Dématérialisation des documents Quelques éléments pour analyser et choisir une solution Illustration avec EdelSafe

Peter Sylvester / Paul-André Pays

EdelWeb

http://www.edelweb.fr/
ps@edelweb.fr / pays@edelweb.fr
tél : +33 (0) 154 561 940 - fax : +33 (0) 154 561 941

EDELWEB

Agenda

- Rappel signature numérique et certificat
- Contextes de dématérialisation
- Des Exigences et critères de choix
- Des Infrastructures (techniques et organisationnelles)
- Exemple d'une architecture: EdelSafe
- Exemple d'un service à valeur ajouté

Signature numérique et certificats

- **Signature : Mécanisme cryptographique pour assurer l'intégrité et l'authenticité de données**
- **Repose sur la cryptographie asymétrique (clé secrète / clé publique)**
- **Association entre clé publique et entité par des certificats**
  - **Infrastructure de gestion de clé / à clé publique (PKI, ICP)**
- **Origine: Contrôle d'accès X.500**
  - **PKI et application intégré**
- **Protection et certification de documents vs l'authentification**
- **Reconnaissance du mécanisme par la législation**

Le document formel

en contexte professionnel et/ou commercial

Identification de l'Entreprise (cf en bas)

Référence Entreprise

Date

Contenu

Signature 1

Cachet de l'entreprise

Signature 2 (visa, daté)

Complément identification entreprise (officiel, légal)

Infrastructure pour documents dématérialisés

- **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 »**
- **Savoir « traiter » des documents**
  - **de longue durée,**
  - **liés au temps**
  - **signé 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 externes sont reconnues**
      - ✓ **…**

Document ‘formel’ et durée de vie

- **La vérification d’une signature d’un document ancien est difficile**
  - **Un décret de Charlemagne**
  - **L’annuaire d’entreprise n’existe plus.**
  - **L’algorithme ou des clés peuvent être devenus ‘non sûrs’.**
- **Une approche classique :**
  - **Utiliser les services d’un tiers (lui-même ‘fiable’)**
  - **Combiner plusieurs mécanismes complémentaires**
    - **Ex: signature « fiable » + attestation et/ou dépôt légal**
    - **Ex: publication, …**

Exigences techniques

- **Formats normalisés**
  - **vs définition par l'outil de traitement**
- **Contexte professionnel (vs contexte personnel)**
  - **multiple signatures (+ tampon de l'entreprise)**
  - **documents datés**
  - **confidentialité sous contrôle de l'entreprise**
- **L'authenticité vérifiable longtemps après la création**
  - **Même après expiration des certificats**
- **Traçabilité 'fiable'**
  - **de la création de documents**
  - **voire même des vérifications déjà effectuées**
- **Tout autant que la simple 'fiabilité' de la signature**
  - **Fiabilité du certificateur, fiabilité du mécanisme utilisé**

Approche & Environnement

- **Sécurisation de documents vs sécurisation d'outils de traitement (ex: messagerie)**
- **Gestion de confiance centralisée (conforme à une politique et des procédures « entreprise » ou locale (choix individuels)**
- **Intégration simple avec des outils et formats standards, messagerie, web, traitement de fichiers, ...**
  - **par protocoles de communication**
- **Interfaces et formats de fichiers 'attestations' normalisés**
- **Délégation de taches au entités (serveurs) compétentes**
  - **Communication fiable par protocoles sécurisés**
  - **Utilisation d'enceintes de sécurité bien identifiés.**

