LA PROTECTION DU DOCUMENT ÉLECTRONIQUE : ASPECTS TECHNIQUES ET JURIDIQUES

Rapport du groupe de travail sur l'infrastructure juridique du document avec signature numérique

Collection en ingénierie documentaire : 5

Mai 1999

Réalisé dans le cadre du Chantier en ingénierie documentaire
Coordonné par : Richard Parent et Nicole Boulet

Conseil du trésor
Sous-secrétariat à l'inforoute gouvernementale
et aux ressources informationnelles

REMERCIEMENTS

Ce rapport est issu de la réflexion d'un groupe de travail qui s'est penché sur l'infrastructure juridique du document avec signature numérique

Nous remercions de leur collaboration les personnes suivantes :

Membres du groupe de travail :

TABLE DES MATIÈRES

INTRODUCTION

Au moment de sa formation, le groupe de travail avait pour mandat de traiter de la signature des documents électroniques. Cependant, il a vite compris la nécessité d'élargir son analyse à l'infrastructure juridique du document électronique afin d'aborder les principaux aspects de la protection de la validité juridique des documents électroniques. En effet, seule cette approche globale était susceptible de favoriser efficacement l'utilisation de la signature numérique dans l'information gouvernementale.

Ainsi adapté en cours de réflexion, l'objectif du groupe de travail était de déterminer les moyens à mettre en œuvre à l'échelle gouvernementale pour assurer la valeur juridique des documents électroniques :

1° définir les des conditions juridiques, techniques et administratives nécessaires au scellement et à la signature des documents électroniques;

2° fournir une aide ~~à~~ pour l'application des conditions juridiques, techniques et administratives nécessaires au scellement et à la signature des documents électroniques;

3° déterminer, à partir du *Recueil de délais de conservation des documents communs des ministères et organismes gouvernementaux*, quelques types de documents électroniques susceptibles d'être scellés ou signés.

Le déploiement de l'inforoute exige l'utilisation généralisée du document électronique. Le principal obstacle réside dans le fait que la majorité des documents administratifs doivent être signés, notamment les formulaires. Il faut donc pouvoir signer le document électronique, de façon que sa valeur juridique soit égale à la signature manuscrite du document papier.

La situation actuelle est marquée par trois éléments :

- L'urgence d'agir : foule de projets sont en marche concernant les citoyens, les entreprises et d'autres partenaires, pour gérer les transactions liées aux services gouvernementaux.

- Le développement des services communs de l'inforoute gouvernementale, en particulier la définition du cadre administratif pour les services de répertoire et de certification de clés publiques.

- Le cyberespace est soumis à des forces irrésistibles d'interfonctionnement en matière de commerce électronique, et le rôle de normalisation en technologies de l'information dévolu au SCT permet de se rallier dès aujourd'hui aux consensus en émergence et établis dans le monde Internet. Ce degré de convergence est suffisant pour établir l'infrastructure juridique nécessaire à la confirmation de la valeur probante des documents électroniques. Des efforts en ce sens, du reste convergents, se manifestent dans les Lignes directrices de l'OCDE, dans l'architecture PKIX et dans les protocoles de l'IETF, de l'UIT/ISO, du W3C, etc.

Ce rapport est issu d’un groupe de travail qui était composé de Nicole Boulet, Jean-Maurice Demers, Louise Gagnon-Arguin, Yvan Lauzon, Richard Parent et Jeanne Proulx. Nous les remercions de leur collaboration.

CHAPITRE 1

TYPES DE DOCUMENTS ÉLECTRONIQUES, VALEURS DE CONSERVATION ET NIVEAUX DE PROTECTION

En vue de cerner les diverses conditions juridiques, administratives et techniques de la validité du document électronique, il faut au préalable déterminer :

- les différents types de document électronique ;
- les différentes valeurs que prennent ces documents au cours de leur cycle de vie dans l'Administration ;
- les différents niveaux de protection qui leur sont applicables en fonction de leurs particularités techniques et de leur valeur.

1.1 Les différents types de document électronique

Il existe deux grands types de codage de l'information contenue dans un document : le contenu textuel est généralement conservé sous forme de jeux de caractères encodés et de langages graphiques, comme c'est le cas avec les outils bureautiques courants ainsi qu'avec les formats du Web; mais beaucoup de documents semblables sont emmagasinés sous forme de documents numérisés après avoir été transférés vers une forme électronique par un traitement optique de leur support papier si largement utilisé dans la communication. Les deux modes d'emmagasinage des données correspondant à un document électronique se trouvent liés, quoique de façon distincte, dans le format PDF d'Acrobat inc. tout autant que dans le format HTML.

1.2 Les différentes valeurs des documents électroniques

Qu'elle soit consignée sur un support traditionnel ou sur un support électronique, l'information peut se voir attribuer des valeurs différentes, soit en fonction de son seul contenu, soit en fonction de son évolution dans le temps. Ainsi, par exemple, il est évident que la loi constitutive d'un ministère ou d'un organisme gouvernemental aura une valeur fondamentale dès son adoption ; mais la valeur de la loi originelle diminuera après sa modification et sera même totalement transformée après son abrogation. En effet, cette loi, dans un premier temps, est essentielle aux fins administratives de l'organisme ; elle pourra ensuite servir de référence sur l'état du droit relatif à une activité abandonnée par l'organisme ; enfin, elle pourrait n'être utile qu'à l'historien qui recherche un témoignage de la réalité d'un organisme dissous.

L'archivistique nord-américaine qualifie habituellement la première de ces valeurs de valeur primaire, c'est-à-dire la qualité d'un document fondée sur les utilités premières et administratives que lui ont données ses créateurs, en d'autres mots sur les raisons pour lesquelles le document a été créé. Elle répond à des besoins administratifs, financiers et juridiques. La seconde, la valeur secondaire, se définit comme la qualité du document fondée sur ses utilités secondes ou scientifiques, c'est-à-dire essentiellement la valeur de témoignage privilégié.

