Webinaire « Signature Électronique »

le 21 avril 2016

@ADULLACT
@StephaneVast

ADULLACT

Association des Développeurs et des Utilisateurs de Logiciels Libres pour les Administrations et les Collectivités Territoriales

CC BY NC SA

SOMMAIRE

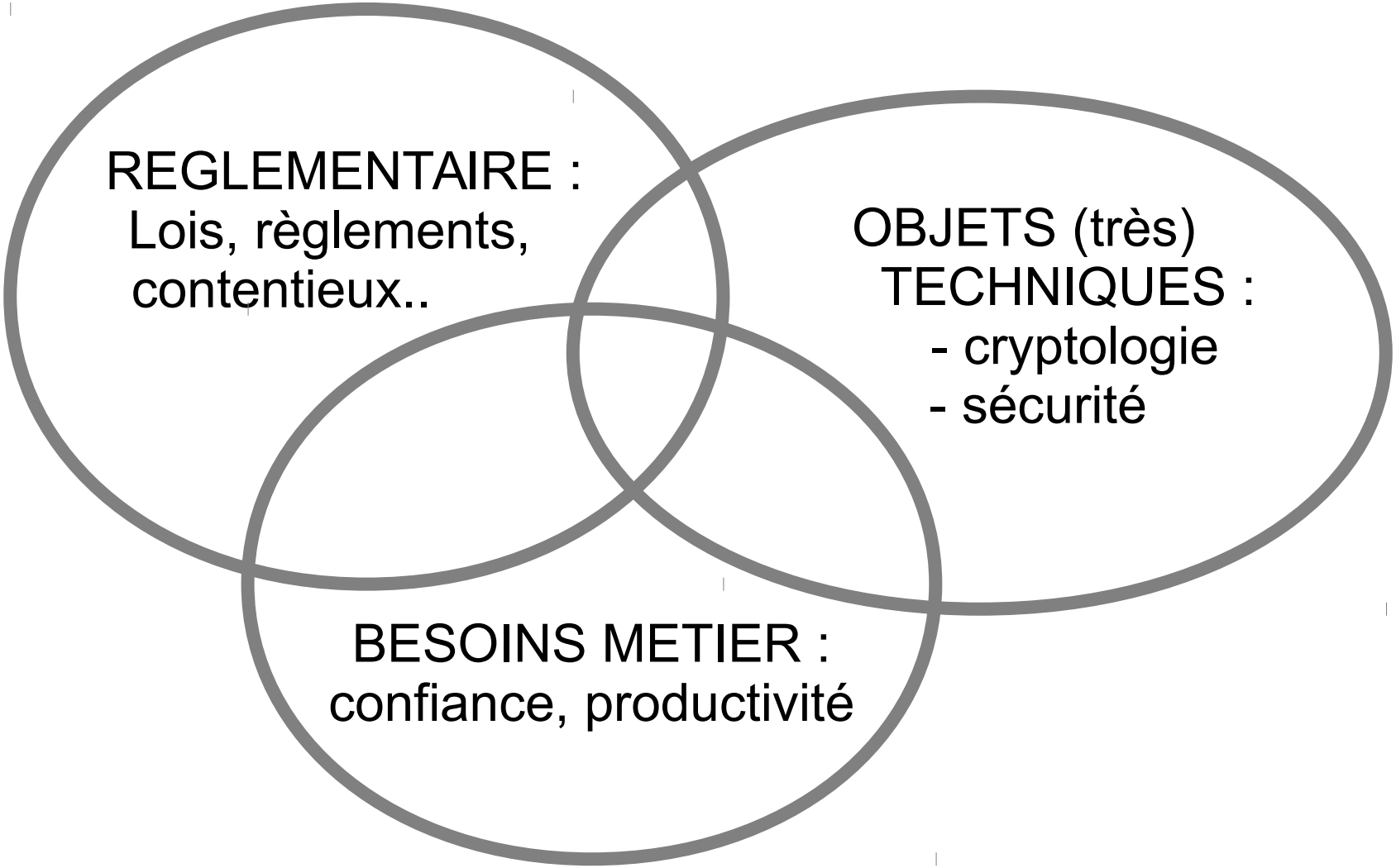
Suivez/Réagissez :
@ADULLACT
@StephaneVast

Webinaire: SIGNATURE ELECTRONIQUE

- Introduction
- Certificat et signature électroniques
- Réglementation(s) administrative(s)
- Cas pratiques
- Futurologie, Q&A

CC BY NC SA

Une présentation multi-axes



BY NC SA

SOMMAIRE

Suivez/Réagissez :
@ADULLACT
@StephaneVast

Webinaire: SIGNATURE ELECTRONIQUE

- **Introduction** : un peu d'histoire de la signature
- Réglementation administrative
- Certificat et signature électroniques
- Cas pratiques
- Futurologie, Q&A

CC BY NC SA

Qu'est-ce qu'une signature ?

- La signature identifie l'auteur
  - Marque le consentement, engage les parties
  - « Paraphe » = forme abrégée de la signature
- Caractéristiques
  - **Singularité** : éviter la confusion avec autrui
  - **Produit dérivé** : doit être produite par la personne
  - **Invariance** : la personne doit signer de la même façon dans le temps
  - **Concision** : elle doit être aussi courte que possible
  - Production aisée

BY NC SA

Un peu d'histoire

- Que fait une signature ?
  - Transformer un document en acte juridique qui authentifie et engage les parties intéressées
- 1ères traces.... 3000 ans AC : Mésopotamie
  - Validation des écrits juridiques : sceaux cylindriques
  - Moyen-Âge : sceaux, seings, souscriptions
  - XVI° siècle : ordonnance de Henri II aux notaires de faire signer les parties contractantes « s'ils savent écrire » avec sceau nominatif.
  - Puis le nom patronymique

cc BY NC SA

Signer, à travers les âges....

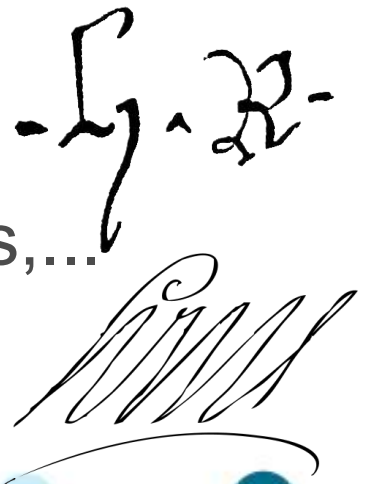
- Avant la signature moderne
  - **Sceau** : façonné dans l'argile, le plomb, la cire
  - Anneau sigillaire avec armoiries
    - Chez les Romains : **sceau** = ***annulus***
  - Signet royal, au Moyen-Âge

BY NC SA

Signer, à travers les âges....

- Avant la signature moderne
  - **Sceau** : façonné dans l'argile, le plomb, la cire
  - Anneau sigillaire avec armoiries
    - Chez les Romains : **sceau** = ***annulus***
  - Signet royal, au Moyen-Âge

- Signature moderne
  - Apparaît au XIV°siècle (Jean le Bon) : Rois
  - Culture de l'écrit (notaires, secrétaires)
  - Puis diffusion aux officiers, artistes, artisans,...



