



***Recommandations
pour la sécurisation
de l'horodatage électronique***

30 novembre 2002

version 2J

Membres du Groupe de Travail commun horodatage électronique :

Didier Adda (TPC)	cabinet.tpc@wanadoo.fr
Nadia Antonin (Banque de France, Edifrance)	nadia.antonin@banque-France.fr
Brigitte Candebat (Cessi / Cnam-TS)	brigitte.candebat@cnamts.fr
Anne Cantéro (Cabinet Caprioli, avocats)	annecantero@yahoo.fr
Michel Chevrier (IALTA)	mp.chevrier@wanadoo.fr
Michel Lesourd (CS-OEC, EDIFICAS)	mlesourd@wanadoo.fr
Etienne Pelletier (IALTA)	etiennep@aol.com
Isabelle Petit-Peucelle (Advance)	ipp@advanceinknowledge.com
Thierry Piette-Coudol (avocat, IALTA)	piettecoudol@wanadoo.fr
Max-Henri Pinton (CIC)	pintonma@cic-i.com
Hervé Schauer (HSC)	herve.schauer@hsc.fr

Avec la participation de : Gilbert Abulafya (GIP CPS), Thierry Autret (Ernst & Young), Catherine Bastoni-Laborderie (BNP Paribas), Me Eric Caprioli (Cabinet Caprioli Avocats), Michèle Copitet (Egona Technologies), Nathanaël Cottin (MSG-Software), François Couillard (Certplus), Jean-Marc Desperrier (Certplus), Bruno Grelaud (BNP Paribas), Maxime de Jabrun (GIP-MDS), Didier Liroulet (CESSI CNAM-TS), Guillaume de la Mettraie (Cas-hware), Jean-Claude Monnier (MSG-Software), Thierry Pecquet (Thales Secure Solutions), Sébastien Ropartz (Deloitte & Touche), Cédric Rougier (Elexience Datum), Emilie Savary (Deloitte & Touche), Eduard Tric (GIP-MDS), Jean-François Varenne (Neartech), Pierre Weiss (Française des Jeux), Geneviève Wirth (Posteasy).

Sous la direction de Michel Lesourd, expert-comptable diplômé, Directeur des Etudes informatiques du Conseil supérieur de l'Ordre des experts-comptables et Délégué général de l'association EDIFICAS, et de Thierry Piette Coudol, avocat, Cabinet d'avocats Bertrand & associés, Président de l'association IALTA.

Un **Comité de Suivi** procédera à une mise à jour du document. Toute observation, contribution ou critique peut lui être communiquée à l'une des adresses suivantes :

mlesourd@wanadoo.fr ou ialta@ialtafrance.org

Reproduction du document autorisée, moyennant la citation de l'intitulé exact du document *Recommandations pour la sécurisation de l'horodatage* et de l'auteur "EDIFICAS & IALTA", en mentions claires, apparentes et parfaitement lisibles, et son affectation à une utilisation personnelle ou strictement non commerciale, quel que soit le support. Cependant, toute reproduction sur un support tel que cédérom, disquette ou tout autre média permettant une diffusion de masse, y compris mais sans limitation une diffusion sonorisée, visualisée, etc., doit être autorisée préalablement par écrit par l'auteur. La demande d'autorisation doit être adressée à l'une des adresses électroniques suivantes :

mlesourd@wanadoo.fr, ialta@ialtafrance.org.

SOMMAIRE DU GUIDE

PREAMBULE	5
PREMIERE PARTIE : LES BESOINS EN HORODATAGE DES ECHANGES ELECTRONIQUES	7
1. LA MESURE DU TEMPS EN DROIT ET DANS LA TECHNIQUE	8
1.1. LA MESURE JURIDIQUE DU TEMPS ET DE L'HEURE	8
1.1.1. <i>L'heure sur le territoire de la République</i>	8
1.1.2. <i>La date et les notions voisines</i>	8
1.1.3. <i>La date dans les déclarations administratives</i>	9
1.2. LES NORMES ET STANDARDS DE L'HORODATAGE TECHNIQUE.....	10
1.2.1. <i>Les sources de temps</i>	10
1.2.2. <i>Les protocoles de distribution du temps</i>	11
1.2.3. <i>L'initiative européenne dans le cadre de la signature électronique</i>	11
2. L'HORODATAGE DU MESSAGE ÉLECTRONIQUE	13
2.1. L'HORODATAGE DU MESSAGE DANS LE DOMAINE COMMERCIAL	13
2.2. L'HORODATAGE DU MESSAGE DANS LE DOMAINE ADMINISTRATIF	15
3. L'HORODATAGE DE L'ÉCHANGE ÉLECTRONIQUE	16
3.1. L'HORODATAGE DE L'ÉCHANGE ÉLECTRONIQUE DANS LE DOMAINE COMMERCIAL.....	16
3.2. L'HORODATAGE DE L'ÉCHANGE ÉLECTRONIQUE DANS LE DOMAINE ADMINISTRATIF.....	17
3.2.1. <i>Le droit administratif et l'horodatage des téléprocédures</i>	17
3.2.2. <i>L'aménagement de la date administrative dans les téléprocédures</i>	19
3.2.3. <i>L'application concrète des principes dans la téléprocédure EDI-TDFC</i>	20
3.2.4. <i>L'application concrète des principes dans la téléprocédure DUCS-EDI</i>	21
3.2.4.1. ACOSS	21
3.2.4.2. UNEDIC - AGIRC-ARRCO	22
4. L'HORODATAGE ET L'ARCHIVAGE SÉCURISÉS	23
4.1. LES RECOMMANDATIONS SUR L'ARCHIVAGE ÉLECTRONIQUE SÉCURISÉ.....	23
4.2. L'HYPOTHÈSE : L'ARCHIVAGE INTERNE SÉCURISÉ.....	24
4.2.1. <i>L'opération d'archivage</i>	25
4.2.2. <i>La restauration des données et la vérification du certificat</i>	25

DEUXIEME PARTIE : VERS L'HORODATAGE SECURISÉ	26
1. L'HORODATAGE ORGANISÉ PAR CONTRAT	27
1.1. LA SOLUTION CONTRACTUELLE	27
1.2. ILLUSTRATION DE LA SOLUTION CONTRACTUELLE : LE PORTAIL JEDECLARE.COM	27
2. L'HORODATAGE SÉCURISÉ.....	30
2.1. L'HORODATAGE CERTIFIÉ.....	30
2.1.1. <i>La finalité de l'horodatage certifié</i>	30
2.1.3. <i>Horodatage et certification</i>	31
2.1.3.1. L'autorité d'horodatage	31
2.1.3.2. Le jeton d'horodatage.....	31
2.1.4. <i>Les scénarios d'horodatage certifié</i>	34
2.2. LE TIERS HORODATEUR	35
2.2.1. <i>Organisation de la profession de tiers horodateur</i>	35
2.2.1.1. Au niveau du tiers horodateur.....	35
2.2.1.2. Au niveau général de la profession de tiers horodateur	37
2.2.1.3. Au niveau du donneur d'ordre.....	37
2.2.2. <i>Exigences juridiques</i>	38
2.2.2.1. Exigences juridiques préalables au niveau de la profession de tiers horodateur	38
2.2.2.2. Exigences juridiques préalables entre tiers horodateur et donneur d'ordre	40
2.2.2.3 Exigences juridiques préalables au niveau du donneur d'ordre.....	42
2.2.3. <i>Services ajoutés par les tiers horodateurs</i>	42
GLOSSAIRE	44
LISTE DES TEXTES LÉGAUX ET RÉGLEMENTAIRES	47

PREAMBULE

Les actes juridiques nécessitent souvent une gestion pointue de la date et du temps dans les étapes de leur cycle de vie. Il en est ainsi pour leur formation, leur transmission, et leur archivage. Le droit parle de *datation* des actes et réclame souvent une *date certaine*. Les technologies de l'Information et de la Communication gèrent également le temps pour leur propre besoin. On parle d'*horodatage*, terme résultant de la contraction de date et heure, puisque dans l'informatique et les télécommunications le temps ne s'évalue plus en journées mais en fractions de secondes.

Les exigences juridiques et techniques de la gestion du temps doivent être rapprochées lorsque les actes juridiques empruntent une forme électronique, et/ou sont transmis par voie télématique ou électronique. En 1997, une Communication de la Commission de Bruxelles, le document COM503, rappelait l'importance des questions relatives à l'horodatage :

"Dans un contexte de relations juridiques, il existe de nombreuses situations où la preuve de l'heure exacte d'une action déterminée (transmission, création ou réception d'un document, ou l'heure à laquelle a été faite une déclaration d'intention) est cruciale."

Dans une table ronde de la *Mission Lorentz pour le Commerce Electronique* en novembre 1999 portant sur *"la reconnaissance de la valeur probante du document numérique"*, la notion de temps a été évoquée en ce qui concerne le cycle de vie des certificats électroniques (en particulier, pour la révocation). Aussi, la question de la gestion du temps semblait être d'actualité avec l'intégration de la signature électronique dans le Code Civil, par la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique¹. Cependant, la loi qui ne comprend que cinq articles ne dit rien de l'horodatage et beaucoup attendait des précisions dans le décret d'application en Conseil d'Etat annoncé par l'article 1316-4, alinéa 2 du code civil.

Le document COM503 avait bien annoncé les enjeux de la gestion du temps dans la signature électronique et son cortège technologique, les clés cryptographiques et le certificat électronique :

"Il est important de pouvoir prouver l'heure exacte à laquelle une clé a été révoquée afin d'éviter d'être lié par la signature de contrats signés avec une clé qui n'est plus sûre. C'est pourquoi des services d'enregistrement numérique de l'heure capables de confirmer de manière sûre l'heure exacte de certaines actions seront nécessaires. Les services d'enregistrement de l'heure sont également essentiels pour les applications dans le domaine des droits de propriété intellectuelle. Ces services pourraient être fournis par l'AC [Autorité de Certification], mais évidemment également par une autre entité."

¹ JO du 14 mars 2000, p. 3968.

Le décret sur la signature électronique n° 2001-272 du 30 mars 2001 l'a confirmé lors de sa publication : l'horodatage n'est pas pris formellement en compte dans la signature électronique². Pourtant la question devient critique avec le déploiement des *téléprocédures*. Comme pour les déclarations écrites, les téléprocédures devront être effectuées avant la date limite fixée par les textes. La loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations le précise bien dans son article 16 qui fait référence à un "[...] *procédé télématique ou informatique homologué permettant de certifier la date d'envoi.*"

L'objet du présent document est d'exposer au lecteur tant les exigences juridiques que techniques dans la gestion du temps, de lui proposer les éléments de réflexion nécessaires pour croiser les deux domaines d'exigences en matière de messages électroniques à vocation juridique et des solutions pratiques qui peuvent être mises en œuvre rapidement.

Après un rappel des règles en matière de gestion du temps en droit et dans la technique, la PREMIERE PARTIE – LES BESOINS EN HORODATAGE étudie les besoins en horodatage pour chaque étape du cycle de vie des messages électroniques.

Prenant en compte la forme avancée de la gestion du temps, la DEUXIEME PARTIE – L'HORODATAGE SECURISE décrit l'intervention d'un tiers de confiance spécifique, sa déontologie et son organisation professionnelle.

2 Par contre, le décret traite de la gestion temporelle du certificat électronique. Le décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique indique dans son article 6.I.c- qu'un certificat électronique qualifié doit comporter l'indication du début et de la fin de la période de validité du certificat électronique. De plus, l'article 6.II.n. ajoute qu'un prestataire de services de certification électronique doit veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision.

PREMIERE PARTIE : LES BESOINS EN HORODATAGE DES ECHANGES ELECTRONIQUES

Cette première partie comporte un premier paragraphe décrivant les normes et protocoles juridiques et techniques de l'horodatage et de la mesure du temps. Les paragraphes suivants envisagent la description des différents types d'interrelations entre les notions d'horodatage juridique et d'horodatage technique.

Plan de la première partie :

1. La mesure du temps en Droit et dans la technique
2. L'horodatage du message électronique
3. L'horodatage de l'échange électronique
4. L'horodatage et l'archivage sécurisés

1. LA MESURE DU TEMPS EN DROIT ET DANS LA TECHNIQUE

1.1. La mesure juridique du temps et de l'heure

Sur le territoire de la République, métropole ou terres d'Outre-Mer, la loi détermine la date et l'heure. D'autre part, plusieurs notions juridiques tournent autour de la mesure du temps.

1.1.1. L'heure sur le territoire de la République

La définition légale du temps repose sur les deux décrets suivants :

- le décret n° 78-855 du 9 août 1978 relatif à l'heure légale française ;
- le décret n° 79-896 du 17 octobre 1979 fixant l'heure légale française.

En croisant les textes cités, les principes de l'heure légale sont les suivants :

- sur l'ensemble du territoire de la République française, le temps légal (ou heure légale) est défini à partir du temps universel coordonné (U.T.C.) établi par le bureau international de l'heure.
- le temps légal (ou heure légale) est obtenu en ajoutant ou en retranchant un nombre entier d'heures au temps universel coordonné.
- l'heure légale dans les départements métropolitains de la République française est obtenue en ajoutant une heure au temps universel coordonné (U.T.C.), à l'exception de la période d'été pendant laquelle l'heure légale est obtenue en ajoutant deux heures à l'U.T.C.