Mais la pratique de la gestion de l'information démontre que les valeurs primaire et secondaire peuvent coexister depuis la création d'un document (sur support papier ou électronique) jusqu'à son versement éventuel au service d'archives de l'organisme. Ainsi, la loi constitutive dont nous parlions plus haut peut-elle être utile à l'historien d'un organisme alors même qu'elle continue d'être en vigueur, particulièrement si elle est un peu ancienne. Et, comme nous l'avons signalé, elle peut également être utile à un gestionnaire qui veut vérifier l'état du droit à un moment donné dans le passé afin d'évaluer la portée exacte d'un dossier donné.

De manière plus concrète, les gestionnaires de l'information reconnaissent habituellement trois types de valeur à la matière qu'ils gèrent : la valeur administrative, la valeur juridique, la valeur patrimoniale.

1.2.1 La valeur administrative

La valeur administrative de l'information équivaut exactement, nous l'avons souligné plus haut, à la valeur primaire du document qui la contient. Elle correspond, par conséquent, à l'utilisation de l'information aux fins de gestion du personnel, des ressources financières, matérielles et informationnelle ainsi qu'aux fonctions propres à chaque organisme. Dans le premier cas, on parlera de documents de gestion; dans le second, de documents de fonction, dits aussi d'exploitation.

Toute information qui possède une valeur administrative ne la détient cependant pas au même degré. L'importance des divers documents dans la bonne marche de l'organisme qui les détient varie en fonction de la nature plus ou moins stratégique de leur contenu. Cette réalité a conduit les gestionnaires de l'information à désigner précisément les documents essentiels de l'organisme employeur, c'est-à-dire ceux dont l'organisme ne pourrait se passer pour reprendre ses activités à la suite d'une catastrophe. Il faut donc en conclure qu'il existe deux catégories de documents qui possèdent une valeur administrative : ceux qui sont essentiels au fonctionnement de l'organisme, et les autres, qu'on n'a pas gratifiés d'un qualificatif propre et dont les mesures de protection pourront varier en conséquence.

Enfin, il est primordial de reconnaître qu'un document, que son information soit consignée sur support électronique ou sur papier, n'atteint ce statut qu'au moment de son enregistrement dans un système institutionnel de gestion de l'information. Les esquisses, notes, brouillons ou projets sont bien, en principe, des documents visés par la *Loi sur les archives*, mais, en pratique, leur inscription au calendrier de conservation de l'organisme n'intervient qu'au moment de leur enregistrement, par exemple dans un dossier qui prend habituellement place dans une série inscrite au calendrier. L'introduction de cette notion d'enregistrement vise donc à rendre compte de la différence, reconnue dans la pratique, entre les documents institutionnels d'un organisme et les documents personnels de ses employés.

1.2.2 La valeur juridique

La valeur juridique de l'information tient essentiellement à deux considérations distinctes : d'une part, la loi impose un encadrement particulier de l'information; d'autre part, l'organisme détenteur de l'information veut pouvoir l'utiliser éventuellement aux fins de preuve.

Dans le premier cas, une loi ou un règlement peut rendre obligatoire la création et même la facture de certains documents ou obliger la conservation de certains documents pendant une période donnée, et même prévoir des mécanismes de reproduction et d'élimination de certains documents. Le gestionnaire de l'information devra donc non seulement déterminer les documents seront l'objet d'un encadrement légal particulier, mais il devra également prendre les mesures nécessaires pour s'assurer que ces documents sont gérés conformément aux dispositions légales ou réglementaires. C'est donc non seulement la forme, mais l'existence même et la gestion d'un document (information consignée sur un support) qui peuvent être encadrées par une loi ou par un règlement.

Dans le deuxième cas, on pense plus particulièrement aux documents qui pourraient être requis pour faire valoir un droit dans le cadre d'une procédure judiciaire ou quasi-judiciaire, ou, plus rarement, dans un but purement préventif. Ce sont donc les documents qu'un organisme peut vouloir conserver aux fins de preuve, c'est-à-dire de démonstration de l'exactitude d'une proposition (établir la vérité délivrée du doute ou de l'incertitude). Habituellement, la loi ou un règlement prévoit un délai de prescription après lequel une affaire ne peut plus être amenée devant le tribunal. Une telle prescription se traduit, dans la pratique, par un délai de conservation (équivalant à la durée de la prescription plus d'une année de sécurité) pendant lequel le document sera considéré comme actif ou semi-actif au sens de la *Loi sur les archives*.

1.2.3 La valeur patrimoniale (ou valeur d'information et de témoignage)

La valeur patrimoniale d'une information consignée sur un support correspond, nous l'avons signalé plus haut, à sa valeur secondaire, ou, en d'autres mots, à sa valeur aux fins de la recherche. Il faut cependant se garder de réduire l'intérêt d'un document pour la recherche à sa seule valeur historique : l'établissement de la « généalogie » de certaines maladies héréditaires par le biais des données de l'état civil est un exemple de la diversité du potentiel de recherche de l'information consignée dans un document ou dans une base/banque de données.

Par ailleurs, si la valeur patrimoniale d'un document ou d'une base/banque de données est généralement associée à son versement dans un service d'archives, la qualité « patrimoniale » d'un document naît parfois au moment même de sa création. Dans tous les cas, cependant, cette valeur patrimoniale (présente ou virtuelle) devra être prise en compte dans la gestion et la protection de l'information.

Enfin, on estime habituellement à 10 % ou 15 % la proportion de l'ensemble des documents produits ou reçus par un organisme qui détiennent ou acquièrent une valeur patrimoniale.

1.3 Les différents niveaux de protection des documents électroniques

Les niveaux de protection des documents électroniques sont au nombre de trois, si l'on s'en tient aux seuls documents institutionnels : l'enregistrement dans le système institutionnel de l'organisme, le scellement et la signature. Les informations consignées sur papier sont également l'objet d'enregistrement (lorsqu'elles sont classés dans un dossier, par exemple) et de

signature (le plus souvent à la main), mais il est maintenant rare que l'on sente le besoin de les sceller à la manière ancienne. Dans ce dernier cas, on considère généralement que le seul fait de coucher une information sur papier ou sur un autre support traditionnel suffit à en protéger, sinon à en garantir, l'intégrité. Dans certains cas particuliers, on utilisera cependant différentes techniques de protection de l'intégrité, comme, par exemple, un enduit de plastique, un papier spécial filigrané ou un code à barres.