BY NC SA

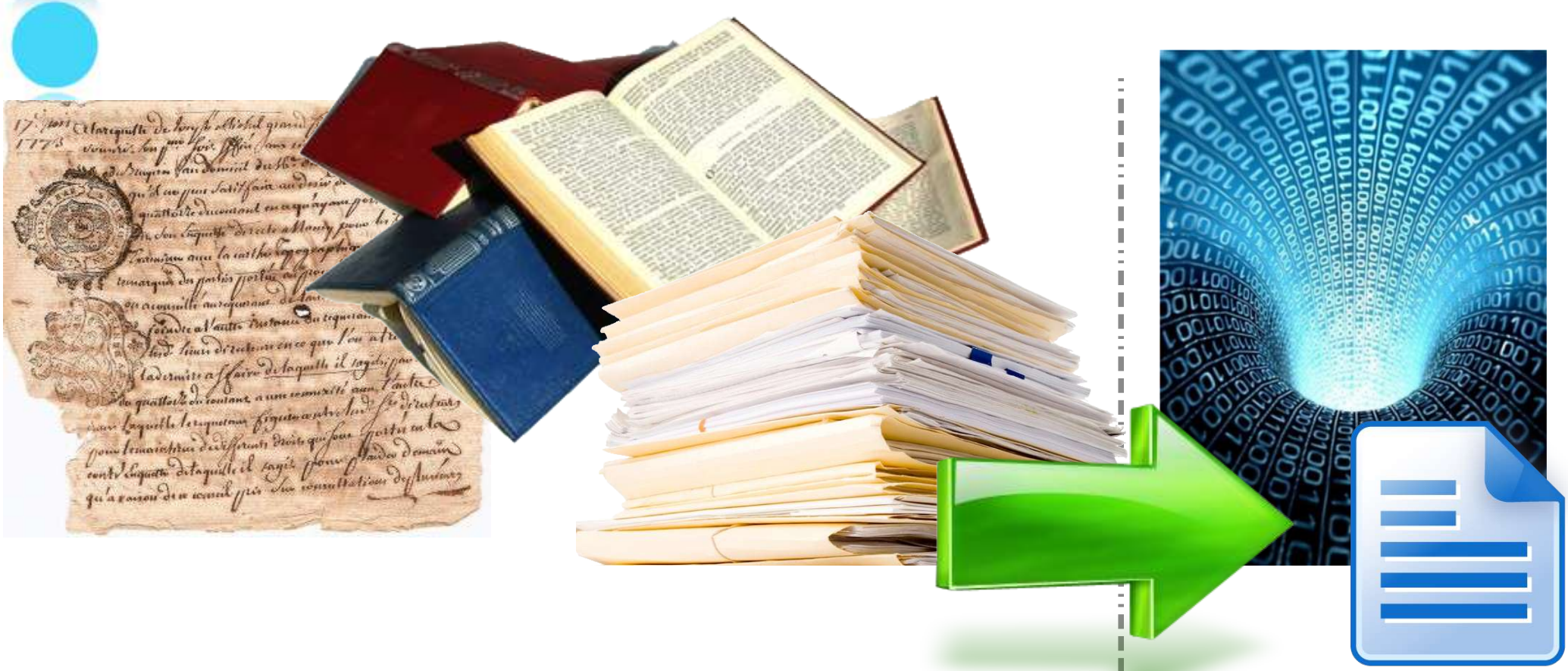
Signer, à travers les âges....

- Jusqu'au XX° siècle : des documents signés...

BY NC SA

Signer, à travers les âges....

- … XXI° siècle : révolution numérique !



BY NC SA

Signer, à travers les âges....

- XXI° siècle : Avec la dématérialisation des documents, comment continuer à signer ?

La signature électronique **n'est pas visuelle**,
C'est une suite de nombres.

BY NC SA

Signature au service de la dématérialisation

- Donner une valeur juridique équivalente à celle d'un document papier signé :

1. Marque du consentement et de l'engagement (non répudiation)

2. Sécurité technique avec des fonctions de cachet, d'horodatage, qui garantiront :
   - la qualité du signataire,
   - la provenance de la signature,
   - l'intégrité du document
   - la date de réalisation

cc BY NC SA

SOMMAIRE

Suivez/Réagissez :
@ADULLACT
@StephaneVast

Webinaire: SIGNATURE ELECTRONIQUE

- Introduction : un peu d'histoire
- **Certificat et signature électroniques**
- Réglementation(s) administrative(s)
- Cas pratiques
- Futurologie, Q&A

CC BY NC SA

SOMMAIRE

- **Certificat : définition**
- Organes de gestion : IGC, AC, AE
- Délivrance : où, comment, pourquoi ?

Qu'est-ce qu'un Certificat électronique ?

- C'est une « Carte d'identité » numérique
- Fonctionnement basé sur le chiffrement et sur la confiance

- **Chiffrement** :
  un couple de clés mathématiques
- **Confiance** :
  un tiers gère les clés
  → « autorité de certification ».

Source: http://fr.wikipedia.org/wiki/Certificat_électronique

cc BY NC SA

Chiffrement asymétrique RSA

- Couple de clés mathématiques :
  Clé Privée + Clé Publique
  - Chiffrement asymétrique (Diffie-Hellman, 1976)
  - RSA en 1978 (Rivest, Shamir, Adelman)

  - Analogie : boite à deux serrures
    - Une clé pour déposer le message en sûreté
    - Une autre clé pour découvrir le message à réception

Source: http://fr.wikipedia.org/wiki/Certificat_électronique

cc BY NC SA

Certificat électronique = IDENTITE NUMERIQUE

ADULLACT

- BUT : « être » identifiable sur les réseaux
- Selon contexte, différents types d'identités !

  - Personne physique : Prénom/Nom/e-mail
    → signer courrier, souscrire contrat (banque,...)

  - Professionnel : Nom + entreprise + SIRET
    → signature A.E., réponse A.O., etc.

  - Personne morale : Nom organisme !! (+nom porteur)
    → sceau de provenance, signature de facture...

cc BY NC SA

Certificat électronique = IDENTITE NUMERIQUE

- BUT : « être » identifiable sur les réseaux
- Selon contexte, différentes identités !

Identité numérique =

capacité fiable à identifier
une personne physique
sur un support immatériel

cc BY NC SA

Certificat électronique = carte d'identité

Carte d'identité

- Identité du titulaire
- Période de validité
- Photo et signature du titulaire
- Autres informations
- Signature de l'autorité (préfet)

- Identifie le porteur (nom, prénom)
- Durée de vie limitée
- Permet de reconnaître un individu (photo, empreintes, signature...)
- Fiabilité liée au fournisseur : **préfecture (signé par le préfet)**

BY NC SA

Certificat électronique = carte d'identité

ADULLACT

Carte d'identité

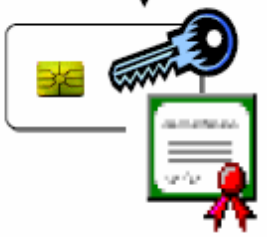
- Identité du titulaire
- Période de validité
- Photo et signature du titulaire
- Autres informations
- Signature de l'autorité (préfet)

Scellement permettant de vérifier l'intégrité et l'authenticité des informations

Certificat électronique

- Identité du titulaire
- Période de validité
- Clé publique
- Autres informations
- Signature de l'Autorité de Certification

Clé privée



CC BY NC SA

Certificat électronique : propriétés

- PKCS12, BC
  - Magnien Bernard
    - Certificates
      - Certificate 1 of 2
        - 3
        - EMAILADDRESS=b.magnien@adullact.org, CN=Magnien Bernard, OU=S2LOW-Pr
        - EMAILADDRESS=systeme@adullact.org, CN=AC ADULLACT Projet g2, OU=ADULL
        - C5DB DB0C 3011 F230
        - 3 nov. 2011 16:24:05
        - 1 nov. 2016 16:24:05
        - RSA (2 048 bits)
        - SHA1withRSA
        - B6:CB:D7:BD:F3:77:85:32:12:75:8C:AC:C4:69:B2:39:89:D3:D4:6D
        - 80:3C:FF:D1:F3:B2:39:98:78:52:AA:7B:2B:74:EE:56
      - Certificate 2 of 2
        - 3
        - EMAILADDRESS=systeme@adullact.org, CN=AC ADULLACT Projet g2, OU=ADULL
        - EMAILADDRESS=systeme@adullact.org, CN=AC ADULLACT Projet g2, OU=ADULL
        - C5DB DB0C 3011 ED96
        - 15 nov. 2010 14:38:22
        - 12 nov. 2020 14:38:22

BY NC SA

SOMMAIRE

- Certificat : définition
- **Organes de gestion : IGC, AC, OC, AE**
- Délivrance : où, comment, pourquoi ?

