
Microsoft®

Le rôle des Tiers de Confiance dans la sécurisation des échanges

Jean-Marc RIETSCH
Représentant de la FNTC
Expert au CoDiL

Microsoft

Plan de l'exposé

1. Présentation de la FNTC
2. Positionnement
3. Chaîne de confiance, tiers de confiance
4. Aspects légaux
5. Preuve, pas seulement

1. Présentation de la FNTC
(Fédération Nationale des Tiers de Confiance)

- Pourquoi des tiers de confiance ?
- Objectifs
- Organisation
- Labellisation

Pourquoi des tiers de confiance?

La demande en solutions de confiance est la conséquence:

- des évolutions technologiques permettant:
  - le développement d'Internet
  - la dématérialisation des flux et des documents
- la mondialisation de l'économie

Pourquoi des tiers de confiance?

Pour réussir il faut dépasser le doute avec une logique de la confiance:

- On ne se pose plus la question :
  “Qui dois-je craindre ?”
- mais :
  “En qui puis-je avoir confiance ?”

Pourquoi des tiers de confiance?

La confiance sur Internet repose notamment sur :

- La preuve électronique (actes juridiques)
  - Intelligibilité
  - Identification
  - Intégrité
  - Pérennité

Pourquoi des tiers de confiance?

- Un nouvel outil « la signature électronique »
  - Identification des parties contractantes
  - Intégrité des messages (adhésion au contenu)
  - Confidentialité
  - Non répudiation (non contestation par l'émetteur)

Des tiers doivent garantir les organisations et les procédures dans un environnement normatif et juridique stricte

Un nouveau modèle organisationnel

Caractéristiques principales du modèle:

- Environnement ouvert
- Basé sur des processus commerciaux et/ou administratifs
- Sécurisation du flux (échanges des données)
- Sécurisation du contenu (conservation)

Des tiers devront garantir les transactions car nul ne peut se pré constituer de preuves à lui-même (Article 1315 code civil)

Un nouveau modèle économique, les acteurs

- **Les « officiers » de la confiance (Autorités)**
  - La Poste
  - Le système bancaire
  - Les assureurs
  - Les professions réglementées et les OPM
  - Les organisations consulaires

Ils garantissent le service en ayant une responsabilité juridique et financière vis-à-vis des utilisateurs

Un nouveau modèle économique, les acteurs

- **Les opérateurs de services de confiance (OSC)**
  - Certificateurs
  - Horodateurs
  - Archiveurs

Ce sont des prestataires de services qui opèrent dans un contexte contractuel avec leurs donneurs d'ordre

Objectifs de la FNTC

- **Rassurer les usagers et favoriser le développement du marché en matière de:**
  - Services de confiance
  - Assurance de la qualité
- **Comment ?**
  - Charte d'éthique
  - Qualification des services avec des labels
  - Garantie de plate formes conformes
  - Procédures d'interopérabilité entre prestataires
  - Audit et contrôle des procédures

Organisation de la FNTC

Groupes de travail et commissions :

- Commission adhésion
- Commission communication
  - Organisation du FETC (Forum Européen des Tiers et des Acteurs de la Confiance)
  - Lettre de la Confiance
- Commission technique composée des groupes :
  - « stock » (stockage, archivage, hébergement)
  - Flux (sécurité des échanges: certification, horodatage)
  - Juridique et garanties

Labellisation de services

- **Une démarche structurée basée sur :**
  - Une procédure d'attribution publiée
  - Un référentiel des services, homologué par la FNTC
- **Une démarche transparente :**
  - Création d'un Comité d'Attribution (CoDiL) composé entre autre de: Jean DONIO, Eric HAYAT, Serge YABLONSKY, Jean-François LEGENDRE,…
  - Audits de conformité par des organismes indépendants suivant la méthode COBIT

COBIT ® : Control Objectives for Information and related technology 3rd Edition by AFAI the French Chapter of the Information Systems Audit and Control Association (ISACA)

Découpage

- Collège 1: **Prestataires de Service (21)**
- Collège 2: **Professionnels garants de la confiance (4)**
- Collège 3: **Experts & Associations (23)**
- Collège 4: **Institutionnels (3)**

En liaison avec d'autres organismes

- MINEFI
  - Aspects certification
- Forum des Droits sur Internet
  - Groupe de travail archivage
- EDIFRANCE
  - Adaptation de la directive européenne 115
- AFAI
  - Méthode Cobit dans le cadre du label
- APROGED
  - Evolution des techniques d'archivage
- AFNOR
  - Connaissance et évolution de la norme Z42-013

2. Positionnement

- Sécurisation des échanges
  - Sécurité par rapport au risque technique
  - Sécurité par rapport au risque juridique
- Rapport sécurité - confiance

