EdelWeb
Peter SYLVESTER
Peter.sylvester@edelweb.fr

# IETF -LTANS

## Long Term Archive and Notary Service

## Travaux IETF : archivage et notarisation

EdelWeb

**Ossir 9 juilllet 2007**

© EdelWeb, 2007

# Ordre du jour

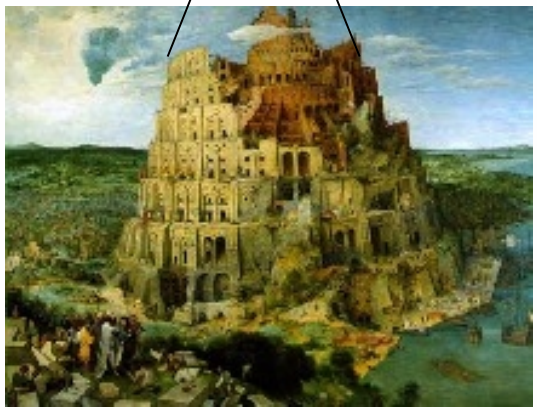
- Motivations et définitions
- Activités précédentes et autour
- Le groupe de travail LTANS
- Protocôle LTAP
- Les autres travaux du groupe

EdelWeb

© EdelWeb, 2007

# L’approche babylonienne

Signature éléctronique

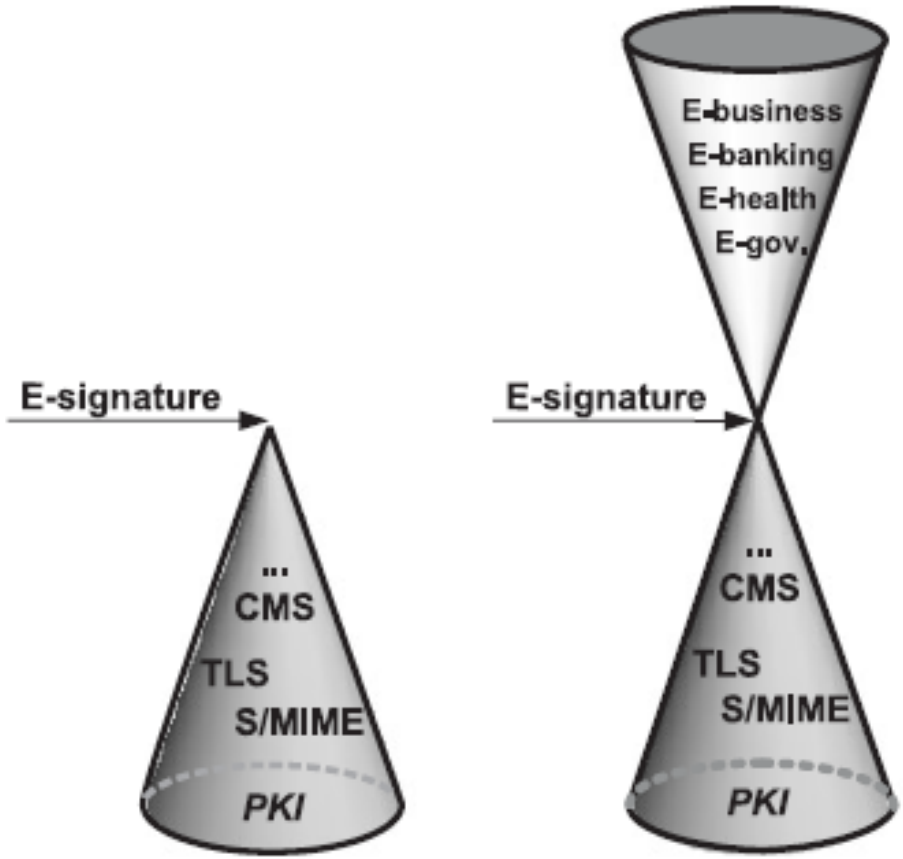


horodatage

EdelWeb

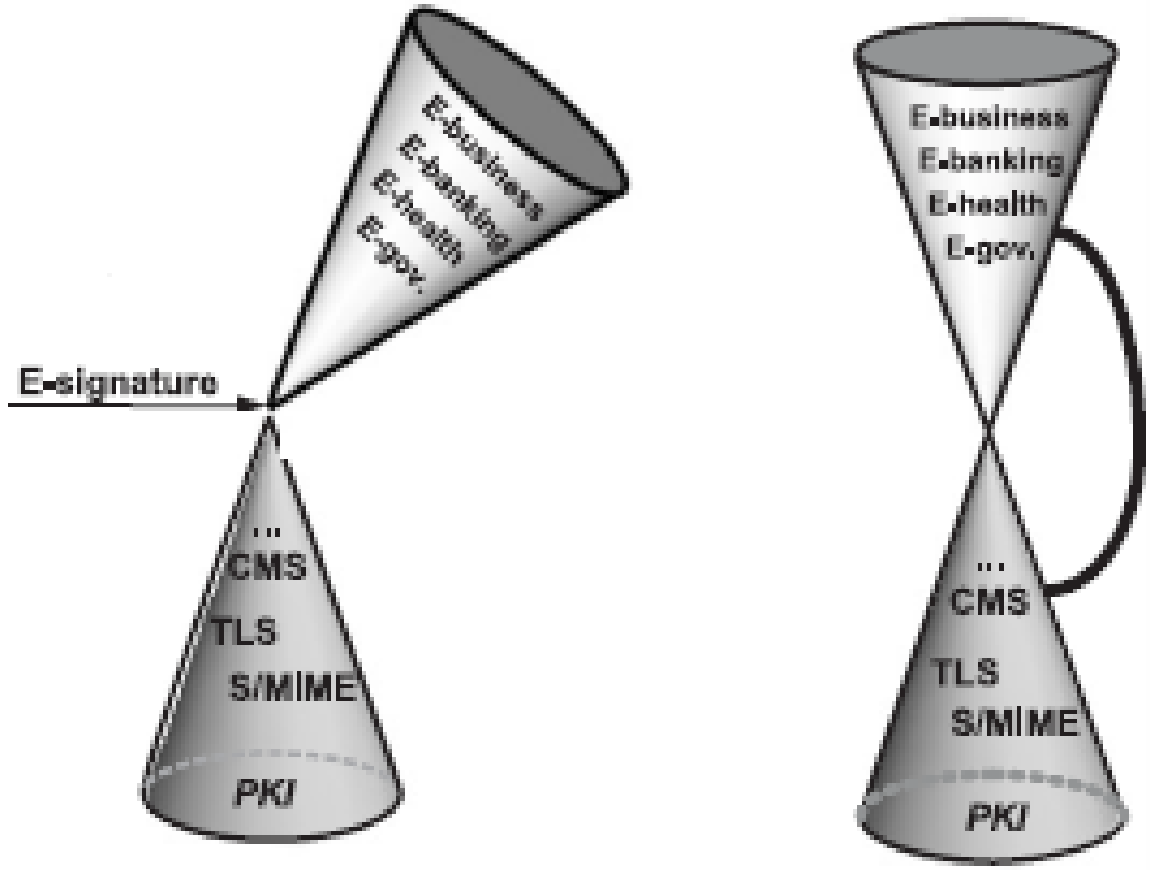
© EdelWeb, 2007

# Le cônes de Sylvester




*Copyright L. Dostalek, M. Vohnoutova*

# Les cônes ...




*Copyright L. Dostalek, M. Vohnoutova*

# Motivations

- **La conservation est essentielle pour la « valeur probante » document (son opposabilité).**
  - **Sans procédure de conservation un document n'existe pas dans plusieurs contextes législatifs.**
- **La conservation s'applique dans plusieurs contextes très différents**
  - **Enregistrements d'appels d'un opérateur tel.**
  - **Factures, documents fiscaux, …**
  - **Contrats, documents de propriétés**
  - **Biens culturels, archives historiques**

EdelWeb

© EdelWeb, 2007

# Contexte dématérialisation de documents

- **L'objet essentiel : le document**
  - **Question fondamentale : savoir si un document est « valable »**
    - **Pas si une signature est correcte, si un certificat est valide**
    - **Fondamental : apporter la possibilité de vérification**
    - **Conséquence : faire ce qui est nécessaire lors de la création**
- **L'objectif principal : apporter une version dématérialisée de chacun des éléments qui contribuent à la « valeur » du document**
    - **modèle de document dématérialisé**
    - **Infrastructures et procédures pour les « manipuler »**