BY NC SA

La confiance : gestion des clés par un tiers

- IGC = ICP = PKI : ensemble de composants (processus, matériels, humains) organisé pour gérer le cycle de vie des certificats :
  - Enregistrement des utilisateurs
  - Génération, renouvellement, publication des certificats
  - Révocation des certificats, publication de la LCR (CRL)
  - Archivage, séquestre, recouvrement

Source: http://fr.wikipedia.org/wiki/Infrastructure_à_clés_publiques

cc BY NC SA

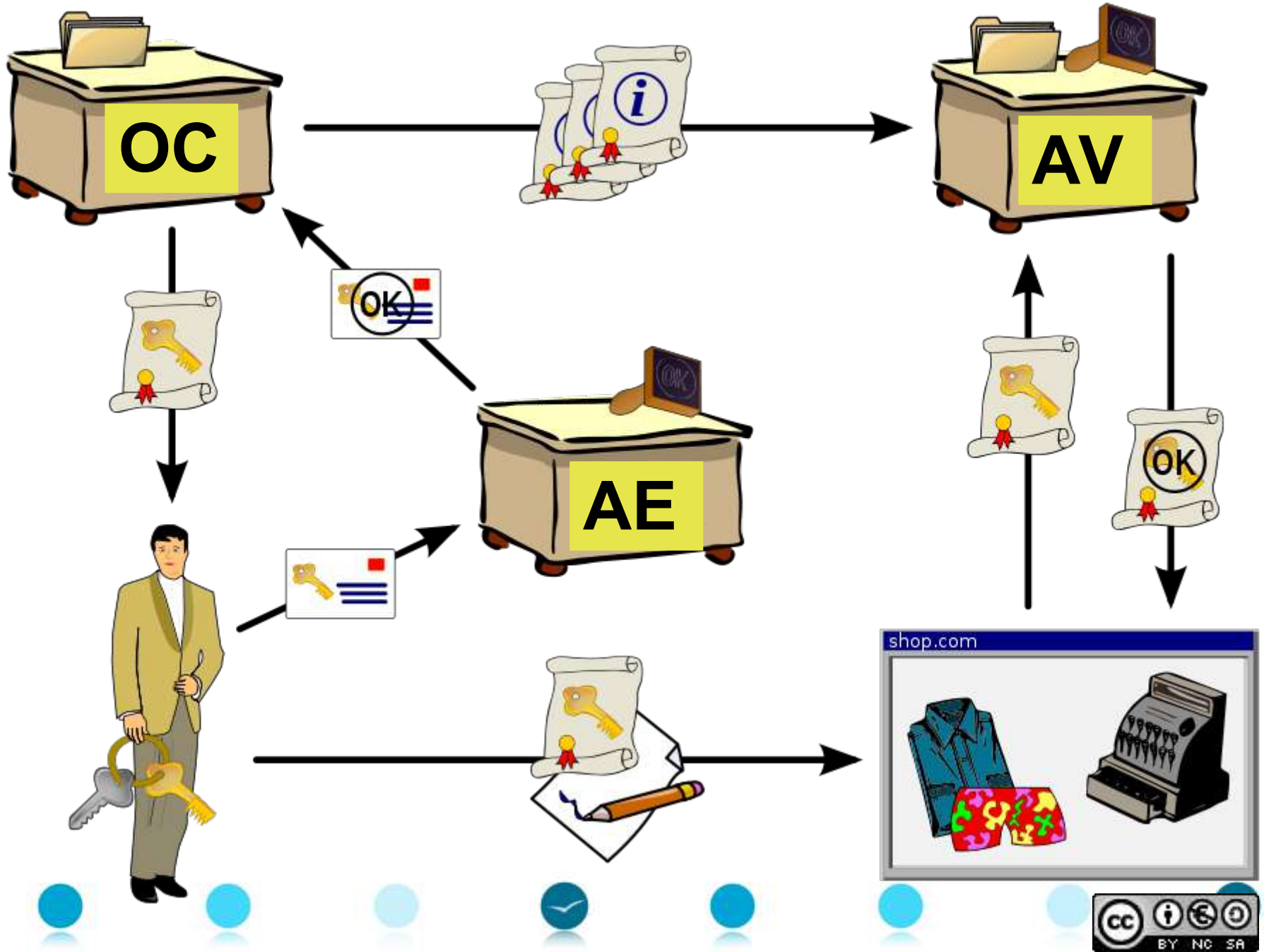
La confiance : gestion des clés par un tiers

ADULLACT

Comment s'orchestre le
Fonctionnement
d'une **AC** (Autorité de Certification)

BY NC SA

La confiance : gestion des clés par un tiers



BY NC SA

Exploitation des Certificats électroniques

ADULLACT

- **s'identifier** face à un service en ligne, exemple : depuis un navigateur web

- **signer** avec un outil de production de signature
(exemple : applet JAVA « LiberSign »)

BY NC SA

SOMMAIRE

- Certificat : définition
- Organes de gestion : IGC, AC, AE
- **Délivrance : où, comment, pourquoi ?**

BY NC SA

Délivrance : où, comment, pourquoi ?

- **Si** équivalent de pièce officielle d'identité
  - Fourni par l'État (Ministère de l'intérieur, Préfectures)
  - En délégation auprès de PSCo certifiés :
    - Banques, CCI, Greffe de tribunal,...
    - Pure players : Dhimyotis (Certigna), Keynectis,...
- Processus de délivrance :
  - Demande en ligne : fourniture de justificatifs
  - Vérification par le PSCo des pièces fournies
  - Fourniture en face-à-face sur présentation de PI officielle (carte nationale d'identité, passeport,...)

Et après... « crypto-hardware »

ADULLACT

- Équivalent de pièce officielle d'identité
  - On y fait attention comme une pièce d'identité
  - ...comme sa CB , ou son Tél. Mobile !
  - … ON NE DIFFUSE PAS LE **CODE SECRET** !!!
- Et si il y a vol, compromission ?
  - Faire comme sa CB ou sa carte SIM (mobile)
  - → Révoquer le certificat auprès du fournisseur.

cc BY NC SA

SOMMAIRE

Suivez/Réagissez :
@ADULLACT
@StephaneVast

- **Signature électronique : signer, vérifier**
- Propriétés d'une signature
- Formats et interopérabilité

cc BY NC SA

Défis de la signature électronique

ADULLACT

- Assurance d'un certificat valide !
- Accès à la clef privée (support matériel HSM)
  - Existence de liaison physique ?
  - Liaison logicielle (pilote) ?

BY NC SA

Défis de la signature électronique

ADULLACT

- Assurance d'un certificat valide !
- Accès à la clef privée (support matériel HSM)
  - Problème : Faire face à des messages (objet, document, etc) de taille potentiellement très lourds...
    - Le cryptogramme est très très gros aussi
    - Le temps de production est en O(n), trop long.
    - ==> il faut réduire le temps de traitement pour produire le message chiffré.
      La signature doit être la plus courte possible
- Pouvoir à destination contrôler la validité de la signature (non altération, falsification, etc.)

cc BY NC SA

Contrôles sur Certificat électronique

- La validité du certificat est établie avant chaque utilisation :
  - Chaîne de certification (AC racine connue?)
  - Fichage en CRL ?

Algorithme de condensation 1/2

ADULLACT

- **Application** : scellement d'une donnée, contrôle d'intégrité
- Fonction de calcul d'une empreinte numérique à partir du message
- **Intérêt** : pouvoir chiffrer un équivalent fortement réduit du message
- **Attention** : efficace tant que la fonction de condensation résiste aux attaques de collision

cc BY NC SA

Algorithme de condensation 2/2

- Propriétés :
  - Sens unique ! Difficile de retrouver le message d'origine
  - Difficile d'avoir un autre message donnant une empreinte identique
  - Difficile d'avoir deux messages aléatoires donnant la même empreinte
- Algorithmes de hachage existants :
  - MD5 (128bits) : dépassé
  - SHA1 (160bits) : cassé, non pérenne
  - SHA256, SHA384, SHA512... SHA3 !

BY NC SA

Comment produire une signature ?

Mon document (peut-être très très volumineux)

Ma clé privée

Comment produire une signature ?

- Signer c'est :
  - 1) Condenser le document pour obtenir une empreinte
    NB : Cette empreinte est UNIQUE :
    - Elle dépend directement du document source.
    - Si le document change (un peu), l'empreinte sera (très)différente
  - ...

Comment produire une signature ?

- Signer c'est :
  - 1) Condenser le document pour obtenir une empreinte
  - 2) Chiffrer l'empreinte avec la clé privée du porteur
  - Le résultat est « unique », modulo le document + la clé privée : c'est la **donnée signée**.
  - ...

Comment produire une signature ?

- Signer c'est :
  - Condenser le document pour obtenir une empreinte
  - Chiffrer l'empreinte avec la clé privée du porteur
  - Le résultat est « unique », selon le document et la clé privée : c'est la donnée signée.
  - Associée avec le certificat du porteur ==> Signature

BY NC SA

Comment vérifier une signature ?