Illustration : solution EdelSafe

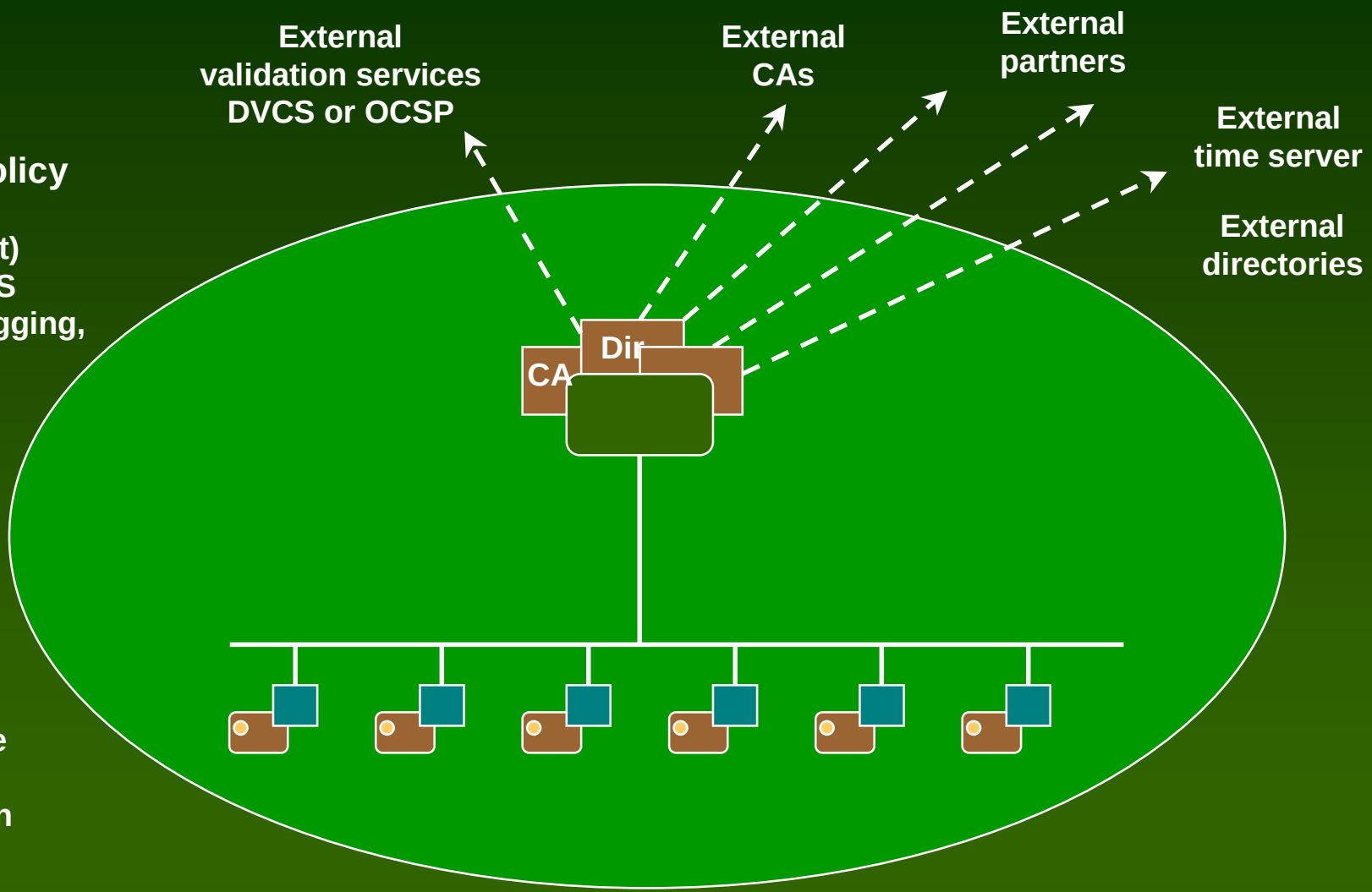
- ***À prendre comme une illustration d'une tentative de réponse aux exigences précédentes***
- **PRINCIPES**
  - **1 modèle de documents : CMS (cf S/MIME V3)**
  - **1 architecture répartie**
    - **Serveur de confiance et de sécurité**
      - ✓ **Sous le contrôle des responsables**
      - ✓ **Implémente la politique de sécurité et de confiance**
        - Offre des services internes (attestations, traces,…)
        - Relaie vers les services externes (CA, TSA, …)
    - **Clients : pour faire le travail demandé par les utilisateurs**
  - **1 forme unificatrice de dialogue : les attestations**
    - **Utilisables comme attributs CMS**
      - ✓ **authentifié («L'entreprise me donne le droit de signer sous cette politique avec ce certificat»)**
      - ✓ **non-authentifié (Contre Signature): «Ce document est conforme aux règles de l'entreprise»**
    - **Un protocole fédérateur : DVCS**
  - **1 trousseau de sécurité par entité**
    - **Bi-clés et certificats (signature & confidentialité)**
    - **Plus certificat du serveur de sécurité correspondant**

