Gestion de la preuve pour les échanges dématérialisés

Problèmes, principes et technologies

-

Paul André PAYS
Olivier CHAPRON
Peter SYLVESTE

Mardi 11 mai 2004

EdelWeb

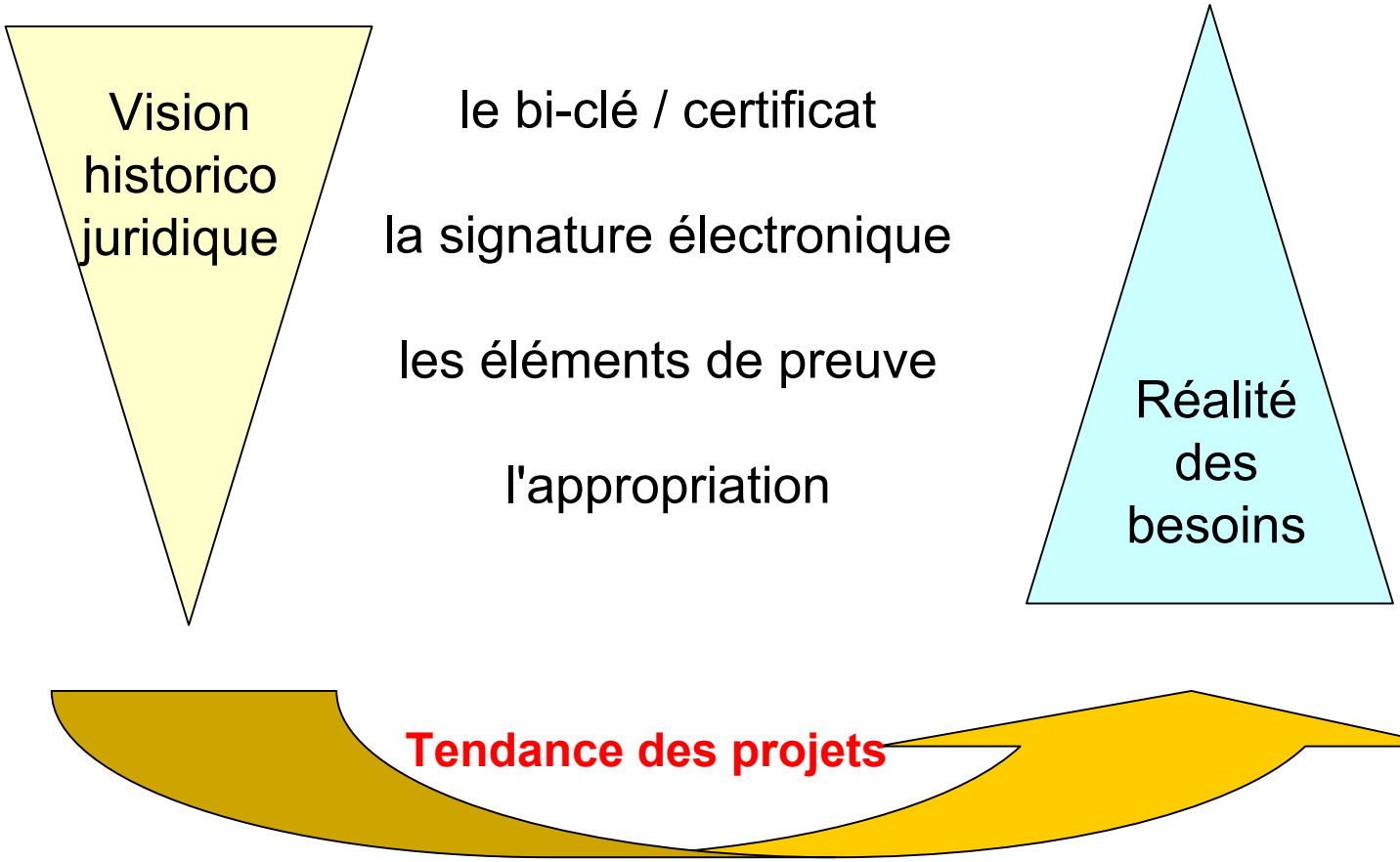
Agenda de la conférence

- Rappels de la problématique
- Gestion de la preuve
- Facteurs de succès
- Questions / Réponses

EdelWeb

Rappel de la problématique

Historiquement une mauvaise appréciation !



