LATP

CHRONOS : CHRONOgraphie Sécurisée

Horodatage des documents électroniques

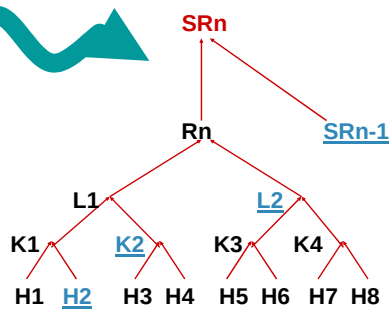
Principe

L'horodatage permet de certifier qu'un document a été créé à une certaine date et qu'il n'a pas été modifié depuis sa création.

Objectifs

1. Etude des systèmes d'horodatage existants
2. Concevoir des systèmes d'horodatage plus sécurisés

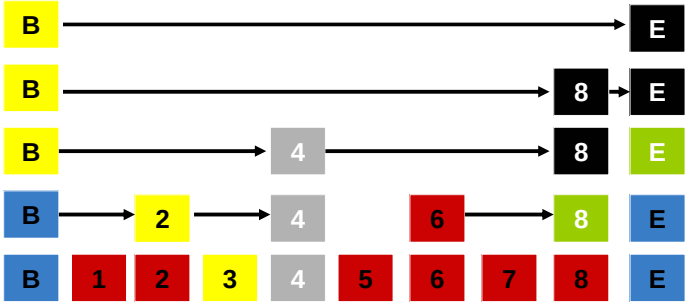
1. Modèles binaires : arbre de Merkle, schéma de liaison binaire, threaded trees…
   L'ordre de soumission des requêtes dans un tour ne peut être déterminé et le nombre de requêtes doit être une puissance de 2
2. Systèmes à accumulateurs
   L'ordre de soumission des requêtes dans un tour ne peut être déterminé et présence d'un "Trapdoor" cryptographique
3. Systèmes distribués
   La plupart en sont restés au stade de la conception ou ne tirent pas un réel avantage du caractère distribué du système



Systèmes centralisés

Principes

1. Utilisation des Skip Listes parfaites
2. Une requête appartient à un ou plusieurs niveaux
3. Une preuve est formée de deux parties:
   Une HeadProod est renvoyée immédiatement à la réception de la requête, et une TailProof est renvoyée ultérieurement.



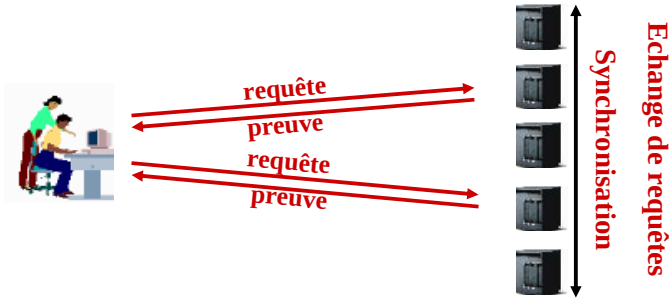
Avantages

1. Ordre de soumission des requêtes établi
2. Plus besoin de faire confiance à l'autorité
3. Pas de contraintes sur le nombre de requêtes
4. Pas de *Trapdoors*

Systèmes distribués

Principes

1. Le système est composé de *n* autorités
2. Une requête est traitée par *k* autorités
3. Un cachet global d'horodatage est calculé
   Le système opère par tours et les serveurs sont synchronisés
   Les requêtes sont accumulées pour former un cachet global



Avantages

1. Confiance dans le système global
   pas besoin de faire confiance à une autorité donnée
2. Pas de déni de service
   les requêtes sont envoyées à k autorités au lieu d'une seule

Contacts : Alban Gabillon, Kaouthar Blibech
E-mails : alban.gabillon@univ-pau.fr
k.blibech@etud.univ-pau.fr

ACI Sécurité Informatique CHRONOS (2003-2006)