe cependant un obstacle majeur : le seul

standard actuel de paiement électronique est la carte bleue. C'est donc ici qu'intervient le cryptage, qui n'est pourtant pas encore légal dans tous les pays.

En effet, un problème d'Internet est la question de la sécurité et de la confidentialité. Par nature Internet, étant ouvert à tous, se prête facilement aux piratages de toute nature. Des logiciels de cryptographie permettent d'assurer une relative confidentialité des échanges.

6.45 Protocole SSL

SSL (Secure Sockets Layers, *couche de sockets sécurisée*) est un procédé de sécurisation des transactions effectuées via Internet mis au point par *Netscape*, en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics. Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur Internet Le système SSL est indépendant du protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP (consultation de sites) que des connexions via le protocole FTP (téléchargement de fichiers) , POP (consultation de mails), etc. En effet, SSL agit telle une couche supplémentaire, permettant d'assurer la sécurité des données.

De cette manière, SSL est transparent pour l'utilisateur (c'est à dire que l'utilisateur peut ignorer qu'il utilise SSL). Par exemple un utilisateur utilisant un navigateur Internet pour se connecter à un site de commerce électronique sécurisé par SSL enverra des données chiffrées sans avoir à s'en préoccuper.

La quasi intégralité des navigateurs supporte désormais le protocole SSL. *Netscape Navigator* affiche par exemple un cadenas verrouillé pour indiquer la connexion à un site sécurisé par SSL et un cadenas ouvert dans le cas contraire, tandis que *Microsoft Internet Explorer* affiche un cadenas uniquement lors de la connexion à un site sécurisé par SSL.

Un serveur sécurisé par SSL possède une URL commençant par *https://*, où le "s" signifie bien évidemment *secured* (*sécurisé*).

Au milieu de l'année 2001, le brevet de SSL appartenant jusqu'alors à Netscape a été racheté par l'*IETF* (*Internet Engineering Task Force*) et a été rebaptisé pour l'occasion TLS (*Transport Layer Security*).

La sécurisation des transactions par SSL 2.0 est basée sur un échange de clés entre client et serveur. La transaction sécurisée par SSL se fait selon le schéma suivant:

- Dans un premier temps, le client, se connecte au site marchand sécurisé par SSL et lui demande de s'authentifier. Le client envoie également la liste des cryptosystèmes qu'il supporte, triée par ordre décroissant de la longueur des clés.
- Le serveur a réception de la requête envoie un certificat au client, contenant la clé publique du serveur, signée par une autorité de certification (CA), ainsi que le nom du cryptosystème le plus haut dans la liste avec lequel il est compatible (la longueur de la clé de chiffrement - 40 bits ou 128 bits - sera celle du cryptosystème commun ayant la plus grande taille de clé).
- Le client vérifie la validité du certificat (donc l'authenticité du marchand), puis crée une clé secrète aléatoire (plus exactement un bloc prétendument aléatoire), chiffre cette clé à l'aide de la clé publique du serveur, puis lui envoie le résultat (la clé de session).

Figure 11. Cryptage SSL

Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée. Ainsi, les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs. Le reste des transactions peut se faire à l'aide de clé de session, garantissant l'intégrité et la confidentialité des données échangées.

CONCLUSION

La dématérialisation de formulaires est une chose avantageuse pour une entreprise mais risquée. Il faut s'assurer d'une bonne démarche, légale, tout en n'objectant pas les risques éventuels d'une dématérialisation. C'est une étape importante et sans retour possible : une fois numérisés, les documents papiers sont généralement détruits. C'est pour cela q'une très bonne conception relève le plus souvent d'une bonne connaissance du traitement de ces données.

Les risques de sécurité des données ainsi que les craintes encore réelles pour une numérisation complète bloquent cette avancée. Cependant, de nombreuses entreprises ont passé le cap avec succès, notamment l'administration française qui se félicite du succès de la déclaration des revenus en ligne par exemple. L'avenir des documents d'une entreprise devra apparemment passer par une dématérialisation.

