



# Guide de l'horodatage

Collection  
Les Guides de la Confiance

Novembre 2004

Version 2.97

Copyright 2004 © FNTC

« Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article 122-5, 2°) et 3°), d'une part, que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective », et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction, intégrale ou partielle, faite sans le consentement de l'auteur ou de ses ayants droits ou ayants cause, est illicite » (alinéa premier de l'article 122-4). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 335-1 et suivants du Code de la propriété intellectuelle».

Ce Guide pratique a été élaboré par les  
groupes de travail « Flux » et Juridique »  
la Fédération Nationale des Tiers de  
Confiance

## Sommaire

<b>1. PREAMBULE.....</b>	<b>4</b>
1.1. CONTEXTE .....	4
1.2. OBJET DU GUIDE.....	6
<b>2. GENERALITES SUR LA NOTION DE DATE .....</b>	<b>7</b>
2.1. EXEMPLES D'UTILISATION DE LA DATE .....	7
2.1.1. LA DATE COMME CONDITION DE VALIDITE D'UN ACTE .....	7
2.1.2. EXIGENCE D'UNE DATE A TITRE PROBATOIRE.....	8
2.1.3. LA DATE EN TANT QU'OUTIL A USAGE INTERNE DANS LES PROCEDURES DE GESTION.....	10
2.2. LA DETERMINATION DE LA DATE PAR LA VOIE CONTRACTUELLE .....	10
2.3. DISPOSITIFS TECHNIQUES AYANT DES CONSEQUENCES JURIDIQUES .....	11
<b>3. SERVICE D'HORODATAGE.....</b>	<b>12</b>
3.1. SERVICE D'HORODATAGE.....	12
3.2. CONTREMARQUE DE TEMPS.....	12
3.3. PRINCIPES GENERAUX DE MISE EN ŒUVRE D'UN SERVICE TECHNIQUE D'HORODATAGE.....	12
3.4. LES SOURCES DE TEMPS .....	15
3.5. PRINCIPE DE PRODUCTION ET DE VERIFICATION D'UNE CONTREMARQUE DE TEMPS .....	17
3.5.1. PRINCIPE DE PRODUCTION D'UNE CONTREMARQUE DE TEMPS .....	17
3.5.2. PRINCIPE DE VERIFICATION D'UNE CONTREMARQUE DE TEMPS .....	18
3.6. DUREE DE VERIFICATION DES CONTREMARQUES DE TEMPS.....	18
<b>4. LA NOTION DE TIERS HORODATEUR .....</b>	<b>19</b>
4.1. LE TIERS HORODATEUR .....	19
4.1.1. ROLE ET FONCTIONS DE L'AUTORITE D'HORODATAGE.....	19
4.1.2. ROLE ET FONCTIONS DE L'OPERATEUR DE SERVICES D'HORODATAGE .....	19
4.2. EXEMPLE D'INTERVENTION D'UN TIERS HORODATEUR : LA DECLARATION DES REVENUS D'UN CONTRIBUABLE.....	20
4.3. OBLIGATIONS DU TIERS HORODATEUR .....	20
4.4. RESPONSABILITES DU TIERS HORODATEUR .....	21
<b>5. ANNEXE 1 : STANDARDS ET TECHNOLOGIES DESCONTREMARQUES DE TEMPS SECURISE .....</b>	<b>23</b>
5.1. FONCTION TECHNIQUE DE L'AUTORITE D'HORODATAGE.....	23
5.2. FONCTION TECHNIQUE DE LA CONTREMARQUE DE TEMPS .....	23
5.3. AUTRES SCENARIOS D'HORODATAGE ENVISAGES .....	25
<b>6. GLOSSAIRE .....</b>	<b>27</b>
<b>7. ABRÉVIATIONS .....</b>	<b>28</b>

## 1. PREAMBULE

### 1.1. Contexte

Les technologies de l'Information et de la Communication gèrent le temps pour leurs propres besoins. On parle alors de dispositif d'*horodatage*, terme résultant de la contraction de date et heure, puisque dans le monde électronique la seconde a une importance accrue.

Toute la difficulté est de savoir ce qui est l'objet d'un horodatage et dès lors quelles formes il peut ou doit prendre. En effet, la date fiable fait partie intégrante des données gérées par un système informatique sécurisé.

Il faut partir de la notion de preuve traditionnelle pour comprendre la notion de preuve de date dans le monde électronique.

La notion de preuve est avant tout une notion juridique qui intervient en cas de litige ou de contestation. En droit, **les divers procédés de preuve** ont pour finalité de convaincre le juge. La fonction de juger conduit ainsi à la recherche de l'établissement de la véracité ou plus exactement de la vraisemblance des actes et des faits juridiques au regard des éléments qui sont soumis. Sans preuve, il est impossible de faire valoir ses droits. « *Ne pas être prouvé ou ne pas être, c'est tout un* » (*idem est non esse et non probari*) confirme l'adage.

Dans le système juridique français deux systèmes de preuve coexistent : la preuve légale et la preuve libre. Ils varient selon la matière juridique en cause (droit civil, droit commercial, droit administratif, droit pénal, ...) ou selon la qualification d'acte ou de fait juridique.

Par **acte juridique**, on entend « *l'opération juridique (negotium) consistant en une manifestation de volonté ayant pour objet et pour effet de produire une conséquence juridique* » (V. Gérard Cornu, Vocabulaire juridique). C'est un écrit (*instrumentum*) rédigé en vue de constater un acte juridique ou un fait juridique (ex : constat d'accident, inventaire), et dont l'établissement peut être exigé soit à des fins de validité (*ad validitatem*) ce qui entraîne, en cas de non respect du formalisme, la nullité de l'acte, soit à des fins probatoires (*ad probationem*). Dans ce dernier cas, si l'*instrumentum* est exigé en principe, il existe des hypothèses où celui-ci ne s'avère pas forcément nécessaire (présomptions, ..).

Le **fait juridique** se définit comme : « *un fait quelconque (agissement intentionnel ou non de l'homme, événement social, phénomène de la nature, fait matériel) auquel la loi attache une conséquence juridique (acquisition d'un droit, création d'une obligation, etc.) qui n'a pas été nécessairement recherchée par l'auteur du fait. Ex. : le délit oblige son auteur à réparer le dommage causé, la possession d'un immeuble pendant 30 ans fait acquérir la propriété ; une force majeure exonère le débiteur* ». (Gérard Cornu, Vocabulaire juridique 2001).

Concernant la preuve légale, le régime juridique de la preuve des actes électroniques est régi, en droit civil, par la loi du 13 mars 2000 et les textes réglementaires qui lui sont associés. Hormis, les dispositions relatives aux conventions de preuve, cette loi impose des exigences fonctionnelles (identification et intégrité) en matière d'admissibilité de la preuve électronique, mais elle ne s'applique qu'aux actes juridiques (actes sous seing privé) et non aux faits juridiques. En ce qui concerne la validité des actes juridiques, dans la loi sur la confiance dans l'économie numérique, les nouveaux articles 1108-1 et 1108-2 du Code civil consacrent le principe de la validité des actes juridiques électroniques dans les conditions prévues aux articles 1316-1 et 1316-4 du code civil.