L'heure légale est obtenue :

- dans les départements de la Guadeloupe et de la Martinique, en retranchant quatre heures à l'U.T.C., à l'exception de la période d'heure d'été pendant laquelle l'heure légale est obtenue en retranchant trois heures à l'U.T.C. ;
- dans les départements de la Guyane et de Saint-Pierre-et-Miquelon, en retranchant trois heures à l'U.T.C. ;
- dans le département de la Réunion, en ajoutant quatre heures à l'U.T.C. ;
- l'heure légale est obtenue dans la collectivité territoriale de Mayotte en ajoutant trois heures à l'U.T.C. ;
- l'heure légale est obtenue dans le territoire de la Polynésie française, en retranchant dix heures à l'U.T.C., dans le territoire de la Nouvelle-Calédonie, en ajoutant onze heures à l'U.T.C. et dans le territoire de Wallis et Futuna, en ajoutant douze heures à l'U.T.C..

La période d'heure d'été est fixée chaque année par arrêté conjoint du ministre de l'Industrie, du ministre des Transports et du secrétaire d'Etat auprès du ministre de l'Intérieur (Départements et Territoires d'outre-mer).

1.1.2. La date et les notions voisines

En droit, une notion de date est fréquemment employée, celle de *délai*. Le délai indique une période de temps dont on considère la date de fin pour produire des effets juridiques particuliers. Dans notre perspective, on dira qu'il s'agit d'un système de double date. En effet, lorsqu'une personne se met dans un certain cadre juridique à une date déterminable dite "*date*

d'ouverture du délai", le laps de temps prévu par la loi commence à s'égrener et les effets juridiques ne se produiront qu'à la fin de la période à partir d'une date dite "*date d'expiration*". Il existe aussi les notions de *date abstraite* et de *date concrète* (cf. les travaux du Professeur Blanche Sousi-Roubi³). La date abstraite est non précise dans le temps, mais liée à un événement (ex : le cachet de la poste faisant foi de la date d'expédition). La date concrète est une date calendaire (ex : le 1^{er} mars 2001).

Nous nous trouvons donc face à deux types de dates que nous nommerons *date technique* et *date juridique*. Si l'on considère l'angle juridique des opérations, la date technique doit être rapprochée de la *date juridique certaine*. La date juridique pourra bénéficier du caractère certain apporté par la certification de la date technique. Mais la date juridique est précise et unique, alors que la date technique peut être multiple. Il faut donc établir quel instant, quelle date technique retenir, voire sécuriser. Pour ce faire et dans une hypothèse particulière, il convient de relever dans les textes juridiques la date juridique à retenir. Cette date ou plutôt sa fonction doit être non pas adaptée mais transposée dans un monde sans *écrit-papier*. La transposition devra être justifiable et justifiée en droit. A partir d'une semblable démarche, il devrait être possible de dire quel est le moment technique correspondant. C'est ce temps technique qui fera l'objet d'une sécurisation et qui sera retenu par un instrument juridique (contrat ou réglementation) comme *date certaine*.

Le rapprochement entre Droit et Technique conduit à s'interroger également sur l'intérêt de la distinction entre *date absolue* et *date relative*. La date absolue renvoie à une date calendaire ; la date relative à une période ou un délai. Cette dernière fait apparaître le besoin de *chronologie* qui est sans doute aussi important que la date et l'heure au point de vue de l'U.T.C. En effet les actes de la vie courante conduisent plus à se poser la question de savoir si un événement est survenu avant tel ou tel autre événement (un événement pouvant aussi être un moment dans le temps ; remise d'une proposition avant 17 h 00 par exemple). Il en est de même en informatique, où par exemple, les traces d'audit sont horodatées pour leur chronologie et non pas pour la date absolue.

Enfin, il convient de distinguer les cas où la date s'applique à un acte ou à un fait (ou un événement). Dans la vie réelle, le cachet de la poste est apposé sur l'enveloppe ; on horodate alors l'envoi et non le document. La date peut être encore une simple mention (instrumentation) ou prendre une valeur d'information légale si elle donne lieu à litige (ex : date de fabrication/péremption sur un produit alimentaire).

1.1.3. La date dans les déclarations administratives

En matière de déclaration administrative, la date n'est plus la date du document, mais une date administrative, soit fixée par la loi (*date butoir*), soit déterminable par référence à la survenance d'une date extérieure (*délai*), soit enfin en combinant le délai et la date butoir, lorsque le délai tombe notamment un jour férié. Les autorités publiques se doivent, au nom du principe d'égalité devant le service public, d'apprécier la recevabilité ou la tardiveté d'une demande, du dépôt d'une déclaration, d'exécution d'un paiement, de production d'un document ou du respect d'une obligation, lorsque des textes fixent une date limite ou un délai à l'administré.

3 Blanche Sousi-Roubi, *Variations sur la date*, R.T.D. Civ., 1991, pp. 69 et s.

Les déclarations doivent, en principe, être produites dans un délai spécifique prévu par la loi. Toutefois, ce délai est prorogé dans un certain nombre de cas soit par la loi elle-même, soit par des mesures permanentes ou prises par l'administration. Le délai fixé par la loi est impératif (sanctions administratives, fiscales ou pénales), mais reçoit les atténuations suivantes :

- Lorsqu'un délai expire un samedi ou un jour férié, il est admis que cette date limite soit reportée au jour ouvrable suivant⁴ ;
- Lorsqu'un délai de déclaration expire un dimanche, la date de son expiration est reportée au lundi⁵. Lorsqu'elle est envoyée par la poste, la date limite s'apprécie en fonction de la date d'expédition, le cachet de la poste faisant foi⁶ ;
- Lorsqu'une déclaration est déposée directement dans la boîte aux lettres du service des impôts, la date de réception des documents est fixée au dernier jour ouvrable précédant celui où elle a été trouvée dans la boîte. Aucune pénalité n'est donc appliquée lorsque la déclaration est trouvée dans la boîte aux lettres à l'ouverture des bureaux le lendemain du jour où ce dépôt aurait dû être effectué⁷.

En outre, comme nous le développerons infra (3.2.2.), désormais, en application de l'article 16 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations⁸, la date d'envoi par l'administré et non celle de la réception par l'administration devient la règle ; exceptions faites des procédures régies par le code des marchés publics, des procédures pour lesquelles la présence personnelle du demandeur est exigée en application d'une disposition particulière et des procédures relevant des articles 1411 et suiv. du Code général des collectivités territoriales.

Bien que cela ne soit pas précisé, les dépôts doivent être réalisés avant minuit (24^h00'). Les délais s'appliquent en principe au lieu de l'entité auprès de laquelle il faut déclarer.

1.2. Les normes et standards de l'horodatage technique

1.2.1. Les sources de temps

Dans les technologies, le temps est défini par les notions de date, d'intervalle et de synchronisation. La date est un positionnement dans le temps par rapport à une origine convenue. L'intervalle est la mesure de temps qui sert de référence. En 1958, les savants mettent au point l'horloge atomique, dont la précision est de 1 seconde pour 3000 ans. Le principe repose sur le fait qu'un atome absorbe ou émet de l'énergie à une fréquence encore plus précise que celle du quartz ; l'atome retenu est le césium Cs :

The second is the duration of 9,192,631,770 periods of the radiation corresponding to the transition between the two hyperfine levels of the ground state of the cesium-133 atom. (13th General Conference of Weights and Measures (CGPM) (1967), Resolution 1).

4 D. adm. 5 B-4214, n° 1, 31 mars 1995.

5 Note 8 juin 1976, 4 A-10-76.

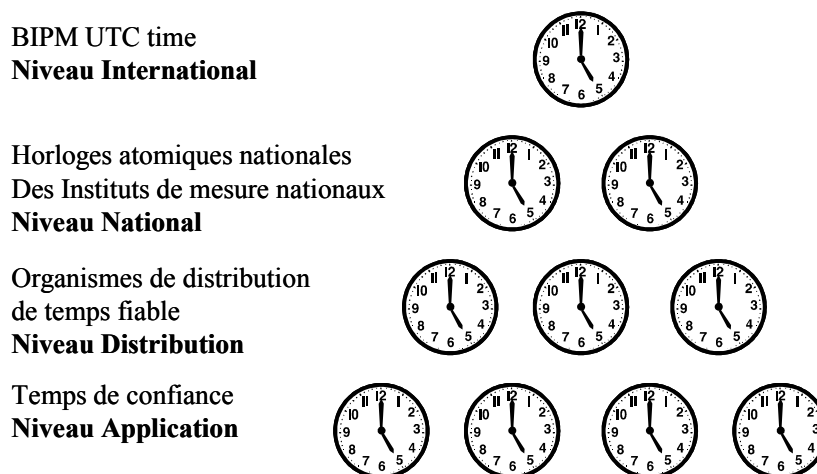
6 D. adm. 5 B-4214, n° 1 et 10, 31 mars 1995 ; Rép. Charbonnel, AN 8 juin 1987, p. 3306, n° 20886.

7 Rép. Godfrain, AN 2 mai 1988, p. 1972, n° 37739.

8 J.O. du 13 avril 2000, p. 5646.

La notion de temps universel a été définie en 1972 dans le cadre d'une conférence du Bureau International des Poids et Mesures (BIMP) des *National Measurement Institutes* dont font partie le NIST (US), le NPL (UK), le PTB (DE), le CRL (Japon), etc. Ces organismes s'accordent alors pour remplacer le Temps Universel de Greenwich par le temps U.T.C. (Unité de temps coordonnée ou *Coordinated Universal Time*).

La hiérarchie de distribution du temps est la suivante :



Comme on le voit, les notions de temps dans le droit et la technique sont intimement mêlées.

1.2.2. Les protocoles de distribution de la date et de l'heure ou du temps

L'IETF (*Internet Engineering Task Force*) a normalisé le protocole NTP (*Network Time Protocol*), qui permet une transmission fiable de la date et l'heure, dans le RFC305, entre un serveur de temps et un consommateur de temps au travers d'un réseau. Un protocole complémentaire, STIME (*Secure Network Time Protocol*), en cours de normalisation (draft-ietf-stime-ntpauth-03.txt) ajoute au protocole NTP l'authentification mutuelle.

1.2.3. L'initiative européenne dans le cadre de la signature électronique

Les industries européennes et les organismes de normalisation dans la voie tracée par la *Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques* ont lancé l'*Initiative de Standardisation Européenne de la signature électronique* (EESSI). L'EESSI a pour objectif d'analyser d'une façon cohérente les besoins futurs des activités de normalisation pour le soutien de la Directive Européenne sur les signatures électroniques, particulièrement dans un environnement d'affaires. Une équipe d'experts nommée par l'EESSI a produit un premier rapport le 1^{er} juillet 1999. Ce rapport a été préparé avec l'intention de proposer des normes sur la base d'un cadre ouvert de mise en œuvre des signatures électroniques face aux exigences d'utilisateurs en conformité avec la Directive.

Parmi les résultats susceptibles de rentrer dans le périmètre de la présente étude, il a été affirmé que les normes internationales adoptées et/ou développées par l'industrie devraient aussi loin que possible écarter le besoin de règles nationales détaillées. Le rapport propose un

cadre qui combine la standardisation et la législation et qui devrait permettre, notamment la spécification de politiques spécialisées pour les fournisseurs de prestations d'horodatage.

En ce qui concerne les travaux normatifs proprement dits, le développement des normes pour la partie liée à l'horodatage est confiée à l'Institut Européen des Normes de Télécommunications (ETSI). A ce jour, sur ce sujet précis, l'ETSI a publié :

- ETSI TS 102 023 V1.1.1 (2002-04) Policy requirements for time-stamping authorities ;
- ETSI TS 101 861 V2.1.1 (2002-03) Time stamping profile.

2. L'HORODATAGE DU MESSAGE ELECTRONIQUE

Il s'agit ici de traiter de la datation et de l'acte juridique sous forme électronique, plus particulièrement sous l'angle de la date et de l'heure de sa création.

On notera qu'à cause des différentes dates susceptibles d'intervenir, il est nécessaire d'opérer une distinction entre :

- messages électroniques, formes dématérialisées d'actes juridiques, échangées entre particuliers et qui relèvent généralement du droit privé (B to B ou C to C) ;
- messages électroniques entre citoyens et administrations, notamment les téléprocédures (B to A ou C to A).

2.1. L'horodatage du message dans le domaine commercial

Les actes juridiques privés se datent selon des exigences rendues nécessaires par le droit de la preuve. Les exigences sont indiquées ci-dessous.

En droit privé, l'apposition d'une date sur un acte n'est pas une condition de validité, mais constitue une énonciation essentielle⁹. La date d'un acte ou d'un fait est fondamentale pour que le droit qui découle de cet acte ou de ce fait juridique soit rendu opposable aux tiers. En effet, la preuve d'une date permet de se prévaloir d'un droit antérieur. *Prior tempore, potior jure*¹⁰, le premier en date étant le premier en droit. Il en résulte l'un des intérêts de rapporter cette preuve.