À l'extérieur de l'espace électronique institutionnel, il faut cependant constater qu'existe parallèlement un espace électronique personnel géré exclusivement par chaque employé de l'organisme et non soumis, en général, à l'application du calendrier de conservation de l'organisme. On y retrouve des projets, des brouillons, des copies de documents institutionnels, les messages électroniques, etc. Il en va de même pour les documents sur papier : ainsi, par exemple, la version provisoire, ou de travail, d'un document sera-t-elle conservée dans un dossier personnel de l'employé, tout comme ses notes de lecture ou ses messages électroniques imprimés, à moins que des circonstances particulières ne l'amènent à poser consciemment le geste d'enregistrer l'un de ces documents plus ou moins éphémères dans un dossier institutionnel de son employeur.

1.3.1 La sauvegarde d'un document dans un espace personnel

Il est rare que l'espace personnel de sauvegarde sur micro-ordinateur est encadré par des règles administratives de conservation. En conséquence, les documents ne seront l'objet d'aucune mesure de protection particulière mise en œuvre par l'organisme. Leur utilisation et leur conservation resteront donc du ressort exclusif de la personne qui les aura sauvegardés dans son espace électronique personnel ou, dans le cas de documents sur papier, conservés dans son espace de rangement personnel.

Parmi les modes de production de documents qui seront sauvegardés dans un espace personnel, on retrouve évidemment les documents bureautiques, puisque ces outils, comme la consignation d'une information sur une feuille de papier, ont constitué jusqu'à maintenant essentiellement des outils personnels. C'est seulement dans une étape ultérieure à leur production que les documents bureautiques pourront être enregistrés dans un système institutionnel de gestion de l'information. Il en sera également ainsi des documents électroniques résultant d'une opération de numérisation tant et aussi longtemps qu'ils n'auront pas été enregistrés sur un support de conservation (souvent un disque optique) à partir de leur support de travail effaçable (ce dernier étant généralement un disque dur).

Enfin, on peut douter que l'information contenue dans une base/banque de données puisse jamais être conservée dans un espace électronique personnel, si ce n'est, à la rigueur, sous forme de copie. On notera que les données extraites d'une base/banque de données sont insérées généralement dans des documents directement lisibles par l'œil, avec ou sans l'aide d'une machine. En d'autres mots, leur structure interne est intelligible sans traitement autre, éventuellement, que celui de son exécution présentée sur une surface de visualisation.

1.3.2 L'enregistrement dans un espace institutionnel : une protection de base

L'enregistrement d'un document ou d'une information dans un espace électronique institutionnel constitue, en soi, une reconnaissance de sa valeur administrative, puisqu'en l'absence d'une telle valeur on ne prendrait pas la peine de réaliser les opérations nécessaires à son enregistrement, si peu onéreuses ou si automatiques soient elles.

Concernant les bases/banques de données, on peut dire que celles-ci sont pour la plupart institutionnelles (sauf chez les chercheurs) et, à ce titre, elles sont enregistrées dès leur création dans un espace électronique institutionnel. Il en va cependant tout autrement du document ou de l'information produits dans un espace électronique personnel ou sur papier, qui doivent normalement faire l'objet d'une manœuvre d'enregistrement expresse pour acquérir leur valeur administrative pour l'organisme. Cet enregistrement peut cependant être automatique dans le cas des documents sur support électronique répondant à des critères établis au préalable.

La définition des procédures et l'attribution des responsabilités doivent auparavant avoir été adoptées puis déployées via une infrastructure pour garantir la sécurité juridique du document électronique. Ce travail a été amorcé dans les *Lignes directrices pour l'enregistrement des documents de transaction* dans le but de déterminer les métadonnées essentielles pour garantir la valeur juridique d'un document électronique. La conservation d'un document signé comporte des exigences. Les métadonnées doivent permettre de définir la place du document électronique dans les processus de gestion de l'information, ce qui constitue une partie intégrante de sa validité juridique. Cela concerne aussi un éventuel rattachement des bases de données au calendrier de conservation de l'organisme tel qu'il est appliqué aux documents.

1.3.3 Le scellement : une protection de l'intégrité de l'information

L'un des éléments fondamentaux de cette protection est de sceller « électroniquement » le document ou l'information électronique de manière à en garantir l'intégrité. Cette protection de l'intégrité de l'information électronique est également nécessaire dans le cas où celle-ci présente une valeur légale, soit parce que sa création ou sa conservation sont prévues par la loi, soit parce que le document qui la contient peut devoir être mis en preuve devant le tribunal. Enfin, certains documents sur support électronique peuvent devoir être scellés à cause de leur importance intrinsèque pour le fonctionnement de l'organisme.

On doit s'assurer que le document électronique est complet et qu'il comprend tous les éléments nécessaires à la reconnaissance de sa valeur légale, sans que rien n'ait été retiré ni ajouté après son scellement.

L'identification des parties constituant un document est donc obligatoire pour certains types de documents. Il faut aussi que soient élaborés des modèles de contenu en vue de servir comme référence de validation grâce à la structure logique du document, ou « DTD », qui est traitée par les logiciels. La structure logique interne d'un document, c'est-à-dire son balisage et son contenu, sont l'objet principal de la validation. La validation porte aussi sur les métadonnées qui concernent le document pris comme un tout.

1.3.4 La signature numérique : une reconnaissance de la responsabilité

C'est le propre de toute signature, et non pas seulement de la signature numérique, de constituer une forme de reconnaissance de la responsabilité. La question est de savoir si l'on peut apposer une signature au moyen d'un procédé électronique.