Concernant la preuve libre, a contrario, le Code du commerce rappelle que la preuve est libre entre commerçants.

La preuve des faits juridiques est libre également. Cependant, la liberté de la preuve ne signifie pas absence de preuve. En réalité, cela signifie que tous les moyens de preuve sont recevables par le juge (présomptions, témoignages, aveux, serments, commencement de preuve écrite, ...). On peut donc prouver par tout moyen.

Une preuve établie par une machine est recevable.

Reste alors la question de la force probante de celle-ci, réglée soit par les divers textes existants, soit par le juge saisi du litige. La date ou de façon plus générale la chronologie des évènements s'avère alors fondamentale pour estimer la force probante de la preuve qui lui est soumis.

S'agissant de ces éléments de preuve des échanges électroniques qui portent pour l'essentiel sur la **notion de date** au sens juridique, il convient de préciser que la date est en elle-même un fait juridique et que l'administration de sa preuve est libre.

Pour convaincre le juge, il conviendra en pratique, la plupart du temps, d'établir la fiabilité du procédé utilisé pour produire les moyens de preuve de ces faits juridiques. On entend par « sécurité juridique » le fait pour les parties à un échange électronique de pouvoir connaître voire s'assurer au préalable et de façon raisonnable, de la valeur juridique de celui-ci.

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<sup>1</sup>, 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."*

La question de l'horodatage se situe dans le prolongement de 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 électronique<sup>2</sup>. La loi qui ne comprend que cinq articles ne dit rien de la datation électronique (ou horodatage : information donnée sur la date mais aussi l'heure, la minute voire les secondes) 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."*

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 électronique<sup>3</sup>.

Au plan technologique il apparaît pourtant immédiatement que l'état de l'art et les consensus concernant l'horodatage sécurisé s'établissent autour d'un processus reposant sur la fourniture d'un temps normalisé et signé.

---

<sup>1</sup> COM(97)503, projet de communication de la Commission : "Assurer la sécurité et la confiance dans la communication électronique - vers un Cadre Européen Pour Les Signatures Numériques Et La Cryptographie".

<sup>2</sup> JO du 14 mars 2000, p. 3968.

<sup>3</sup> En revanche, 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 traite de la gestion du temps en matière de certificat électronique, v. les articles 6.I.c- et 6.II.n. du décret.

## 1.2. Objet du guide

La vocation de la F.N.T.C. est d'éclairer le marché tant sur l'état de l'art technologique que réglementaire sur tous les aspects des services de confiance sur les réseaux ouverts.

Pour ce faire elle émet différentes recommandations à vocation pratique que les prestataires diligents ou les organisations se doivent de mettre en oeuvre.

Ces recommandations génériques doivent aller de pair avec une réflexion poussée tant juridique que technique de ces prestataires ou organisations pour l'établissement de leur système d'horodatage.

C'est dans cette optique que le Guide de l'Horodatage a été rédigé.

Il constitue un outil permettant d'identifier les bonnes pratiques en matière d'horodatage à destination des entreprises, des organisations ou des professionnels du domaine.

## 2. GENERALITES SUR LA NOTION DE DATE

La détermination d'une date fiable peut être requise par la loi, la réglementation ou pour d'autres usages comme la gestion interne des documents, flux ou autres au sein d'une entreprise ou d'une administration (1.1). En l'absence de toute disposition légale concernant les procédés fiables de datation, les parties à un contrat pourront déterminer la valeur juridique d'une date émise par voie électronique (1.2). La notion de fiabilité du procédé d'horodatage est très importante et doit donc être clairement explicitée (1.3).

### 2.1. Exemples d'utilisation de la date

Les recours réglementaires et légaux à la notion de date sont nombreux, ces recours pouvant avoir diverses fonctions.

Ainsi, la notion de date certaine s'applique à un acte dont la date fait foi à l'égard des tiers, soit parce qu'elle a été vérifiée et attestée par un officier public, soit parce qu'une formalité (l'enregistrement aux services des impôts) ou un évènement (le décès du cocontractant) l'a mise hors de doute (article 1328 du Code Civil).

La loi peut également imposer le respect de délais, tels que des délais d'action, des délais d'attente, des délais de prescription, des délais de réflexion, des délais de carence, des délais franc, des délais préfix.

La loi peut exiger la détermination d'une date fiable comme condition de validité d'un acte juridique. La date peut également être requise à titre probatoire. La date fait courir des droits (pénalités, intérêts de retard, etc.).

#### 2.1.1. La date comme condition de validité d'un acte

Lorsque la date conditionne la validité de l'acte auquel elle fait référence, l'impossibilité d'établir avec certitude la date de formation de l'acte ou l'absence de mention de la date pourra entraîner la nullité de l'acte.

On peut notamment citer les hypothèses suivantes :

- Le vote électronique, notamment pour les assemblées générales d'actionnaires ou les élections des délégués du personnel ou des membres du Comité d'Entreprise, sont appelées à se développer et imposent de faire l'objet d'une datation fiable.
- L'acte authentique électronique, qui fait actuellement l'objet d'un avant-projet de décret, doit être daté à peine de nullité. L'acte notarié doit comporter, aux termes de l'article 6 du décret n° 71-941 du 26 novembre 1971, la date à laquelle est apposée chaque signature à peine de nullité.
- Le décret n° 2002-692 du 30 avril 2002, pris en application du nouvel article 56 du Code des Marchés Publics encadre les modalités de passation d'un marché public par voie électronique. Or, la procédure est soumise à des exigences précises de délais, qui doivent être respectées à peine d'irrecevabilité de l'offre. L'horodatage permet alors de s'assurer que la réponse à un appel d'offres a été soumise dans les délais et à en accuser réception.
- La loi de finances rectificative pour 2002 prévoit la possibilité pour toute entreprise d'utiliser des factures signées électroniquement. Une instruction du 7 août 2003 précise les conditions de validité des factures dématérialisées ou signées électroniquement et exige expressément que figure sur celles-ci la mention d'une date d'émission ou d'établissement, à peine de non déductibilité de la TVA pour le destinataire des factures.

## 2.1.2. Exigence d'une date à titre probatoire

La date est également requise à titre probatoire dans de nombreuses hypothèses, par exemple pour faire valoir ses droits, prouver l'existence d'un droit actuel, déterminer si une action est ou non prescrite ou calculer des intérêts éventuellement dus.

### 1.1.2.1 Dans les relations de droit privé

La preuve de la date de formation d'un contrat est essentielle à plusieurs égards.