Dans le droit privé de la preuve, il faut distinguer la preuve d'un acte juridique qui est la manifestation de volonté destinée à produire des effets de droit, et la preuve d'un fait juridique qui est un événement, susceptible de produire des effets de droit. En effet, le mode de preuve est différent s'il s'agit d'apporter la preuve d'un acte ou d'un fait. Dans le premier cas, l'article 1341 du code civil régit ce mode de preuve : seule est admise la preuve littérale lorsque la valeur de la prestation en litige excède la somme de 762,25 € (soit 5 000 FF).

L'article 1328 du code civil dispose :

les actes sous seing privé n'ont de date contre les tiers que du jour où ils ont été enregistrés, du jour de la mort de celui ou de l'un de ceux qui les ont souscrits, ou du jour où leur substance est constatée dans les actes dressés par des officiers publics, tels que procès-verbaux scellés ou inventaire.

Ce qui signifie, comme l'ont écrit les professeurs Planiol et Ripert, que : *A l'égard des tiers l'indication de la date contenue dans un acte privé n'a aucune valeur probante. L'acte ne leur est pas opposable tant que la date n'est pas devenue certaine par l'un des moyens déterminés par la loi...*

⁹ Pierre STRASSER, *Force probante de la date d'un acte sous seing privé*, Jurisclasseur droit civil.

¹⁰ "Celui qui est le premier dans le temps, en droit l'emporte", Emmanuel PUTMAN, *Le temps et le droit*, Droit & Patrimoine, janvier 2000, n°78, p. 43.

Le mode de preuve est libre pour un fait juridique, c'est à dire que la preuve peut être apportée par tout moyen (témoignage, présomption...). De plus, le mode de preuve des actes de commerce est une exception au principe de l'article 1341 du code civil puisque la preuve est libre (article 109 du code de commerce).

L'article 1316-1 du code civil dispose *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*. La force probante d'un écrit sur support électronique est conditionnée par l'identification de la personne dont il émane, et par la garantie de son intégrité lors de son établissement, de sa conservation, et ce, jusqu'à la fin de ses effets juridiques. Comme on l'a dit, la notion de date n'est pas prise en compte dans ce texte. En outre, le texte ne nous éclaire pas sur les modalités et les conditions de conservation de l'écrit pour garantir son intégrité.

Suite aux préconisations du *Guide d'archivage électronique sécurisé*¹¹, la FNTC¹² met actuellement en place une procédure sécurisée qui permet la conservation des informations en recourant à des tiers archiveurs dont la profession est en cours d'organisation. L'AFNOR préconise une modalité pratique par sa norme NF Z 42-013 relative à la conservation électronique, dont les exigences répondent aux conditions de nature à garantir l'intégrité d'un écrit électronique.

Toute solution mise en œuvre est donc une sorte de pari sur l'avenir. La question est de savoir si l'horodatage technique peut être utilisé comme moyen de preuve de l'existence d'un fait ou d'un acte juridique. L'horodatage permet de façon précise d'attribuer une heure et une date. Seule une autorité tierce peut donner par son indépendance et sa neutralité, une force probante à l'horodatage. Cette autorité est un tiers de confiance qui génère une marque de temps afin de démontrer qu'une donnée existe à un instant déterminé.

11 Etude produite par un groupe de travail commun à l'Ordre des Experts-Comptables, IALTA, Edificas, document téléchargeable sur www.edificas.org.

12 FNTC : Fédération Nationale des Tiers de Confiance.

2.2. L'horodatage du message dans le domaine administratif

En droit administratif, tous les moyens de preuve sont recevables devant le juge administratif, même si l'administration aménage des règles et des procédures qui lui sont spécifiques, à des fins probatoires. Ainsi, il n'y a pas de réponse globale à la problématique juridique des téléprocédures avec les administrations. Ce d'autant plus que les principes dégagés par la loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, transposés dans le code civil, ne semblent pas, de droit, applicables au droit administratif. Néanmoins, en matière administrative, la date de création de l'acte revêt une importance juridique moindre que la date et l'heure de la transmission postale ou électronique des demandes ou déclarations notamment.

3. L'HORODATAGE DE L'ECHANGE ELECTRONIQUE

La loi du 13 mars 2000 définit l'écrit (ou plus exactement la preuve par écrit) à l'article 1316 du code civil qui dispose qu'il résulte d'une *suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission*. Ce faisant, cet article insiste sur une dimension de l'écrit papier, souvent négligée : l'écrit fait l'objet d'une transmission, depuis son auteur jusqu'à son ou ses destinataire(s) naturel(s).

3.1. L'horodatage de l'échange électronique dans le domaine commercial

La date de création est appliquée sur l'acte juridique au moment de la formation. Mais comme cette date est apposée par l'auteur lui-même, elle sera de peu de foi en cas de contestation par ses destinataires. Comme l'acte doit être transmis de l'un aux autres, il est possible de faire dater l'envoi par le tiers chargé de l'acheminement, traditionnellement La Poste. A défaut de date de création, ce tiers, qui n'a aucun intérêt dans l'affaire, atteste par son compostage de l'existence du contenant d'un acte au moment où il a été déposé par l'auteur pour acheminement.

Lorsque cette date s'avère critique, seul l'envoi recommandé avec ou sans avis de réception offre un véritable service de sécurisation. L'intérêt serait grand de disposer d'une procédure de même type dans le monde électronique. Malheureusement, le droit français ne possède pas actuellement de *recommandé électronique*. On peut observer cependant les enseignements d'autres législations, comme celle du Luxembourg.

La *Loi luxembourgeoise sur le commerce électronique* réforme son droit interne pour favoriser le développement de cette nouvelle façon de faire des affaires en adoptant notamment, la signature électronique. Dans la section 9 de la loi, un article 36 traite ainsi du recommandé électronique :

Le message signé électroniquement sur base d'un certificat agréé dont l'heure, la date, l'envoi et le cas échéant la réception, sont certifiés par le prestataire de service de certification accrédité conformément aux conditions fixées par règlement grand-ducal constitue un envoi recommandé.

Le législateur luxembourgeois a documenté sa loi, en phase de projet, par quelques commentaires reproduits ci-dessous *in extenso* :

Le recommandé déposé électroniquement offre à l'instar de celui déposé matériellement la possibilité pour l'expéditeur d'un message signé numériquement de se constituer une preuve de l'envoi, de la date et, le cas échéant, de la réception de ce message.

Dans le contexte des échanges électroniques de données, effectués en temps réel, il est nécessaire de prévoir, en outre, une certification de temps.

Preuve de l'envoi : l'intérêt qu'offre le recommandé est celui pour l'expéditeur de se ménager une preuve de son envoi. Cette preuve pourra être réalisée, pour le recommandé électronique grâce au récépissé électronique qui lui sera remis lors du dépôt électronique.

Preuve de la date et de l'heure de l'envoi : la loi impose, dans certains cas, un délai pour l'envoi d'une lettre ou d'un document. Tout comme pour la preuve de l'envoi, le recommandé offre à l'expéditeur la possibilité de se ménager la preuve que les délais ont été respectés.

Preuve de la réception : grâce au recommandé avec accusé de réception, l'expéditeur peut prouver que le destinataire a reçu l'envoi et a été en mesure d'en prendre connaissance.

L'expéditeur du document est responsable des moyens techniques à mettre en œuvre pour garantir efficacement le contenu du message contre les risques d'atteinte à l'intégrité et à la confidentialité de celui-ci.

La signature digitale permet de garantir le message contre les risques d'atteinte à son intégrité. Puisque cette fonction revêt une importance capitale dans le contexte électronique, il était nécessaire de faire de la signature digitale une condition de l'envoi recommandé. C'est la raison pour laquelle, cette disposition relative au recommandé électronique trouve sa place dans la présente loi.

On trouve ici un premier texte qui fait référence pour le recommandé électronique. Avec des termes qui ne sont pas forcément appropriés, les moyens techniques à mettre en œuvre réunissent ceux de la signature électronique et de l'horodatage.

3.2. L'horodatage de l'échange électronique dans le domaine administratif

3.2.1. Le droit administratif et l'horodatage des téléprocédures

L'horodatage dans l'acheminement des téléprocédures vers le centre de regroupement ou de traitement de l'administration devient primordial puisque l'acheminement doit respecter une date butoir ou être effectué dans un certain délai. Le principe de sécuriser les télédéclarations empruntant une voie télématique était présent dès la loi Madelin. La loi n° 94-126 du 11 février 1994¹³ parle en effet dans son article 4 d'un contrat entre télédéclarant et administration :

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.

Un autre alinéa de la loi Madelin rappelle le principe selon lequel "la date du cachet de la poste fait foi". La question posée dans les téléprocédures est celle de la transposition de ce

¹³ Loi n° 94-126 du 11 février 1994 relative à l'initiative et à l'entreprise individuelle.

principe du monde postal au monde électronique. Un premier essai de transposition a eu lieu dans le document préparé en son temps avec le cabinet du Ministre Madelin :

Clauses modèles pour la transmission par voie électronique de la déclaration de ... en application de l'article 4 de la Loi n 94-126 du 11 février 1994 .../...

E- Date et heure de la déclaration

*E1. Conformément à l'article 4-II de la loi n 94-126 du 11 février 1994 relative à l'initiative et à l'entreprise individuelle, les parties conviennent expressément que la date et l'heure de la déclaration correspondent **au moment où la transmission par voie électronique de la déclaration sous le format prévu devient irréversible.***

La date et l'heure de la télédéclaration sont bien prévues. Elles doivent se concilier avec la date administrative comme on le verra ci-dessous.

S'il est couramment admis que le cachet de la poste permet d'établir la date d'envoi, certains services publics¹⁴ retenaient, jusqu'à la loi du 12 avril 2000¹⁵ la date de réception alors que d'autres¹⁶ prenaient en compte la date d'expédition. De plus, les textes qui imposent une date limite pour effectuer une déclaration ou produire un document ne précisent pas toujours s'ils intègrent ou non les délais d'acheminement des correspondances (dépôt des dossiers d'inscription à l'université, par exemple).

La loi du 12 avril 2000 a unifié les règles de preuve en matière de certification de date ou de délai. Dans son article 16, la loi précise que :

Toute personne tenue de respecter une date limite ou un délai pour présenter une demande, déposer une déclaration, exécuter un paiement ou produire un document auprès d'une autorité administrative peut satisfaire à cette obligation au plus tard à la date prescrite au moyen d'un envoi postal, le cachet de la poste faisant foi, ou d'un procédé télématique ou informatique homologué permettant de certifier la date d'envoi. [...] Les modalités d'application du présent article sont fixées par décret en Conseil d'Etat.

La loi généralise la règle selon laquelle la date limite d'exigibilité correspond à la date d'envoi certifiée par le cachet de la poste. Cette règle est étendue à toutes les formalités pour lesquelles les administrés sont tenus de respecter un certain délai¹⁷. L'administré dispose donc jusqu'au dernier jour du délai imparti pour envoyer une demande ou satisfaire à une obligation, le cachet de la poste faisant foi. Cette même loi précise que l'envoi des documents par un procédé télématique ou informatique homologué permettant de certifier la date d'envoi produit les mêmes effets que l'envoi par la poste. Un décret en Conseil d'Etat doit en fixer les modalités d'application. Ce texte n'a pas encore été adopté à ce jour.

14 Le code de la sécurité sociale pour les Unions de recouvrement de sécurité sociale et d'allocations familiales.

15 Article 16 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.

16 La circulaire n° 1388 du 13 juin 1954 du ministère de l'économie, des finances et du budget et la lettre de l'UNEDIC n° 92-117 du 31 décembre 1992.

17 Toutefois ces dispositions ne sont applicables ni aux procédures régies par le Code des marchés publics ni à celles pour lesquelles la présence personnelle du demandeur est exigée en application d'une disposition particulière, ni à celles relevant des articles 1411 et s. du Code général des collectivités territoriales (article 16 de la loi n° 2000-321 modifié).

Pour l'application des téléprocédures, il ressort de ces deux lois que :

- il y a une corrélation forte entre la date d'envoi, le cachet de la poste faisant foi, et le procédé télématique ou informatique homologué certifiant la date d'envoi ;
- la date d'envoi se fixe au moment où l'entité n'a plus la maîtrise de son envoi : boîte aux lettres de la poste dans le 1^{er} cas, envoi au Fournisseur d'Accès à Internet (FAI) ou à un Partenaire EDI DGI (PED¹⁸) dans le 2^{ème} cas ;
- le décret d'application permettant de fixer les règles d'homologation du procédé télématique ou informatique n'a toujours pas été adopté, et qu'en son absence, les destinataires publics et parapublics font chacun leur meilleure interprétation.

Dans le cadre de la mise en œuvre des téléprocédures, la certification de la date d'envoi par un procédé fiable est essentielle pour assurer la confiance, les usagers devant acquérir la certitude que leurs informations ont bien été acheminées dans les conditions prévues. Pour ce faire, l'administration, dans la plupart des cas, assure, après réception de l'envoi, un retour d'informations vers l'utilisateur par un simple avis de remise, par un accusé de réception¹⁹ ou par l'envoi d'une information sur le résultat du traitement effectué suite aux informations transmises.