La signature numérique, le niveau de protection le plus élevé de l'information électronique, est essentiellement de nature juridique puisqu'elle vise, d'une part, à formaliser la responsabilité d'une personne vis-à-vis cette information et, d'autre part, à instaurer des conditions de non-répudiation de la même information. De même que la signature manuscrite sur papier, la technologie dite de signature numérique répond aux critères juridiques de ce qui constitue une signature, à savoir : ce procédé permet la réalisation d'une marque qui peut être personnelle, qui peut être fixée au document et qui est susceptible d'exprimer le consentement du signataire. En effet, la technologie dite de signature numérique offre actuellement le niveau de protection le plus élevé de l'information électronique, car elle permet à la fois d'assurer l'intégrité du document, la confidentialité de l'information et la non-répudiation du document, en plus de permettre d'attribuer la responsabilité d'un document à une personne identifiée.

La signature numérique apposée sur un document bureautique ou sur un document numérisé, quoique de manière différente, a la même signification pour le signataire que la signature manuelle sur le papier. La signature a pour effet d'assurer la valeur juridique et aussi administrative d'un document. Il pourra cependant être nécessaire d'apposer une signature numérique sur plusieurs éléments constitutifs d'une base/banque de données, par exemple sur les données ou des sous-ensembles de données.

Par ailleurs, qu'elle soit numérique ou manuscrite, la signature n'intervient que très indirectement dans la valeur patrimoniale de l'information. En effet, un document non signé et qui ne devait pas l'être conserve toute sa valeur patrimoniale si celle-ci a été établie dans le calendrier de conservation de l'organisme. Par contre, un document non signé alors qu'il aurait dû l'être peut voir sa valeur patrimoniale diminuée, voire annihilée. Mais, en soi, la signature n'augmente pas ni ne diminue la valeur patrimoniale d'une information.

La valeur de la signature numérique repose sur la vérification de l'identité du « créateur » d'un document. Cette vérification comprend deux opérations distinctes, bien que très intimement liées : la vérification de l'autorisation accordée à une personne d'effectuer une opération sur un document électronique (ces autorisation sont enregistrées et contrôlées par le service de répertoire) la vérification de l'identité de la personne qui veut effectuer cette opération (le service de répertoire enregistre et vérifie les clés publiques associées aux signatures du personnel).

En d'autres mots, il faut pouvoir authentifier l'identité de la personne autorisée à produire ou à modifier un document électronique qui possédera une valeur juridique.

L'authentification peut être raffinée en fonction des différents types d'opération qui peuvent être accomplis (lecture, création, modification, etc.), de même qu'elle peut comprendre différents niveaux de garantie. Il faut que la définition des procédures et l'attribution des responsabilités et autorisations aient auparavant été adoptées puis déployées via une infrastructure pour garantir la sécurité juridique du document électronique.

La source des autorisations peut (a) être un pouvoir expressément prévu dans la loi, (b) faire l'objet d'une délégation de pouvoir ou de signature, ou (c) être associée à l'occupation d'un poste donné.

Les unités administratives responsables de la gestion du personnel fournissent les renseignements associant les personnes à des rôles dans l'organisation et aux autorisations rattachées à ces rôles.

Les unités administratives responsables de la gestion financière disposent de l'expertise sur les procédures de délégation de signature ainsi que sur les règles et procédures relatives aux autorisations rattachées à des rôles dans l'organisation.

Les unités administratives responsables de la gestion des ressources informatiques fournissent le support aux outils de création et d'exploitation des documents électroniques de même qu'aux outils de contrôle d'accès aux premiers.

CHAPITRE 2

LES CONDITIONS TECHNIQUES DE VALIDITÉ DU DOCUMENT ÉLECTRONIQUE

Introduction

Le document électronique se situe dans un monde où la sécurité de l'information est principalement protégée grâce à une branche des mathématiques. En effet, la cryptographie est la source des principaux moyens, tels le chiffrement et le déchiffrement de l'information par des algorithmes utilisant une seule clé (symétrique) ou alternativement deux clés (asymétriques) attachées dans une biclé, ou encore tels les algorithmes pour résumer mathématiquement un document de manière à le rendre fiable, l'altération ultérieur du document ne pouvant échapper à la détection. L'application combinée de ces algorithmes et des clés associées est ce qui permet de produire la signature numérique d'un document électronique. Voici quelques exemples d'utilisation possible des techniques de cryptographie dans l'administration publique :

- assurer la confidentialité de l'information enregistrée ou transportée, par exemple quand un sous-ministre écrit à un autre sous-ministre, ou quand un hôpital ou un pharmacien adresse à la RAMQ un message contenant des renseignements personnels (chiffrement et déchiffrement par clé symétrique) ;

- authentifier l'identité d'un usager du cyberespace, ~~si~~ quand par exemple un citoyen veut avoir accès aux renseignements le concernant dans les banques d'information gouvernementale ou pour toute transaction comportant un risque de fraude (chiffrement par clé asymétrique);

- assurer la non-répudiation des documents de transaction grâce au mécanisme de signature numérique qui garantit l'intégrité du document (par l'empreinte) en même temps que l'intention du signataire d'assumer la responsabilité à l'égard du contenu et de sa signification en contexte (par le chiffrement avec clé asymétrique).

La réalisation de transactions est parfois désignée sous le nom global de commerce électronique, qui, du point de vue gouvernemental, comporte trois volets à incidence financière et d'autres volets à incidence sociale, professionnelle, etc., dans les communications avec les clientèles :

- le volet fiscal : versement de taxes, d'impôts, de droits, par les citoyens et les entreprises au gouvernement ;
- le volet bénéfices : versement de pensions, d'allocations, de subventions, de remboursements à des citoyens et des entreprises ;
- le volet acquisitions : achat de biens et services par le gouvernement auprès des entreprises ;
- le volet accès à son propre dossier par un citoyen, un patient, un étudiant, un contribuable, etc. ;
- le volet demande ou inscription dans le cadre d'un programme gouvernemental avec transmission de renseignements personnels ou stratégiques ;
- le volet utilisation de registres gouvernementaux, comme celui des droits personnels et réels mobiliers (RDPRM).

Les sous-sections ci-après présentent de façon brève les conditions techniques pour garantir l'intégrité des documents électroniques et la non-répudiation des documents électroniques signés, les conditions de transfert des documents entre les supports papier, électronique et d'image numérique, le contexte technique de la conservation des documents ayant valeur probante et le *Modèle des communications d'affaires acceptables*.