On peut ici aussi donner plusieurs exemples :

- Les conditions de validité d'un contrat (prévues à l'article 1108 du Code civil) s'apprécient au jour de la formation de l'acte.
- La preuve de la date de formation du contrat s'avère aussi importante au regard de la mise en œuvre des droits de réflexion et de rétractation accordés aux consommateurs. En effet, la loi prévoit des délais incompressibles subordonnant la validité du contrat à l'octroi effectif de ces délais, ainsi qu'à l'absence d'exercice par le consommateur de ses droits durant cette période.
- Les contrats à durée déterminée peuvent soumettre leur entrée en vigueur ou leur terme à un événement, et non à une date déterminée. C'est le cas d'un contrat qui prévoit une durée de 6 mois à compter de sa signature. Il faut alors pouvoir établir avec certitude la date à laquelle le délai prévu a commencé à courir, afin de déterminer le terme du contrat.
- La Loi pour la Confiance dans l'Economie Numérique (LCEN) prévoit que les contrats sur Internet ne sont valablement conclus que si le destinataire de l'offre a eu la possibilité de vérifier le détail de sa commande et son prix total, ainsi que de corriger d'éventuelles erreurs, avant de confirmer sa commande pour exprimer son acceptation. Il existe deux exceptions à cette procédure : lorsque les parties sont toutes deux professionnelles ou lorsque le contrat se conclut uniquement par message électronique. L'horodatage est un des éléments qui participent à la détermination des conditions requises en assurant la traçabilité des échanges.

Dans d'autres hypothèses, la date peut être exigée pour déterminer la légitimité des droits. C'est le cas par exemple :

- En matière de propriété intellectuelle (par exemple lorsqu'il est nécessaire de déterminer l'antériorité d'une marque). En particulier, l'INPI permet désormais de déposer une demande de brevet par voie électronique, qui doit être datée de manière fiable.
- En matière de procédures collectives, particulièrement en ce qui concerne les privilèges et priorités de paiement ou le classement entre plusieurs créanciers.

### 1.1.2.2 Dans les relations avec l'administration

Dans de nombreuses hypothèses, les textes légaux ou réglementaires fixent des dates limites pour l'envoi de certains documents ou déclarations. De même que les déclarations manuscrites, les téléprocédures ou déclarations dématérialisées doivent être envoyées avant l'expiration du délai imparti pour la formalité concernée.

Ainsi, la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations se réfère dans son article 16 au « *cachet de la poste ou à tout procédé télématique ou informatique homologué permettant de certifier la date d'envoi* ».

- Téléprocédures fiscales et sociales :

La multiplication des téléprocédures fiscales et sociales, pour lesquelles le dépassement des délais peut entraîner des conséquences financières importantes

pour les entreprises et les particuliers, suppose que la date de déclaration soit établie avec certitude.

L'article 1649 quater B bis du Code général des impôts prévoit une procédure permettant aux entreprises soumises à un régime réel d'imposition de transmettre, par voie électronique, directement ou par l'intermédiaire d'un ou plusieurs tiers, leur déclaration de résultats ainsi que la quasi-totalité de la liasse fiscale au Centre de Services Informatiques. La Direction Générale des Impôts a ainsi créé la procédure de transfert des données fiscales et comptables (TDFC), qui constitue une obligation pour certaines entreprises relevant de la Direction des Grandes Entreprises.

Que ce soit du point de vue de l'administration fiscale, qui doit être en mesure d'apporter la preuve du dépassement de l'échéance, si tel est le cas, ou du point de vue des entreprises, qui doivent détenir une preuve confirmant qu'elles ont effectivement rempli leurs obligations en temps et en heure, le recours à l'horodatage semble ici encore essentiel.

- Archivage

Des obligations de conservation des documents relatifs à l'entreprise sont par ailleurs imposées aux entreprises, notamment dans le cadre des prérogatives de contrôle exercées par les administrations fiscales et sociales. Le délai de conservation de droit commun est de 30 ans, sauf en matière commerciale où il est réduit à 10 ans<sup>4</sup>. Les documents comptables doivent également être conservés 10 ans<sup>5</sup>. Le délai de conservation à des fins fiscales est de 6 ans. En matière sociale, en principe, le délai varie entre 3 à 5 ans suivant la nature des documents.

La datation non équivoque du début de l'archivage des documents permet ainsi de déterminer la date à laquelle l'obligation d'archivage électronique prendra fin.

S'agissant des téléprocédures et plus généralement des formulaires électroniques, qui sont appelés à se développer, des enjeux importants sont attachés à la fiabilité de la datation et à l'horodatage.

L'horodatage pourra également s'appliquer aux courriers électroniques des usagers du service public, qui sont désormais opposables à l'administration.

### 1.1.2.3 En matière de signature électronique et de certification électronique « qualifiées »

Aux termes de l'article 6.1 f) du décret n° 2001-272 du 30 mars 2001, pris pour l'application de l'article 1316-4 du code civil relatif à la signature électronique, un certificat électronique ne peut être considéré comme qualifié que s'il comporte notamment « *l'indication du début et de la fin de la période de validité du certificat électronique* ». Par ailleurs, un dispositif de vérification de signature électronique ne peut être certifié que si le prestataire est en mesure de vérifier les conditions et la durée de validité du certificat électronique utilisé lors de la vérification de la signature électronique.

En outre, il est important de pouvoir prouver l'heure exacte à laquelle un certificat a été révoqué. La responsabilité du prestataire de services de certification électronique ne doit pas pouvoir être engagée en cas de consultation de sa liste de certificats révoqués à un moment où la révocation d'un certificat a bien été enregistrée et publiée.

---

<sup>4</sup> Article L. 110-4 du code de commerce

<sup>5</sup> Article L123-23 du Code de Commerce

### 2.1.3. La date en tant qu'outil à usage interne dans les procédures de gestion

Mais la date peut également avoir une importance dans un autre contexte que purement juridique. Les applications effectives ou potentielles d'un procédé fiable de datation électronique dans les procédures de gestion interne semblent difficiles à énumérer de façon exhaustive, dès lors qu'elles sont propres à chaque entreprise ou administration.

A titre d'exemple on peut noter l'utilité de l'horodatage dans les hypothèses suivantes :

- L'horodatage de courriers électroniques échangés à l'intérieur d'une entreprise ou administration, lorsque la date et l'heure doivent être déterminées avec précision.
- L'horodatage des documents archivés électroniquement permet d'optimiser la gestion de l'ensemble des documents de l'entreprise, ainsi que de reconstituer la chronologie des échanges survenus dans l'entreprise.
- Le contrôle des accès à distance aux ressources internes ou aux espaces de partage.
- la mise en place de procédures internes pour la validation par de multiples services du contenu d'un document (projet de contrat mais également contenu publicitaire, ...)
- Le suivi des plannings.

Dans le secteur public, le recours à l'horodatage est déjà envisagé, par exemple en matière de gestion des habilitations d'agents publics, d'accès aux dossiers des agents publics ou de suivi des instructions.

Cependant, en matière de gestion interne, se pose la question de la possibilité ou non de se pré-constituer une preuve pour ses propres besoins. La date dans cette procédure devrait être prise ici comme indice d'un événement à qui l'on cherche à conférer une valeur juridique.

## 2.2. La détermination de la date par la voie contractuelle

Le droit n'a pas prévu en l'état actuel de règles générales et universelles qui permettraient de disposer, par analogie au procédé fiable d'identification associé à la signature électronique (loi n° 2000-230 du 13 mars 2000), d'un procédé fiable de datation électronique pour les échanges électroniques. A défaut de loi, les parties aux échanges électroniques peuvent utiliser le contrat.

