OpenEvidence

projet IST

technologies pour la valeur probante

Paul-André PAYS & Peter Sylvester – EdelWeb

pays@edelweb.fr - sylvester@edelweb.fr

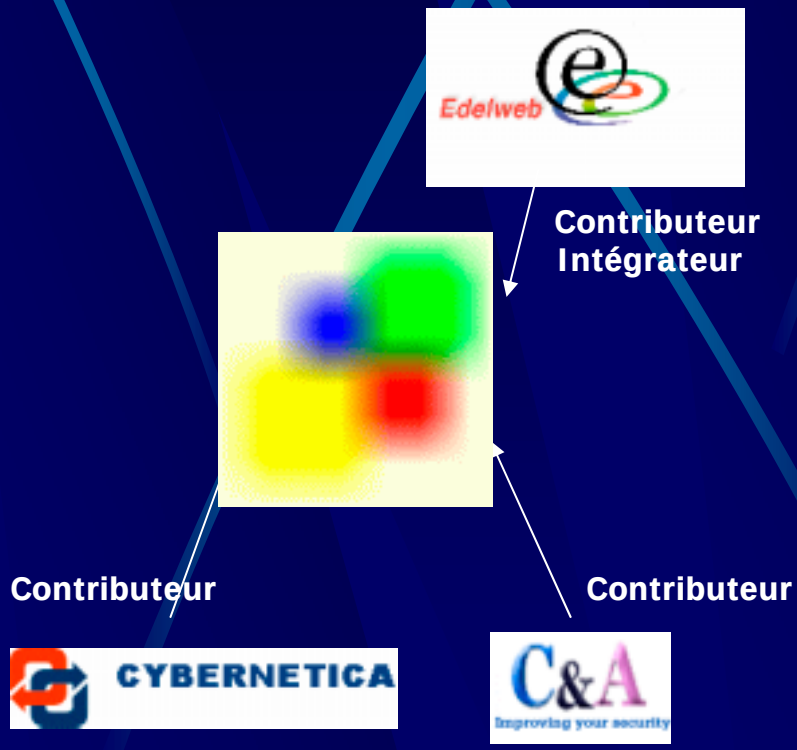
http://www.openevidence.org/

http://sourceforge.net/projects/openevidence/

Plan de l ’intervention

- **Contexte et objectifs**
  - **besoins de certification de documents et de leurs échanges**
  - **ensemble de techno et services de bases en OpenSource**
- **Approche - Modèle**
  - **service « guichet unique » de délivrance d ’attestations en ligne (et conservation des journaux sécurisés)**
  - **en frontal/intégrateur des services de tiers classiques que sont PKI, TSA et archiveurs**
- **Choix et réalisation**
  - **sur base logiciels libre (OpenSSL, Appache…) et protos existants**
  - **XML et CMS**
- **Retour de première expérience**

Les contributeurs



OpenEvidence : objectifs

- **DOMAINE**
  - valeur probante (opposabilité) des documents dématérialisés et de leurs échanges
- **OBJECTIFS**
  - développer et fournir les briques technologiques nécessaires
    - en complément de la signature numérique et des certificats
    - avec une approche très pragmatique
    - accompagné de modèles de services facilement implémentables
  - logique : logiciel libre - OpenSource

Le contexte OpenEvidence

- Disponibilité du contexte légal pour
  - la reconnaissance de la valeur de la signature électronique
  - la conservation de longue durée
- Modèle : services de tiers (de confiance)
  - pour la création, la validation et la conservation des éléments de preuve
- Techniques
  - horodatage, validation de signature, archivage, notarisation
- Problèmes
  - solutions propriétaires, concurrence, …
  - --> standardisation très très lente (des années!)
  - Limite des techniques courantes de la cryptographie pour la protection et la certification des documents

OpenEvidence : contexte

- De nombreux travaux sur authentification, autorisation, comptabilisation,
  - E.g. OASIS: SAML, W3C XMKS, IETF, AAA
- presque rien sur la « valeur » sur le long terme
  - IETF PKIX: data certification, time stamping
  - ISO, ETSI, CEN, X9 : time stamping
- comités vs vendeurs vs les véritables développeurs

OpenEvidence : approche

- **Combiner des prototypes et développements existants en une souche cohérente & « libre »**
  - **seule chance d ’éviter les multiples, incompatibles te coûteuses solutions propriétaires**
  - **opportunité majeure de mettre un sérieux coup d ’accélérateur à la « dématérialisation »**
- **sans guerre technologique**
  - **ni : XML contre ASN1**
  - **ni : archivage contre horodatage**
  - **ni signature contre « hash-linking »**
- **en utilisant le « savoir » de véritables développeurs**
  - **pas vraiment le cas des « standard bodies »**
  - **ni même toujours celui des éditeurs**