2.1 Le scellement pour garantir l'intégrité de l'information

Comparé au document papier qui est visible sur un support durable et difficile à altérer sans que cela soit perceptible, et qui peut être doté de signature(s) et date(s) incluses dans son contenu, un fichier conventionnel contenant un document électronique doit être protégé de façon particulière si l'on veut qu'il conserve sa valeur probante. La technique conventionnelle permettant de garantir qu'un document électronique n'a pas été modifié est de traiter la chaîne de caractères constituant le document avec un algorithme qui calcule une sorte de résumé mathématique du document, appelé son *empreinte* (*digest*). Comme plusieurs algorithmes peuvent servir à calculer l'empreinte, celui qui est utilisé doit être identifié de façon à permettre la vérification de celle-ci ; la protection vient du fait que le moindre changement dans le contenu du document provoquera inévitablement la production d'une empreinte différente. Cette empreinte comporte le plus souvent 128 bits qui, avec le nom de l'algorithme qui l'a produite, viennent s'ajouter aux métadonnées du document dont on veut garantir l'intégrité. La délimitation précise du contenu du document signé est cruciale pour assurer la validité de la prise d'empreinte. On peut considérer que l'inaltérabilité du contenu d'un document est mieux garantie avec des moyens mathématiques que par le contrôle physique de papier et d'encres à usage réservé.

2.2 L'authentification par la signature numérique pour garantir la non-répudiation

Quand, en plus d'être ainsi scellé, un document électronique doit être signé, son empreinte est traitée avec un algorithme de chiffrement qui prend pour valeur de calcul un grand nombre secret, détenu exclusivement par le signataire du document. Le résultat obtenu par ce second calcul constitue la signature numérique du document et vient s'ajouter aux métadonnées garantissant l'intégrité. De façon abstraite, la signature est un énoncé relatif au contenu du document et par lequel une personne dont l'identité peut être retracée affirme que le contenu du document est ce qu'elle a écrit et qu'elle en assume la responsabilité. La valeur contenue dans cette métadonnée sert à la vérification de l'identité du signataire (son authentification) en vertu des certificats de clés publiques formant des biclés avec leurs clés privées correspondantes. La signature numérique permet de satisfaire aux conditions juridiques pour qu'il y ait non-répudiation du signataire, que sa responsabilité puisse être établie sur la base du document conservé (comprenant les données et les métadonnées). Le prochain chapitre explique comment.

On voit donc que, dans le cas des documents électroniques en ASCII ou ISO-latin qui sont facilement altérables, la solution générale est du côté des techniques de cryptographie et d'une infrastructure à clés publiques permettant d'utiliser les techniques de signature numérique, lesquelles sont combinées avec des techniques préexistantes d'empreinte numérique du document (par hachage, « checksum » ou autre « MAC » ou code d'authentification de message).

Prenons pour exemple le procédé dit de signature biométrique qui tente d'effectuer une percée avec des produits appelés Pen-Op, Cadix et ApproveIt. Ces logiciels fonctionnent généralement de la façon suivante. L'utilisateur voit à l'écran le document qu'il entend signer, clique sur la commande « Je veux signer » et saisit un crayon électronique pour apposer sa signature manuscrite (généralement son nom autographié) sur la surface de l'écran ou sur une tablette graphique. Le logiciel capture le tracé effectué avec le crayon sur la surface sensible ainsi que des mesures effectuées l'exécution même de la signature : vitesse, angle, arrondi des boucles, types de lignes et de points de croisement du tracé. Divers calculs sont effectués sur le document signé et sur les mesures biométriques associées à la signature autographe et à d'autres éléments de contexte (temps, dispositif) pour obtenir un jeton (*token*) biométrique unique associé à ce document. L'utilisation de mesures biométriques pour apposer une signature semble à première vue fort attrayante, en raison de son apparente continuité avec le processus de signature manuscrite.

Cependant, il faut d'abord souligner un inconvénient majeur qu'entraîne l'utilisation de mesures biométriques. On entend, par biométrie, tout moyen ou toute méthode de vérifier l'identité d'une personne sur la base d'une caractéristique physique de l'individu ou d'actions répétables, s'il existe une telle caractéristique personnelle unique et mesurable. D'aucuns s'insurgeront contre un tel procédé en raison de son caractère intrusif dans la vie privée des gens. D'autres dénonceront son inefficacité en raison de la lourdeur de la vérification, car celle-ci demeure dépendante du facteur de probabilité d'appariement avec les formes canoniques préenregistrées. Si l'on renonce à une telle banque de données biométriques sur les personnes devant être identifiées, la vérification de la signature pourrait être assujettie à une vérification *a posteriori* de l'exactitude de la mesure biométrique choisie : en ce cas, on pourrait devoir constamment faire revenir la personne pour bien vérifier qu'il s'agit de sa signature manuscrite, de l'iris de son œil, de la forme de sa main ou de son empreinte digitale, ce qui est impraticable.

Un autre désavantage crucial de la signature biométrique en version Pen-Op est de faire naître un grand secret. En effet, la constante (requise par le procédé mathématique) ne pouvant plus être l'identité du signataire comme avec la clé privée, et le document à signer étant lui aussi une variable (son empreinte), la solution est de considérer le document comme la source d'une valeur constante lors de la vérification d'un document signé pour décomposer le jeton biométrique en ses éléments. Le grand secret (et la menace) réside dans cet algorithme qui permet, étant donné un document et un jeton biométrique, de déchiffrer le jeton pour en extraire la signature et tenter de la valider parmi des formes canoniques préenregistrées. Cette faiblesse est d'ailleurs pressentie par les vendeurs de Pen-Op qui argumentent que la signature en affaires est un contrôle latent, mais que les signatures n'ont pas à être vérifiées ni validées en général !