Dans ce contexte, les parties (particuliers et entreprises) doivent prévoir au sein du contrat la convention de preuve qui fera foi en matière de date.

Par exemple, dans les échanges entre les entreprises et l'administration, l'article 4 de la loi Madelin (11 février 1994, JO du 13 février 1994, p.2493) propose également le système contractuel, en indiquant que « *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* ».

Dans les échanges bilatéraux de type EDI, mêmes 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. La recommandation européenne pour l'EDI la place dans les garanties de sécurité à appliquer<sup>6</sup>.

*"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. Les parties déterminent dans leur convention la validité et la force probante de certains modes de preuve, et peuvent instaurer une hiérarchie entre ceux-ci.

L'horodatage peut être réalisé en faisant appel à un tiers indépendant des parties ou en utilisant un système d'horodatage interne reconnu fiable et régulièrement contrôlé, conditions minimales permettant de garantir juridiquement la datation d'un échange.

### **2.3. Dispositifs techniques ayant des conséquences juridiques**

Une date fiable est une date que l'on peut considérer comme exacte des opérations, des activités ou des faits, qu'elle atteste, et sur lequel on peut s'appuyer lors d'opérations, d'activités ou de faits ultérieurs. Elle doit pouvoir être utilisée à tout moment, pour apporter la preuve d'un droit par exemple, et de ce fait, elle doit être intègre dans le temps.

La fiabilité du procédé de datation est une question de technique et de confiance. Soucieux de cet aspect, divers intervenants travaillent afin de déterminer « un état de l'art ». A l'instar de ce qui avait été proposé pour les signatures électroniques, la Direction centrale de la sécurité des systèmes d'information (D.C.S.S.I./SGDN) – dans le cadre d'un groupe de travail au sein de l'association française de normalisation (A.F.NOR) – a en projet l'établissement d'un modèle standard de politique d'horodatage. Cette politique d'horodatage doit permettre de déterminer les conditions entourant la délivrance fiable d'une date (le cas échéant par un tiers horodateur).

Mais ce choix pourrait également prendre en considération le respect de certaines exigences juridiques et organisationnelles propres à la délivrance d'une contremarque de temps. L'horodatage doit ainsi permettre de s'assurer que les échanges électroniques existaient à un instant donné et qu'au cours de l'échange ou de l'archivage dont ils ont fait l'objet, leur fiabilité, leur sécurité et leur intégrité a été assurée et ceci de manière continue et pérenne.

---

<sup>6</sup> 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.

### 3. SERVICE D'HORODATAGE

D'autres modèles de service d'horodatage existent (ex : horodatage sans signature à base de hash linking). La F.N.T.C. ne traite que du service d'horodatage basé sur une signature électronique.

#### 3.1. Service d'horodatage

Le service d'horodatage intervient au niveau de la création des contremarques de temps.

Ce service consiste d'une part, en une apposition d'une « contremarque » de temps sur des données afin d'attester leur existence à une date et une heure données et d'autre part en la production, délivrance et conservation des éléments permettant d'attester l'évènement associé.

Cette fonction est réalisée en utilisant une contremarque de temps – élément résultant de l'association de données à une marque de temps fiable, dont les éléments technologiques sont décrits dans l'annexe technique.

Chaque contremarque émise par le service d'horodatage comprend une signature électronique de l'AH afin d'en garantir l'intégrité et l'authenticité.

#### 3.2. Contremarque de temps

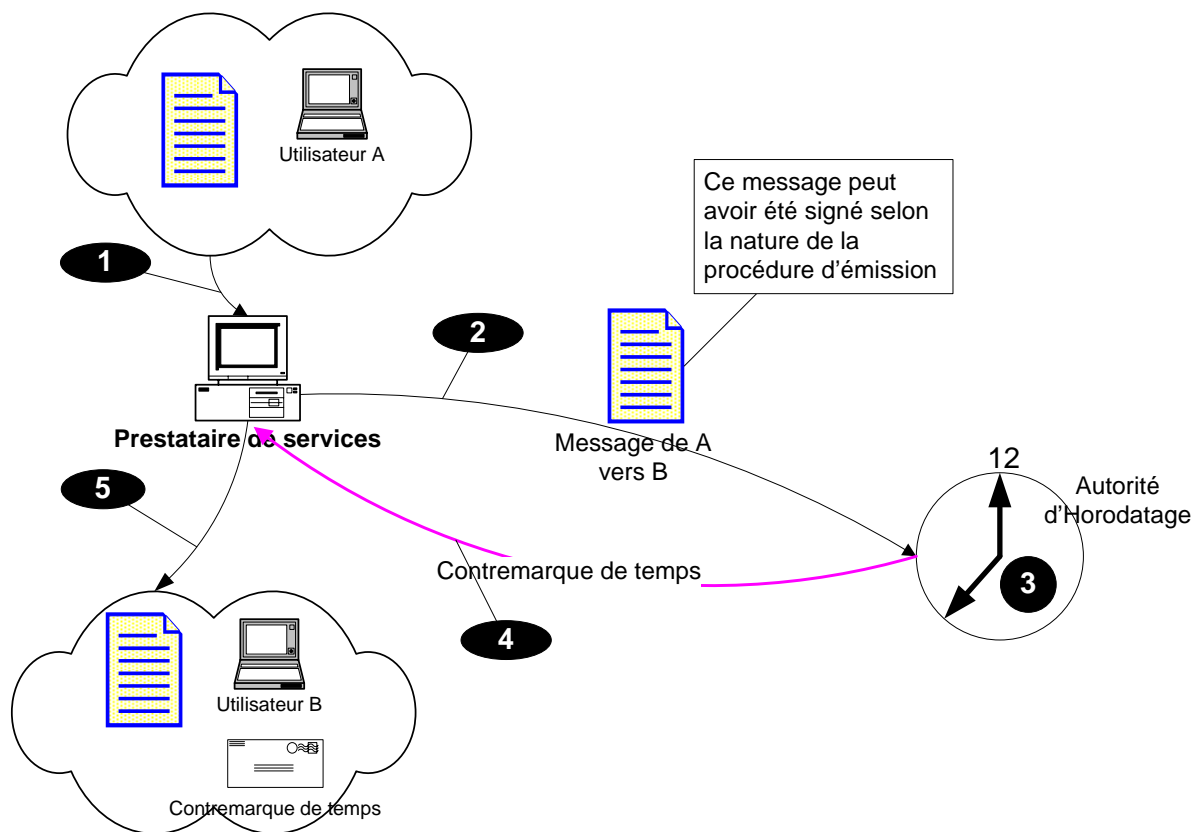
Une marque technique d'horodatage, aussi appelée « contremarque de temps », est l'élément de données résultant de l'association de données à une date et une heure qui sont obtenues à partir d'une source de temps réputée fiable, le tout étant signé électroniquement par l'AH.

L'utilisation principale de l'horodatage est d'horodater des données afin de pouvoir attester que celles-ci ont été créées avant une date et une heure données.

La date/heure qui fait foi est celle contenue dans la marque technique d'horodatage sauf spécification ou usages particuliers indiqués explicitement dans les éléments contractuels et la Politique de l'AH.

