Comment intégrer les signatures électroniques dans ma propre infrastructure IT

Bernard Hauzeur, Woobe s.a.s.

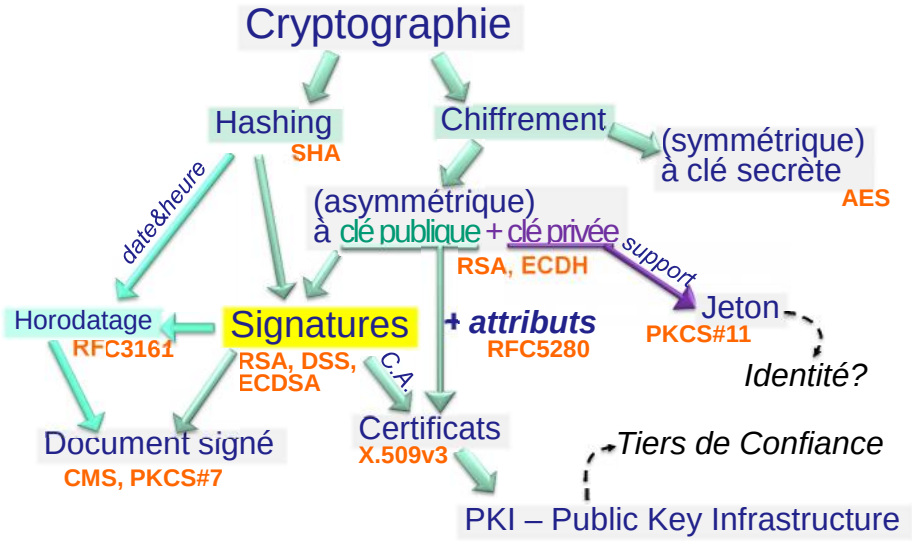
Table des matières

- **Les signatures électroniques, guide de survie (im)pertinent:**
  - la Techno, les Standards, la Loi ↔ les règlements
- **"Je veux garder le contrôle"**
  - déléguer ou intégrer?
- **Solution**
  - un peu d'organisation...
  - un support pérenne: PDF/A
  - et des signatures qualifiées

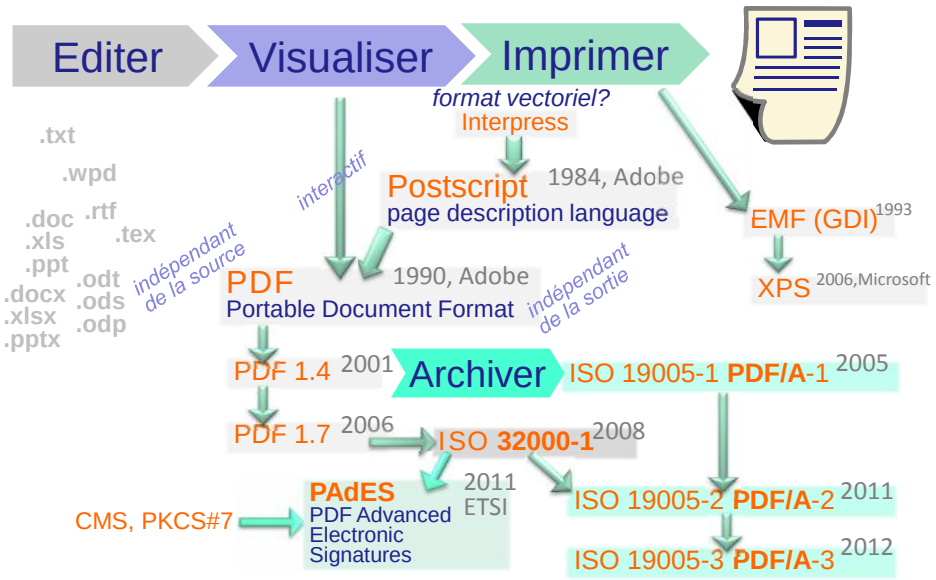
La techno, les standards, le Droit, la Loi, …