Le projet IST OpenEvidence

- Intégration de technologies pour
  - création et validation d ’éléments de preuve
  - Contexte : documents dématérialisés
  - valeur sur le long terme
- Technologies et standards complémentaires
  - RRFC 3029 (DVCS) , RFC 3161 (TSP)
  - Hash Linking Schemes pour l ’horodatage
    - surtout pour les « journaux » des tiers
- Validation par de l ’expérimentation en situation
  - service démonstrateur couplé à un service d ’archivage

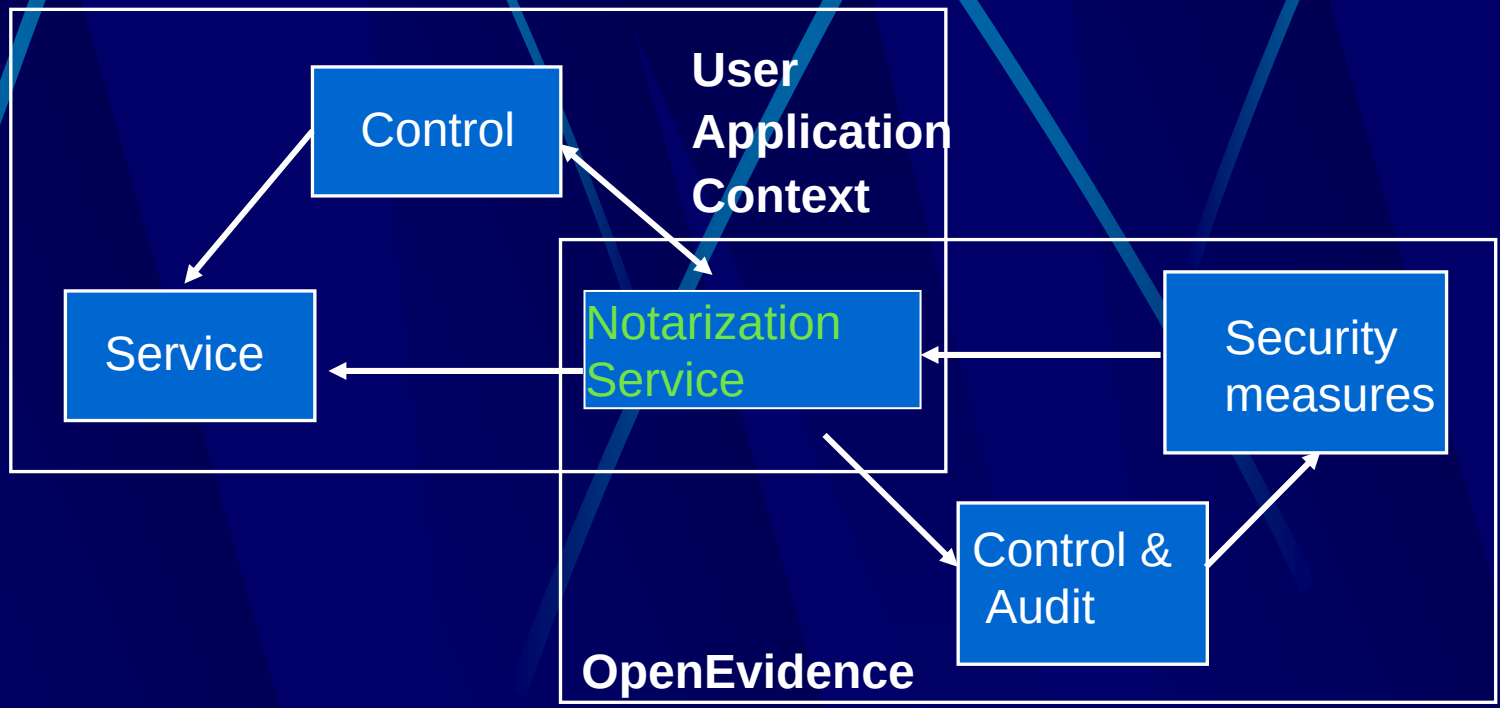
OpenEvidence : Livrables

- **Les logiciels « libres »**
  - **Client**
    - **gestion locale des documents et attestations, utilisation des services (tiers)**
  - **Serveur**
    - **TSAs, DVCS, journaux (registre) sécurisés en format standardisés**
    - **Création et validation d ’attestations (dématérialisées elles-mêmes)**
  - **Documentation**
  - ***Open-Source Community Support***
- **Expérimentation prévue à mi 2003**
  - **les fonctions de bases & la gestion d ’utilisateurs**
  - **le long terme (y compris cessation d ’activité d ’un tiers),**

OpenEvidence : bases

- **Clepsydre**
  - **http://clepsydre.edelweb.fr**
- **C&A time stamp authority**
  - http://www.com-and.com/products/TSA_test.html/
- **EdelWeb Demonstration TSA**
  - **http://timestamping.edelweb.fr/**
- **Cybernetica Cuculus project**
  - **http://www.cyber.ee/research/cuculus.html/**