#### 3.3. Principes généraux de mise en œuvre d'un service technique d'horodatage

**Cas N°1** : Le prestataire de services intègre le service d'horodatage dans son offre

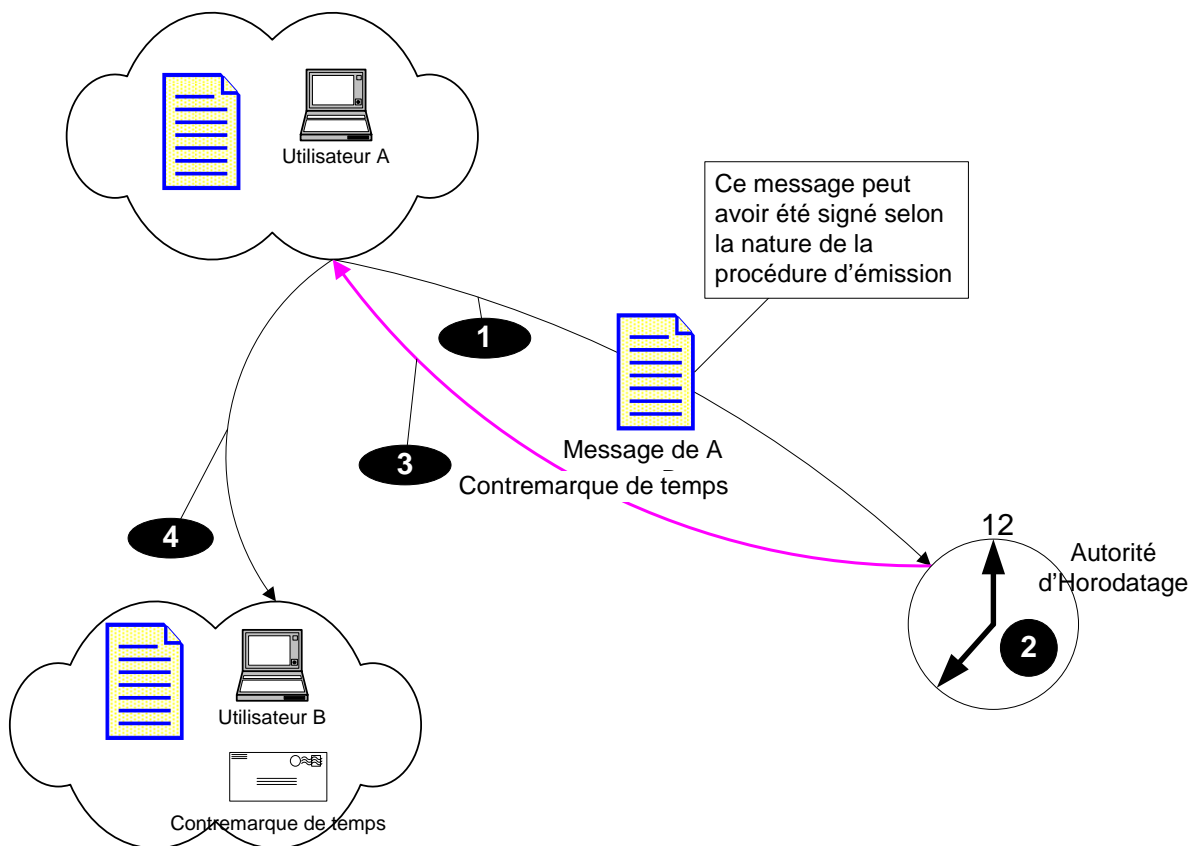


Explication du schéma :

Etape	Explication
1	L'utilisateur A envoie ses données au prestataire de services.
2	Le prestataire envoie un condensat des données ou les données de A à l'AH
3	L'AH élabore la contremarque de temps suivant les dispositions de sa PH applicable.
4	L'AH retourne la contremarque au prestataire.
5	Le prestataire envoie les données de A à B auxquelles est associée la contremarque de temps.

**Note :** le prestataire doit garantir techniquement et juridiquement le lien entre les données et la contremarque de temps.

**Cas N°2 :** Les utilisateurs A et B se sont mis préalablement d'accord sur l'intégration dans leurs échanges d'une contremarque de temps



Etape	Explication
1	L'utilisateur A envoie ses données ou un condensat de celles-ci à L'AH.
2	L'AH élabore la contremarque de temps suivant les dispositions de sa PH applicable.
3	L'AH retourne la contremarque à l'utilisateur A.
4	L'utilisateur A envoie les données à B auxquelles est associée la contremarque de temps.

**Note :** l'application de l'utilisateur A doit garantir le lien entre les données et la contremarque de temps conformément aux stipulations contractuelles établies entre A et B.

### 3.4. Les sources de temps

Nous ne traiterons pas ici des notions d'heure universelle et d'heure légale sur le territoire national (cf décret n° 78-855 du 9 août 1978 relatif à l'heure légale française ; décret n° 79-896 du 17 octobre 1979 fixant l'heure légale française).

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.

Définition officielle de la seconde :

*La seconde est représentée par la durée de 9.192.631.770 périodes de la radiation correspondant à la transition entre deux niveaux d'énergie de l'atome de césium 133 à l'état naturel.*

*1<sup>ère</sup> résolution de la 13<sup>ème</sup> conférence générale des poids et mesures (CGPM) (1967)*

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 :

BIPM UTC time  
**Niveau International**



Horloges atomiques nationales  
Des Instituts de mesure nationaux  
**Niveau National**



Organismes de distribution  
de temps fiable  
**Niveau Distribution**



Temps de confiance  
**Niveau Application**



#### 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 RFC 1305, 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 d'étude (draft-ietf-stime-ntpauth-04.txt) ajoute au protocole NTP l'authentification mutuelle. Aucun RFC n'a été produit à ce jour.

#### 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 1er 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 confié à l'Institut Européen des Normes de Télécommunications (ETSI).

A ce jour, sur ce sujet précis, l'ETSI a publié :

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

Et l'IETF a publié :

- RFC 3161 (TSP) Time-Stamping Protocol
- RFC 3029 (DVCS)

Un service d'horodatage est produit au plan technique de façon à répondre aux engagements techniques souscrits à travers la politique d'horodatage - cf : ETSI TS 102 023 V1.1.1 (2002-04).

Les conditions de production des contremarques de temps sont définies dans le document ref : ETSI TS 101 861 V2.1.1 (2002-03) Time stamping profile.