Mon document

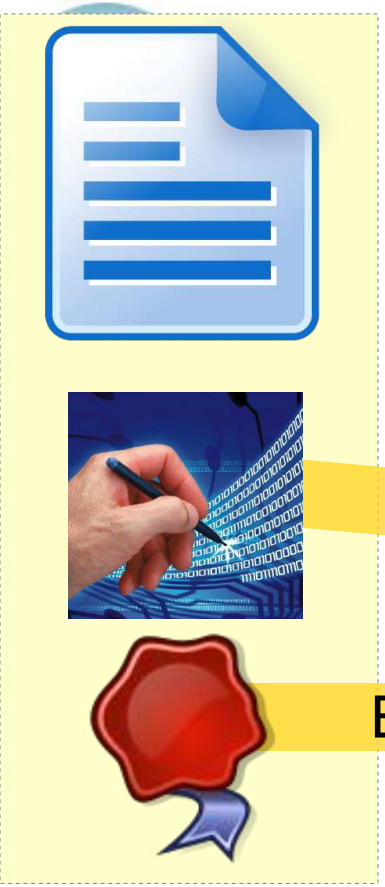
Ma signature : donnée signée + certificat

(+ infos sur algorithmes utilisés)

- Vérifier c'est :
  - …. Faire les opérations à l'envers, grâce à la cryptographie asymétrique

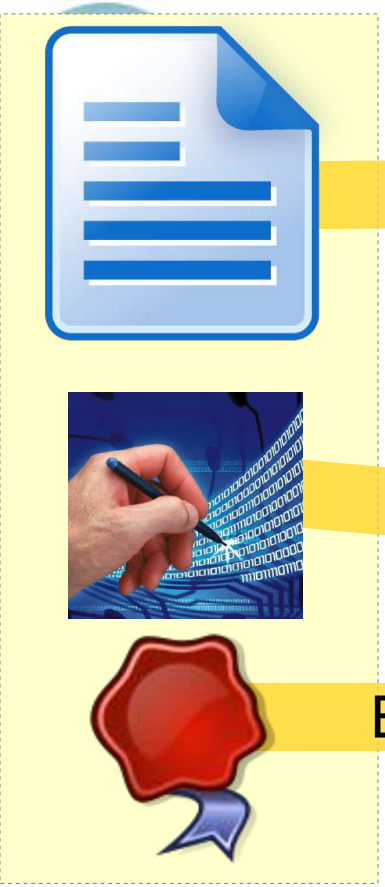
BY NC SA

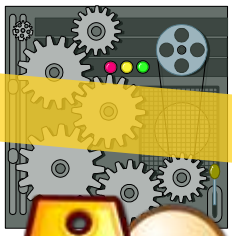
Comment vérifier une signature ?



- Vérifier c'est :
  - Vérifier le certificat et extraire la clé publique,
  - Pour re-Chiffrer la donnée signée !

Comment vérifier une signature ?





Extraire

CLE PUBLIQUE

Comparer les résultats: OK ou KO ?

Vérifier c'est :

- Recalculer l'empreinte du document
- Chiffrer la donnée signée avec la clé **publique**
- ==> Comparer les résultats : OK ou KO

SOMMAIRE

Suivez/Réagissez :
@ADULLACT
@StephaneVast

- Signature électronique : signer, vérifier
- **Propriétés d'une signature**
- Formats et interopérabilité

CC BY NC SA

Propriétés de la Signature électronique ?

- **Authentique** : L'identité du signataire doit pouvoir être retrouvée de manière certaine.
- **Infalsifiable** : La signature ne peut pas être falsifiée. Quelqu'un ne peut se faire passer pour un autre.
- **Non réutilisable** : La signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document.
- **Inaltérable** : Un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier.
- **Irrévocable** : La personne qui a signé ne peut le nier.

Source : http://fr.wikipedia.org/wiki/Signature_numérique

SOMMAIRE

- Signature électronique : signer, vérifier
- Propriétés d'une signature
- **Formats et interopérabilité**

BY NC SA

RGS : les différents types de certificat

ADULLACT

- Formats de stockage de certificats :
  - Norme IETF : **X509v3** (créé en 1988, RFC 2459),
  - Capsule complète : **PKCS#12** (certificat + clé privée)
    - PKCS est une « standardisation » des laboratoires RSA
    - Microsoft a « personnalisé » PKCS#12 avec le format **PFX**
  - Autres formats de capsule : JKS, PEM, JCEKS,...
- Formats de signature électronique :
  - très nombreux, nous avons besoin d'interopérabilité !
  - Différentes façon de lier signature/document
    - Détaché, enveloppé, enveloppant

cc BY NC SA

Stocker ma signature électronique...

Mon document

Ma signature : donnée signée + certificat

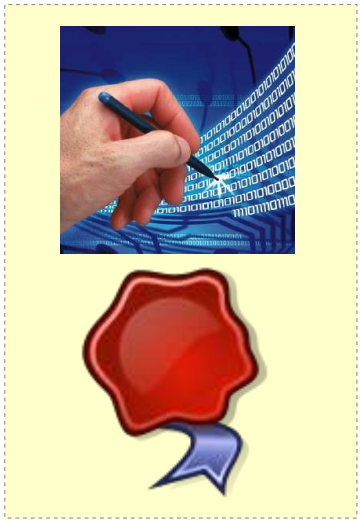
(+ infos algorithmes utilisés)

- Il y a plusieurs façons de structurer ces éléments

Différentes façons de signer

- Signature détachée :
  - Le document source n'est pas touché
  - La signature est stockée dans un fichier séparé

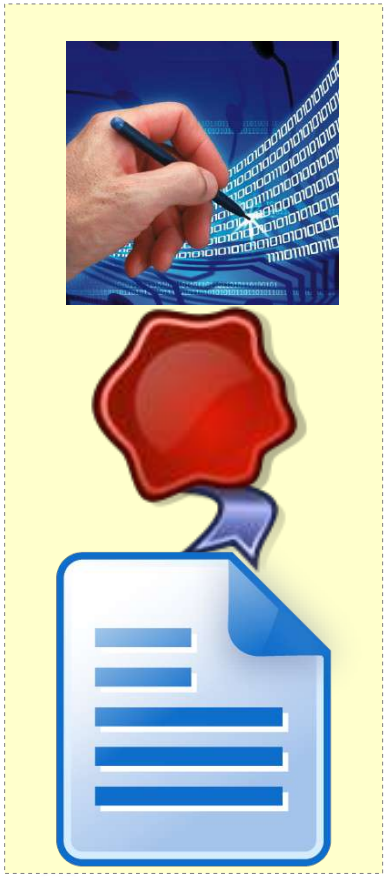
Mon document



Ma signature :
donnée signée
+ certificat +...

Différentes façons de signer

- Signature enveloppante :
  - La signature embarque le document dans une propriété complémentaire ==> il faut un outil pour lire le document



BY NC SA

Différentes façons de signer

- Signature enveloppée :
  - La signature est injectée dans le document source
  - ==> Altération du document source
  - ==> Difficulté accrue sur l'opération de vérification

Différentes façons de signer

- Signature détachée :
  - Le document source n'est pas touché
  - La signature est un fichier distinct
- Signature enveloppante :
  - La signature embarque le document dans une propriété ==> il faut un outil pour lire le document
- Signature enveloppée :
  - La signature est injectée dans le document source
  - ==> Altération du document source
  - ==> Difficulté accrue sur l'opération de vérification

BY NC SA

Les formats couramment utilisés

- **PKCS#7** = S/MIME
  - Le plus connu, le plus utilisé, le plus standard
  - Format retenu pour : ACTES, marchés publics, PJs,...
- **XAdES** : XML Advanced Encryption Standard
  - La signature est produite au format XML, avec certaines propriétés étendues lisibles en clair
  - Différents profils : 'BES', 'EPES', '-C', '-T', '-A'...
  - Utilisable en enveloppée dans des documents XML
  - C'est le format retenu pour : PESv2 (HELIOS), DIA, Bordereaux de versement SEDA, etc.

BY NC SA

Les formats utilisés

- **PAdES** :

- Signature enveloppée dédiée aux fichiers PDF
- Très adapté pour la signature de document bureautique
- Pas besoin de « liseuse » complexe
- Pas besoin de gérer un fichier de signature annexe
- Normalisé ISO, avec 5 profils (simple, à LTV) :
  - /!\ la DGME n'a pas de recommandation sur le profil à utiliser.