En définitive, prenant acte du développement des échanges électroniques, les textes juridiques tentent d'adapter le besoin d'horodatage en recourant à des périphrases diverses comme :

- *la détermination certaine de la date de leur réception*, de l'article 56 du Code des marchés publics relatif aux candidatures²⁰ ;
- *un procédé télématique ou informatique homologué permettant de certifier la date d'envoi*, de l'article 16 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations ;
- *un procédé fiable [...] de datation*, du décret n° 2000-489 du 29 mai 2000 à propos de la publicité foncière ;
- *la date et l'heure de réception de la déclaration (heure de Paris)*, de l'arrêté du 22 mars 2002 portant création par la Direction Générale des Impôts d'un traitement automatisé d'informations nominatives permettant la transmission, par voie électronique, des éléments déclaratifs en matière d'impôt sur les revenus et portant conventions types relatives à ces opérations.

3.2.2. L'aménagement de la date administrative dans les téléprocédures

Le développement des nouvelles technologies a amené l'administration à assouplir dans les téléprocédures²¹ les règles relatives à la date administrative dans les déclarations papier (cf. paragraphe 1.2.3.). On prendra ici l'exemple de l'EDI-TDFC²².

18 PED : Partenaire EDI DGI. Entité (SSII, profession libérale, entreprise, etc.) ayant fait l'objet d'un agrément de la part de la DGI pour être autorisée à émettre vers elle.

19 D'ailleurs, en ce qui concerne l'accusé de réception pour les demandes des administrés, l'article 19 de la loi du 12 avril 2000 prévoit qu'il s'agit là d'une obligation pour l'administration sous réserve des exceptions visées. Le décret prévu par cette disposition a été adopté le 6 juin 2001 : décret n° 2001-492 du 6 juin 2001 pris pour l'application du chapitre II du titre II de la loi n° 2000-321 du 12 avril 2000 et relatif aux accusés de réception des demandes présentées aux autorités administratives, J.O. du 10 juin 2001, p. 9246.

20 Le décret n° 2002-692 du 30 avril 2002 pris en application du 1^{er} et du 2^{ème} de l'article 56 du Code des marchés publics et relatif à la dématérialisation des procédures de passation des marchés publics fixe les conditions de communication par voie électronique des candidatures et offres en la matière.

21 Voir BOI 13 K-8-00 N° 132 du 18 juillet 2000.

22 EDI-TDFC : Transfert de Données Fiscales et Comptables par EDI (Echange de Données Informatisé).

Un délai supplémentaire de 15 jours, accordé à titre de tolérance aux adhérents de la téléprocédure de déclaration des résultats EDI-TDFC au-delà de la date limite fixée pour le dépôt des formulaires papier²³ de déclarations de résultat, est reconduit.

Pour les documents déposés dans les délais requis et rejetés par la Direction Générale des Impôts (DGI) pour un motif d'ordre technique, les contribuables disposent d'un délai supplémentaire de 15 jours pour effectuer le dépôt du fichier corrigé. A titre de tolérance, aucune amende ou pénalité ne sera appliquée si la régularisation intervient avant l'expiration de ce délai.

Il n'est pas prévu de délai supplémentaire pour les télédéclarations et les télépaiements²⁴ de TVA.

3.2.3. L'application concrète des principes dans la téléprocédure EDI-TDFC

Afin d'observer la mise en application pratique des principes définis dans l'horodatage des téléprocédures, on continuera avec l'exemple des TDFC.

Des différentes législations ci-dessus rappelées, il ressort que la DGI a fixé une règle arbitraire qui peut être lourdement préjudiciable à l'entité déclarante. En cas de contentieux, la règle qui s'applique est la suivante : *lorsqu'un contentieux porte sur la date de dépôt, la date figurant sur les documents papier restitués par le CRI (Centre Régional des Impôts) fait foi.*

Pour en connaître les répercussions, il convient de rappeler le scénario utilisé par une entité déclarante dont les étapes sont les suivantes :

Etape	Opérations effectuées	Dates et observations
1	Envoi de la télédéclaration à un PED si l'entité déclarante n'est pas elle-même PED ;	Date limite de dépôt TDFC = 15 juin 2001 par exemple à 23 heures
2	Vérification de la lisibilité du message par le PED (vérification de la syntaxe du message) ; rejet et retour à l'émetteur si absence de visibilité ; sinon routage du message vers le CSI de Strasbourg ;	Routage avant le 15 juin à 24 heures
3	Vérification de la lisibilité du message et contrôle 1 ^{er} niveau de vraisemblance réalisés dans un délai de 48 heures ; si erreur syntaxique, envoi d'un message Contrôle (CONTRL) ; si erreur de cohérence, envoi d'un message Contrôle (INFENT CR) ; ces messages sont envoyés au PED ;	Date maximum d'information du partenaire EDI = 19 juin (16 et 17 jours fériés)
4	Si retour d'un message CONTRL, un délai supplémentaire est accordé pour procéder à la régularisation d'un envoi ayant fait l'objet d'un rejet technique ; dans cette hypothèse, aucune amende ou pénalité relatives au respect des dates de dépôt n'est appliquée lorsque survient, avant l'expiration de ce délai, l'acceptation des données EDI-TDFC ou un dépôt papier au centre des impôts ; retraitement du message par le PED dans un délai de 15 jours ;	Date limite de dépôt TDFC suite à rejet technique = 1 ^{er} juillet (30 juin férié)
5	Réexpédition de la télédéclaration au CSI de Strasbourg ;	A réexpédier avant le 1 ^{er} juillet par exemple à 23 heures
6	Vérification de la lisibilité du message par le PED (vérification de la syntaxe du message) ; rejet et retour à l'émetteur si absence de visibilité ; sinon routage du message vers le destinataire (final) ;	Routage avant le 1 ^{er} juillet à 24 heures

23 Il s'agit soit de la date légale de dépôt telle qu'elle est précisée dans le Code général des impôts, soit de la date fixée annuellement par décision ministérielle, en l'espèce le 3 mai pour l'année 2000.

24 Il faut entendre par télépaiement, le télé règlement option A prévu dans le scénario EDI-TVA. Le virement n'est pas considéré comme un télépaiement.

7	Vérification de la lisibilité du message et contrôle 1 ^{er} niveau de vraisemblance réalisés dans un délai de 48 heures ; si erreur syntaxique, envoi d'un message Contrôle (CONTRL) ; si erreur de cohérence, envoi d'un message Contrôle (INFENT CR) ; ces messages sont envoyés au PED ;	S'il subsiste de nouvelles erreurs, étapes 3 et 4 (et 5) à réaliser dans le laps de temps restant jusqu'au 1 ^{er} juillet
8	Contrôle 2 ^{ème} niveau de vraisemblance réalisé dans un délai de 45 jours maximum par envoi d'un accusé de réception papier ;	L'accusé de réception est envoyé à l'entité déclarante avant le 16 juillet à minuit (15 juillet férié)
9	Appréciation du respect de la date de dépôt par l'inspecteur chargé du dossier au Centre des Impôts de l'entité déclarante.	

Il ressort de cette succession d'étapes les informations suivantes :

- l'entité déclarante PED n'est plus maître de ses déclarations après les étapes 1 correspondant au "primo" envoi, et au 4, au 2^{ème} envoi ;
- l'entité déclarante PED n'est pas maître des délais de traitement du CSI de Strasbourg (étapes 2 à 4, puis 6 à 8) ; de ce fait, tout retard du côté de l'administration le pénalise ;
- l'entité déclarante n'a pas connaissance de la date figurant sur les documents papier restitués par le CRI.

Il convient de prendre note que le partenaire EDI intermédiaire et indépendant de l'entité déclarante se comporte comme La Poste pour le courrier papier. Sous réserve de l'appréciation par la DGI des niveaux de sécurité mis en œuvre, l'envoi immédiat d'un accusé de réception horodaté par un tiers horodateur indépendant, et signé, pourrait remplir les conditions exigées pour être agréé par la DGI. Dans ces conditions, rien n'interdirait de considérer la date de réception par le partenaire EDI intermédiaire comme la date limite de dépôt TDFC.

En outre, sans précision de l'opérateur, l'horodatage semble être déterminé par l'horloge interne du système informatique.

Pour la protection de l'entité déclarante, la loi n° 2000-321 du 12 avril 2000 devrait être considérée dans l'esprit du législateur, à savoir que la date doit pouvoir être connue par l'émetteur initial et être fixée indépendamment de l'émetteur et du récepteur par un dispositif fiable et sécurisé.

3.2.4. L'application concrète des principes dans la téléprocédure DUCS-EDI

3.2.4.1. ACOSS

La lettre circulaire n° 2000-110 de l'ACOSS du 29 décembre 2000, l'agence centrale des organismes de Sécurité sociale, précise son interprétation de l'article 16 de la loi du 12 avril 2000 dans les termes suivants :

- Les **déclarations dématérialisées**, réalisées par EDI, Internet ou Minitel peuvent être transmises par les cotisants jusqu'à la date limite de l'exigibilité 12 h. Dans l'attente de précisions relatives à la procédure d'homologation permettant la certification de la date d'un envoi dématérialisé, le cotisant recevra, après chaque opération déclarative, un numéro de certificat valant accusé de réception. Ce document devra être conservé par le déclarant.
- Il convient de souligner que les **ordres de virement et les autorisations de paiement, par prélèvement ou télé règlement**, qui donnent seulement un mandat de transférer des

fonds, ne peuvent être assimilés à l'exécution d'un paiement, cette opération intervenant ultérieurement.

En cas de paiement par virement, pour vérifier le respect de la date de paiement, sera prise en considération la date de règlement interbancaire mentionnée par la banque, ou la date d'opération sur le compte spécial d'encaissement de l'organisme de recouvrement en cas d'absence d'échange interbancaire (transfert de compte à compte au sein d'une même banque ou virement postal).

Ainsi, le règlement interbancaire, ou la date d'opération sur le compte spécial d'encaissement de l'organisme de recouvrement, doit intervenir au plus tard à la date limite d'exigibilité.

En cas de paiement par prélèvement, la présentation en compensation caractérisant l'exécution du paiement doit intervenir à la date limite d'exigibilité.

En cas de paiement par télépaiement, il sera cependant toléré que l'accord de paiement puisse être transmis par le débiteur jusqu'à la date limite d'exigibilité 12 h, la présentation en compensation intervenant dans ce cas, compte tenu du délai technique, le jour suivant ouvré. Il ressort de ces décisions provisoires que seule la date de réception attribuée par les centres de traitement informatique des URSSAF est prise en compte et confirmée à l'émetteur physique. L'entreprise n'est donc pas protégée contre des interruptions de traitement volontaires ou non. En outre, sans précision de l'opérateur, l'horodatage semble être déterminé par l'horloge interne du système informatique.

3.2.4.2. UNEDIC – AGIRC – ARRCO

L'UNEDIC et les Caisses de Retraite regroupées au sein de l'AGIRC et de l'ARRCO n'ont pas encore pris de position sur l'application de l'article 16 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.

Deux cas ont été étudiés :

- A. l'entité fait appel à un tiers archiveur,
- B. l'entité développe un service d'archivage en interne et fait appel à un tiers archiveur pour sécuriser ses fichiers.

Quelle que soit la solution retenue, il convient de prendre les mesures nécessaires pour que l'archivage interne, tout comme l'archivage chez un tiers archiveur, se présente comme *sécurisé*²⁶.

4.2. L'hypothèse : l'archivage interne sécurisé

Le cas A exposé ci-dessus semble logique au niveau théorique. Le tiers archiveur intervient dans un processus d'échanges électroniques qui se poursuit vers lui, après que le processus d'utilisation des messages électroniques ait été purgé. L'inconvénient est cependant qu'il équivaut à transférer par voie de télécommunications un volume important de données. Un tel transfert est générateur de risques techniques et de coûts non négligeables. D'où la tentation de procéder à un archivage en interne devant rester valide en faisant appel, par exemple, à un horodatage externe. Une fois encore, l'utilisateur peut avoir recours à un témoin sur lequel il n'a pas de prise directe : un tiers horodateur.

²⁶ Le précédent technique et juridique de la signature permet de définir la *sécurisation* comme étant la caractéristique d'une chose ou d'une procédure présentant des garanties de sécurité, telles que (selon les cas) l'identification, l'authentification, l'intégrité, la non répudiation, la confidentialité, la mise en œuvre de ces garanties étant favorisée ou fournie par un tiers de confiance spécifique. Actuellement, on peut rencontrer une signature électronique sécurisée (décret d'application de l'article 1316-4 du Code Civil), un archivage sécurisé (décret par les *Recommandations*) et un horodatage sécurisé qui est l'aboutissement de la présente étude.

4.2.1. L'opération d'archivage

Lorsque les archives sont chez l'utilisateur final, émetteur ou destinataire des éléments électroniques archivés, le risque existe que, volontairement ou involontairement, les éléments archivés soient modifiés, corrigés, altérés ou détruits. Au moment de l'archivage, les messages électroniques et autres éléments ont bouclé leur cycle de vie normal. Ils sont dans un état final qui peut être constaté comme un "instantané" de leur contenu. De là, on voit apparaître la notion de temps. Le cycle de vie des messages est terminé à un moment déterminé ; tout changement de contenu qui surviendrait après le moment *m* de leur fin de cycle n'est que manipulation des archives.