EdelWeb

Le contexte général dématérialisation

Signature numérique et dématérialisation
Le document formel en contexte professionnel

A Paris, le 4 mai 2004 → **Date**

→ **Identification de l'établisse**
(cf. en bas) sur papier à en

EdelWeb

Monsieur Xavier
Directeur xxx

Objet : Convocation
Réf : 3245/ADAE → **Référence Document**

Dans le cadre des travaux
sur les cartes électronique,
nous avons le plaisir de vous
faire parvenir ... → ***Contenu***

F.M. Arrouet,
Contrôleur

J.J. Rousseau,
Chef de service → **Nom et Titre du signataire**

→ **Cachet de l'établissement**

→ **Signature**

Société EdelWeb – RCS Nanterre *B 339 590 580*
Siret 00033 Code APE 721 Z → **Complément identification établissement (officiel, lég**

EdelWeb

Les éléments de la dématérialisation

- L'objet essentiel : **le document**

  La question posée : savoir si un ensemble de données est « valable » et "crédible« , donc si c'est la représentation d'un document.

- L'objectif principal : **apporter une version dématérialisée de chacun des éléments** qui contribuent à la « valeur » du document pour les 2 parties (émetteur et récepteur)

- Savoir **« traiter »** des documents
  - pour une longue durée,
  - avec des éléments liés au moment de création
  - signé par des personnes autorisées
  - dans un contexte défini :
    - composantes légales et réglementaires comme contractuelles,
    - droits à émettre/signer,
    - contrôles effectués (à la création, à l'utilisation),
    - d'archivage et notarisation, etc.

EdelWeb

Vers une dématérialisation sereine

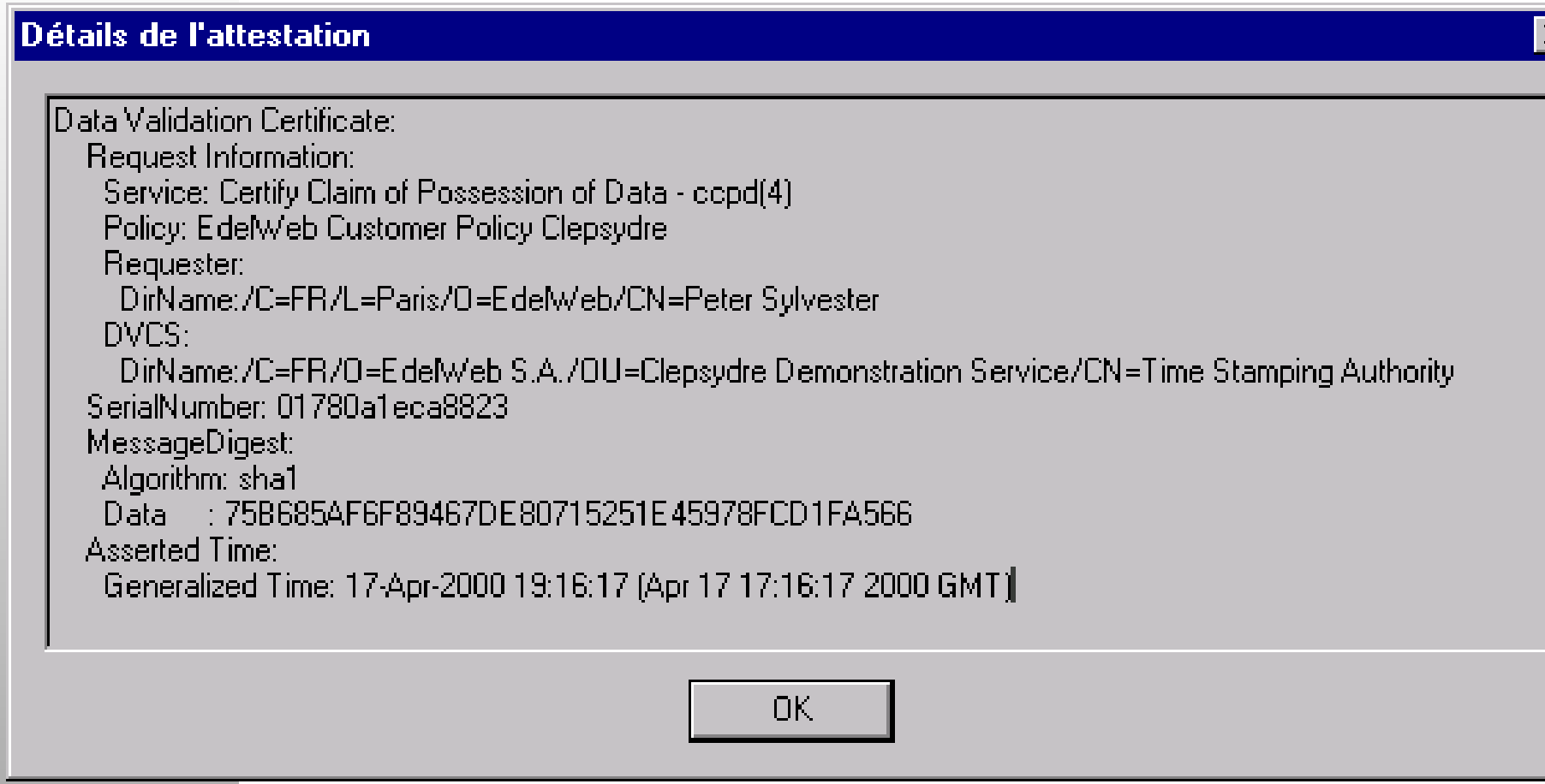
- prévoir les cas de contestation :
  - lever les ambiguïtés sur un document – écarter les mauvaises interprétations
  - limiter les malveillances