REFERENCES BIBLIOGRAPHIQUES

Aproged, *Dématérialisation et documents*, Paris, MEDEF, Mars 2004

LOMME Laurence, *L'administration électronique*, séminaire du CNRS, 2004

Site du magazine Réseaux du droit, www.village-justice/reseaux – Avril 2005

TENOR Conseil, *XML pour l'EDI*, Etude pour la CNAV et la MTIC, juin 2000

D'ERCEVILLE Hubert, *mutations des fonctions*, 01 INFORMATIQUE – 6 juin 2003

IPLS, *X400, protocole de messagerie*, Editeur pour IBM, 2005

PIETTE-COUDOL Thierry, *Icare*, consortium 2003

JONAS Sylvie, *La sécurité des échanges*, Paris, séminaire, 2005

BORDAGE F., *Le point sur… la dématérialisation des échanges*, DECISION MICRO, 2003

GLOSSAIRE

ASP : Langage de programmation

Bit : Information binaire qui ne peut prendre que deux valeurs (1 ou 0). Tout ce qui est numérique est une suite de bits.

Bug : problème informatique.

Cryptogramme : texte chiffré

Cryptologie : science pure énonçant les principes et les idées de la cryptographie.

Cryptographie : science appliquée englobant à la fois les techniques du chiffre et de la cryptanalyse.

Cryptanalyse : technique étudiant les moyens de chiffrement et recherchant les méthodes permettant de décrypter en bits

GED : Gestion Electronique de Documents

HTML : HyperText Mark-up Language. Langage de programmation servant à décrire des pages Web à l'aide de balises.

Intranet : Site Web diffusé uniquement sur un seul et même réseau contrairement à un site Internet diffusé dans le monde entier.

Java : Langage de programmation utilisé essentiellement pour le développement d'application pour les téléphones portables.

PDF : Créé par Adobe, c'est le format de référence pour des documents textes sur Internet.

PHP : Langage de programmation, comme le ASP, s'exécutant coté serveur.

MIT: (Massachusetts Institute of technologie), établissement américain d'enseignement supérieur et de recherche. Outre l'enseignement, une grande part de son activité est vouée à la recherche fondamentale. Il possède un réacteur nucléaire, de cybernétique, de souffleries aérodynamiques et différents centres d'étude.

Serveur : Ordinateur distant. Le système Client/Serveur correspond à une intéraction entre l'ordinateur d'un utilisateur et la machine où se trouve le site web.

SGBD : Système de Gestion de Bases de Données.

W3C : C'est une organisation qui publie des normes dans le domaine du Web.

Workflow : processus métiers. Par exemple, pour poster une lettre le Workflow correspond à : dépôt de la lettre dans une boite aux lettres, récupération de la lettre par un facteur, dépôt de cette lettre au centre de tri, tri de la lettre, redirection vers le lieu correspondant, […], dépôt de la lettre dans la boite aux lettres du destinataire.

XML : Standard du Web.

ANNEXES

I – Législation : les textes

Textes relatifs à l'administration électronique

- Circulaire du 12 septembre 2003 relative au développement de l'administration électronique.
- Décret 2003-141 du 21 février 2003 portant création de services interministériel pour la réforme de l'Etat.
- Circulaire du 31 décembre 1999 relative à l'aide aux démarches administratives sur l'Internet.
- Décret 99-68 du 2 février 1999 relatif à la mise en ligne des formulaires
- Projet de loi habilitant le Gouvernement à simplifier le droit (dont l'article 3 est consacré à l'administration électronique : sécurité des échanges, dématérialisation des procédures administratives, dématérialisation des pièces justificatives, changement d'adresse en ligne, signature électronique des autorités administratives, diffusion en ligne des données publiques… Première lecture à l'Assemblée Nationale le 10 juin 2005
- Loi pour la confiance dans l'économie numérique (LEN) : Texte destiné à favoriser le développement du commerce par Internet, en clarifiant les règles pour les consommateurs et les prestataires.