La technologie dite de signature numérique n'offre peut-être pas la même facilité visuelle à son utilisateur, car la marque personnelle qu'elle constitue pour réaliser un des éléments essentiels de la signature ne ressemble en rien à une signature manuscrite. Il s'agit en effet d'un code mathématique qui permet l'identification certaine du signataire grâce à un procédé faisant appel à des valeurs mathématiques appariées. Ce code est nécessairement lié au document, car il est constitué à partir des éléments d'information que porte le document et il est créé avec une biclé, dont l'une des valeurs n'est connue que de l'utilisateur et que lui seul doit pouvoir utiliser, répondant ainsi aux exigences de la notion juridique de signature.

Par ailleurs, la technologie de signature numérique offre d'énormes avantages pratiques, notamment quant aux coûts de vérification. En effet, la signature ainsi produite ne nécessite

qu'une intervention pour sa création, mais elle peut être vérifiée autant de fois qu'il est requis. En outre le degré de standardisation atteint par la technologie de signature numérique est en avance de plusieurs années sur les mécanismes encore boîteux associés à l'utilisation de mesures biométriques ayant valeur de signature.

La signature numérique est compacte puisqu'elle est le résultat d'une variable d'intégrité (l'empreinte du texte) et d'une constante d'authentification d'identité (la valeur de la clé privée du signataire). Une mesure biométrique ne peut, par sa nature même, résulter en une constante, sauf par le recours à une forme canonique préenregistrée pour obtenir cette constante permettant d'éliminer toute élasticité des caractéristiques de l'empreinte grâce à cet appariement. Cette différence de base se répercute sur la complexité de l'implantation.

La forme de signature électronique à retenir pour l'avenir prévisible est donc la signature numérique. Cependant, là comme ailleurs, il ne faut pas se fier aux apparences. Avant d'accepter comme signature un nouveau procédé électronique, il faut l'évaluer au regard des critères de reconnaissance d'une signature que nous fournit le droit applicable tant dans le monde papier que dans le monde électronique.

2.3 Le transfert de l'information d'un support à un autre

C'est la transformation des documents entre ces deux mondes qui s'avère le plus difficile pour le maintien des garanties de la signature. Les deux supports de document, papier et électronique, vont continuer longtemps de coexister dans la société et c'est ce qui rend essentiels des mécanismes de va-et-vient permettant de conserver la valeur juridique attribuée à un original. Si l'original est sur papier, il pourra être numérisé par un procédé photographique, tandis que si l'original est sur support électronique, il pourra être imprimé et certifié conforme à l'original électronique signé numériquement.

La numérisation est entendue ici au sens limité de l'utilisation de procédés de saisie optique et de transcription en une image électronique sur un support non effaçable et non réinscriptible. La numérisation de documents papier ne les soustrait pas à leur mode de validation basé sur le regard humain, puisque c'est encore l'image de la signature manuscrite à un certain endroit du document qui demeure le moyen de validation d'un original papier qui a été numérisé.

L'opération de transfert elle-même du papier à l'électronique électronique est un point évident de vulnérabilité. C'est pourquoi tout transfert doit être certifié selon les modalités propres au support du « double ». Si ce double est sur papier (résultat d'une impression ou matérialisation), il pourra être certifié avec un papier spécial, avec un sceau, ou avec tout moyen matériel difficile à reproduire et signé de façon manuscrite par un officier public. Si ce double est électronique (résultat d'une numérisation), le contrôle de la saisie peut comporter des certifications apposées sur le support et pouvant être l'application des techniques d'empreinte et de signature numérique pour ces images comme pour tout autre document.

2.4 La conservation des documents électroniques ayant valeur de preuve

La conservation des documents électroniques devant avoir valeur probante est en partie déterminée par les conditions techniques de production et de vérification des signatures numériques. L'évolution est rapide, il y a des zones de turbulence dans l'encadrement technique, mais plusieurs dimensions sont bien établies et doivent dès maintenant être prises en compte.

Il existe un modèle général, l'architecture PKIX (de l'IETF), qui sous-tend le déploiement de la signature numérique. Des aspects variés y sont couverts, notamment des services notariaux visant à garantir la conservation des documents en raison de leur valeur probante, des services de certification, des services d'horodatation certifiés, des algorithmes de cryptographie, etc. Même si plusieurs autres instances internationales sont actives dans ce domaine (ISO, UIT, CEN, UNESCO, W3C, ANSI), il existe une collaboration effective en voie de formalisation et un accord général sur les grandes dimensions représentées dans ce modèle d'architecture.

Des protocoles standards sous-tendant ces services sont en développement. Il y a déjà des poids lourds par secteur, par exemple le protocole SET (Secure Electronic Transactions) convenu par les multinationales majeures de cartes de crédit et les institutions bancaires qui leur sont presque toutes associées pour le fonctionnement d'un paiement par Internet et des communications de garantie qui y sont associées.

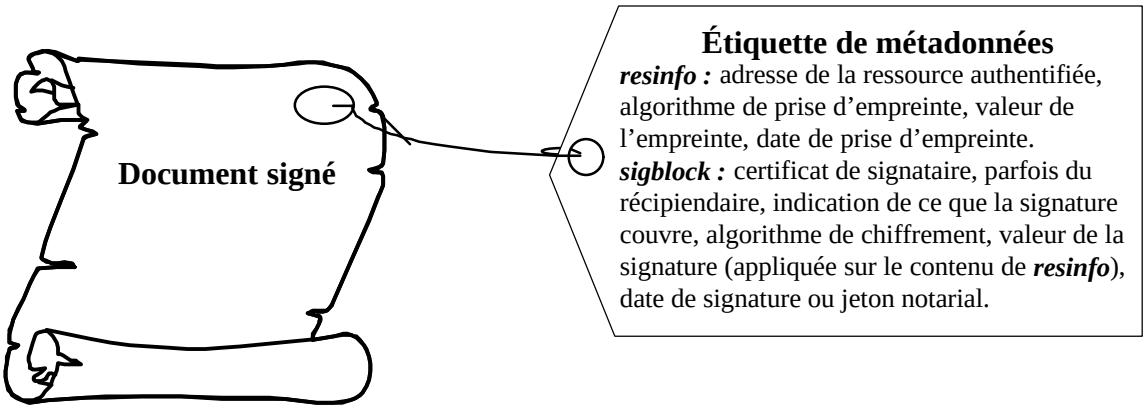
Le savoir-faire acquis en « EDI » (échange électronique de document) est transposé présentement dans le nouveau langage XML sur le Web, en même temps que sont conçus des messages adaptés aux besoins de l'ensemble des consommateurs, soit une toute nouvelle classe d'utilisateurs de l'EDI par rapport à la clientèle traditionnelle. Les règles de conservation édictées dans ce secteur méritent d'être considérées (voir, par exemple, XML/EDI Group Home Page à l'URL : http://www.xmledi.net).