- préparer un faisceau d'éléments probants
  - pour au cas ou, pour dissuader de mauvais contentieux
  - dans la logique « *si vis pacem, para bellum* »

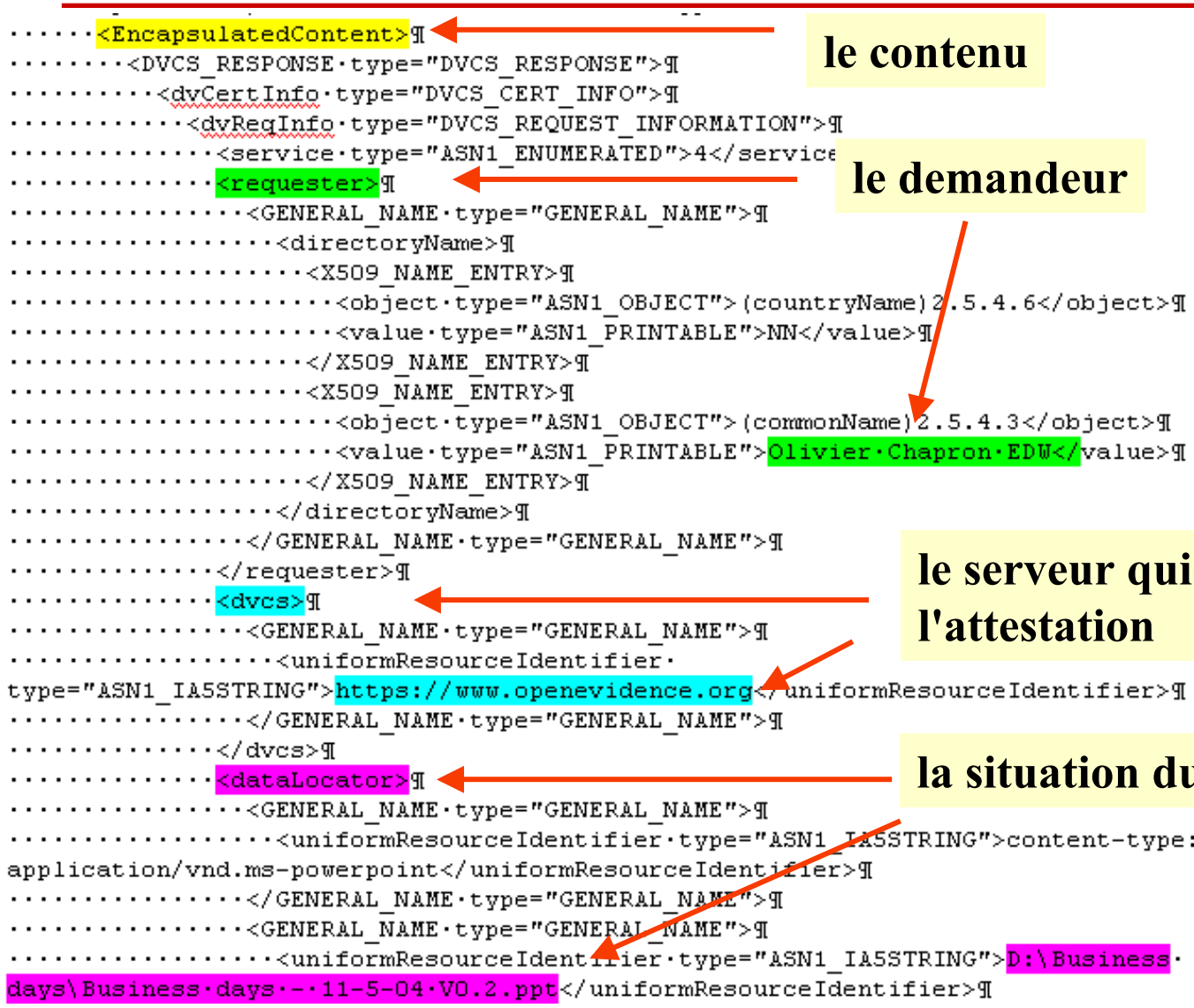
- pouvoir re-matérialiser un document et les éléments de preuve connexes (si nécessaire) :
  - bénéficier de l'expertise d'un « Peter Sylvester »
  - amener au juge ou la partie adverse des éléments :
    - sous forme d'une liasse papier
    - **Et** l'équivalent électronique sous forme d'un CD non réinscriptible
  - utiliser des techniques bien connus et/ou normalisées et libres