EdelWeb

© EdelWeb, 2007

# Savoir traiter des documents

- de longue durée,
- liés au temps
- signés par des personnes autorisées
- dans le contexte d'une entreprise, d'un organisme, d'un service
- En respectant sa politique de confiance et sa politique de sécurité
  - Dans ses composantes légales et réglementaires comme contractuelles
  - Qui à le droit de signer ?
  - Quels contrôles sont effectués (à la création, à l'utilisation)?
  - Quelles archives sont conservées?
  - Quelles autorités/tiers externes sont reconnus?
  - …

EdelWeb

© EdelWeb, 2007

# Documents électroniques

- **La stabilité d'un document électronique dans le temps ne peut pas être assuré par une signature numérique seule.**
  - **Les signatures ont tendance à s'évaporer :-)**
  - **Les techniques d'horodatage utilisent des signatures**
- **La qualité du support est relativement faible**
  - **Cf. NASA les enregistrements de « voyager »**
  - **Bandes magnétiques des années 70-90**
- **Garantir la confidentialité est difficile**
  - **Le chiffrement n'est pas fait pour la durée**

EdelWeb

© EdelWeb, 2007

# L'archivage de documents

- La conservation n'est pas seulement le stockage de données brutes
- L'intégrité et dans certains cas la confidentialité sont importantes.
- La destruction doit être possible et effective, mais également l'archivage (historique) de très longue durée.
- Il faut prévoir un changement de support et de format de données.
- …

EdelWeb

© EdelWeb, 2007

# Quelques problèmes opérationnels

- **Cessation d'activité d'un prestataire de service**
  - Nécessité de copier des données
- **Changement de durée de conservation**
  - Litige ou intérêt (par exemple culturel) nécessite ou justifie une prolongation
- **Destruction complète**
  - … et les sauvegardes ?
- **Intégrité des archives**
  - pas de vrais faux insérés après coup,
  - Inversement, pas de suppression non-détectable
- **Stabilité de l'interface et de formats**
  - Mais évolutive

EdelWeb

© EdelWeb, 2007

# Activité précédentes

- **Projet OpenEvidence – 2002-2003**
  - **France, Estonie, Italie**
  - **Rep. tchèque, Slovénie, Autriche, Pologne**
- **Projet Archisig - 2003**
  - **Allemagne**
- **IETF: horodatage et notarisation**
  - **RFC 3161 (TSP) et RFC 3029 (DVCS) - 2001**
  - **Draft ATS (archive time stamp syntax) - 2003**
  - **Draft TAP (trusted archive protocol) - 2003**
- **Evidence d'un intérêt commun**
  - **PKIX n'est pas le groupe approprié**
  - **Nov. 2003 nouveau groupe de travail LTANS**

EdelWeb

© EdelWeb, 2007

# Activités autour du sujet

- **Nombreuses dans le contexte d'archivage « historique »**
  - **Ex. interpares**
- **Gestion d'archives**
  - **Ex. OAIS**
- **DGME avec les archives de France**