Exemple de service : notarisation



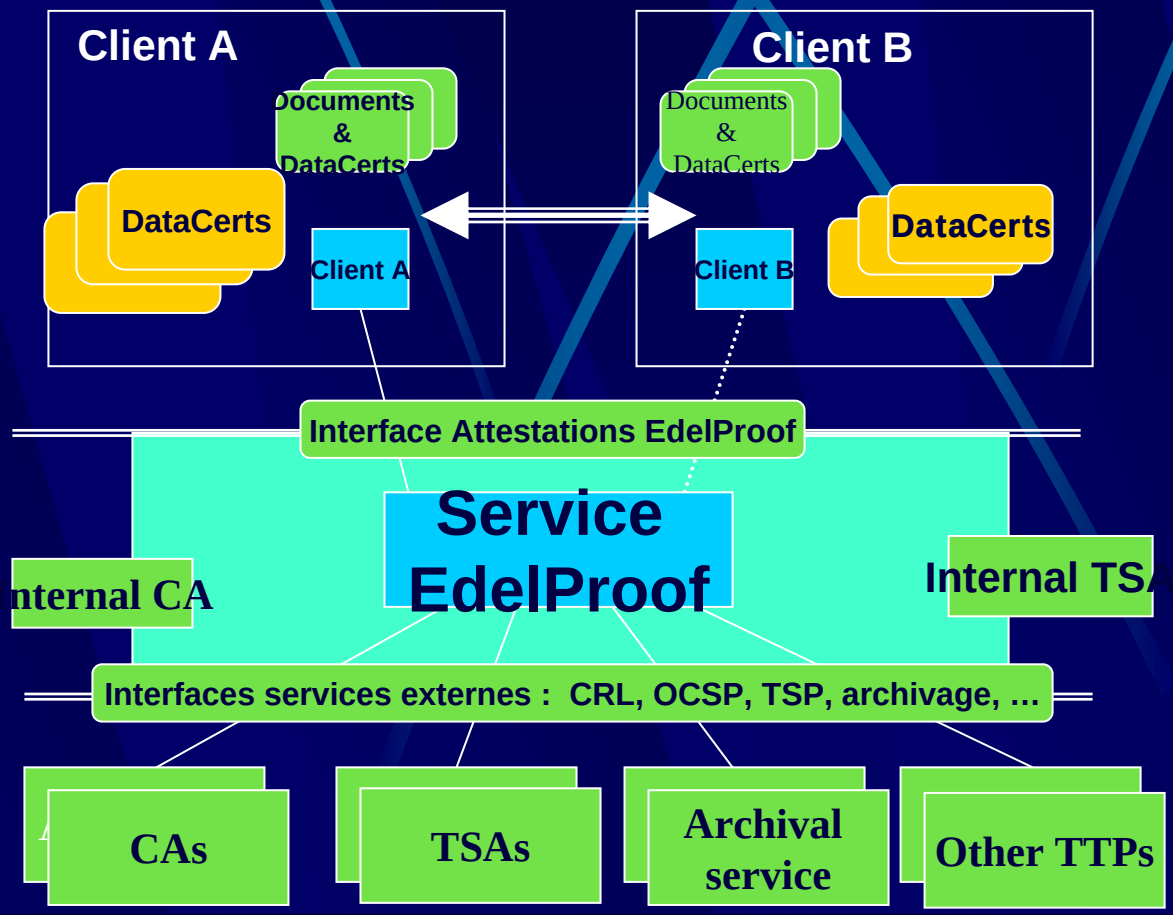
Journaux et Archives sécurisées

- Quasiment indispensable pour qu ’un service de ce type atteigne le niveau de sécurité voulu
- journalisation et archivage des attestations délivrées
  - jamais de destruction
  - chacune horodatée, mais le journal est sécurisé par du chaînage de condensat (hash linking)
  - Auditable facilement
- hiérarchies d ’utilisateurs pour refléter responsabilités et délégation de responsabilité
- en prévoyant une possible cessation d ’activité totale ou partielle
  - archivage pour une durée donnée limitée mais garantie

Les services possibles

- **Validation de certificats (avec RFC 3029)**
  - **pour certificats de signature**
  - **pour certificats de chiffrement**
- **Validation de documents signés**
  - **documents & assertions**
  - **Validation par deux services**
    - ***à la date indiquée***
    - **validation de la signature**
      - **et donc du certificat à la date donnée**
    - **et/ou par recherche dans les archives**
      - **journaux au minimum ou archives complètes**

Exemple d ’architecture service EdelProof



Aspects techniques

- **RFC 3029 et 3161, codage et crypto avec OpenSSL**
  - **CMS data-cert format**
- XML pour journal (schéma en ASN1)
- intégrité et transférabilité du journal
  - Archivage et horodatage du journal
- Implémentation par cgi + ssl de service de démonstration
- API + interface client ‘dossier=document+attestations’
- ...

Merci

- **Des critiques, des questions, des suggestions?**