La signature électronique

Concepts et enjeux

Nathanaël Cottin

contact@ncottin.net
http://www.ncottin.net

version 0.0.4

Conditions de recevabilité

- Une relation forte envers l'identité du signataire
- Un lien étroit avec les informations signées

Différences techniques avec la signature manuscrite

- Signature manuscrite immuable
- Chaque signature électronique est propre au contenu signé

Signature électronique avancée

Équivalente à la signature manuscrite

Exigences :

- Être liée uniquement au signataire
- Permettre d'identifier le signataire
- Être créée par des moyens que le signataire peut garder sous son contrôle exclusif
- Être liée aux données auxquelles elle se rapporte

Conditions de validité

Valeur juridique déterminée par :

- La nature des procédés de création et de vérification
- Le degré de sécurité de l'environnement dans lequel la signature a été établie
- La nature des pièces justificatives

Bref historique technique

1. 1978 : cryptosystème RSA
2. 1978 : thèse de doctorat de Loren Kohnfelder
3. 1985 : ECC
4. 1988 : format X.509 du groupe PKIX
5. 1991 : système PGP
6. 1991 : MD5
7. 1993 : SHA-0
8. 1996 : standard DSA

Terminologie

Signature numérique

Données issues d'une opération de signature à l'aide d'une clé privée

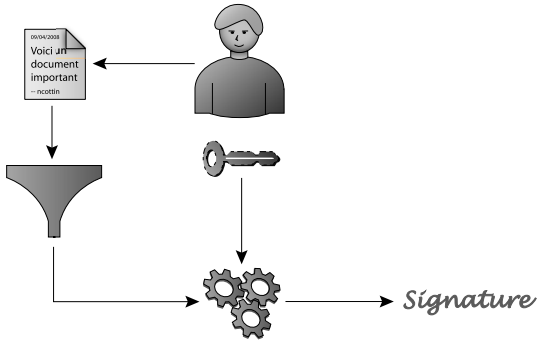
Signature électronique (technique)

Données complémentaires permettant de restituer les informations nécessaires à la validation de signatures électroniques avancées

Format de signature numérique

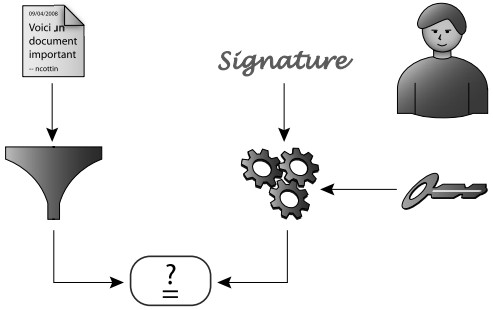
Algorithme de signature
Valeur de signature

Processus de création



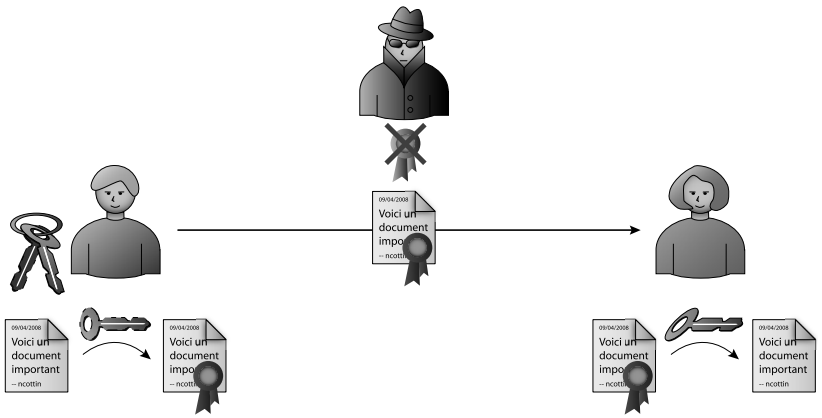
Le signataire utilise sa clé *privée*

Processus de vérification



Utilise la clé *publique* du signataire

Transmission d'une information signée



Limites de la signature numérique

Manque des informations de validation :

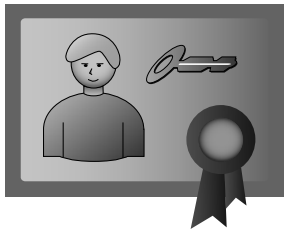
- Lien certifié avec le signataire
- Informations relatives à l'environnement de signature
- Repère temporel

⇒ Définition d'une signature *électronique* technique faisant appel à un *notaire électronique*

Deux orientations

- Le vérificateur détermine lui-même le statut
- Le statut lui est fourni par un tiers de confiance

Utilisation des certificats au format X.509



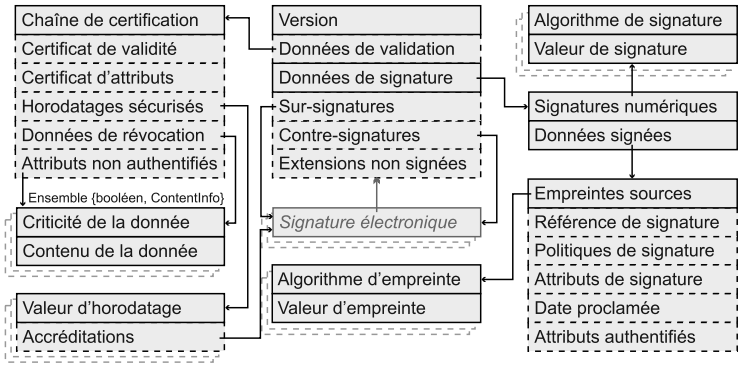
- Délivré par un PSCE
- Atteste du lien entre identité et clé publique