L'idée consiste dans ce cas à faire reconnaître l'*instantanéité* des messages par un tiers objectif qui dans ce cas est ... un *tiers horodateur*. Selon les spécifications du *Time Stamping Profile* de l'EESSI²⁷, le mode opératoire est le suivant :

- l'utilisateur final crée un *condensé* de l'état actualisé du message électronique par une fonction de hachage ;
- il l'expédie via une requête électronique normalisée au tiers horodateur ;
- ce dernier constate le moment de l'arrivée de la requête ;
- et renvoie un message signé contenant entre autres, le jeton d'horodatage et le certificat électronique de l'autorité d'horodatage,
- le jeton d'horodatage et le certificat sont archivés en l'état.

4.2.2. La restauration des données et la vérification du certificat

Si l'archivage a été réalisé en interne, la restauration des données sera plus facilement réalisée. L'utilisateur devra alors vérifier par lui-même si les archives sont bien dans l'état primitif. Cette vérification pourra procéder par degré, toujours par rapport à un étalon qui est le certificat d'horodatage :

- au degré 0, les fichiers chronologiques de son système d'information démontreront que les archives et le certificat sont de la même génération ;
- au premier degré, comme le certificat d'horodatage inclut un condensé du texte des archives, il est possible de relancer l'algorithme de hachage pour produire un condensé des éléments désactivés ;
- au second degré, on pourra se tourner vers le tiers horodateur pour comparer le certificat de l'entreprise et celui qu'il a émis.

Ce cas d'école montre simplement que l'horodatage n'est ni éloigné de l'archivage ni sans lien avec celui-ci. En l'occurrence, la phase d'archivage du message électronique (une des étapes de son cycle de vie) fait intervenir un tiers horodateur. La conclusion à en tirer est que l'effet recherché sur un aspect précis de la sécurisation n'est pas toujours fourni par le tiers de confiance de même mission.

27 EESSI : European Electronic Signature Standardization Initiative, organisme lancé sous les auspices de l'ICTSB (European industry and standardization bodies), dont l'objectif est d'analyser les besoins futurs des activités de standardisation pour appuyer la Directive Européenne sur la signature électronique.

DEUXIEME PARTIE : VERS L'HORODATAGE SECURISE

La question de l'horodatage qui constitue un élément contextuel de la signature électronique n'a pas été oubliée dans les réalisations du marché. Les moyens proposés pour prendre en charge cet élément sont divers. On pourra ainsi trouver des dispositifs matériels dédiés de type *dongle*, comme le périphérique spécialisé appelé *iButton* (www.ibutton.com).

Mais dans la perspective de la signature électronique qui met en œuvre une prestation de certification, la préférence pourrait aller vers une prestation spécialisée d'horodatage certifiée (voir ci-dessous, le paragraphe 2). Toutefois comme les protocoles sont récents et que le marché ne montre pas encore une offre très développée, on peut se tourner provisoirement vers un système de traçabilité du temps organisé et validé par une construction juridique (voir ci-dessous, le paragraphe 1).

Plan de la deuxième partie :

1. L'horodatage organisé par contrat
2. L'horodatage sécurisé

1. L'HORODATAGE ORGANISE PAR CONTRAT

1.1. La solution contractuelle

Comme le démontre la première partie, le droit ne fournit pas en l'état actuel de règle générale et universelle qui permettrait de disposer, par analogie au *procédé fiable d'identification* de la signature électronique, d'un *procédé fiable d'horodatage* pour les échanges électroniques.

A défaut de loi, les parties aux échanges électroniques peuvent se tourner vers le contrat. Ce qui semble quasi-impossible pour les particuliers, mais plus facile pour les entreprises surtout si, comme on le dit en EDI, elles sont en relations d'affaires continues. Dans les échanges B to A, l'article 4 de la loi Madelin garde tout son intérêt en proposant également le système contractuel ou conventionnel.

Dans les échanges de type EDI, même s'ils empruntent aujourd'hui la voie de l'Internet et la syntaxe XML, les traditionnels accords d'interchange peuvent être adaptés pour l'horodatage. Même si la question est traitée rapidement et sous le seul angle du *retard*, l'accord²⁸ type européen pour l'EDI le place dans les garanties de sécurité à appliquer.

"Article 6 - Sécurité des messages EDI

6.1. Les parties s'engagent à mettre en œuvre et à maintenir des procédures et des mesures de sécurité afin d'assurer la protection des messages EDI contre les risques d'accès non autorisé, de modification, de retard, de destruction ou de perte."

En application de l'article 1316-2 du Code civil, les parties peuvent aussi aménager la preuve de la datation de leurs échanges.

Une autre façon de procéder aux échanges électroniques sur Internet est de transiter vers un site concentrateur pour les téléprocédures ou un *portail* spécialisé. Un portail peut mettre en œuvre une garantie contractuelle pour l'horodatage. Nous nous arrêterons à l'exemple du portail télédéclaratif de l'Ordre des experts-comptables selon lequel le procédé d'horodatage fiable doit bénéficier au télédéclarant, mais sous le contrôle de l'administration.

1.2. Illustration de la solution contractuelle : le portail jedeclare.com

Le principe accepté par les deux parties, le CS-OEC et la DGI, est un ensemble de 7 points de mesures d'horodatage dans la chaîne de traitement technique des télédéclarations dans le back-office du portail.

Afin de tenter d'optimiser le portail télédéclaratif de l'Ordre en matière de sécurité, certaines contraintes ont été respectées. Ce sont les suivantes :

²⁸ Clause contractuelle extraite de la "Recommandation de la Commission du 19 octobre 1994 concernant les aspects juridiques de l'Echange de Données Informatisées", 94/820/CE.

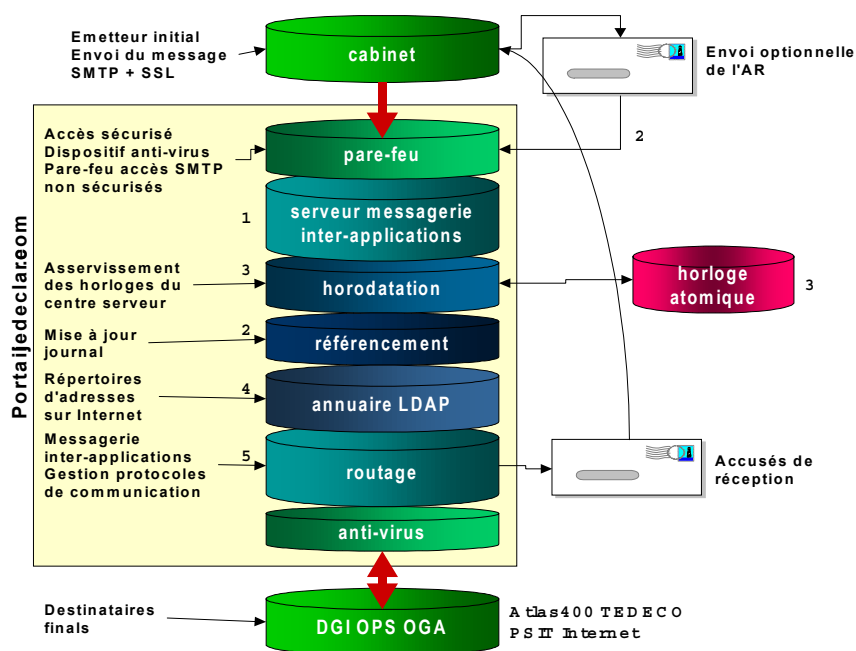
- Les étapes 1²⁹ et 2 n'ont pas été séparées pour éviter l'incertitude sur la date de dépôt réel du message initial. Le portail référence sans délai chaque télédéclaration reçue par messagerie ;
- L'heure de référence du portail (3) est asservie à une source de temps fiable afin de garantir les différentes dates stockées par la base de référence ;
- L'ensemble des dates référant le dépôt et l'acheminement d'une télédéclaration sera accessible en HTML à partir du portail. Le format primaire de la date est jj/mm/aaaa hh:mm. Pour des besoins d'affichage ou de traitement, ce format peut évoluer ;
- Le fichier de référence du portail (4) repose sur un annuaire LDAP³⁰ dont le schéma aura été étendu pour les besoins propres au CS-OEC (adresse destinataire, moyen de communication, option de retour par courriel des AR, etc.) ;
- Les messages à destination de correspondants Internet seront horodatés de manière identique à celle des messages pour les destinataires non Internet. Ainsi, ces messages seront envoyés à l'adresse générique 'quelqu_un@declare.com', l'analyse fonctionnelle prévue dans le cahier des charges établira les règles de transmission des adresses physiques réelles de destination (objet, corps de texte, PJ, etc.) ;
- Les fonctions de groupage/dégroupage de messages en provenance d'expéditeurs différents seront assurés par un processus EDI spécialisé (5) . Un mécanisme de notification inter-applications permet la notification du processus d'horodatage et la corrélation individuelle des messages en retour ;
- Les messages en retour des destinataires 'Internet' et 'non Internet' pouvant être de format très différent, un serveur d'intermédiation permet leur transformation dans un format pivot XML et une notification homogène des processus EDI et d'horodatage afin d'assurer leur rapprochement et leur éventuel envoi vers les expéditeurs initiaux (2) ;
- Dans le cadre d'un envoi en multi-distribution, le message est horodaté globalement dans un premier temps, puis la référence de ce message est transmise au processus EDI qui est chargé de l'extraction individuelle des destinataires et la notification en retour du processus d'horodatage (5).

Sécurisation : L'envoi des télédéclarations via messages SMTP est sécurisé par la mise en place de la couche *Secure Socket Layer* (SSL) assurant l'authentification et le cryptage des échanges. Seule, une réception sécurisée SMTP + SSL³¹ est acceptée par le portail déclaratif afin d'éviter toute intrusion ou malveillance.

29 Les numéros du texte renvoient à ceux du schéma.

30 Lightweight Directory Access Protocol

31 **Pour information** : Le protocole SSL, développé par Netscape et distribué gratuitement, sert à l'authentification et l'encryptage des données sur un réseau TCP/IP. Ce protocole mélange des chiffrements à clé publique et à clé privée. Chaque session sécurisée débute par un échange de données en cryptographie asymétrique, le temps d'échanger une clé privée en toute sécurité, et se poursuit en cryptographie symétrique (nettement plus rapide). Les spécifications de la version 3.0 de SSL ont été publiées en mars 1996.



Tous les services formant le portail déclaratif sont des objets de type COM+. Les écritures dans les bases de données, annuaires et les échanges inter-applications sont rendus transactionnels, ce qui permet d'annuler toutes écritures ou processus si une partie des traitements ne s'est pas correctement déroulée. Afin de garantir le maximum de performances, les services seront écrits en langage C/C++. Le moniteur transactionnel intégré à l'architecture COM+ garantit également la montée en charge et l'absorption des pics de trafic en mutualisant les connexions aux bases de données ou en chargeant en mémoire les objets COM+ en fonction des connexions utilisateurs.

Envoi simple et multiple : Les principes techniques et fonctionnels retenus pour l'architecture du portail déclaratif permettent la mise en œuvre d'un processus homogène entre le traitement des envois simples et celui des envois multiples. Il traite également les contraintes de groupage/dégroupage vis-à-vis des destinataires qu'ils soient Internet ou non. Le module d'interprétation et de traitement des télédéclarations (inclus dans l'étape 5) est également chargé de notifier en retour le service d'horodatage en cas de groupage et d'envoi multiple afin de permettre une référence individuelle des messages de télédéclaration. Une référence unique fournie au module par le système d'horodatage permet le rapprochement des informations délivrées en retour.

Messages en retour : Les convertisseurs sont construits en fonction des formats et des protocoles définis par les destinataires pour leurs messages en retour. Le serveur d'intermédiation se charge de router les messages sur le bon convertisseur en fonction de l'émetteur. Chacun des convertisseurs fournit à la messagerie inter-applicative un fichier XML pivot qui est ensuite traité par le service d'horodatage à des fins de rapprochement et/ou par le module.

2. L'HORODATAGE SECURISE

Un horodatage dit sécurisé fait intervenir un tiers de confiance spécialisé, le tiers horodateur, mettant en œuvre une certification électronique appropriée.

2.1. L'horodatage certifié

2.1.1. La finalité de l'horodatage certifié

Dans le monde des échanges électroniques, la fonction d'horodatage est entendue comme associant un message électronique à un instant déterminé. Cette fonction peut avoir diverses utilités comme :

- dater un message au moment de sa création ou de son émission ;
- certifier le moment de la soumission d'un message quand une date limite est requise ;
- établir la datation des transactions internes informatiques pour leur enregistrement dans un fichier de journalisation ;
- arbitrer plusieurs temps locaux ou internes issus des systèmes informatiques des utilisateurs ou des vecteurs de télécommunications lorsqu'ils n'ont pas tous la même fiabilité, etc.

L'horodatage à lui seul n'est pas une fin en soi. Il est généralement associé à des besoins de non-répudiation. On trouvera ce besoin pour la propriété intellectuelle où il est important de démontrer l'existence et la possession d'un document (musique, brevet, idée, etc.) ou de prouver son antériorité.

Le besoin est également essentiel en terme de signature électronique sécurisée dans son plein sens du terme (cf. Décret n°2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du Code Civil et relatif à la signature électronique³²) où il est nécessaire de savoir à quel moment la signature a été effectuée. Nous conseillons à ce titre au lecteur de consulter le document *ETSI TS 101 733 V1.3.1. (2002-02) Electronic Signature Formats* qui décrit comment utiliser conjointement la signature et l'horodatage pour assurer la pérennité dans le temps d'une signature électronique.