EdelWeb

© EdelWeb, 2007

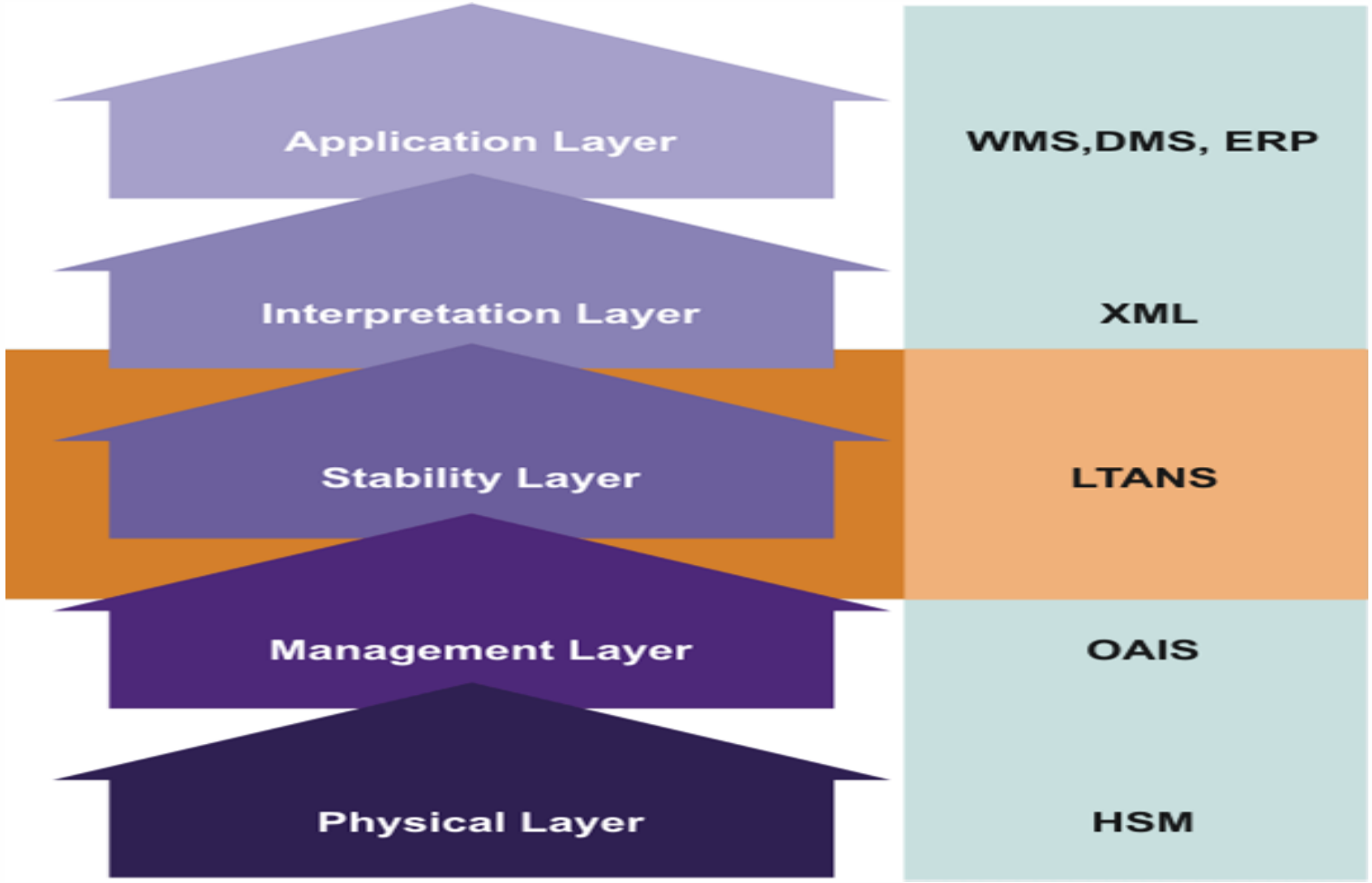
# Rappel IETF –Internet Engineering Task Force

- Une centaines de groupes de travail
- Organisés par domaine (area)
- LTANS dans le domaine de sécurité
- Sorte de « spin-off » de PKIX
- Outils de travail: messagerie, serveur Web, …
- Réunions de travail (3 par an)
- Acteurs LTANS:
  - Orion Security, IXOS, EdelWeb, SETCCE, FhG, DATEV, Adobe