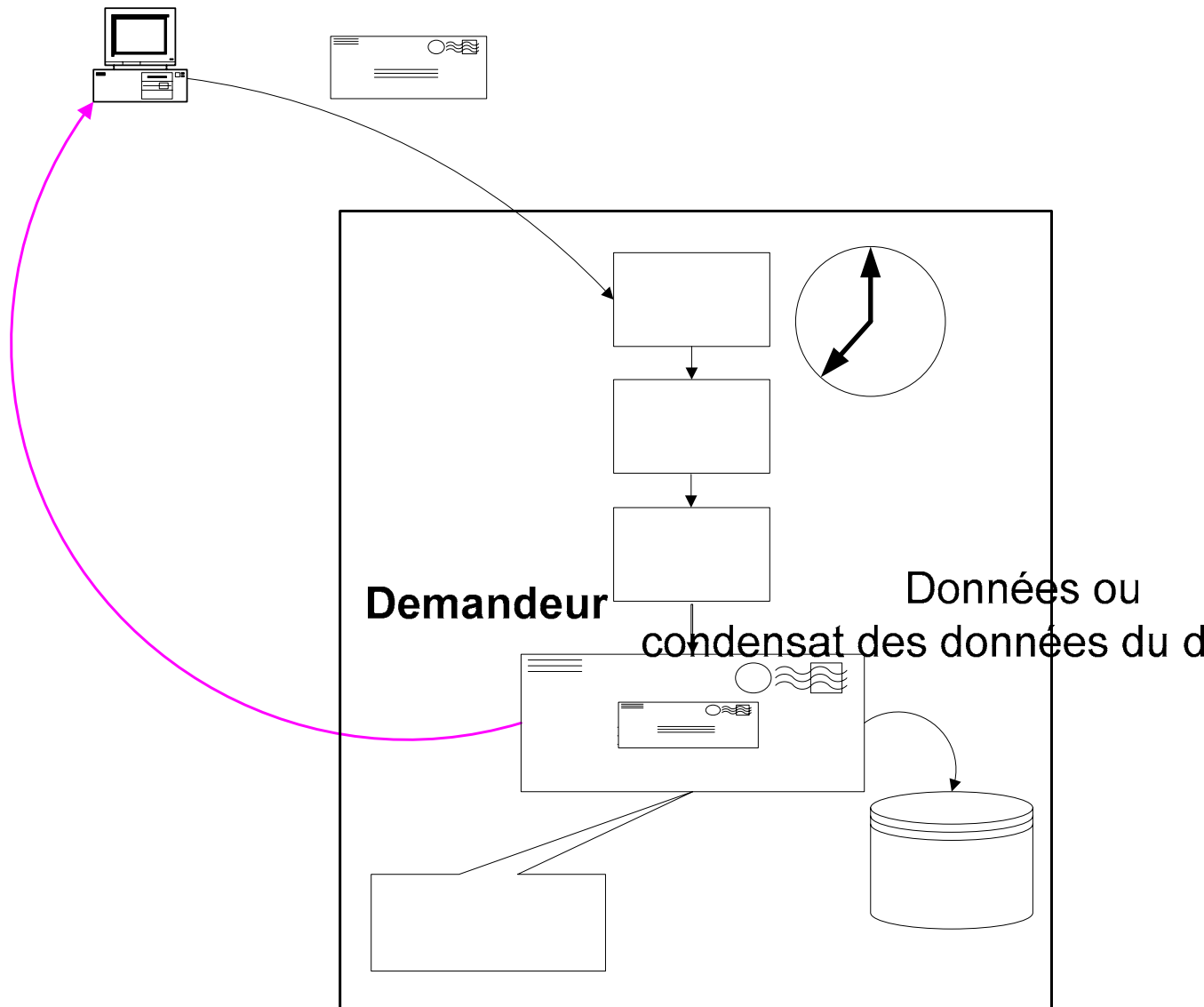
La description des formats et des procédures d'échange des contremarques de temps sont standardisés à travers la RFC 3161.

Les conditions de vérification d'un jeton émis ou reçu sont définies par le standard RFC 3029.

### 3.5. Principe de production et de vérification d'une contremarque de temps

#### 3.5.1. Principe de production d'une contremarque de temps

Le processus d'horodatage



Note : Voir la structure d'une contremarque de temps (Capsule CMS) en annexe 1

### 3.5.2. Principe de vérification d'une contremarque de temps

À la réception d'une demande de vérification d'un client ou d'un tiers utilisateur accompagnée de la contremarque de temps à vérifier, le tiers horodateur procède aux contrôles suivants :

1. Vérification de la durée de validité de la contremarque de temps fournie;
2. Contrôle de la validité du contremarque de temps avec vérifications de :
  - la validité de la signature de la contremarque en regard du certificat de l'AH ;
  - la validité du certificat de l'AH, ainsi que de tous les certificats présents sur sa chaîne de certification ;
  - la validité des données horodatées en regard de l'empreinte de la signature de l'élément de contremarque de temps à vérifier ;

Un élément de contremarque de temps est considéré valide dès lors que tous les contrôles évoqués ci-dessus sont satisfaits.

### 3.6. Durée de vérification des contremarques de temps

La question préalable est de savoir pendant combien de temps il est nécessaire de pouvoir vérifier la contremarque de temps associée à des données.

Pour répondre à cette question il est également nécessaire de s'interroger sur la durée de conservation des données.

D'un point de vue général, la politique d'horodatage d'un tiers horodateur prévoit contractuellement la durée pendant laquelle l'historique des opérations qu'il réalise et les contremarques de temps qu'il émet seront conservés. Cette durée peut être adaptée en fonction des contraintes réglementaires auxquelles est soumis l'utilisateur du service d'horodatage.

A titre d'exemple, dans le domaine de la transmission des factures transmises électroniquement et sécurisées au moyen de la signature électronique, il est souhaitable, sans préjudice d'autres dispositions, que le TH conserve pour le compte de ses clients ses historiques et ses contremarques de temps au minimum pour la période de reprise de l'administration fiscale.

## 4. LA NOTION DE TIERS HORODATEUR

### 4.1. Le tiers horodateur

Le tiers horodateur peut impliquer 2 entités : l'autorité d'horodatage et l'opérateur de service d'horodatage. Pour chaque entité il convient de définir le rôle et les responsabilités.

Différentes entités techniques interviennent dans le cadre de la délivrance d'une contremarque de temps. L'analyse fonctionnelle qui en découle permet uniquement de déterminer les rôles de chacune des entités.

Entité	Rôle	Documents fondateurs	Missions
AH	Maîtrise d'ouvrage du service d'horodatage	Politique d'horodatage	Responsabilité de l'émission des contremarques de temps
OSH	Maîtrise d'oeuvre du service d'horodatage	Déclaration des pratiques d'horodatage	Emission technique des contremarques de temps

#### 4.1.1. Rôle et fonctions de l'autorité d'horodatage

L'AH prend en charge l'ensemble du processus d'horodatage et est donc garante de la validité des contremarques de temps qu'elle émet ou qui sont émises sous sa responsabilité. La garantie apportée par l'AH résulte de la qualité de la technologie mise en œuvre, mais aussi du cadre réglementaire et contractuel qu'elle s'engage à respecter et à faire respecter.

L'Autorité d'Horodatage établit la politique d'horodatage. Dans ce cadre, elle prend en charge l'ensemble du processus d'horodatage.

#### 4.1.2. Rôle et fonctions de l'opérateur de services d'horodatage

L'OSH assure les prestations techniques nécessaires au processus d'émission des contremarques de temps de l'AH. Il est en charge du bon fonctionnement et de la sécurité des moyens informatiques et techniques relatifs aux processus qui lui sont confiés par l'AH. Il doit assurer le bon respect des procédures et des dispositifs nécessaires pour garantir un niveau de fiabilité satisfaisant.