L'horodatage sera le plus souvent associé à des services qui relèvent du dépôt de confiance de la *notarisation*³³ ou de l'archivage sécurisé. Il peut également être utilisé lorsque le besoin se fait sentir de démontrer une action à des tiers comme l'envoi ou la remise d'un document avant une date donnée. Dans ce cas, il peut être important de séparer les services d'horodatage internes à une organisation qui horodate elle-même ses transactions ou actions d'un service d'horodatage et ceux réalisés par une tierce partie d'horodatage, organisme indépendant des parties qui attestera avoir eu connaissance d'une transaction ou action à une date donnée.

L'horodatage concourt au renforcement de la traçabilité des opérations.

32 JO du 31 mars 2001 p. 5070

33 Ce terme est employé par abus de langage, la notarisation relevant uniquement d'un officier public.

2.1.2. Le serveur d'horodatage

Dans le système technique de distribution du temps (cf. 1.2.1.), les niveaux distribution et application sont en partie normalisés ou en cours de normalisation. Ils s'appuient sur des communications fiables (la transmission de la date et de l'heure est juste), et parfois signées, entre les sources de temps et les demandeurs.

Au niveau de la source de temps, les serveurs de temps utilisent par exemple :

- Le GPS (*Global Positioning System*) : c'est un total de 24 satellites (précision 1 μ s) réparti par groupe de 4 satellites sur 6 orbites planes.
- Les horloges atomiques, en direct ou au travers d'une réception FM. Au niveau de la distribution dans les réseaux sont utilisés les protocoles comme NTP et sa version sécurisée STIME. Ils permettent la distribution du temps sur Internet et l'utilisation de plusieurs sources de temps.

Au niveau des logiciels de serveur de temps, les systèmes d'exploitation du marché (Windows, Linux, Unix, MacOS 10) intègrent un serveur de temps supportant le protocole NTP. Des sociétés privées vendent des dispositifs de serveurs de temps, ou des services de temps fiable. Parmi ceux-ci, on peut citer à titre d'exemple les sociétés Datum (www.datum.com), CertifiedTime, TimeCertain, TrueTime. Ces dispositifs peuvent être appelés serveurs de temps fiable.

Il est également possible de bénéficier de serveurs de temps publics sur Internet, voir www.ntp.org.

2.1.3. Horodatage et certification

2.1.3.1. L'autorité d'horodatage

L'horodatage certifié est spécifié dans le protocole développé par l'IETF, organisme normalisateur du monde Internet, dans le document de référence *Internet X.509 Public Key Infrastructure (PKI) Time Stamp Protocol (TSP)* d'août 2001 (RFC 3161).

La fonction d'horodatage, le Time Stamping, est mise en œuvre par un tiers certificateur spécifique qui peut fournir la preuve de l'existence d'un message à un instant déterminé : le *tiers horodateur*, en anglais *Time Stamping Authority (TSA)*³⁴. Le tiers horodateur est neutre vis-à-vis des opérations techniques. Il ne procède à aucun contrôle sur le contenu du message à horodater. Il ne vérifie pas si la qualité des personnes leur permet ou non de demander un horodatage. Le tiers horodateur reçoit une requête contenant, entre autres, l'empreinte des données à horodater et éventuellement la référence à la politique d'horodatage sous laquelle le demandeur souhaite obtenir son jeton.

2.1.3.2. Le jeton d'horodatage

Le tiers horodateur construit une réponse contenant les données de la requête et en particulier l'empreinte, et y rajoute une marque de temps ainsi que des données additionnelles dont

34 ETSI TS 102 023 V1.1.1 (2002-04) Policy requirements for time-stamping authorities.

l'identité du tiers horodateur et la politique sous laquelle il a produit le jeton. Le jeton est contenu dans la réponse sous la forme d'une structure *CMS* (*Cryptographic Message Syntax*) signée. Le jeton d'horodatage permet de fournir la preuve d'existence de données à un instant dans le temps. Le but est de faire le lien entre une chaîne de caractères et une marque de temps :

- la chaîne de caractères : c'est l'empreinte numérique (20 ou 16 octets) d'une chaîne quelconque de données obtenue par une fonction de hachage (SHA-1, MD5, RIPEMD-160) ;
- La marque de temps : c'est la valeur de temps obtenue d'un serveur de temps fiable, sous la forme YYYYMMDDhhmmss. (La norme permet d'introduire des fractions de seconde si nécessaire) ;
- La référence du temps : il est basé sur l'U.T.C. qui est le temps donné par Greenwich.

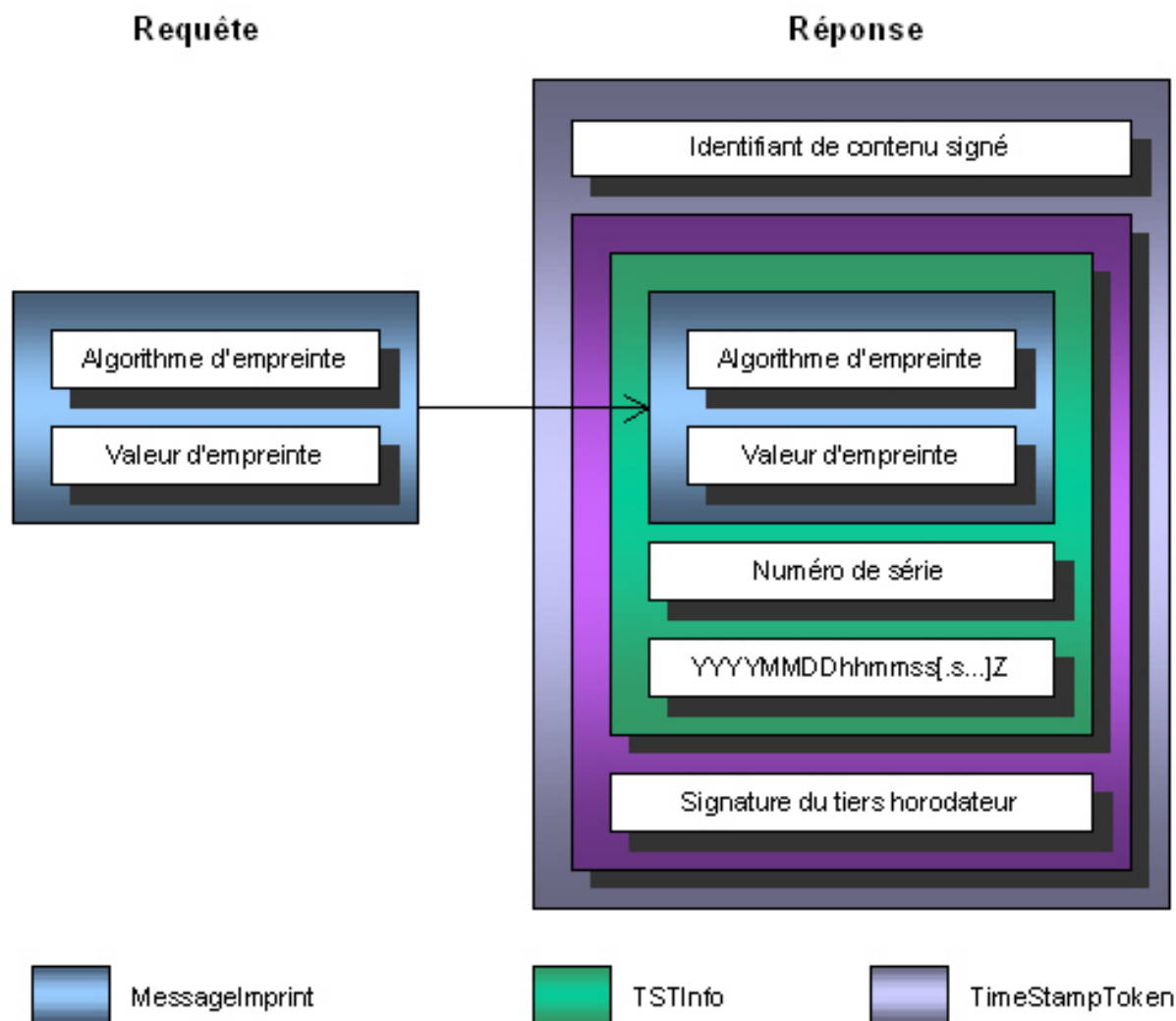
Appartenant au domaine de la certification électronique, la fonction d'horodatage met en œuvre un certificat électronique d'un type particulier, appelé "*jeton*", en anglais "*token*". Ainsi, la RFC 3161 (*Internet X509 Public Key Infrastructure Time Stamp Protocol* (TSP)), publiée par IETF définit un jeton d'horodatage comme suit :

```
TimeStampToken ::= ContentInfo
-- contentType est id-signedData ([CMS])
-- content est SignedData ([CMS])
```

Il doit encapsuler une information signée et être une valeur codée DER de TSTInfo.

```
TSTInfo ::= SEQUENCE {
    version          INTEGER { v1(1) },
    policy           TSAPolicyId,
    messageImprint  MessageImprint,
    -- DOIT avoir la même valeur que le champ similaire TimeStampReq
    serialNumber    INTEGER,
    genTime         GeneralizedTime,
    accuracy        Accuracy OPTIONAL,
    ordering        BOOLEAN   DEFAULT FALSE,
    nonce          INTEGER    OPTIONAL,
    -- DOIT être présent si un champ similaire était présent dans TimeStampReq. Dans ce
    cas, il DOIT avoir la même valeur.
    tsa             [0] GeneralName OPTIONAL,
    extensions      [1] IMPLICIT Extensions OPTIONAL
}
```

```
MessageImprint ::= SEQUENCE {
    hashAlgorithm    AlgorithmIdentifier,
    hashedMessage    OCTET STRING
}
```



Le jeton, présenté ci-dessus, intègre les informations suivantes (figure ci-dessus) :

- la politique d'horodatage utilisée, le statut dans l'ICP, le nom du tiers horodateur et son numéro authentification, l'heure et diverses autres informations de service ;
- une donnée particulièrement significative dite *messageImprint*. C'est un résumé numérique du message à horodater effectuée par un algorithme de *hash coding* (semblable à ceux utilisés dans la signature électronique : SHA-1 et MD5). C'est cette donnée qui permet d'associer un instant donné à un message électronique ;
- un numéro de série qui doit être unique pour chaque jeton d'horodatage délivré par un tiers horodateur donné ;
- En outre, le jeton ne comporte qu'une signature, celle du tiers horodateur, ce qui permet au destinataire d'un jeton de l'authentifier en tant que tiers horodateur. A cet effet, le tiers horodateur utilise une clé de signature spécifiquement dédiée à cet usage, c'est-à-dire que le certificat de clé publique correspondant contient le champ d'extension '*Extended Key Usage*' marqué comme critique pour un usage d'horodatage.

La validité du moment certifié est naturellement celle du jeton, eu égard aux règles spécifiques du cycle de vie des certificats. L'idée principale est que l'horodatage permet d'indiquer d'une façon certaine le moment limite avant lequel le message électronique a été créé. Dit

d'une autre façon, par rapport à la *date certifiée*, le message a été généré auparavant, mais pas après.

Comme pour tous les services de certification, une politique, ici d'horodatage, est nécessaire. L'EESSI a défini la *politique d'horodatage* liée à la directive européenne signature électronique dans la norme ETSI TS 102 023 V1.1.1 (2002-04) : *Policy requirements for time-stamping authorities*.

2.1.4. Scénarios d'horodatage envisagés

Le protocole TSP présenté ci-dessus définit implicitement le scénario d'horodatage normalisé suivant :

1. Une requête contenant un `MessageImprint` est envoyée au tiers horodateur. Celui-ci ne prend donc jamais connaissance du message original, eu égard à la propriété de non-réversibilité de l'empreinte numérique,
2. Le tiers horodateur, connecté à un serveur de temps, génère un `TSTInfo` qu'il signe pour former un jeton `TimeStampToken`,
3. Le jeton est transmis au demandeur qui doit s'assurer de la validité du certificat du tiers horodateur avant de procéder à l'acceptation du jeton.

Afin de vérifier la validité du jeton reçu, le demandeur doit en particulier :

- Contrôler la conformité de l'usage de clé du certificat du tiers horodateur
- Consulter une liste de révocation ou demander via OCSP (Online Certificate Status Protocol, RFC2560) le statut du certificat
- Vérifier la signature apposée sur le `TSTInfo`.

D'autres méthodes d'horodatage sont également envisageables³⁵ :

méthode 1 : *Originator Timestamp Receipt Protocol*,

méthode 2 : *Augmented Originator Timestamp Receipt Protocol*,

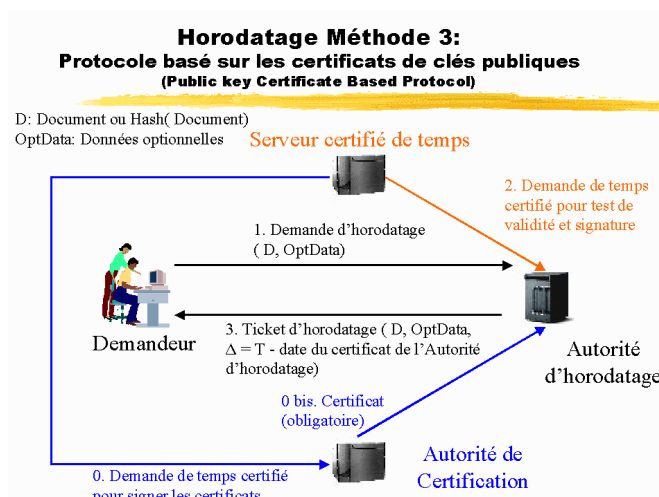
méthode 3 : *Public key Certificate Based Protocol*,

méthode 4 : *Time Based Signing Key Protocol*.