EdelWeb

© EdelWeb, 2007

# La Cible de LTANS




EdelWeb

© EdelWeb, 2007

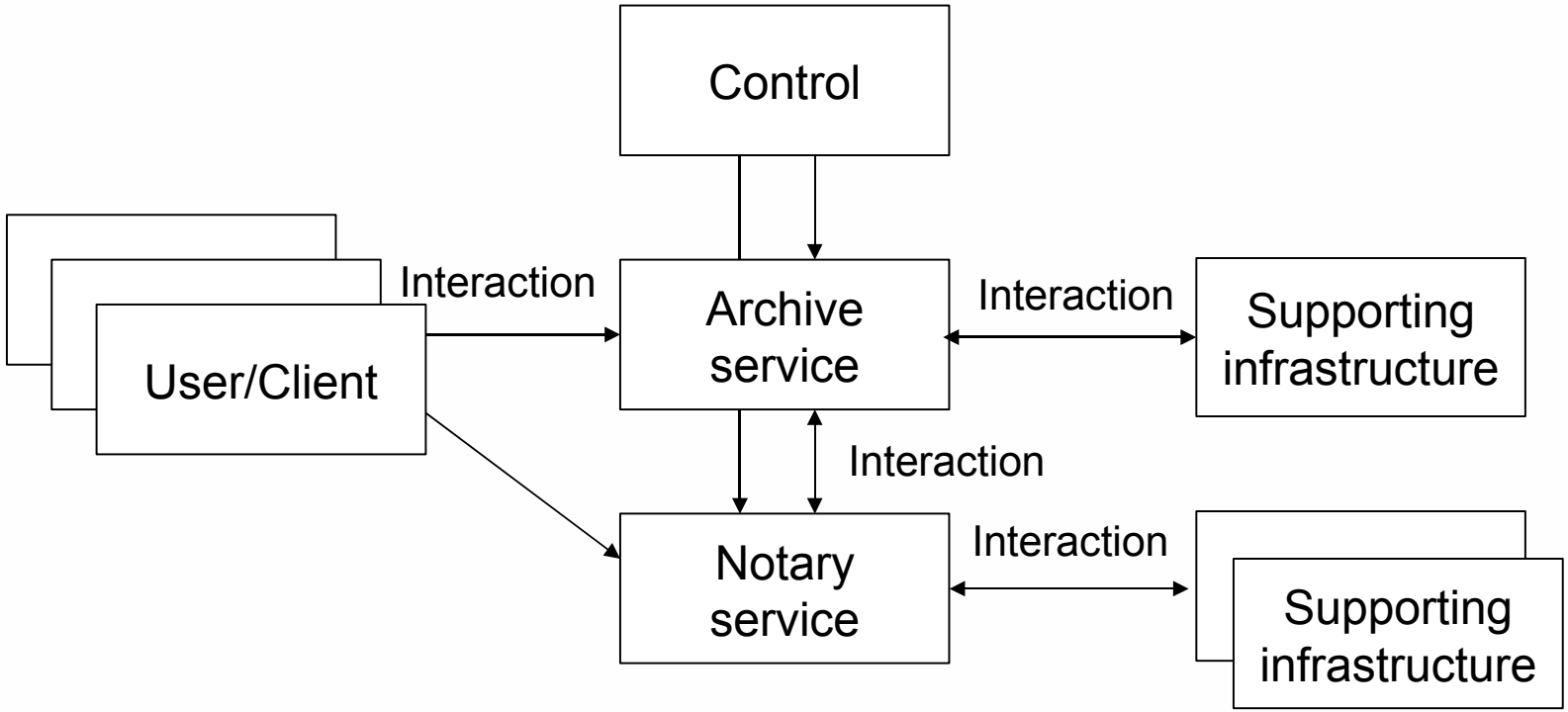
# Long Term Archive and Notary Service

- **Etape 1: l'archivage**
  - **Modèles et protocoles d'accès (LTAP)**
  - **Procédure de sécurisation d'objet (ERS)**
    - **attestations**
- **Etape 2: la notarisation**
  - **Besoins et scenarii**
  - **Protocoles (exemple DVCS amélioré)**