- **CAdES**

- Évolution avancée de PKCS#7

cc BY NC SA

Les formats non souhaitables

- Des signatures spécifiques, ou propriétaires
  - Signatures enveloppantes :
    - Nécessite une « liseuse » pour accéder au document
    - Format à tendance hautement « propriétarisante »...
    - … Donc non interopérable. *(si si ça existe)*
  - Signature dans format de fichier privateur :
    - Signature MS-Office (oui on peut signer dans MS-Word...).
- Des formats décrits en annexes des normes
  - Problème sur la disponibilité d'outil de relecture

cc BY NC SA

SOMMAIRE

Suivez/Réagissez :
@ADULLACT
@StephaneVast

Séminaire: CERTIFICAT ELECTRONIQUE

- Introduction : un peu d'histoire
- Certificat et signature électroniques
- **Réglementation(s) administrative(s) : RGS...**
- Cas pratiques
- Futurologie, Q&A

BY NC SA

SOMMAIRE : réglementation administrative

- **La Loi, les décrets**
- Références :
  PRISv1, PRISv2, RGS

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

BY NC SA

Reconnaissance juridique : Loi – Décret

- Depuis la Directive européenne du 13 déc. 1999
  - Directive 1999/93/CE
    - Du Parlement européen et du Conseil, relatif à la signature électronique
  - Loi n°2000-230 du 13 mars 2000
    - Adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique
  - Décret n°2001-272 du 7 mars 2001
    - Application de la loi 2000-230
  - Décret n°2002-535 du 18 avril 2002
    - Évaluation et Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information

BY NC SA

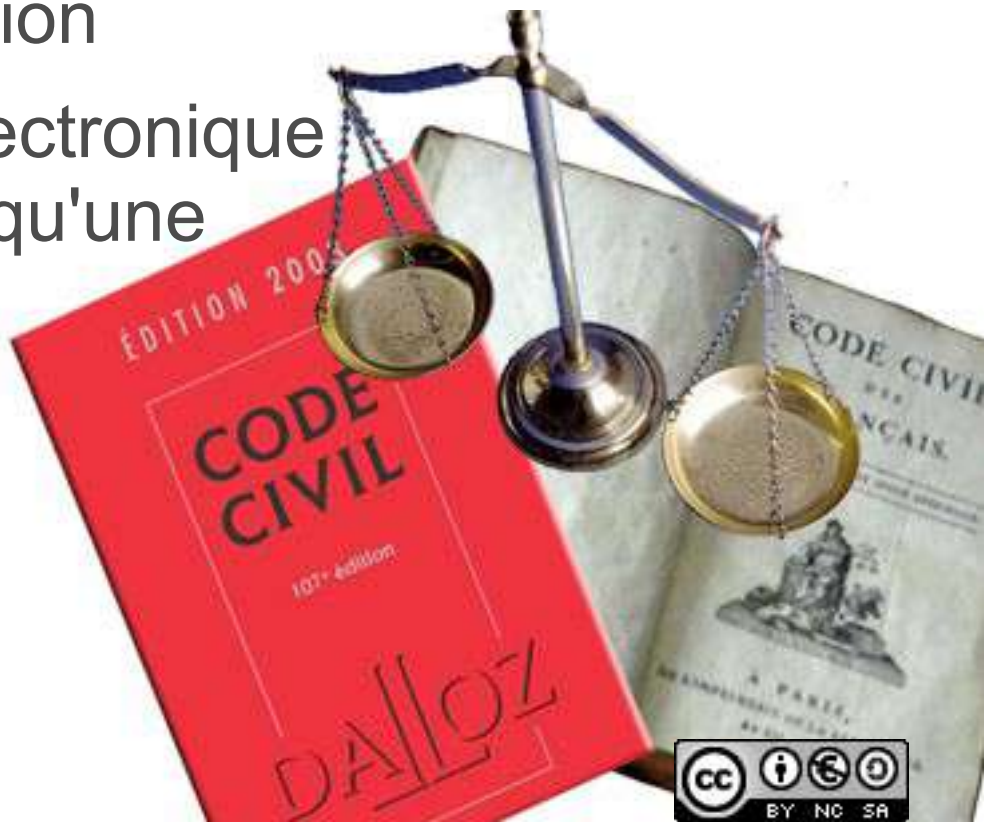
Directive européenne 1999/93/CE

- Objectif : permettre la mise en œuvre d'une signature électronique pouvant se substituer à la signature manuscrite.
- Elle institue un cadre juridique communautaire pour la signature électronique et les services de certification associés, mais elle ne couvre pas :
  - Les aspects liés à la conclusion et/ou exécution des contrats
  - Les actes soumis à formalisme
  - Les différents cadres juridiques communautaires et nationaux limitant l'utilisation de certains documents

cc BY NC SA

Loi n°2000-230 du 13 mars 2000 1/2

- Objectif : transcription au niveau national des prescriptions de la directive 1999/93/CE.
- Elle modifie le **code civil** pour :
  - porter adaptation du droit de la preuve aux technologies de l'information
  - conférer à la signature électronique la même force probante qu'une signature manuscrite :
    - Art. 1316-3
    - Art. 1316-4



BY NC SA

Loi n°2000-230 du 13 mars 2000 2/2

- Art. 1316-3 du code civil :
  - L'écrit sur support électronique a la même force probante que l'écrit sur support papier.
- Art. 1316-4 du code civil :
  - La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose (…) .
  - Lorsqu'elle est électronique, (…) La fiabilité de ce procédé est présumée (…) lorsque
    - la signature électronique est créée,
    - l'identité du signataire est assurée,
    - et l'intégrité de l'acte garantie, (…).

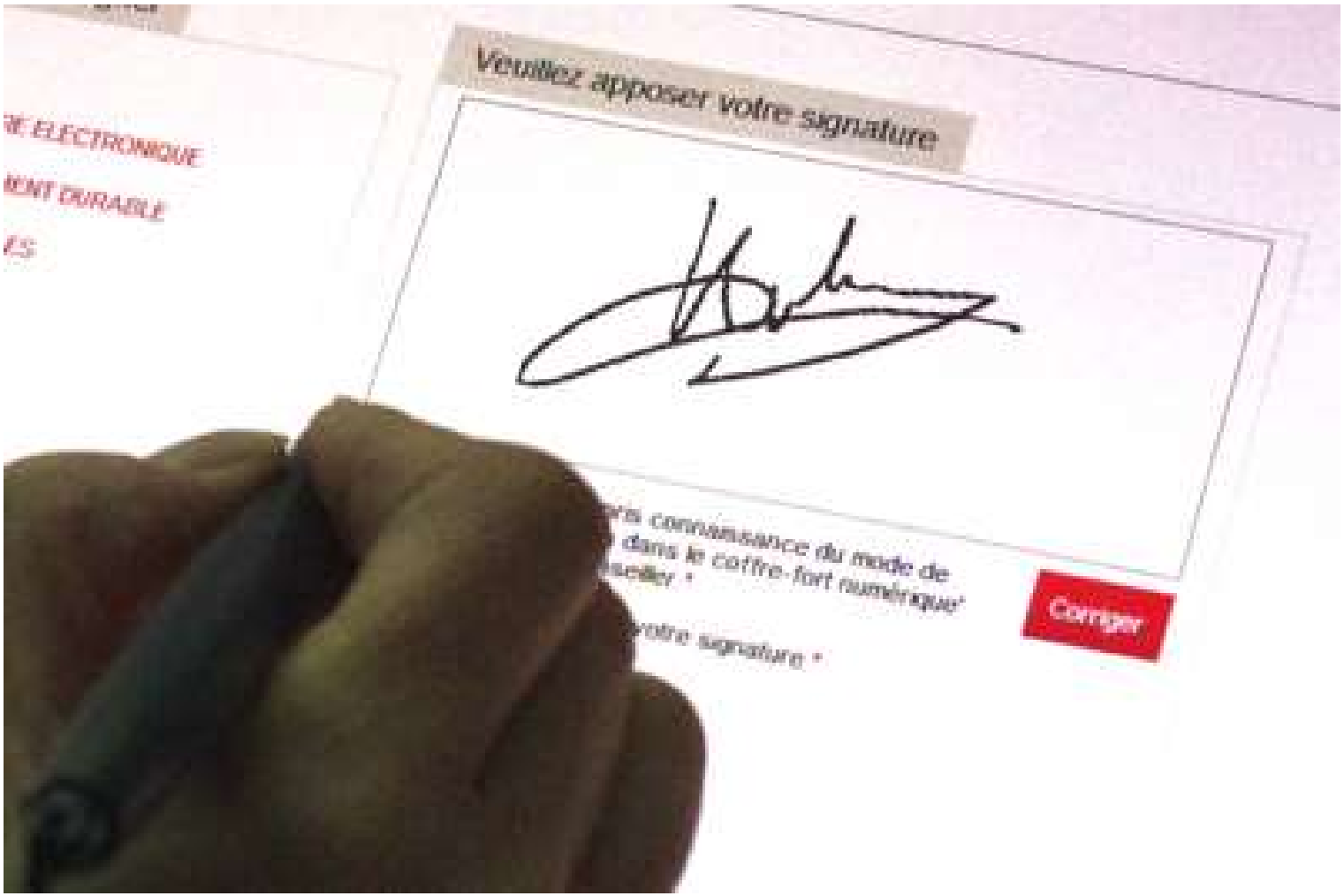
Décret n° 2001-272 du 30 mars 2001

- Le **décret n° 2001-272 du 30 mars 2001** est pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.
- Il rend applicable la loi 2000-230 du 13 mars 2000
- Il introduit les termes suivants :
  - Dispositif sécurisé de création de signature électronique
  - Dispositif de vérification de signature électronique
  - Certificats électroniques qualifiés
  - Prestataires de services de certification électronique

BY NC SA

Business : secteur bancaire (BPCE)

- La signature électronique en agence !