EdelWeb

Un exemple de contenu de visualisation d'une attestation



La version papier de l'attestation en XML (1/2)




```
<EncapsulatedContent>
<DVCS_RESPONSE type="DVCS_RESPONSE">
<dvCertInfo type="DVCS_CERT_INFO">
<dvReqInfo type="DVCS_REQUEST_INFORMATION">
<service type="ASN1_ENUMERATED">4</service
<requester>
<GENERAL_NAME type="GENERAL_NAME">
<directoryName>
<X509_NAME_ENTRY>
<object type="ASN1_OBJECT">(countryName)2.5.4.6</object>
<value type="ASN1_PRINTABLE">NN</value>
</X509_NAME_ENTRY>
<X509_NAME_ENTRY>
<object type="ASN1_OBJECT">(commonName)2.5.4.3</object>
<value type="ASN1_PRINTABLE">Olivier Chapron EDW</value>
</X509_NAME_ENTRY>
</directoryName>
</GENERAL_NAME type="GENERAL_NAME">
</requester>
<dvcs>
<GENERAL_NAME type="GENERAL_NAME">
<uniformResourceIdentifier
type="ASN1_IA5STRING">https://www.openevidence.org</uniformResourceIdentifier>
</GENERAL_NAME type="GENERAL_NAME">
</dvcs>
<dataLocator>
<GENERAL_NAME type="GENERAL_NAME">
<uniformResourceIdentifier type="ASN1_IA5STRING">content-type:
application/vnd.ms-powerpoint</uniformResourceIdentifier>
</GENERAL_NAME type="GENERAL_NAME">
<GENERAL_NAME type="GENERAL_NAME">
<uniformResourceIdentifier type="ASN1_IA5STRING">D:\Business
days\Business days - 11-5-04 V0.2.ppt</uniformResourceIdentifier>
```

La version papier de l'attestation en XML (2/2)