L'OSH est techniquement dépositaire de la clé privée de l'AH utilisée pour la signature des contremarques de temps. Une de ses premières missions est de la protéger contre toute compromission.

Sa responsabilité, qui ne peut être engagée que par l'AH, se limite au respect des procédures établies dans la Déclaration des Pratiques d'Horodatage élaborée par l'OSH et approuvée par l'AH.

L'OSH doit répondre aux exigences et aux spécifications énoncées par l'AH dans sa politique d'horodatage.

#### **4.2. Exemple d'intervention d'un tiers horodateur : La déclaration des revenus d'un contribuable**

##### Cas N°1 : Absence complète de preuve

Dépôt de la déclaration des revenus dans la boîte à lettre du Centre des Impôts de sa localité de rattachement. Aucune preuve de dépôt n'est fournie.

##### Cas N°2 : Absence de preuve fournie par un tiers

Dépôt de la déclaration des revenus en main propre au Centre des Impôts contre remise d'un accusé de réception indiquant la liste des documents joints.

La preuve de date (réception de la déclaration) est fournie par le Centre des Impôts – Il n'est fait aucun recours à un Tiers de Confiance extérieur.

##### Cas N°3 : Preuve fournie par un tiers extérieur

Envoi en recommandé avec avis de réception de la déclaration des revenus.

Il est fait recours à un Tiers de Confiance, par exemple : La Poste. Le rôle d'AH est assumé par celle-ci. Le rôle d'OSH est assumé par l'AH en interne ou par un prestataire technique sous contrat avec l'AH.

##### Cas N°4 : Service de preuve fourni par le destinataire

Dépôt de la déclaration des revenus en utilisant TélÉIR (en 2003).

L'AH et l'AC sont confondues avec le destinataire qui est le Centre des Impôts – Il n'est fait aucun recours à un Tiers de Confiance.

L'OSH est assurée par un prestataire technique sous contrat avec la DGI.

#### **4.3. Obligations du tiers horodateur**

La liste qui suit n'est pas exhaustive.

Le tiers horodateur s'engage à effectuer les prestations liées à son rôle d'AH pour le demandeur, à savoir la génération et la fourniture de contremarque de temps conformes à sa Politique d'Horodatage.

Le tiers horodateur s'engage à fournir à toute personne utilisatrice, sur sa demande, tous les éléments qui permettront d'attester la fiabilité de la date et l'heure contenues dans la Contremarque de temps.

Le tiers horodateur s'engage à conserver les contremarques de temps pendant une durée convenue suivant sa politique à compter de la date figurant dans la contremarque de temps.

Le tiers horodateur s'engage à respecter les normes et standards de l'état de l'art.

Le tiers horodateur s'engage à respecter les dispositions de sa PH.

Le tiers horodateur s'engage à maintenir une équipe compétente et expérimentée pour la continuité des prestations d'horodatage.

Le tiers horodateur s'engage à assurer en permanence la sécurité physique et logique ainsi que l'intégrité des matériels, logiciels, données et des bases de données nécessaires au bon fonctionnement du Service d'Horodatage.

Le tiers horodateur s'engage à surveiller et contrôler le service d'horodatage afin d'empêcher ou de limiter toute perturbation et/ou indisponibilité du service d'horodatage résultant notamment de toute attaque délibérée (notamment intrusion) sur tout ou partie de son service d'horodatage.

Le tiers horodateur s'engage à prendre toutes les mesures de protection nécessaires conformes aux règles de l'art afin d'assurer une sécurité maximale du service d'horodatage et pour prévenir tout dysfonctionnement du service d'horodatage.

Le tiers horodateur met en place un service de secours qui pourra être utilisé par le demandeur en cas d'interruption du service d'Horodatage.

#### **4.4. Responsabilités du tiers horodateur**

La liste qui suit n'est pas exhaustive.

Le tiers horodateur est tenu responsable des conséquences dommageables dans le cadre :

- du respect des exigences explicitées dans la Politique d'Horodatage de l'AH (cf. PH) ;
- de tout manquement à son obligation de confidentialité, et ce notamment au regard des données personnelles que le demandeur lui a transmises ;
- des préjudices causés aux personnes utilisatrices en cas d'inexécution du contrat par l'autorité d'horodatage ;
- des préjudices causés par son personnel dans le cadre des prestations de service offertes et définies dans le contrat ;
- des préjudices subis par le partenaire et/ou par le client et résultant de dysfonctionnement du matériel utilisé par l'autorité d'horodatage ;
- de la précision et de l'intégrité des données qu'il délivre et manipule ;

Le tiers horodateur décline toute responsabilité à l'égard de l'usage qui est fait des contremarques de temps qu'il émet et signe, dans des conditions et à des fins autres que celles prévues dans le Contrat.

Certains actes ou faits électroniques nécessitent l'établissement d'un lien fiable entre des données numériques et un instant spécifique dans le temps qui sera matérialisé par une preuve de date. Cette preuve de date est établie et construite à partir d'une marque de temps appelée horodatage. Les actes ou faits invoquant des contremarque de temps de date peuvent être l'enregistrement de droits intellectuels ou œuvres de l'esprit sous une forme électronique, l'envoi de formulaires électroniques, les télé-procédures, l'accusé de réception électronique, etc.

Les contremarques de temps de date les plus couramment reconnues dans les procédures traditionnelles sont celles mettant en œuvre un cachet de La Poste faisant foi ou Timbre à date d'un bureau émetteur faisant foi (art. 667 du NCPC), le

Timbre à date de l'INPI, la date de l'acte apposée par l'Huissier de Justice, le cachet daté du Notaire, le cachet des Préfectures ou de toutes administrations,....

Dans la suite sont décrits les processus qui permettent d'établir des contremarques de temps qui puissent représenter le pendant électronique des contremarques de temps les plus courantes.

L'annexe technique qui suit traite de l'état de l'art et des moyens techniques associés pour produire une marque de temps fiable appelée «contremarque». Elle décrit en particulier comment il est fait recours à une Autorité d'Horodatage pour établir cette marque de temps utilisée dans la construction des contremarques de temps de date.

**Addendum :**

La politique de référencement intersectorielle de sécurité version 2 (PRIS V2) qui devrait paraître début 2005 de l'Agence pour le Développement de l'Administration Electronique (ADAE) prévoit une partie de qualification et d'homologation des prestataires de service d'horodatage. La finalisation de son contenu est en cours.

## 5. ANNEXE 1 : STANDARDS ET TECHNOLOGIES DESCONTREMARQUES DE TEMPS SECURISE

### 5.1. Fonction technique de 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)<sup>7</sup>. 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.

### 5.2. Fonction technique de la contremarque de temps

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 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 contremarque de temps 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.

---

<sup>7</sup> ETSI TS 102 023 V1.1.1 (2002-04) Policy requirements for time-stamping authorities.