EdelSafe : architecture

EdelSafe Center

trust & security policy

- CA (int or ext)
- Directory (Int or Ext)
- other : OCSP, DVCS timestamping, logging, notary



EdelSafe Client

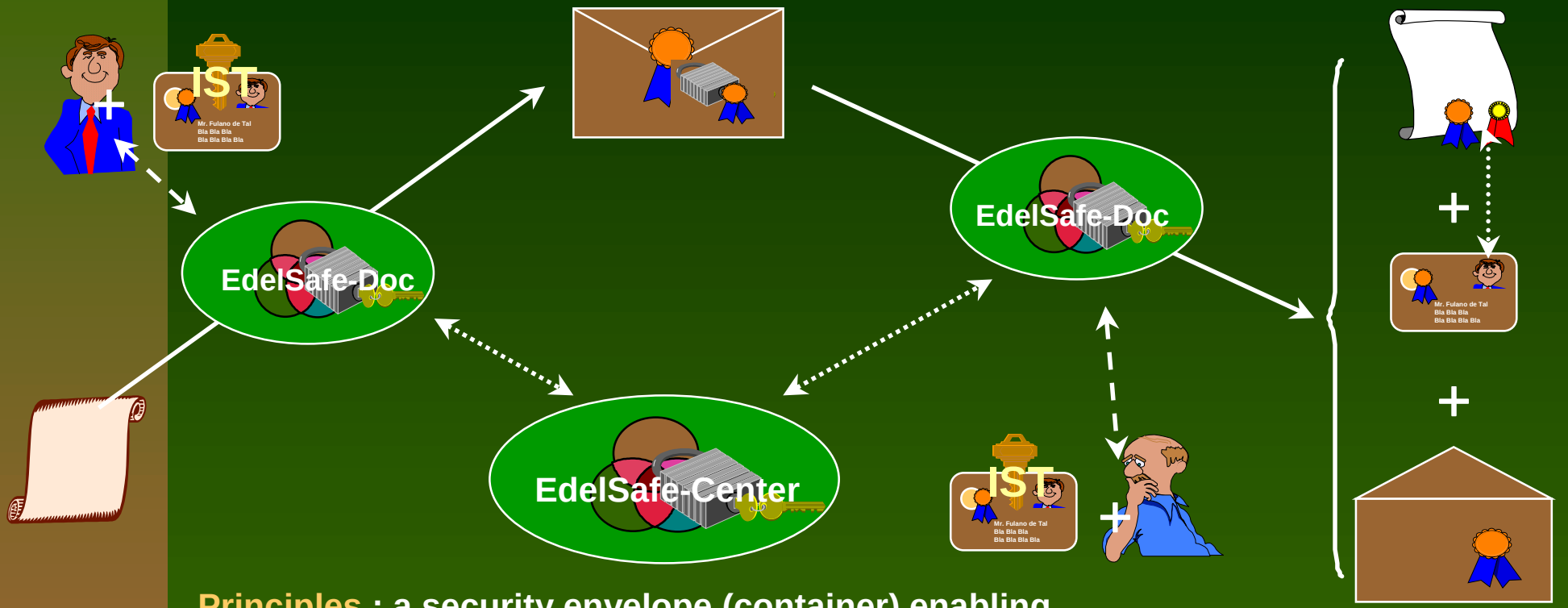
- signature + encryption code
- CMS handling
- Document validation