Les éléments relatifs à l'attestation

```
··············<hashAlgorithm·type="X509_ALGOR">¶
···············<algorithm·type="ASN1_OBJECT">(sh…m>¶
···············<parameter·type="NULL"·/>¶
··············</hashAlgorithm>¶
··············<hashedMessage·
type="ASN1_OCTET_STRING">3c:c8:44:53:09:1a:50:d9:f7:74:1a:f8:ea:09:63:ef:e0:bb:0
c:1d</hashedMessage>¶
·············</messageImprint>¶
·············<serialNumber·type="ASN1_INTEGER">25619718233791151</serialNumber>¶
·············<respTime·type="DVCS_TIME">¶
··············<genTime·type="ASN1_GENERALIZEDTIME">May··6·14:07:14·2004·
GMT</genTime>¶
·············</respTime·type="DVCS_TIME">¶
·············<policy·type="POLICYINFO">¶
··············<policyid·type="ASN1_OBJECT">(EdelWeb·OpenEvidence·DVCS·Demo·
Policy)1.3.6.1.4.1.5309.1.2.3</policyid>¶
·············</policy>¶
···········</dvCertInfo>¶
·········</DVCS_RESPONSE·type="DVCS_RESPONSE">¶
·····</EncapsulatedContent>¶
····</contents>¶
····<cert>¶
·····<X509>¶
·········<cert_info·type="X509_CINF">¶
···········<version·type="ASN1_INTEGER">2</version>¶
···········<serialNumber·type="ASN1_INTEGER">10438500460942</serialNumber>¶
···········<signature·type="X509_ALGOR">¶
```

le numéro de série

la date de fabrication

la politique de référence

etc.

La gestion de la preuve

Quelle contestation potentielle ?

l'élaboration du document :
- le ou les signataires,
- la signature elle-même
- la date
- l'origine,
- l'intégrité ETC.

les échanges :
- le document existait à T0 ?
- X était en possession à T1 ?
- Y avait déposé le document à T2 ?
- Z avait retiré le doc; à T3 ? ETC.

Au delà de la signature ..... et du certificat

On doit bénéficier des éléments suivants :

Techniquement

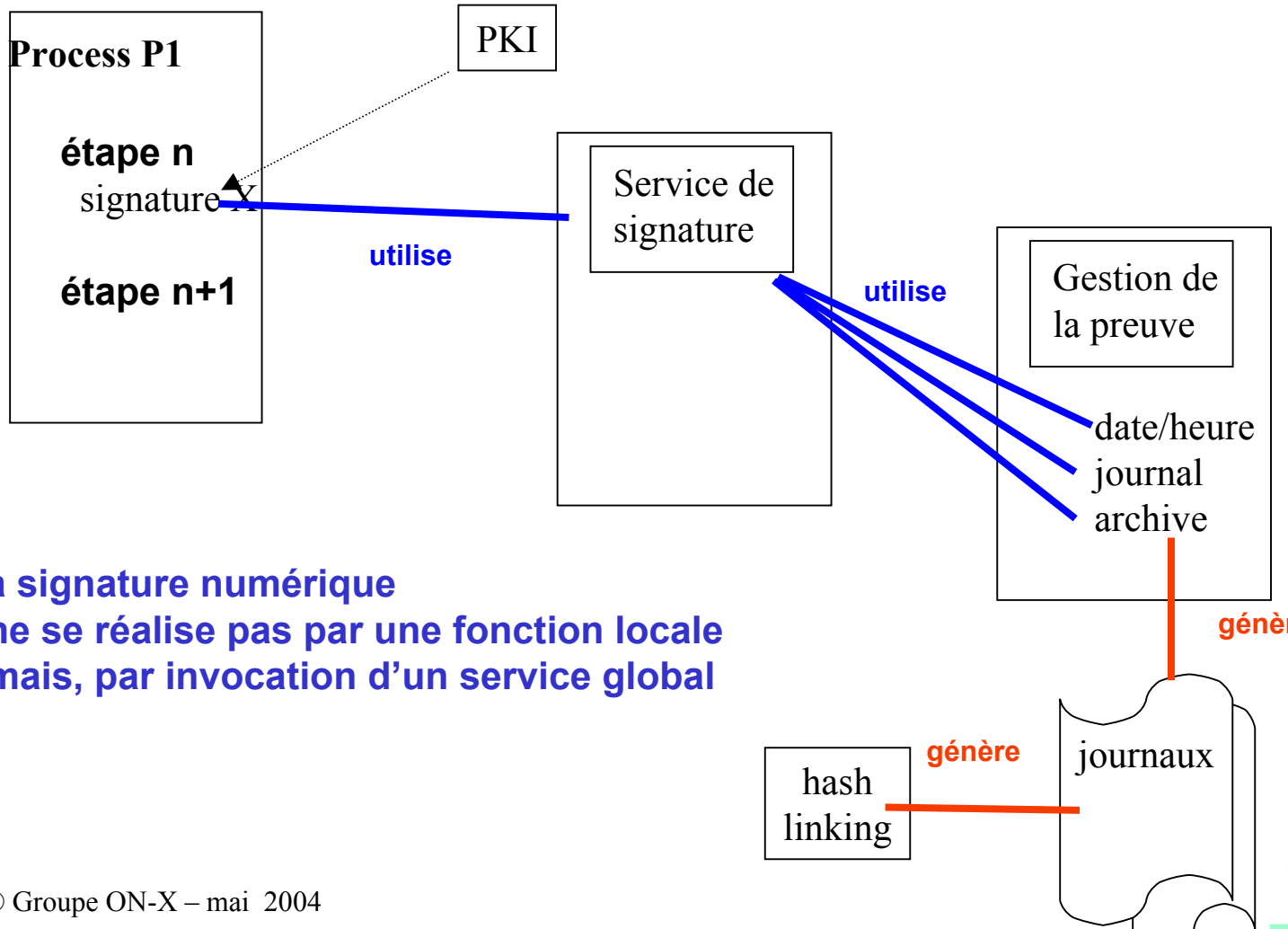
- une date fiable
- un archivage "de confiance"
- des attestations
- des journaux "certifiés", permettant de démontrer à posteriori que rien n'y a été ajouté ou enlevé
- la possibilité de retrouver et d'extraire les éléments "probants"