GUIDE DE SURVIE

La techno et les standards: signatures…



La techno et les standards: documents…



La techno et les standards: zoom sur PDF/Archive

- **Intégrité visuelle:**
  - ni audio, ni vidéo
  - pas de scripts ni de contenus externes
  - profil de couleurs standardisé
  - autonomie: inclusion des polices de caractères
  - restriction aux compressions de données sans dégradation
  - clarifications diverses des spécifications, ex: blancs
- **Rester accessible à long terme → pas de chiffrement!**
- **PDF/A-2 = PDF/A-1 + transparence, signatures PAdES, base ISO**
- **PDF/A-3 = PDF/A-2 + fichiers attachés quelconques**
- **3 niveaux de conformité:**
  - **a** - 1a, 2a, 3a : préservation de la structure du texte selon le sens de lecture, tags
  - **b** - 1b, 2b, 3b : (basic) intégrité visuelle, un scan convient
  - **u** - 2u, 3u : (Unicode) texte intégralement Unicode, sans garantie de structure
- **PDF/A-3 ne remplace pas /A-2, qui ne remplace pas /A-1 !**

Le Droit / la Loi

- *1996 (1998) - Nations Unies - Loi type sur le commerce électronique*
- **1999 - Directive CE sur un cadre européen pour les signatures électroniques …** transposé dans les lois nationales avant mi 2001
  - S.E.Q. = S.E.A. + C.Q. + dispositif sécurisé de création
- **2000 - Code Civil Art.1316 ...de l'équivalence électronique**
- **2000 - USA eSign Act - loi fédérale sur les signatures électroniques**
- *2001 - Nations Unies - Loi type sur les signatures électroniques*
- **2005 - Code Civil Art.1369 ...des contrats sous forme électronique**
- *2005 - Nations Unies – Comm'tions électroniques dans les contrats*

… plus toutes les Lois sur la protection de la vie privée

Réglementations

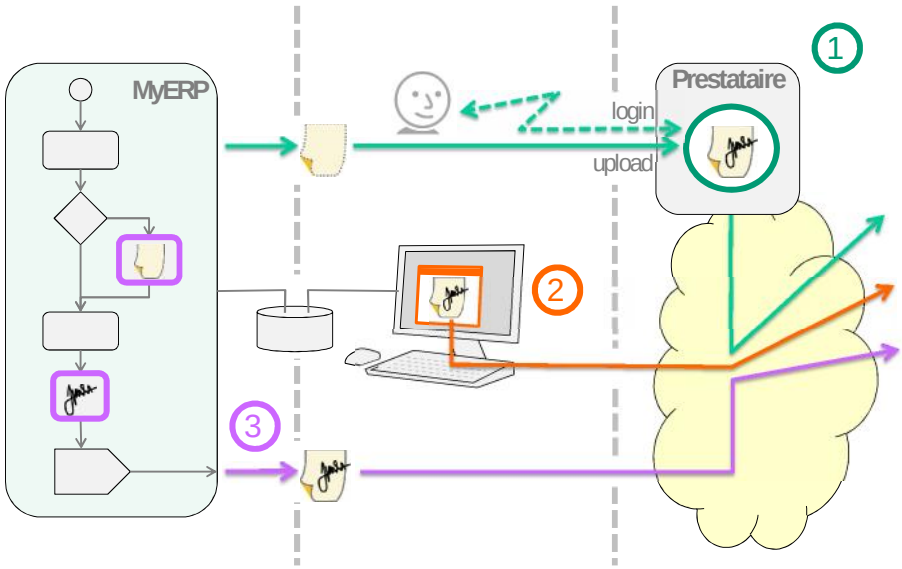
- **2001 (2009) - Décret d'application relatif à la signature électronique**
- **2003 - Décision 2003/511/CE sur les normes de référence**
  - CEN Workshop Agreement 14167-1 & 2 … gestion des certificats
  - CEN Workshop Agreement 14169 … dispositifs de signature
- **2010 – Référentiel Général de Sécurité (RGS)**
  - …pour tous les échanges électroniques avec l'administration française
  - + le RGI : … Interopérabilité → PDF/A
- **2011 (2015) - Décret d'application relatif à la lettre recommandée électronique**
- **2014 - Règlement européen sur l'identification électronique et les services de confiance (eIDAS)**
  - 3 niveaux de 'fiabilité' : faible – substantiel – élevé …
- *2015… Actes d'application du Règlement européen ci-dessus*