EdelWeb

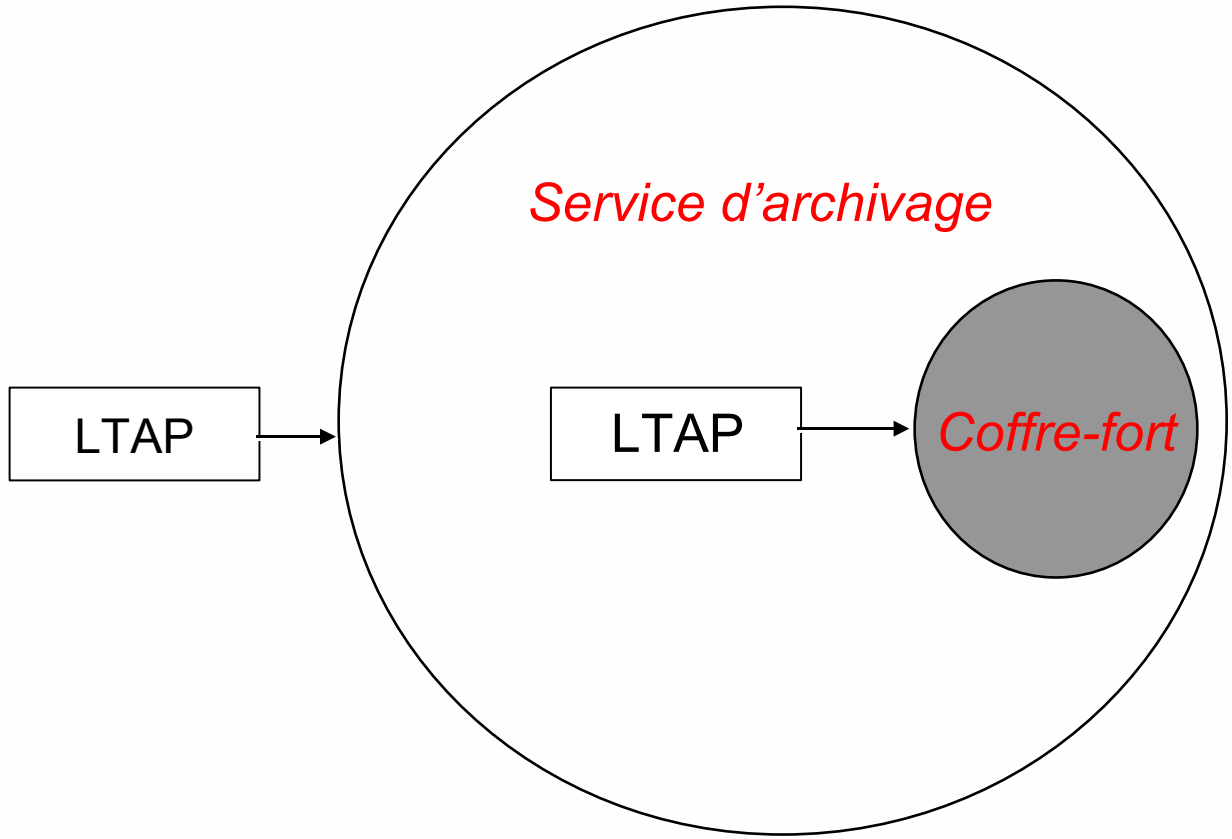
© EdelWeb, 2007

# Model de service LTAP




© EdelWeb, 2007

# Les onions LTAP, service et coffre-fort




EdelWeb

© EdelWeb, 2007

# Infrastructures de support

- Gestion de données et de clients
- Stockage
- Réseau de communication
- Mécanismes de sécurité
- Horodatage