Notarisation de signature

Certificat de validité

Indique le statut attribué à une signature électronique à un instant donné

Format de signature électronique notariée



Création

1. Création des données de signature
2. Éventuellement :
   1. Demande d'un certificat de validité
   2. Ajout des sur-signatures et contre-signatures

Validation

1. Vérification de la signature numérique
2. Vérification du certificat de validité
3. Vérification des horodatages
4. Vérification de la validité du certificat du signataire à la date de signature
5. Validation des sur-signatures et contre-signatures

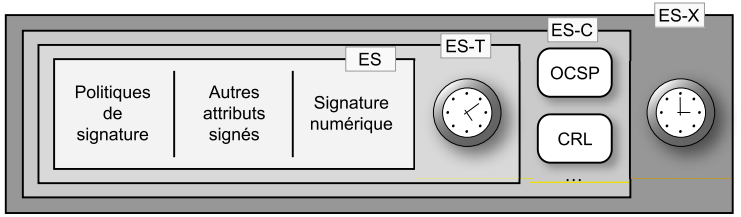
Pourquoi ?

Création de vraies fausses signatures

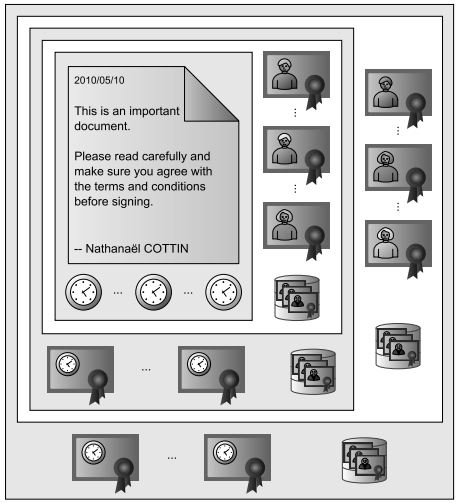
Trois alternatives :

- Le format standard ES-X de l'ETSI
- Le standard CMS de l'IETF
- Le certificat de validité

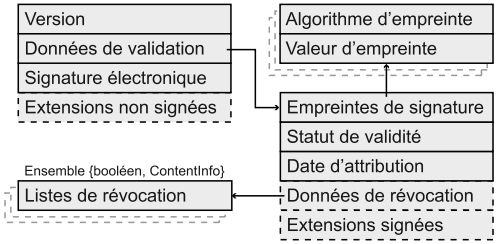
Format standard ES-X de signature à long terme



Format CMS pour signatures à long terme



Format du certificat de validité



Garanties apportées par la signature électronique

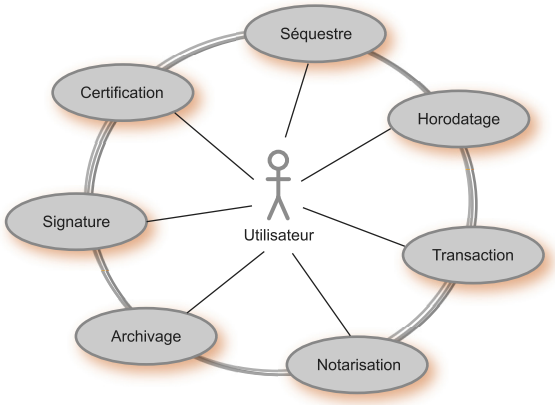
- Valeur juridique
- Intégrité
- Authenticité des contenus
- Non répudiation
- Identification du signataire
- Vérification automatiquement
- Difficulté d'imitation
- Validité sur le long terme

Garanties complémentaires souhaitées

- Contrôle des procédés de multi-signature
- Utilisation de données propres à l'individu
- Stockage sécurisé
- Protection contre l'évolution technologique
- Lisibilité des signatures

$\Rightarrow$ Besoin de services annexes à la signature électronique

Vue d'ensemble



Infrastructure de Gestion de Clés

Consulter la présentation dédiée aux IGC. . .

Séquestre de clés

- Conservation d'un duplicata des clés privées (déchiffrement)
- Soumis à controverse

Notarisation électronique

- Génération des certificats de validité
- Preuve de validité des signatures électroniques

Supervision de transactions

- Labellisation de sites
- Surveillance du bon déroulement des transactions
- Preuve de non complétude le cas échéant
- Enregistrement des traces des transactions
- Distribution des preuves des transactions

Horodatage sécurisé

- Attribution d'une date à une information
- Preuve d'existence de l'information
- Datation de signatures

Archivage sécurisé

Comment répondre à l'obsolescence technologique ?

- Utilisation d'un format pérenne
- Conservation des documents et signatures
- Veille à l'intelligibilité des archives confiées
- Garant de l'authenticité des archives

Multi-signature contrôlée

Comment gérer les processus de multi-signature ?

- À l'initiative d'une entité quelconque (initiateur)
- Respect d'un workflow d'apposition des signatures
- Prise de contact (et relance) automatique avec les signataires
- Collecte et agrégation des signatures
- Retour des signatures à l'initiateur (clos le processus)