# Horodatage Sécurisé

**J.M. Fourneau**

***Laboratoire PRiSM, CNRS UMR 8144***

***Université de Versailles St-Quentin***



## Horodatage Sécurisé

- Le service d'horodatage permet 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 un instant donné et d'autre part en la production, délivrance et conservation des éléments permettant d'attester l'évènement associé.
- Chaque contremarque émise par le service d'horodatage comprend une signature électronique de l'autorité d'horodatage (AH) afin d'en garantir l'intégrité et l'authenticité.
- Horodatage sécurisé = jeton d'horodatage sécurisé par signature numérique et une horloge fiable pour avoir l'heure.

## Contremarque de temps

- 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 chaine de caractères et une marque de temps.
- Chaine : empreinte numérique (128 ou 160 bits) d'une chaine quelconque de données obtenue par une fonction de hachage (SHA-1, MD5, RIPEMD-160).
- Marque de temps : 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.
- Référence du temps : Basé sur U.T.C. (temps donné par Greenwich).



## Pourquoi faire ?

- Eviter de forger un jeton d'horodatage (différence entre horodatage simple et horodatage sécurisé)
- Ne pas antidater les documents
- Prouver sa bonne foi

## Exemples

- Documents contractuels: banque, assurance : ne pas pouvoir modifier la date de la signature.
- Ordre de bourse: être sûr de la date d'achat ou de vente
- Médecine : datage des analyse
- Informatique : log (sécurité), mail (preuve)
- Archivage : Write Once Read Many (WORM). Mais attention à l'évolution des supports de stockage.



## Sources de temps

- Il existe une notion d'heure universelle et d'heure légale sur le territoire national (cf décret 78-855 du 9 aot 1978 et 79-896 du 17 octobre 1979 relatif à l'heure légale française (pas vu ici)).
- Du point de vue technologique, 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. L'intervalle est la mesure de temps en secondes qui sert de référence.
- La seconde est 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 (1ère résolution de la 13ème conférence générale des poids et mesures).
- On suppose ici que l'horloge est fiable.

## Protocoles de diffusion

- Pour distribuer date, heure, temps.
- L'IETF 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, (ajout d'authentification) STIME (Secure Network Time Protocol), est en cours d'étude.



## Horodatage

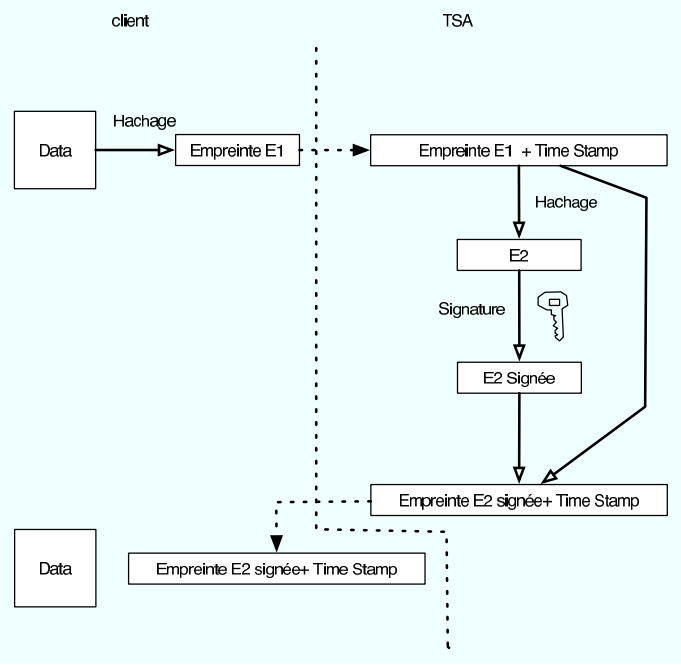
- L'horodatage certifié est spécifié dans le protocole IETF Internet X.509 Public Key Infrastructure (PKI) Time Stamp Protocol (TSP) d'aot 2001 (RFC 3161).
- La fonction d'horodatage (Time Stamping) est mise en oeuvre par un tiers certificateur spécifique qui peut fournir la preuve de l'existence d'un message à un instant déterminé : le tiers horodateur, (Time Stamping Authority, TSA).
- Le tiers horodateur est neutre vis-à-vis des opérations techniques. Il ne procède à aucun contrle 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 politique d'horodatage sous laquelle le demandeur souhaite obtenir son jeton.

## Réponse

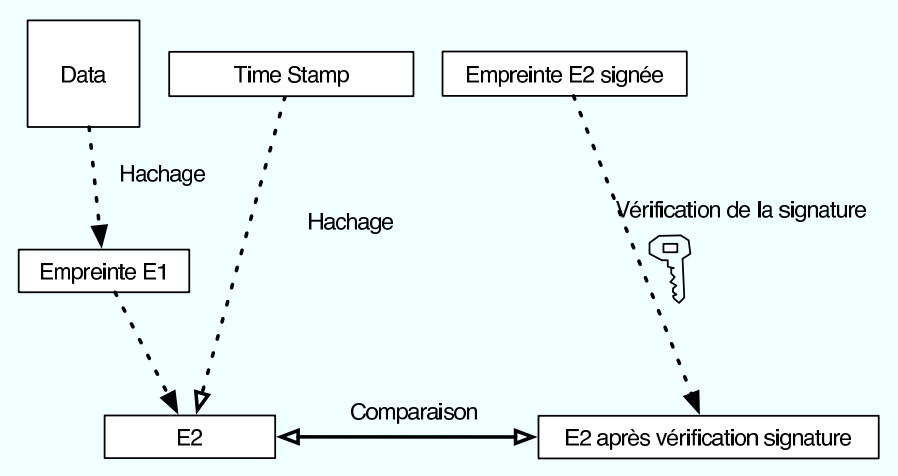
- Le tiers horodateur construit une réponse contenant les données de la requête et en particulier l'empreinte (le résumé)
- Il y rajoute une marque de temps ainsi que des données additionnelles dont l'identité du tiers horodateur et la politique sous laquelle il a produit le jeton.
- Le jeton est contenu dans la réponse sous la forme d'une structure CMS (Cryptographic Message Syntax) signée.