… et toute la documentation de l'ANSSI

Déléguer ou intégrer?

"JE VEUX GARDER LE CONTRÔLE"

Trois approches 1 2 3



Un peu d'organisation, un support pérenne, des signatures qualifiées

SOLUTION

Les ingrédients

Question	Réponse	Solution	Attention à
Capter les données	intégration	serveur / kit de développement	portabilité, universalité
S'intégrer aux processus			
Forme des documents	PDF/A	kit de développement	qualité, universalité; -1? -2? -3?
Certificats cryptographiques	CA : Certifica-tion Authority	prestataire(s)	contenu des certificats, révocations
Signatures	PAdES	kit de développement	type de signature, en batch, ~~en parallèle~~
Horodatage	TSA : Time Stamping Authority	prestataire / serveur SW / matériel sécurisé	rester standard : RFC3161 TSP, question globale
Archivage	Tiers archiveur	prestataire / équipement	opposabilité aux tiers?

Les ingrédients

Question	Réponse	Solution	Attention à
Capter les données S'intégrer aux processus	intégration	PDF-TOOLS.COM	portabilité, universalité
Forme des documents	PDF/A	PDF-TOOLS.COM	qualité, universalité; -1? -2? -3?
Certificats cryptographiques	CA : Certifica-tion Authority	prestataire(s)	contenu des certificats, révocations
Signatures	PAdES	PDF-TOOLS.COM	type de signature, en batch, ~~en parallèle~~
Horodatage	TSA : Time Stamping Authority	prestataire / serveur SW / matériel sécurisé	rester standard : RFC3161 TSP, question globale
Archivage	Tiers archiveur	prestataire / équipement	opposabilité aux tiers?

Convertir, assembler, éditer, signer, …

PDF-TOOLS.COM

Forme des produits:

- API : C, Java, .NET, .COM, C#, VB
- Service
- Commande (batch)
- Desktop
- Plug-in

UNIX, Windows*, OS X*

Qualité:

- performances, fiabilité,
- support, maîtrise des produits,
- expertise
- délégué ISO, co-fondateur de PDF Association (pdfa.org)
- certifications

Universalité:

Conversions, extraction, composition, OCR & scans, métadonnées, chiffrement, signatures, validation, formulaires, impression, visualisation, optimisation, conversion des couleurs, fichiers attachés, indexation, compression, conformité, intégration TSP PKCS#11 OCSP eCard …

PDF 1.4-1.7, PDF/A, PDF/UA, PDF/VT, PDF 2.0

3-Heights = High quality – High volume – High performance

Simplicité

- **Exemple: Signer**

ouvrir…

jeton

identité

date

position

…refermer

C#

```
using Pdftools.PdfSecure;

using (var pdfContainer = new Secure())
{
   pdfContainer.Open(...);
   using (var sig = new Signature())
   {
      sig.Provider = "xxx.dll;slot1";
      sig.Name = "Philip Renggli";
      sig.Reason = "I reviewed the document";
      sig.TimeStampURL = "tsa.server.org";
      sig.TimeStampCredentials = "user:passw";
      sig.PageNo = 1;
      sig.Rect = new PDFRect(x, y, w, h);

      pdfContainer.AddSignature(sig);
   }
   pdfContainer.SaveAs(...);
   pdfContainer.Close();
}
```

demande du code PIN et création de la signature

Quelques Références (Signatures)

swiss sign

QuoVadis

swisscom

woobe