Au-delà de la sécurité technique, les tiers de confiance doivent permettre d'apporter la preuve de l'échange

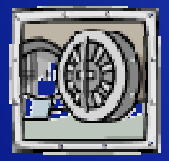
3. Chaîne de confiance, différents tiers de confiance

- Certification, signature électronique
- Horodatage, contremarque de temps
- Archivage, scellement

La chaîne de la confiance

- **Le Tiers Certificateur**
  - Signature du document

- **Le Tiers Horodateur**
  - « Cachet électronique de la poste « »



- **Le Tiers Archiveur**
  - Conservation intègre et pérenne
  - Garantie d’interopérabilité

Certification, définitions

- Bi-clé (clé privée, clé publique)
- Empreinte, condensat
- Certificat de clé publique
  - lien entre signataire et bi-clé
  - responsabilité de l'autorité de certification
  - plusieurs classes de certificats
- Signature électronique

Eléments principaux d'un Certificat

- *version de certificat*
- *numéro de série unique*
- *nom du signataire et sa clé publique*
- *algorithme de signature utilisé*
- *dates de validité du certificat*
- *nom de l'émetteur du certificat (Autorité de Certification)*
- *identifiant de la politique de certification associée à l'utilisation du certificat*
- *signature du certificat par la clé privée de l'Autorité de Certification*
- *éventuelles limitations pour son utilisation*

Différents usages des certificats

- Authentification
- Signature électronique
  - Identification
  - intégrité
- Chiffrement
  - confidentialité

Un certificat destiné à de l'authentification et/ou de la signature électronique ne peut être utilisé pour du chiffrement

Chaîne de confiance de la signature électronique

- Elaboration de la signature
  - vérification d'identité du signataire avec un niveau de sécurité adapté à l'usage du certificat
  - demande d'émission du certificat
  - délivrance du certificat signé par la clé privée de l'Autorité de Certification
- Dispositif de signature
- Vérification de la signature