Les méthodes sont en général intéressantes, mais impliquent une confiance aveugle dans le serveur de temps certifié (*Certified Time Server*). Pour assurer une plus grande confiance, il faudrait que ce serveur de temps soit lui-même une autre autorité d'horodatage (*Time Stamping Authority*). Pour augmenter la sécurité du système, il serait peut-être opportun que les requêtes envoyées par le client (*Originator*) soient signées électroniquement pour en assurer l'intégrité et l'authenticité.

La méthode 3 se rapproche du commentaire exposé ci-dessus car elle n'implique pas que le client soit en relation avec le serveur de temps certifié. Elle est présentée ci-après à titre d'exemple.

³⁵ « *Methods for timestamping electronic documents using certificates and user-specified times* » Mohammad Peyravian, Stephen M. Matyas, Allen Roginsky and Nevenko Zunic (IBM Corp.) - Computers & security, Volume 20, N° 3



Quelques tiers horodateurs existent qui fournissent des services plus ou moins variables. Ils sont en général liés à d'autres services comme la protection intellectuelle ou l'archivage. Parmi ceux-ci, nous pouvons citer par exemple :

DigiStamp <http://www.e-timestamp.com>

Surety: <http://www.surety.com>

Timestamp: <http://www.timestamp.com>

En France, La Poste est en cours de préparation d'un service de preuves électroniques à la disposition des entreprises et des particuliers, reprenant dans un premier temps les fonctions liées aux preuves de dépôt et preuve de retrait (LRAR).

2.2. Le tiers horodateur

Dans ce paragraphe, on s'efforce de définir les principes réglementant une profession spécialisée de tiers horodateur.

2.2.1. Organisation de la profession de tiers horodateur

Certains principes seront applicables à chaque tiers horodateur, en tant qu'entité commerciale, d'autres trouveront à s'appliquer à l'ensemble de la nouvelle profession.

2.2.1.1. Au niveau du tiers horodateur

Rôle, fonctions et organisation

Le tiers horodateur a pour fonction de recevoir des requêtes d'horodatage concernant tous éléments électroniques envoyés par ses clients donneurs d'ordre, entreprises ou mandataires des entreprises et d'y répondre. Sa mission est définie par un contrat de prestation de services. Il assure notamment les fonctions suivantes :

- la réception et la gestion des éléments électroniques à horodater ;

- la tenue et la conservation d'une liste récapitulative ³⁶ des éléments électroniques reçus ou émis ;
- la liste récapitulative doit indiquer de façon claire et précise les anomalies éventuelles intervenues lors de chaque transmission ;
- la liste récapitulative doit mentionner de façon claire et précise les dates de destruction ou de restitution des éléments électroniques ;
- la liste doit pouvoir être éditée séquentiellement dans l'ordre d'arrivée ou d'émission des éléments électroniques.

Obligations

Le tiers horodateur doit respecter strictement le contrat, pour tout ce qui touche les flux d'informations avec ses donneurs d'ordre, et les objectifs de sécurité définis dans la politique d'horodatage. Le tiers horodateur remplit les obligations minimales suivantes :

- disposer d'une capacité suffisante pour assurer sans discontinuité la prise en charge des éléments électroniques arrivants ;
- mettre en place des normes minimales de sécurité ;
- définir des contrôles adaptés ;
- créer et mettre à jour la table de gestion des éléments électroniques ;
- conserver les demandes d'horodatage reçus et non seulement les mentions obligatoires de la liste récapitulative visées ci-dessus ;
- prendre toutes les dispositions pour assurer la sécurité de l'archivage des éléments électroniques qui ont été soumis à horodatage, et des jetons délivrés correspondants ;
- prendre toute disposition matérielle permettant d'assurer la continuité du service ;
- informer les donneurs d'ordre de la perte de la qualification de tiers horodateur ;
- restituer les éléments électroniques avant ou après horodatage sous une forme convenue contractuellement avec le donneur d'ordre ;
- accepter des audits de vérification des dispositions qu'il a prises pour garantir le service ;
- prendre une assurance couvrant les risques liés à l'exécution du service et pendant toute la durée de sa mission ;
- divulguer à l'ensemble de ses clients ainsi qu'aux destinataires les termes et conditions concernant l'utilisation de ces services (politique d'horodatage) ;
- assurer l'intégrité et la confidentialité de sa clé privée de signature durant tout son cycle de vie.

Le tiers horodateur n'est en aucun cas responsable du contenu des éléments électroniques à horodater transmis par le donneur d'ordre.

Responsabilités

36 La liste récapitulative peut être établie sur support informatique et doit être conservée pendant un certain délai de conservation et ce, même en cas de rupture de contrat quelle qu'en soit la raison ; cette liste doit comporter au moins les mentions suivantes :

- la date d'édition de la liste ;
- la version du logiciel utilisé ;
- la date de création et les références de l'élément électronique chez le donneur d'ordre ;
- la date et l'heure de réception ou d'émission de l'élément électronique ;
- la taille de l'élément électronique ;
- le propriétaire du fichier (donneur d'ordre, mandataire, etc.) ;
- un numéro de réception ;
- les identifiants de l'émetteur et du récepteur donnés par le système de télétransmission.

Le tiers horodateur est responsable :

- du respect de ses engagements contractuels vis-à-vis du donneur d'ordre ;
- de tout manquement à son obligation de confidentialité ;
- des préjudices causés au donneur d'ordre en cas d'inexécution du contrat par le tiers horodateur ;
- des préjudices causés par son personnel dans le cadre des prestations de service offertes et définies dans le contrat ;
- des préjudices subis par le donneur d'ordre et résultant de dysfonctionnement du matériel utilisé par le tiers horodateur ;
- de la précision et de l'intégrité des données qu'il délivre et manipule ;
- de l'information du donneur d'ordre de toute évolution technique pouvant modifier le mode d'échange et d'horodatage des éléments électroniques.

2.2.1.2. Au niveau général de la profession de tiers horodateur

Rôle, fonctions et organisation

L'ensemble des tiers horodateurs constitue un groupement de professionnels dont l'intérêt est de se rassembler et de respecter des règles communes, afin d'offrir aux donneurs d'ordre un service de confiance, et de garantir une interopérabilité entre ses membres.

Ce groupement doit :

- être structuré et disposer d'une instance représentative ;
- définir et appliquer une procédure de qualification des postulants au titre de tiers horodateurs ;
- prévoir une démarche de qualité du service en définissant les conditions de transfert et de sortie exceptionnelle de contrat ;
- établir un règlement intérieur de la structure interprofessionnelle mise en place et notamment, sa composition, sa gestion organisationnelle et financière, etc. ;
- définir une charte présentant l'éthique, les services et engagements minima que doivent respecter les tiers horodateurs membres du groupement et qui sera tenue à disposition de tout donneur d'ordre ;
- organiser le bon fonctionnement de la profession en attribuant des missions à d'autres tiers horodateurs du groupement en cas de carence, de cessation d'activité ou d'impossibilité de respecter les engagements contractuels par un tiers horodateur membre, après accord du donneur d'ordre ;
- élaborer un dispositif de contrôle de la qualité des prestations fournies par les tiers horodateurs, afin d'apprécier le respect de la charte ;
- former les professionnels et développer les compétences du groupement.

Responsabilités

Le groupement des tiers horodateurs ne peut être tenu responsable que des manquements à ses seules obligations. Le groupement des tiers horodateurs apporte des garanties au niveau collectif en souscrivant une assurance de groupe.

2.2.1.3. Au niveau du donneur d'ordre

Rôle, fonctions et organisation

Le donneur d'ordre a pour fonction d'envoyer au tiers horodateur les éléments électroniques à horodater.

Obligations

Le donneur d'ordre doit remplir les obligations suivantes :

- préparation et envoi des éléments électroniques en conformité avec les dispositions techniques contractuelles, en particulier par un contrôle d'intégrité pour chaque élément électronique ;
- gestion du cycle de vie des éléments électroniques et détermination de leur durée de conservation minimale, cycle à coordonner avec la durée de conservation de l'élément d'origine à horodater.

2.2.2. Exigences juridiques

Un certain nombre de documents ayant un caractère juridique doivent être rédigés. Ils touchent les tiers horodateurs, les donneurs d'ordre et conjointement les deux.

2.2.2.1. Exigences juridiques préalables au niveau de la profession de tiers horodateur

Afin de garantir aux donneurs d'ordre un service de confiance, notamment ce qui concerne la qualité des prestations, la continuité du service et la conformité des systèmes aux normes applicables, les tiers horodateurs ont intérêt à constituer entre eux un groupement professionnel.

Ce groupement aurait pour mission de définir les conditions d'un service de confiance, d'établir les modalités de mise en œuvre de ces conditions, de les adapter si besoin pour rester en adéquation avec l'évolution des activités de l'horodatage électronique et de veiller à leur respect par tous ses membres.

Pour remplir pleinement l'objectif fixé, un cadre juridique et organisationnel s'impose. Il comprend :

- une charte des tiers horodateurs (voir ci-dessous) ;
- un règlement intérieur venant compléter le code de bonne conduite, règlement qui définit de façon plus détaillée le fonctionnement du groupement, la définition de ses instances et de leur rôle, les modalités pratiques de mise en œuvre des dispositions de la charte : contrôle, continuité de service, garanties financières, contrats d'assurance, etc.

Dans le cadre de cette fonction, et afin de définir les cadres de référence pour l'exercice de leurs activités, les documents suivants sont établis :

- principes directeurs pour la rédaction d'un contrat avec les tiers horodateurs ;
- principes directeurs pour la rédaction d'un contrat avec les tiers certificateurs et/ou avec les transporteurs d'information ;

- principes directeurs pour la rédaction d'un contrat entre les membres du groupement pour la mise en œuvre de modalités spécifiques liées à leur activité : regroupement de plusieurs tiers horodateurs derrière un chef de file pour répondre au besoin d'un même donneur d'ordre, dispositifs de secours, systèmes de sécurité, etc. ;
- déclaration à la CNIL ;
- etc.

Il appartient aux membres de ce groupement de décider si les dispositions qui permettent de garantir au donneur d'ordre la continuité du service d'horodatage doivent être prévues dans une convention spécifique entre membres ou être incluses dans un contrat type de partenariat entre membres.

Outre ces dispositions contractuelles, le groupement peut étudier l'opportunité d'un système d'assurance mutuelle (ou de caution mutuelle) en complément de dispositions techniques et contractuelles entre les membres pour compléter les garanties données aux donneurs d'ordre.

Code de bonne conduite des tiers horodateurs

Le code de bonne conduite des tiers horodateurs est un document qui permet de définir une discipline destinée à mettre en œuvre l'activité de service de tiers horodatage conforme à des engagements prédéfinis et dont le but est de qualifier ledit service proposé par les prestataires informatiques à leurs clients entreprises ou organisation.

Ce code doit aborder les points suivants :

- la définition et le périmètre du service de tiers horodatage ;
- la définition des responsabilités en cas de répartition, de modification ou de création de services ;
- les engagements sur la construction du service :
 - sur le service apporté,
 - sur la fourniture du service,
 - sur les composants du système informatique et leur intégration,
 - sur la sécurité : sauvegarde, restauration, information des donneurs d'ordre, confidentialité, télémaintenance du système, sensibilisation du donneur d'ordre, etc.
 - sur les fonctions d'échanges de données,
 - sur la documentation d'utilisation et d'exploitation (par exemple manuel),
 - sur la maintenabilité (le maintien) et l'évolutivité : documentation technique et gestion de configuration, etc.
 - sur les prestations de services : mise en service de la prestation, support au démarrage, assistance téléphonique, service après-vente, dépannage, maintenance logicielle et suivi, maintenance matérielle, etc.
 - sur le respect des règles de bonne conduite : lettre d'engagement, audit périodique du système informatique mis en place, etc. ;
- les engagements sur la commercialisation du service :
 - sur les pratiques commerciales : présentation du service et démonstration, règles de bonnes pratiques du donneur d'ordre, formation du personnel commercial, liste des responsables du tiers horodateur, catalogue des produits et des prestations de services, conditions préférentielles, référence à des labels ou des agréments, présentation des offres du tiers horodateur,
 - sur le ou les contrat(s) Tiers Horodateur/Donneur d'ordre ;

les engagements sur la réalisation du service :

- sur les relations après-vente entre le donneur d'ordre et le tiers horodateur : compétence du personnel en contact avec le donneur d'ordre, suivi des clients donneurs d'ordre, contenu du dossier de suivi, information des donneurs d'ordre,
- sur les prestations : mesure de la satisfaction des donneurs d'ordre, démarche d'amélioration de la qualité du service.

2.2.2.2. Exigences juridiques préalables entre tiers horodateur et donneur d'ordre

Clause "Objet/Description du service"

Cette clause décrit le service proposé au donneur d'ordre avec, le cas échéant, des options additionnelles disponibles.