Le langage XML déborde de beaucoup le cadre conventionnel de l'EDI et est en train de prendre une expansion remarquée pour le soutien logistique du commerce électronique, en particulier par l'élaboration de vocabulaires adaptés aux contextes d'une application, et ce, à plusieurs échelles (discipline, domaine industriel, type de document d'affaires).

Le langage XML est lui-même un élément important du nouveau *Modèle objet du document* (DOM : Document Object Model) en cours d'élaboration au W3C (World Wide Web Consortium) et qui permettra d'adapter le modèle de conservation des documents documents scellés et signés au moyen du langage RDF (Resource Description Format) spécialisé dans les métadonnées.

Une architecture concrète est en développement, grâce à l'impulsion du W3C (World Wide Web Consortium), sous le nom de Dsig (Digital Signature Initiative) dont la version 2.0, en cours de définition, est exprimée en langage XML dans son extension RDF. L'étiquette Dsig est l'objet d'un protocole qui propose un format standard pour faire des *énoncés* (*assertions*) signés numériquement à propos d'un document. Signer un document, c'est lui attacher une étiquette dont on signe une partie du contenu (*resinfo* dans la figure ci-après qui est expliquée en annexe). Le contenu de cette étiquette constitue une partie des éléments qui forment les métadonnées du document dont on veut assurer la valeur probante.

Aperçu des métadonnées spécifiques pour documents signés



DOCUMENT ÉTIQUETTE

Les métadonnées qui y sont représentées sont reprises dans le modèle produit par le Chantier en ingénierie documentaire et intitulé « Lignes directrices pour la description d'un document-de-transaction enregistré à des fins de conservation ». En ce qui concerne précisément la valeur probante, ces exigences de métadonnées ont été définies en référence au « Modèle des communications d'affaires acceptables » présenté ci-après.

Des protocoles complémentaires sont apparus en 1999, notamment DOMHASH qui améliore la détermination de ce qui est inclus dans le document signé afin de bien délimiter l'objet de l'algorithme de prise d'empreinte du document ; en préparation, SDML (*Signed Document Markup Language*) vise à mieux intégrer logiquement la signature au document et ce, sans affecter la validité des mécanismes de vérification, mais en permettant un traitement plus aisé des documents signés dans tout leur cycle de vie et en fonction d'une variété d'applications. Des mécanismes de signatures conjointes, d'endossement et autres font aussi l'objet de ces travaux.

2.5 Modèle des communications d'affaires acceptables (Pittsburgh)

Les besoins en métadonnées les plus critiques pour les Documents-de-transaction visent à satisfaire aux exigences de préservation de la valeur probante des documents conservés. Les travaux de Bearman et Sochats menés depuis 1995 à l'Université de Pittsburgh s'intéressent à ces exigences concernant la valeur en preuve des documents. Plus d'une douzaine de propriétés liées aux documents conservés sont définies dans ce but, et les métadonnées correspondantes sont définies dans un « Reference Model » pour les « Business Acceptable Communications (BAC) », que nous traduisons par *Modèle des communications d'affaires acceptables*. Les environnements de bureautique typiques de l'ère pré-intranet ne satisfont pas aux exigences relatives aux documents conservés en général.

Les métadonnées doivent être créées en même temps que la transaction. Elles précéderaient le contenu de la transaction avec un quadruplet de propriétés :

- l'identification du document conservé :
- les limites d'accès ;
- la façon d'ouvrir et de lire un document :
- la signification de la communication dans le cours des choses.

Le Modèle de référence BAC s'intéresse surtout aux métadonnées nécessaires pour établir la valeur probante (obligatoires), alors que seraient facultatives les métadonnées répondant aux besoins de gestion documentaire autres qu'aux fins de preuve.

a) Exigences fonctionnelles du Modèle

Organisation conscientisée

1. Conforme aux exigences légales et administratives.

Système de gestion des documents institutionnels

2. Responsable avec des politiques, des rôles définis et des méthodologies documentées pour leur gestion.
3. Déployé en tout temps et partout dans l'organisation.
4. Constance du fonctionnement et des résultats.

Conservation des documents institutionnels

5. Complète, pour toutes les transactions devant avoir valeur probante.
6. Identifiable : le lien entre la transaction et le document conservé doit être clair.
7. Intégrale, du contenu, de la structure et du contexte de la transaction documentée :
    a) Exacte, dont la qualité est contrôlée à la saisie ;
    b) compréhensible, avec une présentation logique des éléments et des liens entre eux ;
    c) significative : replaçable dans son contexte de transaction.
8. Autorisée : tout document a un créateur connu et celui-ci doit avoir les autorisations requises pour une transaction.

Archivage des documents institutionnels

9. Préservation à long terme du contenu, de la structure et du contexte :
    a) aucune altération ;
    b) cohérent, relations retraçables entre les éléments ;
    c) vérifiable.
10. Jetable : le contenu et la structure peuvent être sélectivement retirés des documents conservés, et les traces en sont conservées.

Facilité d'utilisation des documents

11. Exportable sans perte d'information.
12. Accessible, disponible, affichable ou imprimable, bien structuré, de valeur probante et reflétant le contexte de création et l'utilisation des documents conservés.
13. Présentation possible d'extraits partiels de documents.

b) Modèle de référence pour les Communications d'affaires acceptables

Il s'agit d'une structuration des métadonnées en six couches.

1. Emballage (*Handle*) :
   Déclare que ce qui suit est un document conservé, sa provenance et les descripteurs identifiant le document conservé en vue de faciliter le repérage ultérieur.

2. Exigences et conditions (*Terms & conditions*) :
   Indiquent les contrôles sur l'accès, l'utilisation et la destruction des documents conservés.