EdelWeb

© EdelWeb, 2007

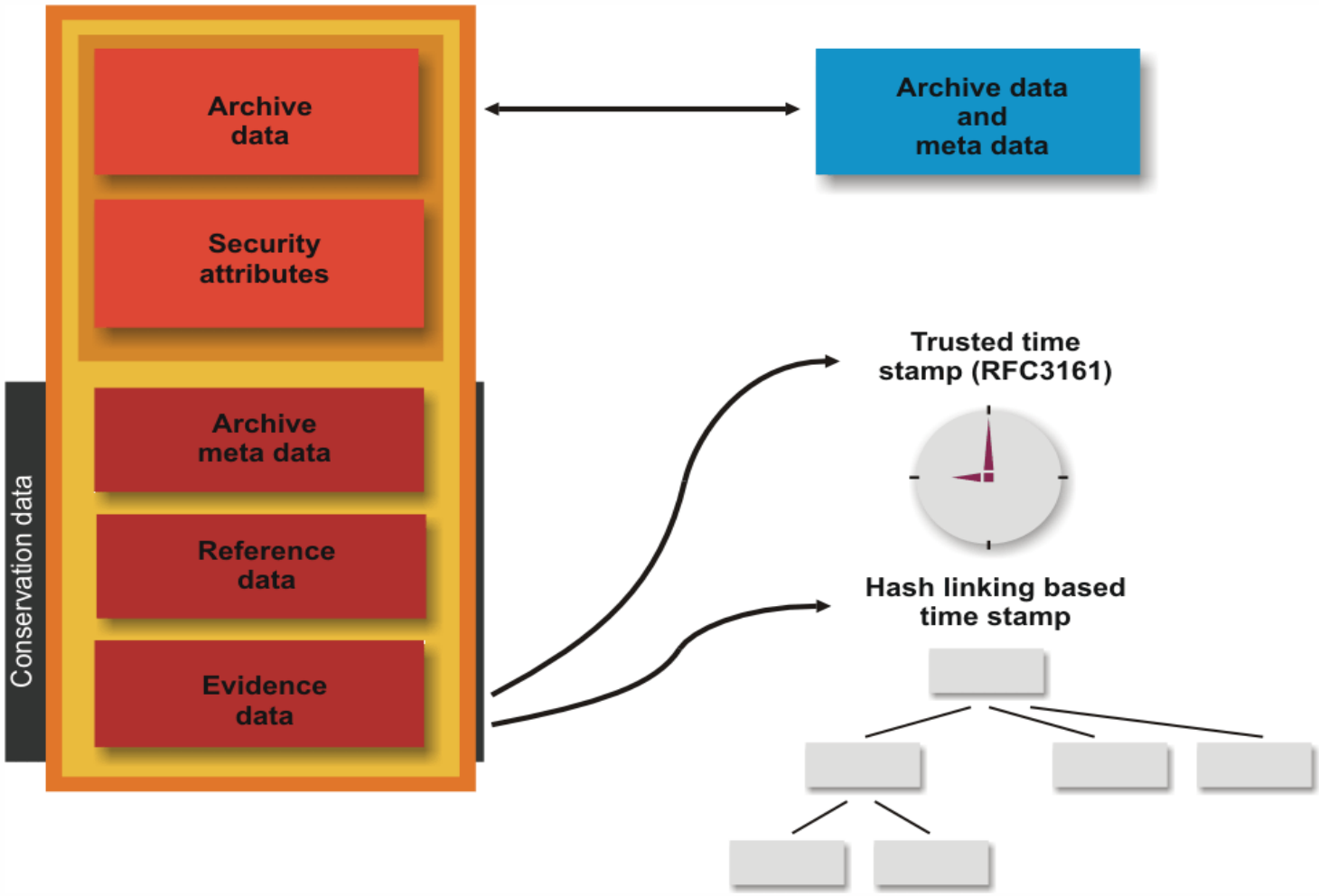
# Modèle d'objets

- **Données à archiver**
  - Les données
  - Metadata
  - Attributs de sécurité
- **Attributs de conservation**
  - Metadata de l'archive
  - Données de gestion
  - Eléments de preuves

EdelWeb

© EdelWeb, 2007

# Modèle d'objets




© EdelWeb, 2007

# Protocole d'accès

- **Des opérations simples**
  - ARCHIVE, EXPORT, DELETE
  - STATUS, VERIFY, LISTIDS
- **Des transactions asynchrones**
  - Envoi d'une requête
  - deux types acquittements
    - Acceptation technique d'une requête
    - Résultat final de l'opération
- **Plusieurs « bindings »**
  - HTTP, ASN.1 et XML, Webservices …
  - SMIME, XML-DSIG, XML-ENC
- **Relais et cascades de serveurs**
  - Frontaux de gestion d'utilisateur, contrôle d'accès
  - Répartition de données ou chiffrement

EdelWeb

© EdelWeb, 2007

# Les opérations

- ARCHIVE: soumettre des données
- EXPORT: transfert de donnée au demandeur
- DELETE: la destruction

- STATUS: enquête de l'état d'une opération
- VERIFY: demande de vérification d'intégrité
  - Ex. ajouter des jeton d'horodatage
- LISTIDS: liste des objets archivés

EdelWeb

© EdelWeb, 2007

# Etat LTAP

- **Draft-IEFT-LTANS-LTAP-05.txt**
  - **8 juillet 2007**
  - **« Last call « pendant l'été**

EdelWeb

© EdelWeb, 2007

# Evidence Record Syntax

- Issu du projet ArchiSig
- Metadata de conservation
- Element de preuves
- Une arborescence de « hash » et de jeton d'horodatage
- Possibilité de mise à jour et de vérification

EdelWeb

© EdelWeb, 2007

# L'étape 2 – la notarisation

- **À venir:**
  - **Document de besoins, scénarii « use cases »**
  - **Format d'attestation générique**
    - **Moi, le service XX atteste que votre document DDD du type YY à a bien été validé et/ou archivé dans les conditions suivantes …**
  - **La vérification ne nécessite pas l'archivage**
  - **L'opération ARCHIVE/VERIFY peut nécessité une attestation de validité**
  - **Très similaire au protocole DVCS**

EdelWeb

© EdelWeb, 2007

# LTANS organisation

- **Serveur Web:**
  - http://ltans.edelweb.fr
- **Mailing List:**
  - http://www.imc.org/ietf-ltans

EdelWeb

© EdelWeb, 2007