IST

Architecture - EdelSafe

- **Relais de requêtes vers d'autres services compétents (agréés / reconnus)**
  - **Le serveur devient client d'un serveur d'un autre organisme**
  - **Intégration par le serveur de 'la date/heure' officielle (celle reconnue)**
- **Intégration de services externes (OCSP, DVCS, Horodatage etc)**
- **Pas d'information cachée**
  - **La Réponse d'une validation d'un document contient tous les éléments qui ont été utilisés pour la décision.**
  - **Les mécanismes de validation sont évolutifs**
    - **Seul contrainte; Le résultat doit être représentable par un ensemble d'attestations: ex: certificats, références, dvcs, time stamps, pkistatus, ocsp responses, crl, ...**

EdelSafe Document



Principles : a security envelope (container) enabling

- **0, 1 or more certified & verifiable signatures**
  each with an "*allowed to sign* attestation"
  and a "certified date"
- **absolute confidentiality**
  only intended recipients are able to open it
- **add'al features**

Clepsydre

- **Clepsydre : un service d'horodatage et de preuve de possession**
  - **Version démonstrateur (actuellement)**
  - **conçu pour et avec La Poste par EdelWeb**
  - **Sur la base d'architecture EdelSafe**
  - **Service de délivrance d'attestations**
    - **Attestations (certificats de données) signées par Clepsydre/laPoste**
    - **Estampille horaire**
      - ✓ **Requête signée ou non**
    - **Preuve d'existence à une date donnée**
      - ✓ **Requête non signée**
    - **Preuve de possession à une date donnée**
      - ✓ **Requête signée**
  - **Architecture**
    - **Un serveur Clepsydre**
    - **Un logiciel client spécifique (disponible en download)**
    - **Un TIA pour chaque client enregistré**
  - ***http://clepsydre.edelweb.fr/***

Clepsydre - Utilisateurs

- **Enregistrement des utilisateurs**
  - **Soit en ligne, soit à partir de bases existantes**
  - **Donne lieu à la délivrance d'un TIA**
    - **Trousseau Individuel d'Accès au service**
      - ✓ **Protégé par un code confidentiel**
    - **Bi-clé « certificat de signature » d'utilisateur enregistré**
      - ✓ **Clé privée + certificat délivré par Clepsydre**
    - **Certificat du serveur Clepsydre**
      - ✓ **Contenant URL du serveur Clepsydre à utiliser**
      - ✓ **Permet d'être certain d'utiliser le vrai serveur**
    - **Permet l'authentification des utilisateurs**
      - ✓ **Accès au service, comptabilisation, etc.**
      - ✓ **Permet les attestations type preuve de possession**
    - **Très voisin du TIS de EdelSafe (mais sans le bi-clé confidentialité)**

Clepsydre - Attestations

- **Attestations DVCS**
  - **Signées et horodatées par le serveur Clepsydre**
    - **Avec un identifiant unique dans le temps (numéro de série)**
  - **Différents types**
    - **Preuve d'existence à un moment donné(= une estampille horaire)**
    - **Preuve de possession à un moment donné**
      - ✓ **Comprenant une identité vérifiée en plus du précédent**
    - **Pourrait être enrichi (preuve de dépôt, de publication, …)**
  - **La requête et l'attestation sont archivées par le serveur Clepsydre**
  - **Utilisables**
    - **Soit en tant que telles (documents à part entière))**
    - **Soit comme attributs dans un document CMS**
  - **Vérifiables**
    - **Signature**
    - **+ si besoin la vérification dans les archives Clepsydre**
    - ***Respecte les exigences ISO***