Business : le cas bancaire BPCE

- Cible : documents contractuels dématérialisés
- Déploiement : signer en ligne, en agence
  - Démarrage progressif (épargne)
- Gains :
  - Facilités de gestion
  - Conservation facilitée pour les parties
- /!\ Analyse de risque, et périmètre de sécurité
    - Gestion juridique du contentieux !

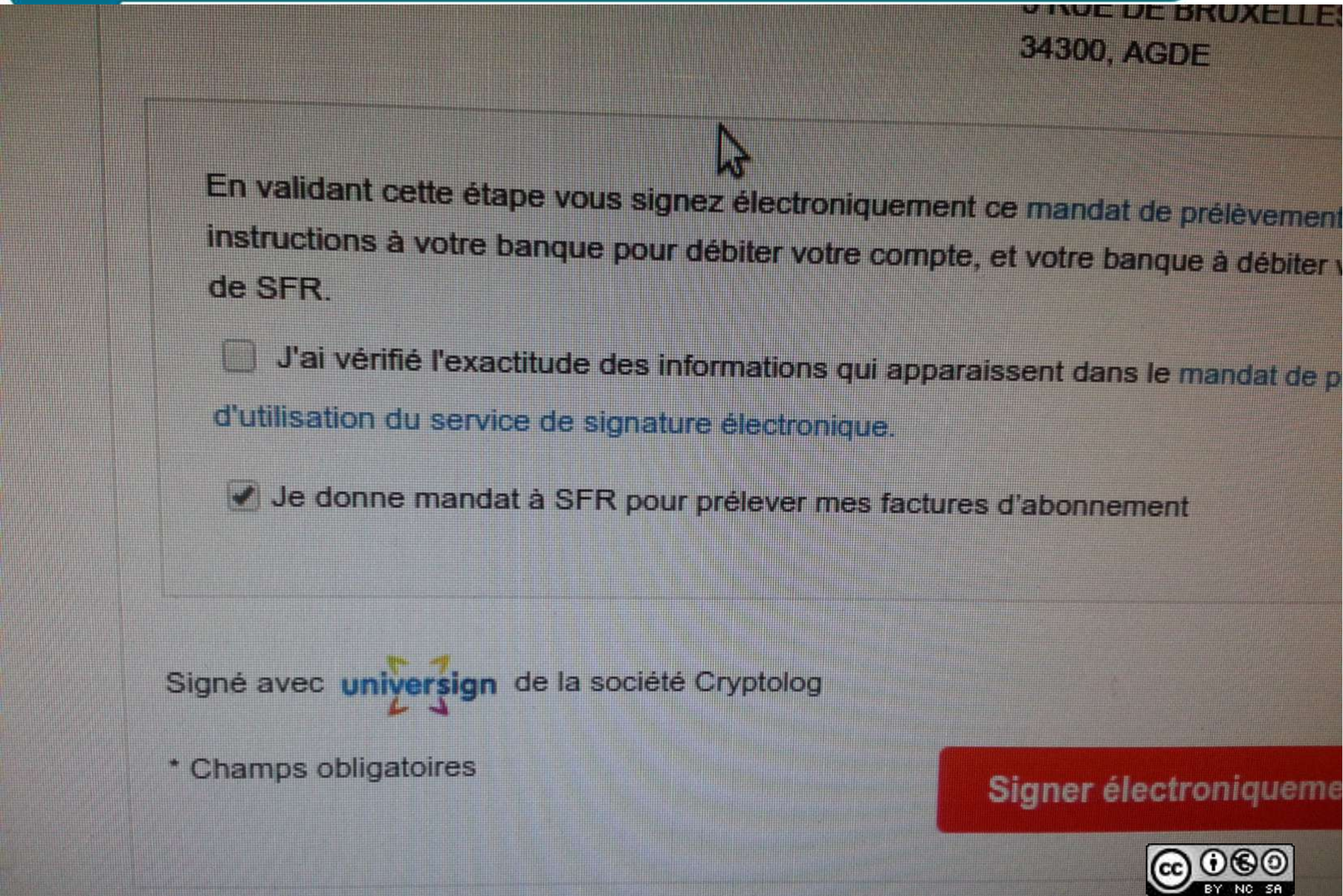
BY NC SA

Le cas bancaire BPCE

- Signature sur Tablette numérique
  - 1 : **authentification**
    - par pièce officielle (CE) devant agent de la banque
    - par code SMS, ou CB (BP)
  - 2 : **consentement** (lecture du contrat sur tablette)
  - 3 : le client signe au stylet, et valide le « dessin ».
  - 4 : le « système » horodate et signe électroniquement le résultat.
- Nécessité quand même de :
  - PKI : horodatage et certificat de signature serveur
  - Stockage sécurisé (coffre fort électronique)

BY NC SA

Contractualisation en ligne



Signature électronique et signature scannée

- L'exemple : affaire Bygmalion...
- Le trésorier de l'UMP nie avoir signé des factures...
  - Ok pour 2/3 signatures scannées
  - Mais pas d'accord pour toutes les autres
- OR : signature scannée n'est pas du tout une signature électronique !
  - Pas de lien entre scan et consentement
  - Hors la loi
  - Donc non recevable si contestation

BY NC SA

SOMMAIRE : réglementation administrative

- La Loi, les décrets
- **Références :**
  PRISv1, PRISv2, RGS

CC BY NC SA

PRISv1 : Définition

- PRIS : Politique de Référencement Intersectorielle de Sécurité, est un référentiel documentaire, et définit :
  - Fonctions relatives à la sécurité numérique :
    - Identification d'une personne, d'un système
    - Signature
    - Confidentialité des échanges
    - Horodatage des actes électroniques
  - Produits de sécurité mettant en œuvre ces fonctions
    - Logiciels, services.
- Le respect de la PRIS donne lieu à **agrément**.

BY NC SA

PRISv1 : en pratique (années 2000-2010)

- L'État a imposé un référentiel documentaire qui décrit les obligations des intervenants au cours du cycle de vie d'un certificat électronique. Il y a 5 niveaux :
  - ~~Classe 0~~ : certificat dit auto-signé, aucune vérification
  - Classe 1 : l'A.E. vérifie uniquement l'email du porteur
  - Classe 2 : le porteur indique son identité à l'AE par l'envoi d'une copie certifiée de sa pièce d'identité
  - **Classe 3** : le porteur décline son identité à l'AE en face à face par présentation d'une pièce d'identité originale
  - **Classe 3+** : idem classe3, mais certificat matériel.

BY NC SA

PRISv1 vers PRISv2 : en route vers le RGS

ADULLACT

- L'État harmonise sa politique de sécurité, c'est le **RGS** : Référentiel Général de Sécurité
  - Prévu par l'ordonnance n°**2005-1516** du 8 déc. 2005
  - Conditions selon le décret n°**2010-112** du 2 fév. 2010
  - Publié par arrêté du Premier ministre le 6 mai. 2010
- Remplaçant de PRISv2.1, le RGS sépare :
  - Les usages : authentification, signature, chiffrement...
  - Les supports : logiciel ou matériel
- Changement de nommages :
  - Classes 1, 2, 3, 3+ ==> étoiles : *, **, ***

http://fr.wikipedia.org/wiki/Référentiel_général_de_sécurité

cc BY NC SA

RGS : les différents types de certificat

Type de certificat		***	**	*
Enregistrement		Face à face obligatoire soit lors de l'enregistrement, soit lors de la remise au porteur		Envoi d'un dossier papier / électronique ou communication par le porteur d'un élément permettant de l'identifier dans une base de données administrative
Remise au porteur				Par messagerie électronique ou téléchargement
Clés du porteur	RSA	2048 bits	1024 bits ou 2048 bits	
	DSA	2048 /q = 256	1024 /q = 256 ou 2048 /q = 256	
	Type	Matériel		Matériel ou logiciel
	Certification	EAL 4+	EAL 2+	Déclaration de conformité aux Exigences
	Niveau de qualification	Renforcée	Standard	

BY NC SA

RGS : les différents usages de certificat

Niveaux RGS	Support	Usages possibles
*	Logiciel, matériel	Authentification + Signature,....
**	Seulement matériel	Authentification + Signature, Authentification seule, Signature seule
***	Seulement matériel	Authentification seule, Signature seule

BY NC SA

Usages métier des certificats RGS

Niveaux RGS	Signature cert. Personnel (2)	Authentification Cliente (1)
*	Bordereaux PESv2 HELIOS !	Connexion Application → TDT (certificat « serveur client »)
**	ACTES, HELIOS, Marchés Publics	Connexion d'individu (3) → TDT (ACTES, HELIOS)
***	Procédures sensibles (État Civil)	Connexion d'individu

(1) , (3) : /!\ Dérogation collectivités < 3.500hab : certificat peut être multi-collectivités , le certificat RGS** d'authentification peut être « multi-mandats » également. Voir : http://www.collectivites-locales.gouv.fr/teletransmission-des-actes-maj-24-fevrier-2015#_ftn5

(2) : le certificat de signature RGS** est « multi-mandats » : c'est une **identité personnelle** , équivalente à CNI, les règles du Code Civil s'appliquent donc de plein droit.