Cette description d'ordre général peut être complétée d'une description technique renvoyée en annexe du contrat (taux de disponibilité/performance du service/délai et restitution).

L'ensemble des dispositions techniques et juridiques définit le périmètre de la prestation.

Il s'agit également de définir les modalités du service en termes :

- d'abonnement (prise de commande, acceptation en ligne, signature électronique) ;
- d'accès au service (transfert, retrait et consultation des fichiers, configuration matérielle minimale requise) ;
- de sécurité (code d'identifiant, mot de passe, signature électronique) ;
- de disponibilités (horaires, période de maintenance, espace disque alloué, serveur dédié ou partagé).

Clause "Obligation du tiers horodateur"

Cette clause rappelle, de manière exhaustive, les obligations du tiers horodateur telles que décrites au paragraphe 2.2.2.1 ci-dessus et notamment l'obligation de :

- conserver l'intégralité des requêtes et des messages de services émis et reçus ;
- prendre toutes les dispositions pour assurer la pérennité de ces fichiers ;
- ne pas utiliser à des fins personnelles ou professionnelles les fichiers ou programmes informatiques confiés par le donneur d'ordre ;
- restituer les fichiers dans leur forme originale, c'est à dire dans leur forme ou format de réception par le tiers horodateur ;
- restituer les jetons d'horodatage aux fins de contrôle ;
- éventuellement, apporter un service de contrôle a posteriori par rapprochement des fichiers émis et des jetons obtenus.

Clause Obligation du donneur d'ordre

Cette clause expose l'ensemble des obligations du donneur d'ordre telles que décrites ci-dessus et notamment concernant :

- les conditions d'utilisation du service conformément aux instructions fournies (respect des protocoles d'envoi) ;
- le signalement de tout défaut constaté ;
- les autorisations légales, réglementaires ou administratives nécessaires ;
- la connexion de son serveur au Centre Serveur du tiers horodateur ;
- la prise en charge du coût des communications téléphoniques ;

- la conformité des messages émis ou reçus aux prescriptions posées par le tiers horodateur ;
- la mise à disposition de toutes informations et documentations nécessaires ou utiles pour la bonne exécution du service.

Clause "Responsabilité"

L'objet de cette clause est de rappeler que :

- le tiers horodateur ne peut être soumis qu'à une obligation de moyens dans le cadre de l'exécution du contrat,
- sa responsabilité ne peut être engagée qu'en cas de défaillance de sa part et sur faute prouvée par le donneur d'ordre,
- le tiers horodateur ne saurait être tenu pour responsable des manquements à des obligations qui ne relèvent pas de sa négligence ou qui auraient pour cause des éléments sur lesquels il n'a aucune maîtrise.

Il convient également de prévoir une limitation de responsabilité et/ou de réparation, clause valable uniquement entre professionnels et destinée à limiter la responsabilité du tiers horodateur à un plafond financier déterminé au moment de la conclusion du contrat.

En outre, il peut être envisagé une préqualification des dommages indirects pouvant être réclamés par le donneur d'ordre en cas de litige.

Clause "Garanties"

Cette clause précise les garanties données tant par le donneur d'ordre que par le tiers horodateur, telles que décrites ci-dessus.

Clause "Autorisations"

Cette clause indique les autorisations dont bénéficie le tiers horodateur au regard de la prestation de services qu'il assure (autorisations légales, administratives, réglementaires, professionnelles).

Clause "Conditions financières"

Cette clause prévoit l'ensemble des conditions financières applicables au service (abonnement, tarifs, modification des tarifs, révision du prix, indices, modes de paiement et de facturation, réclamations, pénalités).

Clause "Durée"

La durée du service est définie en considération des besoins du client et selon les formules de services proposés par le tiers horodateur (abonnement) avec des possibilités de dénonciation du contrat avant chaque période de reconduction du contrat.

Clause "Convention sur la preuve"

Cette clause indique que le tiers horodateur et le donneur d'ordre entendent, dans le cadre de l'exécution du service, donner aux messages électroniques échangés la valeur de preuve entre elles des transmissions, des commandes de prestations et des paiements intervenus ; la portée de la preuve étant celle accordée au titre des dispositions de la loi du 13 mars 2000 réformant le Code civil et portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

Ces dispositions ne seront toutefois pas applicables aux données et informations contenues dans les fichiers transmis et faisant l'objet du service.

Clauses génériques

Les dispositions particulières visées ci-dessus sont à compléter par des dispositions habituelles afférentes à ce type de contrat de prestations de services (force majeure, résiliation, cession, titre, non-renonciation, loi, compétence, etc.).

2.2.2.3 Exigences juridiques préalables au niveau du donneur d'ordre

Il n'y a pas spécifiquement d'exigences juridiques à respecter pour l'entreprise donneur d'ordre en ce qui concerne toute autorité nationale, communautaire ou internationale, qui détient le pouvoir d'effectuer des contrôles et/ou des investigations de par ses statuts ou à la suite d'une décision judiciaire opposable à tout tiers, telle que les autorités douanières, fiscales, policières, de sécurité sociale (URSSAF, etc.), le Conseil de la Concurrence, la Commission des Opérations de Bourse, la Commission de la Concurrence de l'Union Européenne et les services douaniers de cette dernière, les Ordres nationaux de certaines branches, les commissaires aux comptes, un expert judiciaire commis, sans que cette liste soit limitative.

Le tiers horodateur doit informer le donneur d'ordre immédiatement de tout événement lié à ces contrôles et investigations, quels que soient l'heure et le jour en cause.

Le donneur d'ordre doit souscrire une police d'assurance auprès de la compagnie de son choix.

2.2.3. Services ajoutés par les tiers horodateurs

On entend par services à valeur ajoutée, des prestations que le tiers horodateur est susceptible d'offrir au donneur d'ordre, en sus des services de base définis supra.

L'objet de ces services est de contribuer à la continuité de la chaîne de l'horodatage (préparation, prise en charge, horodatage, gestion de l'horodatage, assistance, formation, contrôle a posteriori). Ces services se déclinent en services amont et services aval. Ils visent à couvrir des travaux qui sont du ressort du donneur d'ordre.

Les principaux services amont qui peuvent être rendus sont les suivants :

- conseils, fournitures de logiciels appropriés pour gérer les flux à horodater ;
- formation ;
- information et conseil pour le choix des autres tiers (certificateur, autre horodateur).

Les principaux services en aval qui peuvent être offerts sont les suivants : archivage et certification.

Toutefois, des problèmes d'incompatibilité pourraient se poser, dans certains cas, entre les fonctions de tiers archiveur, de tiers horodateur et de tiers certificateur (ainsi qu'avec les fonctions de transporteur). On peut estimer qu'il en serait ainsi si une *tierce partie de confiance* venait à fournir deux ou plusieurs de ces fonctions à propos d'un même échange électronique.

GLOSSAIRE

Algorithme (algorithm) : Processus de calcul organisé en vue de son traitement informatisé.

AFNOR (Association française de normalisation) : Association loi 1901 chargée d'animer et de coordonner l'ensemble du processus d'élaboration des normes, de promouvoir leur utilisation par les acteurs économiques et de développer la certification des produits et services.

AGIRC : Régime de retraite complémentaire réservé aux cadres.

Archivage électronique (electronic archiving) : Conservation de données dématérialisées ou immatérielles, rassemblées et classées à des fins historiques ou juridiques.

ARRCO : Association pour le régime de retraite complémentaire.

Authentification (authentication) : Processus visant à établir de manière formelle et intangible l'identification des parties à un échange ou une transaction électronique.

Autorité de certification (certification authority) : Autorité de confiance, du point de vue d'un ou plusieurs utilisateurs, pour produire, distribuer, révoquer, suspendre, renouveler ou archiver des certificats de clés.

Certificat (certificate) : Information protégée par une signature électronique établissant le lien entre une identité (ou identifiant) et une clé publique. Ce lien est certifié par une Autorité de certification ou Tiers de confiance.

Clé (key) : Série de symboles commandant les opérations de chiffrement et de déchiffrement.

Clé privée (private key) : Partie du jeu de clés nécessaire au fonctionnement d'un algorithme cryptographique asymétrique, qui n'est connue que de son propriétaire.

Clé publique (public key) : Partie du bi-clé qui est communiquée aux utilisateurs pour vérifier ou chiffrer.

Confidentialité (confidentiality) : Propriété qui assure la tenue secrète des informations avec accès aux seules entités autorisées. Elle est assurée par les techniques de chiffrement.

Date d'exigibilité (Due Date) : date à partir de laquelle le paiement est requis.

Date limite (Dead Line) : dernier jour admissible pour un paiement. Le dépassement de la date limite entraînant généralement une sanction.

Déclaration de Pratiques de Certification (DPC) (*Certificate Practice Statements, CPS*) : Règles et procédures appliquées par l'autorité de certification pour produire des certificats.

Dépôt de confiance (notarisation) : Dépôt de données chez un tiers indépendant permettant de garantir leur conservation dans le temps et leur mise à disposition sous conditions.

Donneur d'ordre : client du Tiers Horodateur.

EDI (Echange de données informatisé) (Electronic Data Interchange) : Echange automatisé de données prédéfinies et structurées pour un objectif « d'affaires » entre les systèmes d'informations de deux ou de plusieurs organisations.

Heure légale (*Legal Hour*) : Temps obtenu en ajoutant ou retranchant un nombre entier d'heures au temps universel coordonné.

Horodatage (*Time stamping*) : Certification de la date et de l'heure par un tiers.

Identification (*identification*) : Opération de vérification ?

Intégrité (*integrity*) : Propriété assurant que des données n'ont pas été modifiées, insérées ou détruites de façon non autorisée.

Jeton d'horodatage (*time-stamp token*) : Suite de bits qui permet de fournir la preuve de l'existence de données à un instant dans le temps.

Politique de certification (*certificate policy*) : Recueil de règles expliquant l'utilisation prévue et autorisée d'un type de certificat.

Scénario (*scenario*) : Séquence spécifique d'actions qui illustre des comportements et qui peut être utilisée pour illustrer une interaction dans un contexte particulier

Signature électronique (*electronic signature*) : Fonction mathématique consistant à calculer une valeur à partir des données d'un message et de la clé privée de son signataire de façon à garantir l'intégrité desdites données et la non-répudiation de la transaction.

Signature électronique sécurisée (*advanced electronic signature*) : Signature numérique basée sur la cryptologie à clé asymétrique qui doit répondre à certaines exigences : être liée uniquement au signataire ; permettre d'identifier le signataire ; être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

Téledéclaration (remote report, teledeclaration) : déclaration émise par voie électronique selon un protocole défini.

Télépaiement (remote payment, telepayment) : paiement émis par voie électronique selon un protocole sécurisé.

Téléprocédure (remote procedure, teleprocedure) : procédure incluant des télédéclarations selon des normes définies. Les Téléprocédures en cours d'application sont EDI-TVA, EDI-CANAM, EDI-TDFC, DUCS-EDI, DEB.

Téléservice (remote service, teleservice) : Service de télécommunication qui assure tous les aspects de la communication entre usagers, conformément à des protocoles établis par l'entité exploitante ou par accord avec cette dernière.

Tiers archiveur (independent archiver) : Personne physique ou morale qui se charge pour le compte de tiers, d'assurer et de garantir la conservation et l'intégrité de documents électroniques.

Tiers certificateur (certifying authority) : Autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer leur clé publique et leur certificat.

Tiers horodateur (time stamping authority) : Autorité qui atteste qu'un document électronique a été créé ou signé (ou avant) une certaine date.

LISTE DES TEXTES LEGAUX ET REGLEMENTAIRES

- Code des Marchés Publics, articles 56 et 27 (dématérialisation des procédures de marché public)
- Loi n°1994-126 du 11 février 1994 dite loi Madelin
- Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
- Loi n°2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.
- Décret n°1978-855 du 9 août 1978 relatif à l'heure légale française
- Décret n°1979-896 du 17 octobre 1979 fixant l'heure légale française
- Décret n°2000-489 du 29 mai 2000 à propos de la publicité foncière
- Décret n°2000-489 du 29 mai 2000 modifiant le décret no 55-1350 du 14 octobre 1955 modifié pris pour l'application du décret no 55-22 du 4 janvier 1955 portant réforme de la publicité foncière
- Décret n°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
- Arrêté du 22 mars 2002 portant création par la Direction Générale des Impôts d'un traitement automatisé d'informations nominatives permettant la transmission, par voie électronique, des éléments déclaratifs en matière d'impôt sur les revenus et portant conventions types relatives à ces opérations,
- Lettre circulaire ACOSS n°2000-110 du 29 décembre 2000
- Lettre circulaire ACOSS n°2001-030 du 7 février 2001
- Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation

LISTE DES TEXTES NORMATIFS TECHNIQUES

- ETSI TS 102 023 V1.1.1 (2002-04) Policy requirements for time-stamping authorities;
- ETSI TS 101 861 V1.1.1 (2002-03) Time stamping profile.
- ETSI TS 101 733V1.3.1. (2002-02) Electronic Signature Formats
- ETSI TS 102 023 V1.1.1 (2002-04) : *Policy requirements for time-stamping authorities.*
- RFC 305 - Network Time Protocol
- RFC 3161 - Internet X509 Public Key Infrastructure Time Stamp Protocol (TSP)