3. Structure de l'information :
   Description de la structure des données et de l'information permettant au document conservé de garder sa valeur probante à long terme et d'être transféré sur de nouveaux supports éventuellement.

4. Contexte :
   Indique la provenance (personne, système ou instrument) du document conservé et les données qui supportent sa valeur probante (preuve d'une transaction).

5. Contenu :
   Contient les données impliquées dans la transaction, qu'elles y aient été créées ou incorporées.

6. Historique de l'utilisation :
   Après la création du document, quelle indexation, quelles extractions en ont été faites ? Journal des types d'utilisation, le moment, l'identité de l'utilisateur, les conséquences dans certains cas.

CONCLUSION

Compte tenu de ses moyens limités, le groupe de travail a exploré les aspects techniques et juridiques de la reconnaissance de la valeur du document électronique et de ce qui peut être considéré comme équivalent à la signature d'une personne liant sa responsabilité à la teneur d'un document. En prenant appui sur le contexte administratif gouvernemental, nous avons principalement cherché à indiquer des façons pratiques de procéder et les conditions à respecter pour que les documents électroniques puissent fonder le monde des affaires. Il avait été prévu d'introduire un chapitre approfondissant les questions juridiques autour des conditions de validité des signatures. Cette partie n'est pas incluse dans le présent rapport et sera traitée dans un document distinct préparé par maître Jeanne Proulx du ministère de la Justice. Ce rapport vient alimenter la préparation des devis techniques et des encadrements administratifs appropriés pour mener les affaires en se servant de documents électroniques.

ANNEXE

Dsig 1.0 Signature Labels : Using PICS 1.1 Labels for Making Signed Assertions (nov. 97)

Le protocole Dsig propose un format standard pour faire des *énoncés* (*assertions*) signés numériquement à propos d'une ressource électronique ou d'un document. Le mécanisme permet à un signataire d'affirmer un *énoncé* (*statement*) à propos d'une ressource (« signer believes statement about information ressource »).

Caractéristiques de Dsig :

- L'*étiquette de signature* (*signature label*) n'enveloppe pas la ressource informationnelle qu'elle signe, mais lui est attachée de manière cryptographique et peut être véhiculée soit en lui étant attachée physiquement (*embedded* dans une balise META), soit en l'accompagnant dans un message HTTP (attachée dans l'en-tête) ou être consultable séparément (*detached*).

- Les énoncés doivent être reliés de manière cryptographique aux ressources informationnelles pour en assurer l'intégrité (empreinte); l'extension **resinfo** vise à attacher l'étiquette à la ressource, pas l'URL lui-même mais le contenu du document (son empreinte), un document pouvant se trouver à plusieurs URL.

- Le signataire crée une étiquette qui contient un énoncé (*énoncé d'étiquette : assertion label*) ; en signant cet énoncé d'étiquette, le signataire confirme sa responsabilité à l'égard du contenu de l'énoncé, de sa signification en contexte.

- Des signatures additionnelles peuvent toujours être ajoutées à une première signature dans une étiquette d'énoncé ; plusieurs signatures parallèles peuvent être juxtaposées dans un *sigblock*. Les signatures en cascade (une signature en signant une autre) ne sont pas possibles dans un seul *sigblock*. Il faut dans ce cas signer une première étiquette en créant une seconde étiquette à cet effet.

- L'énoncé sur une étiquette peut contenir des informations détaillées sur la ressource, en particulier les *empreintes* (*digests*) produites par divers algorithmes de hachage appliqués à la ressource informationnelle visée par l'énoncé.

- Une étiquette est spécifique à un document. Chaque élément de *resinfo* se compose d'un identifiant d'algorithme de hachage, de l'empreinte du document spécifique, et facultativement de la date de prise d'empreinte du document. Les *manifestes* sont des énoncés relatifs à plusieurs ressources interreliées plutôt qu'à une ressource particulière.

- Par convention, un *Bloc-signature-Dsig* (Dsig Signature Block) dans une étiquette signifie que « l'entité détenant la clé privée qui a signé cette étiquette avait accès simultanément à la clé privée et à l'étiquette et cette entité affirme que les énoncés contenus dans l'étiquette sont valides ».

Extensions Dsig

Une étiquette Dsig signe une ressource de façon sûre grâce à un lien cryptographique avec cette ressource. Ce lien est établi en incluant, dans le Bloc-Dsig, une ou plusieurs empreintes résultant d'algorithmes de hachage appliqués à cette ressource.

C'est l'extension **resinfo** qui permet d'emmagasiner plusieurs empreintes résultant de plusieurs algorithmes.

L'extension **sigblock** permet d'emmagasiner une ou plusieurs signatures utilisant un ou plusieurs algorithmes de chiffrement ainsi que des certificats ou des liens avec des certificats. L'extension **sigblock** protège de manière cryptographique l'étiquette avec les techniques de signature numérique. Elle indique : (a) qui a signé, (b) quelles parties de l'étiquette sont signées (elles ne sont pas toutes signées), (c) quels algorithmes ont servi à générer la signature, (d) les données de la signature elle-même. L'extension peut aussi contenir des certificats utilisables par les *systèmes de gestion de la confiance* (*trust management system*) pour vérifier la signature. L'extension comprend une *information attributive* (*attribution information*) et une ou plusieurs signatures. Une signature peut identifier sa marque (*signature suite*) qui informe les applications sur ses modes de création et de vérification.

L'information sur les clés (« Keyholder tokens ») reliées à la signature est soit :

a) la clé publique est transmise directement (ByKey) ;
b) une empreinte de la clé publique est transmise (ByHash) ;
c) un nom associé à une clé publique, tel un « nom distinctif » X.509 (ByName) ;
d) le nom d'une Autorité de certification et l'information pour identifier la clé voulue à l'Autorité de certification (ByCert).

Le moment de la signature est indiqué après un *token* « On » par un « quoted-ISO-Date » dans le *sigblock*.

Le *token* « SigCrypto » *identifie* désigne le champ SigData qui contient les données cryptographiques, soit la signature elle-même.