Sur le plan de l'organisation

- une "séparation des pouvoirs" (ex. archivage)
- l'utilisation d'une "notarisation" pour simplifier les procédures de vérification
- des règles d'applications incontournables !

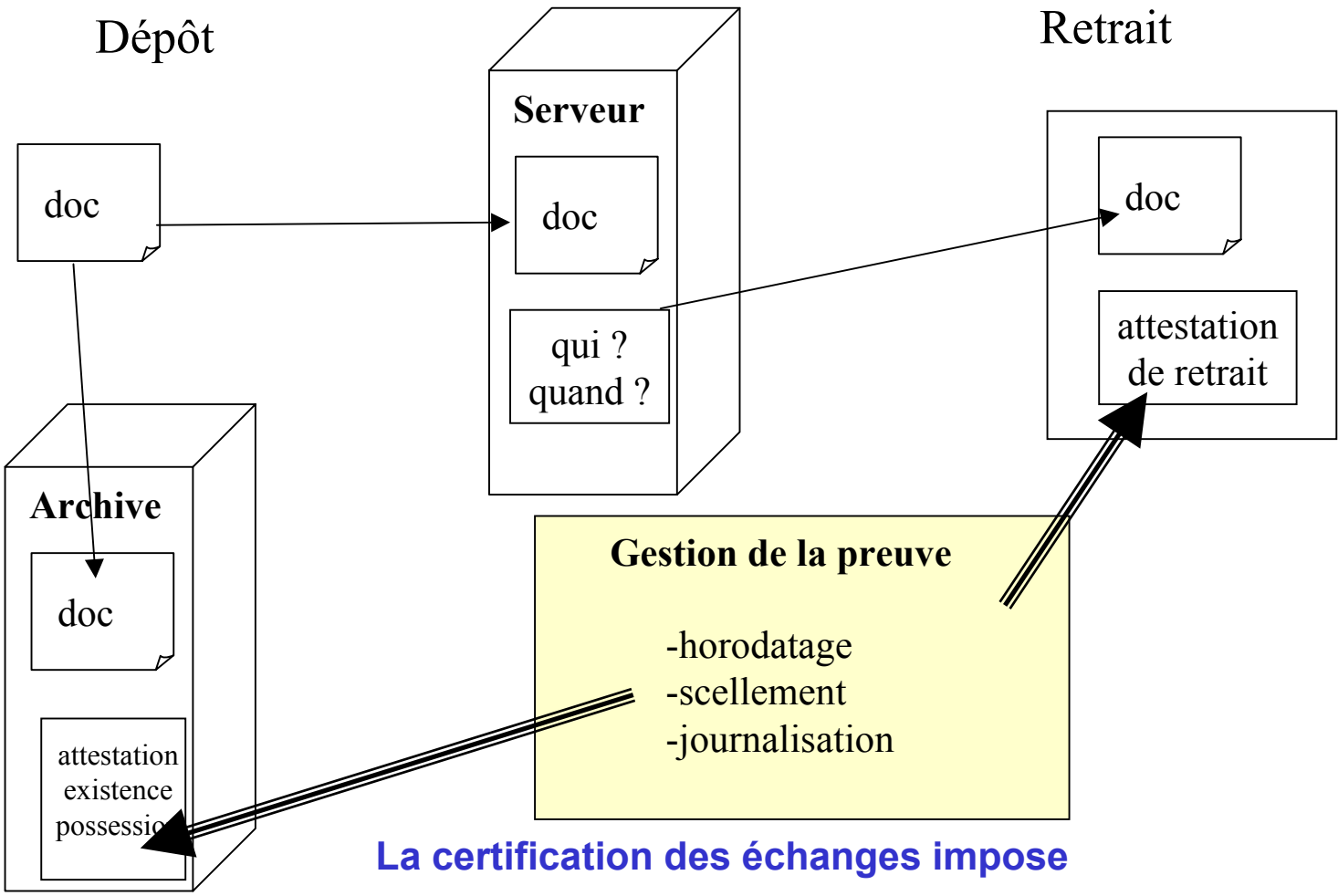
EdelWeb

Exemple d'une signature



La signature numérique
- **ne se réalise pas par une fonction locale**
- **mais, par invocation d'un service global**