CC BY NC SA

SOMMAIRE

Suivez/Réagissez :
@ADULLACT
@StephaneVast

Webinaire: SIGNATURE ELECTRONIQUE

- Introduction : un peu d'histoire
- Certificat et signature électroniques
- Réglementation administrative
- **Cas pratiques**
- Futurologie, Q&A

CC BY NC SA

Cas pratiques

- En navigateur, connexion sécurisée HTTPS
- Les procédures normalisées : Actes, Helios,...
  - Délibérations, ACTES administratifs
  - BJ recette ou dépense, PJ (facture,...)
- Exemple : réponse dématérialisée à AO
  - Signature de la réponse : Acte d'Engagement
  - Scellement du dépôt (chiffrement d'enveloppe)
- Quelques outils : production, vérification

BY NC SA

Exploitation des Certificats électroniques

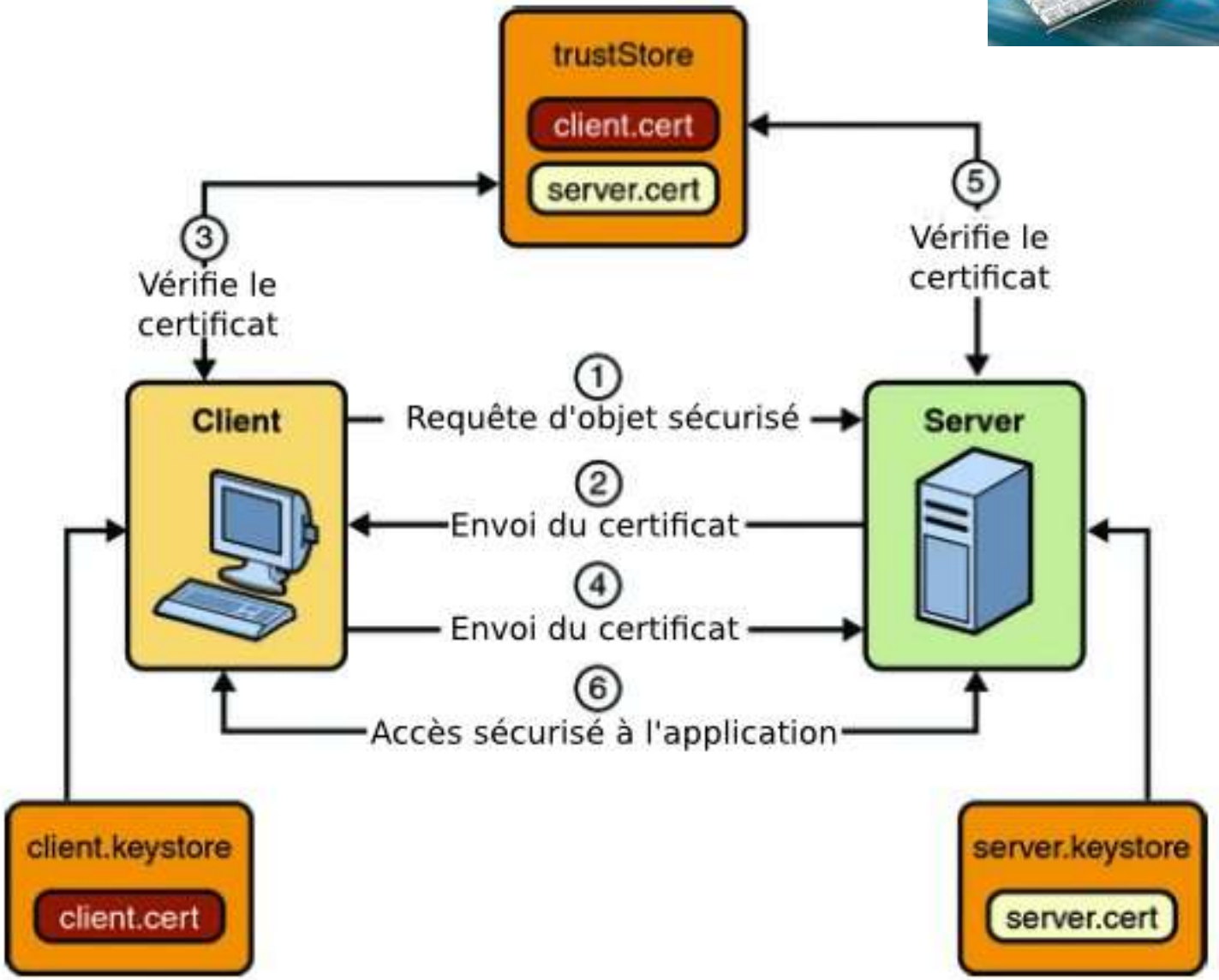
ADULLACT

- Les certificats sont stockés et mis à disposition dans un **keystore** : un « magasin de clés » sécurisé

- Les logiciels doivent avoir accès à un keystore pour exploiter un certificat...

BY NC SA

MCA* = authentification forte



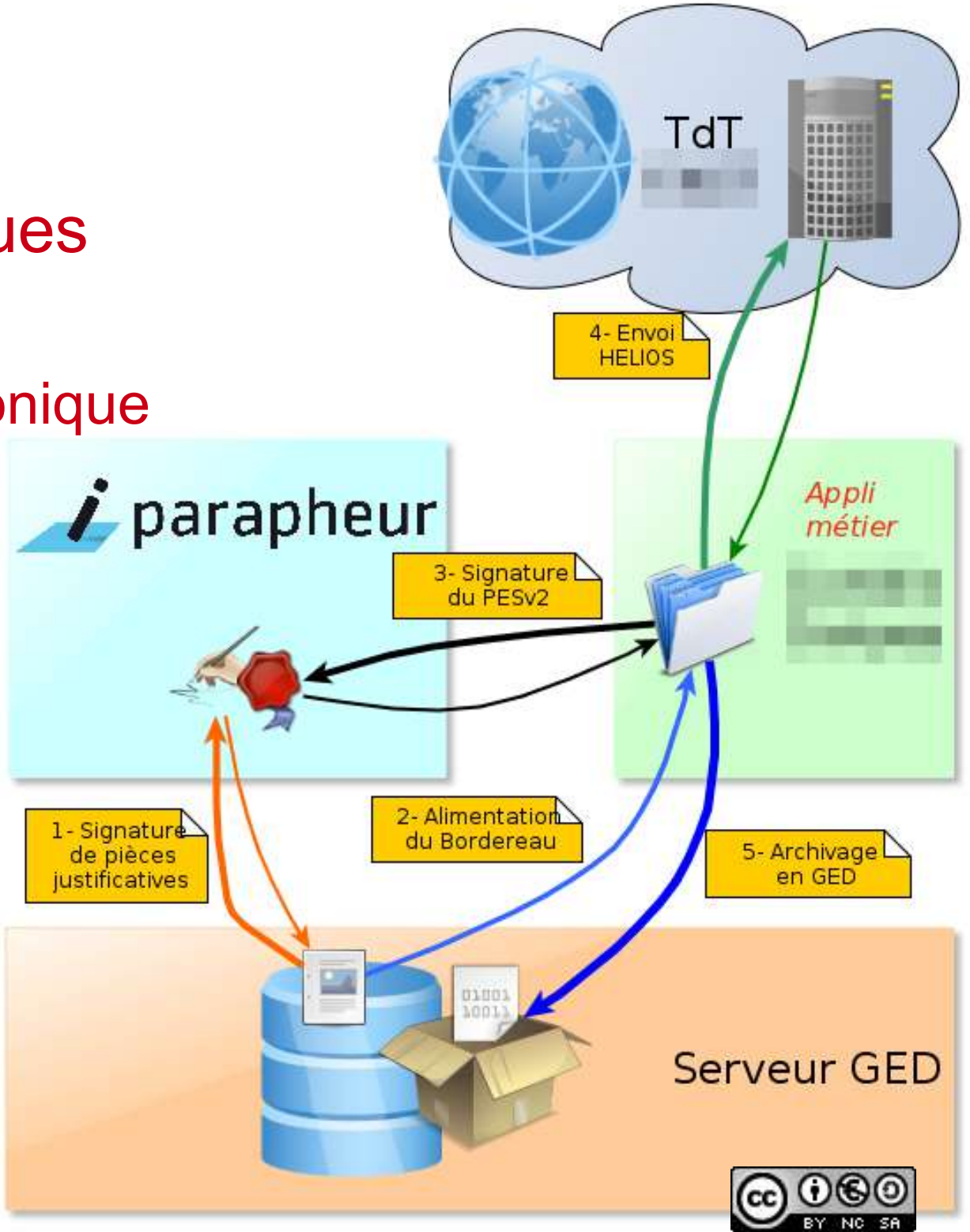
Voir http://www.securiteinfo.com/cryptographie/ssl.shtml