Textes relatifs aux droits des personnes

- Loi 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés (Art. 323-1 à 323-3 du code pénal)
- Décret d'application 78-774 du 17 juillet 1978.
- Convention du conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

- Directive 95/46/CE du parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- Loi 2000-321 du 12 avril 2000, relative aux droits des citoyens dans leurs relations avec les administrations (DCRA)
- Décret 2001-492 du 6 juin 2001 pris pour l'application du chapitre 2 du titre 2 de la loi 2000-321 du 12 avril 2000 et relatif à l'accusé de réception des demandes présentées aux autorités administratives
- Article 226-17 du code pénal
- Article 226-21 du code pénal

Textes relatifs aux sites Internet publics

- Circulaire du 7 octobre 1999 relative aux sites Internet des services et des établissements publics de l'Etat
- Arrêté du 6 novembre 2000 relatif à la création d'un site sur Internet intitulé « service-public.fr »
- Loi du 29 juillet 1881 modifiée sur la liberté de la presse

Textes relatifs à la diffusion des données publiques

- Circulaire du 14 février 1994 relative à la diffusion des données publiques
- Circulaire du 28 janvier 1999 relative à la diffusion gratuite des rapports officiels sur Internet

Textes relatifs à la conservation des documents

- Loi 79-18 du 3 janvier 197 sur les archives
- Loi 94-665 du 4 août 1994 modifiée relative à l'emploi de la langue française
- Décret 96-602 du 03 juillet 1996 relatif à l'enrichissement de la langue française

Textes relatifs à la signature électronique

- Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur le cadre communautaire pour les signatures électroniques
- Loi 2000-230 du 13 mars 2000 portant adaptation de la preuve aux technologies de l'information et relative à la signature électronique
- Décret 2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique
- Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information

Textes relatifs à la cryptologie

- Décret 2002-997 du 16 juillet 2002 relatif à l'obligation mise à la charge des fournisseurs de prestations de cryptologie en application de l'article 11-1 de la loi du 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications
- Décret 2002-688 du 2 mai 2002 modifiant le décret 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie
- Décret 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable
- Décret 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestation de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation

Textes relatifs à la dématérialisation des marchés publics

- Décret 2004-15 du 7 janvier 2004 portant code des marchés publics et notamment son article 56 relatif à la dématérialisation des procédures
- Circulaire du 7 janvier 2004 portant manuel d'application du code des marchés publics
- Décret 2001-846 du 18 septembre 2001 pris en application du troisième point de l'article 56 du code des marchés publics et relatifs aux enchères électroniques
- Décret 2002-692 du 30 avril 2002 pris en application du premier et du deuxième point de l'article 56 du code des marchés publics et relatif à la dématérialisation des procédures de passation des marchés publics
- Arrêté du 30 janvier 2004 pris en application des articles 40 et 80 du code des marchés publics et fixant les modèles de formulaires pour les publications des avis relatifs à la passation et à l'attribution des marchés publics
- Arrêté du 26 février 2004 pris en application de l'article 45, alinéa premier, du code des marchés publics et fixant la liste des renseignements et/ou documents pouvant être demandés aux candidats aux marchés publics
- Arrêté du 27 mai 2004 pris en application de l'article 138 du code des marchés publics et relatifs à la liste des marchés conclus l'année précédente par les personnes publique

Texte relatif à la sécurité des systèmes d'information

- Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information

Textes relatifs à la simplification des démarches administratives

- Décret 2003-301 du 2 avril 2003 modifiant le code général des collectivités territoriales (Modification de la liste des pièces justificatives des paiements

des communes, des départements, des régions et des établissements publics locaux

- Loi 2003-591 du 2 juillet 2003 habilitant le Gouvernement à simplifier le droit

Les textes propres à chaque entité administrative doivent également être pris en compte.

FICHE RESUME

Résumé

La dématérialisation de formulaires est une chose très importante pour une entreprise. Passer du document papier à un logiciel devient intéressant pour une entreprise. Ici nous étudierons les avantages et inconvénients d'une dématérialisation, les risques encourus et la façon de les éviter. Nous étudierons également le fait de réaliser une dématérialisation de son étude à sa réalisation, avec les problèmes techniques.

Une partie est consacrée à la législation qui permettra de bien comprendre comment une dématérialisation peut se faire légalement, car l'administration française, qui a été un pionnier de la dématérialisation de formulaire, a aussitôt rédigé des décrets, lois, directives pour les entreprises et autres administrations.

Mots-clés

Dématérialisation

Formulaires

EDI

GED

Entreprise

Législation

Economie