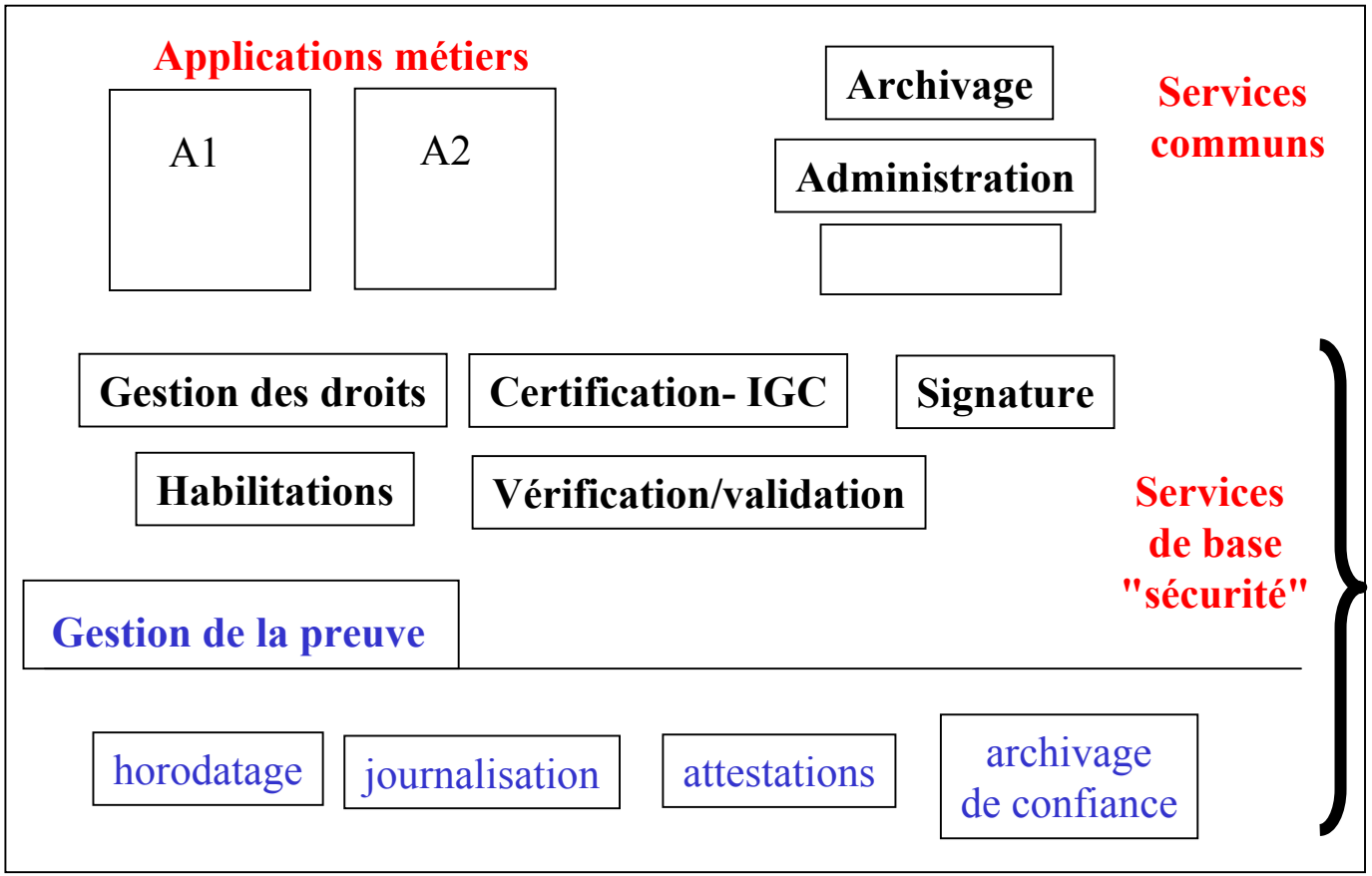
Exemple d'une remise certifiée



La certification des échanges impose

- **la génération et remise d'attestations**
- **la notarisation des journaux (scellement et archivage)**

La mise en œuvre : urbanisation du SI



Urbanisation du système d'information

Les technologies open-sources

- Tool-kit cryptographiques basiques :
  - Open SSL (C & C++)
  - Bouncy-castle (java)
  - OpenEvidence (C basé sur Open SSL)
  - autres ….

Un exemple de contexte européen :
http://www.openevidence.org

EdelWeb

Comment réussir un projet de dématérialisation

La démarche recommandée

- Lors de l'étude préalable, il convient de partir de la preuve (et pas de fonctions techniques):
  - cela couvre les véritables besoins fonctionnels
  - c'est l'objectif ultime,
  - cela impose à partir de ce point de départ de se poser la question et de fixer la politique de la preuve, celle de signature, celle de la politique de certification, celle des traces, celle de la conservation. avant de concevoir et mettre en place l'organisation et les moyens nécessaire
  - ce qui précède impose également d'impliquer vos « juristes » dans le processus au bon moment

- Un des résultats : la GdP
  - la conception d'une organisation et des moyens permettant de fournir des services de gestion de la preuve, qui devront être utilisés par l'ensemble des applications

EdelWeb

Les facteurs clé de succès

- les briques de base permettant de constituer des éléments de preuve :
  - signature électronique (humaine et sceau de l'organisme).
  - attestation,