(*)Mutual Certificate Authentication

cc BY NC SA

Démat. Globale

- Pré-requis : Briques transverses :
  - Un parapheur électronique
  - Une GED
- Signature de PJs
- PJs → PESv2
- Signature du PESv2
- Envoi en Paierie
- Versement en GED du PESv2 + Ack



Formats de signatures admis

- Être précis, les contraintes changent selon la procédure dématérialisée

Procédure	Qualification RGS du certificat	Formats de signature autorisés
Acte administratif	* *	- CMS/PKCS#7 (détaché) - PAdES
Marché public (A.E.)	* *	- Détaché : CMS/PKCS#7, CAdES , XML-dSig - PAdES (PDF seulement)
HELIOS Bordereau	* * * * * *	- XAdES enveloppé v1.1.1

cc BY NC SA

Défi : signer sur tablette !

- Certificat RGS** sur Tablette ….

Pas de port USB !!!

cc BY NC SA

Quelques outils...

- **Certificats de classe 0** : WebOSSL ADULLACT
  - Service gratuit en ligne: http://pki.adullact.org
- **Manipulation de Keystores** : PORTECLE (en Java)
  - Projet hébergé sur SourceForge.
- **Signature électronique** : LiberSign, i-Parapheur
  - Adobe Reader !
- **Vérification de signature** :
  - Logiciel libre (Windows, Linux) : Cryptonit (idealX)
  - Logiciel propriétaire gratuit : mySIGN Verifier
  - Web : http://www.verificarfirmaelectronica.com/en/

SOMMAIRE

Suivez/Réagissez :
@ADULLACT
@StephaneVast

Webinaire: SIGNATURE ELECTRONIQUE

- Introduction : un peu d'histoire
- Certificat et signature électroniques
- Réglementation administrative
- Cas pratiques
- **Futurologie (eIDAS)**, Q&A

CC BY NC SA

Le futur passera par e-IDAS

- Le RGS tel que connu ci-dessous va devoir s'adapter à un nouveau règlement européen

Niveaux RGS	Support	Usages possibles
*	Logiciel, matériel	Authentification + Signature,....
**	Seulement matériel	Authentification + Signature, Authentification seule, Signature seule
***	Seulement matériel	Authentification seule, Signature seule

BY NC SA

Demain... eIDAS

- Règlement (UE) eIDAS n°910/2014 du Parlement européen et du Conseil du 23/7/2014.
  - Publié au JOUE du 28 août 2014
  - Identification numérique & services de confiance
  - Un règlement qui abroge la directive 1999/93/CE

- **BUTS**
  - Identité efficace transfrontalière et fiable
  - 3 niveaux de sécurité : faible, substantiel, élevé (attention aux besoins et analyses de risque)

CC BY NC SA

Demain... eIDAS : nouveautés

- Distinction nouvelle entre :
  - Signature électronique : personne physique
  - Signature de personne morale
- Harmonisation des formats à l'échelle UE.
- Chaque État publie la liste des PSCo qualifiés !
  - A venir → « Label de confiance de l'Union »
- Dates clefs :
    - Normes et spécifications techniques : 18/9/2015
    - Actes pour reconnaissance inter-États : 2nd sem. 2015
    - Applicable : dès **1er Juillet 2016**, obligatoire fin 2018

CC BY NC SA

1er Juillet, le règlement entre en vigueur !!

- /o\

Demain... eIDAS : impacts sur le RGS

- Règlement ==> pas de régime « national »
- Nouveautés :
  - « Signature » électronique de personne morale, en fait est un cachet, pas une signature
  - Signature « à distance » reconnue.
  - La fin du tout « token » en mains propres
- Corollaires :
  - Le document électronique devient une preuve
  - Harmonisation européenne : identités numériques, signature électronique, listes de confiance
  - Consécration de : validation de signature, horodatage.

BY NC SA

Mais... retards et tuilage

- Les « Actes d'exécution » ont tardé :
  - L'ANSSI n'a pu se positionner sur les équivalences avec RGS.
  - Pas de texte → pas de procédure d'accréditation
  - Ce 'flou' va durer probablement sur 2016
- NB sur des exceptions prévisibles :
  - les process 'CT-Etat' pourraient se déclarer « hors eIDAS », et rester pur-RGS
  - Donc seuls les AE (marché public) sont concernés !
  - Détails encore à venir...

BY NC SA

eIDAS, méfiance & prudence & patience :-)

ADULLACT

- ATTENTION aux sirènes des vendeurs !
  - « je suis conforme eIDAS » → où est le tampon ANSSI ?
  - « certificats eIDAS » → qualifiés par qui ? pour quoi ?
  - La seule probabilité tangible concerne **RGS*** ....** (mais qui utilise vraiment du RGS***, 3étoiles !???)
- C'est de la **présomption** de conformité. Il n'y a pas d'organisme certificateur !
- HELIOS/ACTES : rien ne change en 2016 ?
  - Gardez vos certificats RGS** , ils restent valides
  - La DGFiP et la DGCL n'ont pas de position officielle
- Ce qui est « bon » pour le privé ne l'est pas partout

CC BY NC SA

Pour aller plus loin sur le sujet...

- Legifrance

  http://www.legifrance.gouv.fr/

- L'ANSSI

  http://www.ssi.gouv.fr/fr/reglementation-ssi/signature-electronique/

- Wikipedia, l'encyclopédie libre !

  http://fr.wikipedia.org/wiki/Certificat_électronique

  http://fr.wikipedia.org/wiki/Signature_numérique

  http://fr.wikipedia.org/wiki/Signature_électronique_manuscrite

  https://en.wikipedia.org/wiki/Transport_Layer_Security#Client-authenticated_TLS_handshake

  .....

CC BY NC SA

Quelques références documentaires...

- Vu pour système ACTES

  http://www.collectivites-locales.gouv.fr/teletransmission-des-actes-maj-24-fevrier-2015

  « Le propre du certificat d'authentification et/ou de signature (...) [RGS**] est d'être nominatif. Seul leur titulaire peut l'utiliser. »

  « les établissements publics locaux de communes de moins de 3 500 habitants peuvent utiliser, **pour la télétransmission**, les certificats d'authentification de leur commune de rattachement. La personne qui, dans les deux collectivités, est habilitée à télétransmettre pour ces deux émetteurs utilisera le même certificat d'authentification utilisateur, que ce soit pour télétransmettre au nom de la commune ou au nom de l'établissement public local. De même, en cas de secrétaire de mairie employé par plusieurs communes, cette personne pourra utiliser le même certificat d'authentification utilisateur, quelle que soit la commune émettrice de l'acte télétransmis. »

BY NC SA

MERCI !

Webinaire: LA SIGNATURE ELECTRONIQUE

par Stéphane Vast
chef produits i-Parapheur & LiberSign

Suivez/Réagissez :

@ADULLACT

@StephaneVast

ADULLACT

Association des Développeurs et des Utilisateurs de Logiciels Libres pour les Administrations et les Collectivités Territoriales

CC BY NC SA

Espace démo, Q&A

ADULLACT

Des questions ,

des projets ?

Suivez/Réagissez :
@ADULLACT
@StephaneVast

CC BY NC SA