## Schéma d'horodatage



## Schéma de vérification






## Avantage

- Le client n'envoie qu'une empreinte pour obtenir un horodatage.
- Donc les informations confidentielles peuvent être horodatées sans être lues.
- Il est nécessaire d'avoir des fonctions de hachage à sens unique sûres.

## Inconvénients

- Fragilité des serveurs d'horodatage
- Compararaison des horloges pour comparer des horodates issues de serveurs différents.
- Comment avoir un totale confiance dans le serveur ?



## Des solutions

- Modèle de Liste/chainage
- Modèle Distribué
- Modele en Arbre

## Chainage

- Le TSA envoie $(n, ID_n$ pour répondre à une sollicitation du client.
- Le client retourne $H_n$ le résumé du message d'indice $n$.
- Le TSA récupère la date $t_n$ et construit un label $L_n$ à partir des informations précédentes

$$L_n = t_{n-1}, ID_{n-1}, H_{n-1}, H(L_{n-1})$$

- Le jeton est $S(n, t_n, H_n, ID_n, L_n)$.



## Avantage/Inconvénients

- On peut ajouter plusieurs chainages dans le jeton
- Difficile de modifier la date du jeton car on ne maitrise pas le flux de demande
- Vérification plus difficile
- besoin de moins de confiance dans le TSA.

## Distribution

- La demande d'horodatage est envoyé à plusieurs autorités.
- Algorithme:
  1. on tire au hasard $k$ autorités d'horodatage
  2. on envoie le résumé du document à chacune.
  3. le jeton est l'ensemble des réponses.



## Avantage/Inconvénients

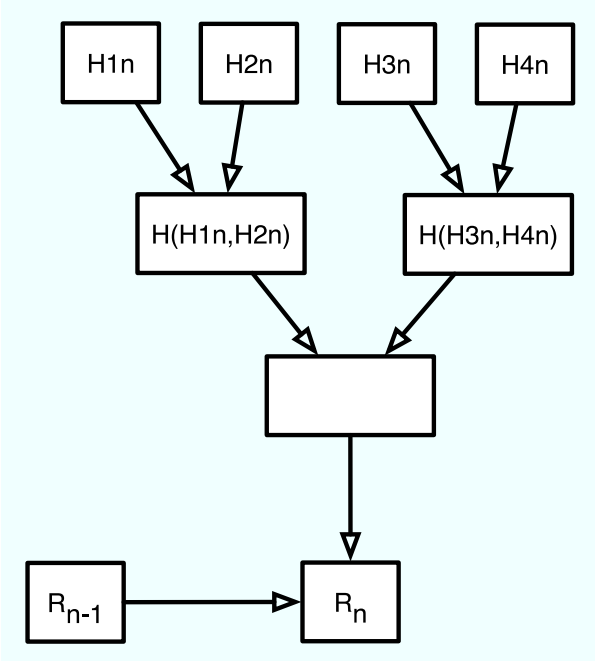
- Il est moins probable que les $k$ autorités soient compromises.
- La vérification est simple mais longue.

## Arbre Binaire

- Idées: on définit un tour.
- Toutes les demandes dans un tour sont combinées dans un arbre binaire.
- A chaque noeud de l'arbre on applique $H$ sur les feuilles pour produire $R_n$ à la racine.
- La vérification ne nécessite pas la sauvegarde de toutes les demandes du tour mais seulement d'une partie (en log).
- Seulement utile si il y a bcp de demande par tour.
- le jeton est constitué de la date, du chemin vers $R_n$, de $R_{n-1}$ et $R_n$.



## Arbre de Merkel



## Entités composant le TSA

- Le tiers horodateur peut impliquer 2 entités : l'autorité d'horodatage (AH) et l'opérateur de service d'horodatage (OSH).
- Le tiers horodateur a un engagement de continuité.
- AH : matrise d'ouvrage, responsable de l'émission des contremarques
- OSH : matrise d'oeuvre, émission techniques des contremarques.



## AH et OSH-1

- L'AH prend en charge l'ensemble du processus d'horodatage et est donc garante de la validité des contremarques de temps émises sous sa responsabilité.
- La garantie apportée par l'AH résulte de la qualité de la technologie mise en oeuvre, et de son engagement à un cadre réglementaire et contractuel.
- AH établit la politique d'horodatage.

## AH et OSH-2

- 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.
- 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.
- Première mission : protéger la clé
- Sa responsabilite ne peut être engagée que par l'AH. Elle est limitée au respect des procédures établies entre AH et OSH.
- L'OSH doit répondre aux exigences et aux spécifications énoncées par l'AH dans sa politique d'horodatage.



## Exemple tiers horodateur: déclaration des revenus

1. Absence complète de preuve Dépôt de la déclaration des revenus dans la bote à lettre de son Centre des Impôts. Aucune preuve de dépôt n'est fournie.
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.
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 (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.

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.