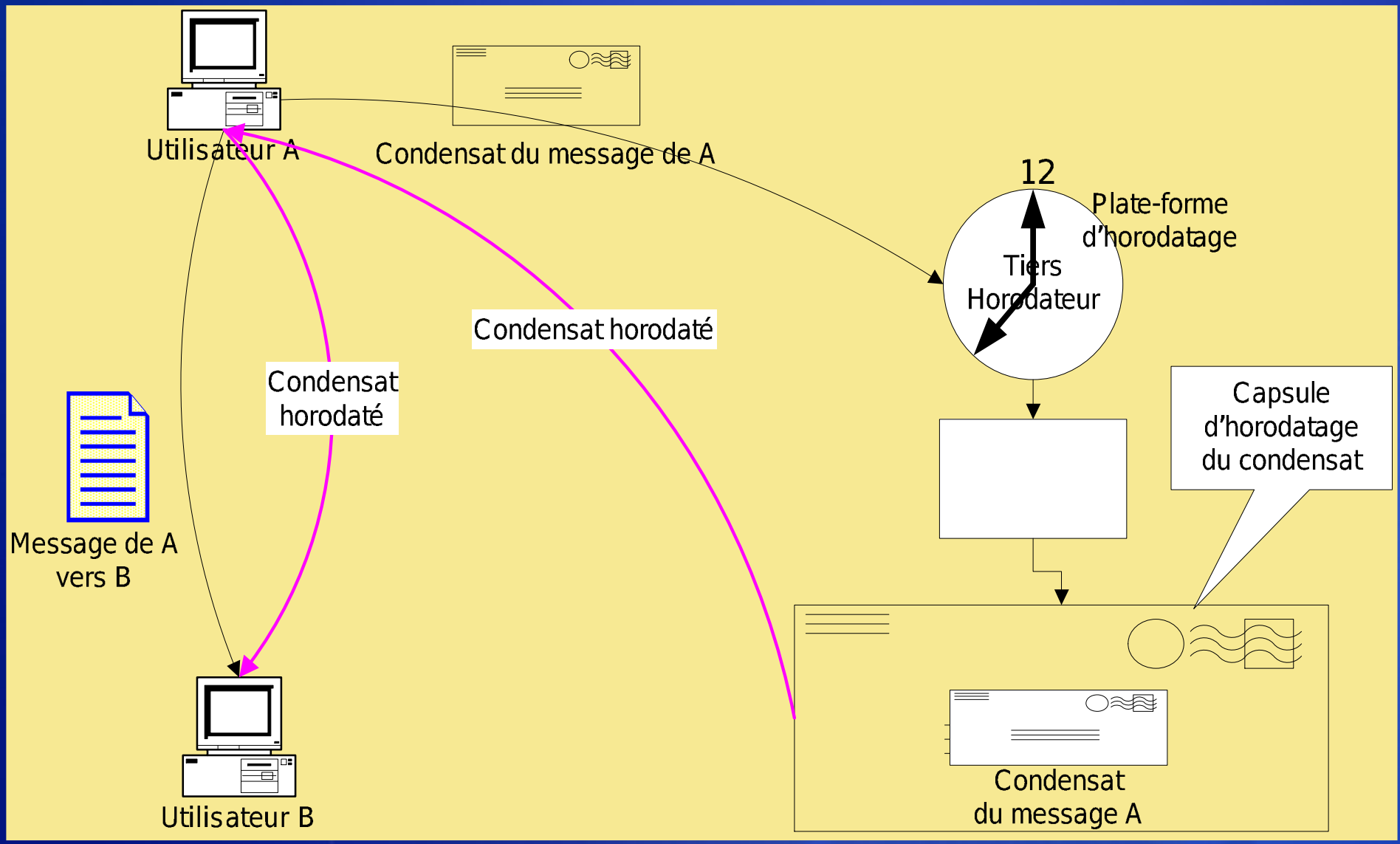
Les acteurs

- Autorité de Certification (AC)
- Autorité d'Enregistrement (AE)
- Centre de Publication (CP)
- Autorité de Validation (AV)
- Autorité de Recouvrement (AR)
- Autorité Horodatage (AH)

Horodatage, contremarque de temps

- Fournir la preuve de l'existence d'un message à un instant donné
- Horodateur neutre / opérations techniques
  - Aucun contrôle du contenu du message
  - Pas de contrôle du bien fondé de la requête

Principe de production



Contenu du jeton d'horodatage

- Politique d'horodatage utilisée
- Nom du tiers horodateur et son numéro authentification
- Marque de temps
- Empreinte du message à horodater
- Numéro de série unique
- Signature du tiers horodateur
- Diverses autres informations de service

Archivage électronique, scellement

- Garantir
  - L'intégrité dans le temps
  - La pérennité de l'information
- Comment ?

Les outils techniques

- Norme NF Z42-013 (évolution ISO 18509)
- Label FNTC de tiers archivage

Il s'agit de vérifier plus des procédures que des produits (cf notion de chaîne de traitement)

Label FNTC de tiers archivage

- Aspects techniques
  - Norme NF Z42-013
  - Notes techniques publiées par la FNTC
  - Réversibilité/interopérabilité
- Aspects juridiques
- Aspects assurance

Destiné aux tiers archiveurs et aux services équivalents internes aux organisations

4. Aspects légaux

Loi du 13 mars 2000 (Code civil) portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique.

- Art. 1316. - *La preuve littérale ou preuve par écrit résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.*

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

- Art. 1316-2. - *Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable quel qu'en soit le support.*

Aspects légaux, compléments

- Art. 1316-3. – *L'écrit sur support électronique a la même force probante que l'écrit sur support papier*
- Art. 1316-4. - *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.*
- Alinéa 2 : *Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.*

Exigence identification intégrité

- Identification de l'auteur, imputabilité de l'acte
- Le texte impose à la preuve littérale l'intégrité de l'acte dans tout son cycle de vie

La solution:

- Signature électronique (cf article 1316-4)

mais:

- Recours à des tiers qualifiés et utilisation de produits répondant à des normes publiées au JOCE du 17 juillet 2003
- Prévoir la possibilité de « re signer » périodiquement

Interprétation pour l'archivage

La loi vise bien la conservation des documents électroniques et impose des exigences :

- Intelligibilité: peu importe la forme de l'information, l'essentiel est qu'elle soit restituée de façon intelligible par l'homme et non par la machine
- Identification de l'auteur
- Garantie d'intégrité
- Pérennité: respecter les durées de conservation prescrites par les textes, fonction de la nature du document et des délais de prescriptions

Référence à l'horodatage

Le décret français ne réglemente pas le service d'horodatage

Il y fait toutefois allusion lorsqu'il exige d'un prestataire de certification électronique de :

- « veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision. » (Art 6 du décret).

5. Preuve, pas seulement

- Simplification des procédures
  - Plutôt que d'avoir à bâtir une convention, faire appel à un tiers
  - Déporte une partie de la responsabilité
- Aspect économique
  - Evident dans le cas d'une infrastructure PKI
- Une forme d'ASP

Merci pour votre attention

Questions - Réponses

Tél : +33 (0)6 07 58 81 17
jm.rietsch@fntc.org
www.fntc.org
www.fetc.net