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 contremarque de temps 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
}

```

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

- la politique d'horodatage utilisée, le statut dans l'ICP (Infrastructure à clé publique), 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 contremarque de temps 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.

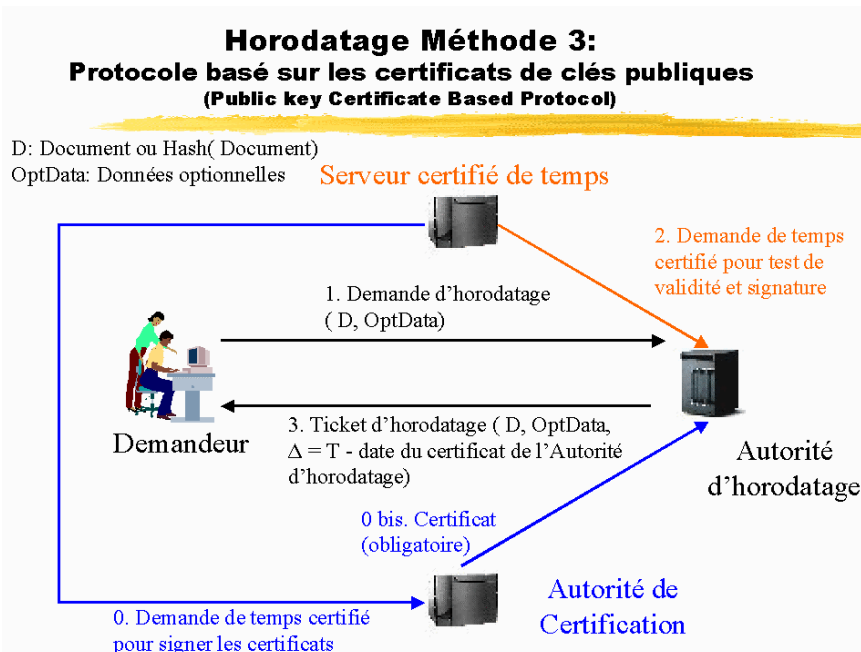
### 5.3. Autres scénarios d'horodatage envisagés

Pour la mise en œuvre pratique de la certification d'horodatage, plusieurs méthodes d'horodatage sont envisageables 8 :

- 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 1 et 2 sont en général intéressantes, mais impliquent une confiance totale 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.



<sup>8</sup> « *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, spécialement certains des adhérents de la FNTC, qui fournissent des services plus ou moins variables. Ils peuvent être liés à d'autres services comme la protection intellectuelle, la facturation électronique, les marchés publics en ligne ou l'archivage. Mais ils peuvent également fournir le service d'horodatage seul.

## 6. GLOSSAIRE

**Autorité de Certification (AC) :** Entité émettant des Certificats après vérification de l'identité de la personne ou du représentant du système applicatif, ou de la procédure ayant mené à son identification. L'AC est responsable de l'ensemble des composantes matérielles, humaines et organisationnelles utilisées dans le processus de création et de gestion des Certificats.

**Autorité d'Horodatage (AH) :** Autorité responsable de la gestion de l'environnement d'horodatage et de la production des contremarques de temps sur les données qui lui sont présentées afin d'attester de l'existence de ces données à la date de la marque de temps.

**Composante de l'AH :** Plate-forme constituée d'au moins un poste informatique, une application, un moyen de cryptologie, un support réseau et jouant un rôle déterminé au sein du système.

**Contremarque de temps :** C'est l'élément de données résultant de l'association de données à une date et une heure obtenues à partir d'une source de temps réputée fiable, le tout étant signé électroniquement par l'AH.

**Déclaration des pratiques d'horodatage (DPH) :** Document décrivant précisément les pratiques mises en place par l'AH ou par l'OSH pour la fourniture de contremarques de temps.

**Dispositif d'horodatage :** Ensemble de composants logiciels et matériels, géré comme une entité particulière et ayant une seule clé de signature des contremarques de temps. Dans le contexte présent, cette entité est le Serveur Primaire d'Horodatage (SPH).

**Echelle de temps Universal Time Coordinated (UTC) :** Heure basée sur le méridien de Greenwich (+0, heure GMT). Cette heure est utilisée afin de n'avoir pas à jongler avec les décalages horaires lorsque l'on s'adresse à plusieurs interlocuteurs situés dans des fuseaux horaires différents.

**Echelle de temps UTC(k) :** Heure fournie par la source de temps « k » avec une précision suffisante pour l'usage envisagé. Cette précision est au plan strictement technique de  $\pm 100$  ns, si l'on souhaite impérativement se conformer à la recommandation S5 du Comité Consultatif pour la Définition de la Seconde (référence : [ITU-R TF.536-1])

**Empreinte (empreinte numérique ou condensat ou hash) :** Résultat d'une fonction de hachage appliquée sur une chaîne de caractères de longueur quelconque visant à

réduire celle-ci en une donnée de longueur fixe représentative de cette chaîne de caractères.

**Opérateur de Service d'Horodatage (OSH) :** L'OSH assure les prestations techniques nécessaires au processus d'horodatage. Il est en charge du bon fonctionnement et de la sécurité des moyens informatiques et techniques. Il est en charge de la sécurité des personnels, des locaux et, plus généralement, du bon respect des procédures, toutes choses indispensables pour garantir le niveau de fiabilité requis.».

**Politique d'horodatage (PH) :** Texte contractuel qui établit les obligations et responsabilités de l'Autorité d'Horodatage, de l'Opérateur des Services d'Horodatage, des services demandeurs et des utilisateurs finaux. Elle est librement consultable par les clients, les abonnés ainsi que par tous les tiers utilisateurs.

**Signature électronique sécurisée -** Une signature électronique qui est liée de manière unique au signataire, qui est créée par des moyens que le signataire est en mesure de maintenir sous son seul contrôle, et qui est liée à la donnée signée de telle manière que tout changement ultérieur est détectable.

**Source de temps :** Une source de temps est une composante interne ou externe d'une AH fonctionnant comme une tierce partie de confiance technique qui est chargée de restituer une heure fiable selon l'usage requis.

**Service d'horodatage :** Ensemble des dispositifs et composantes de l'AH permettant la fourniture des contremarques de temps.

**Tiers Horodateur :** Tiers de confiance composée d'une entité ou de plusieurs entités intervenant dans la fourniture et la gestion de contremarques de temps.

**Utilisateur final :** L'utilisateur final est la personne physique ou morale identifiée ou non qui reçoit par l'intermédiaire du service demandeur une contremarque de temps correspondant à la fourniture d'un service d'horodatage par l'AH.

## 7. ABRÉVIATIONS

<b>AH</b>	Autorité d'Horodatage
<b>DPH</b>	Déclaration des Pratiques d'Horodatage
<b>EDI</b>	Echange de données informatisées
<b>ETSI</b>	European Telecommunication Standards Institute
<b>LCR</b>	Liste des certificats révoqués
<b>OID</b>	Object IDentifier (Identifiant d'Objet)
<b>OSH</b>	Opérateur de Service d'Horodatage
<b>SPH</b>	Serveur Primaire d'Horodatage
<b>UTC</b>	Universal Time Coordinated
<b>XML</b>	Extended Markup Language

Certaines parties de ce document sont issues de travaux réalisés par les associations EDIFICAS et IALTA. La F.N.T.C. les remercie pour leur aimable collaboration.