  - horodatage,
  - hash-linking
  - stockage sécurisé (redondance, etc.)

- une organisation de ces briques au sein du SI pour offrir ces services de gestion de la preuve
  - Et (miracle!) au passage l'ensemble des fonctions nécessaires à la dématérialisation (maîtrisée)

- l'appropriation par l'ensemble des acteurs :
  - les responsables concepteurs/architectes/développeurs d'applications
  - les utilisateurs finaux.

EdelWeb

La check-list avant décollage

- études amont sur les flux :
  - qui, quand, comment sont réalisés/manipulés les documents en interne à l'organisme
  - Comment ils seront échangés avec des tiers
- communication auprès des développeurs d'application :
  - concept de certification, signature, gestion de la preuve
  - intégration dans les projets
- information des destinataires :
  - Politique de certification, Politique de signature, Politique de Preuve
- infrastructures et techniques mises en place :
  - Workflow incluant les appels au service GdP
  - IGC, horodatage, Infrastructure de sauvegarde, etc.
  - techniques :
    - délivrances d'attestations,
    - sauvegardes "intelligentes" (hash-linking),
    - outil d'administration

EdelWeb

Coordonnées des intervenants

- Paul André Pays – Directeur Pôle Sécurité
  - 01 40 99 14 14
  - paul-andré.pays@edelweb.fr
- Olivier Chapron – Consultant manager
  - 01 40 99 14 14
  - ochapron@on-x.com
- Peter Sylvester – Expert technique
  - 01 40 99 14 14
  - peter.sylvester@edelweb.fr
- Information sur nos activités :
  - http://www.on-x.com
  - http://www.edelweb.fr