Les ateliers de la démat'

La signature électronique

Céline Guyon – 24 novembre 2016

Signature électronique et confiance numérique

A quoi sert une signature ?

Signature électronique et confiance numérique

- La signature électronique ne fournit pas, comme la signature manuscrite, un élément graphique immédiatement identifiable et qui suffise à reconnaître le signataire

- La signature électronique est souvent présentée comme indispensable dans l'univers numérique. Mais qu'entend-on par-là exactement ?
- Quelle différence entre clef, certificat, empreinte, horodatage ?
- Juridiquement, une signature électronique a-t-elle la même valeur qu'une signature manuscrite ?

Contexte

- La dématérialisation des documents et des échanges est désormais une réalité incontournable
- Elle s'accompagne de nouvelles exigences, notamment en matière de confiance et de valeur juridique
  - Permettre au lecteur d'un document d'identifier la personne ou l'organisme qui l'a émis,
  - Garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a rédigé et le moment où le lecteur le consulte,
  - Au même titre que les documents papier sont authentifiés par une signature manuscrite, les documents dématérialisés doivent offrir toutes les garanties en matière de preuve

Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de preuve aux technologies de l'information et relative à la signature électronique

- L'écrit devient indépendant de son support
  - Jusqu'alors, c'était le principe d'indissociabilité entre le support matériel et l'information qu'il porte qui faisait la qualité d'une preuve
- Définition fonctionnelle de l'écrit
  - *« La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d 'une signification intelligible, quels que soient leur support et leur modalités de transmission »*
- Définition de l'écrit électronique
  - *« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier,* ***sous réserve*** *que puisse être dûment* ***identifiée la personne dont il émane*** *et qu'il soit établi et conservé dans des conditions de nature à en garantir l'****intégrité*** *»*

Contexte

- Définition fonctionnelle de la signature électronique (article 1397 du Code civil)
  - *« La signature nécessaire à la perfection d 'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte »*
  - *« Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache »*

- Décret n°2001-272 du 30 mars 2001 relatif à la signature électronique
- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives est venue préciser le cadre juridique relatif aux échanges électroniques dans la sphère publique. Elle pose notamment des règles en matière de signature électronique dans le secteur public
- Règlement eIDAS (règlement européen du 23 juillet 2014)

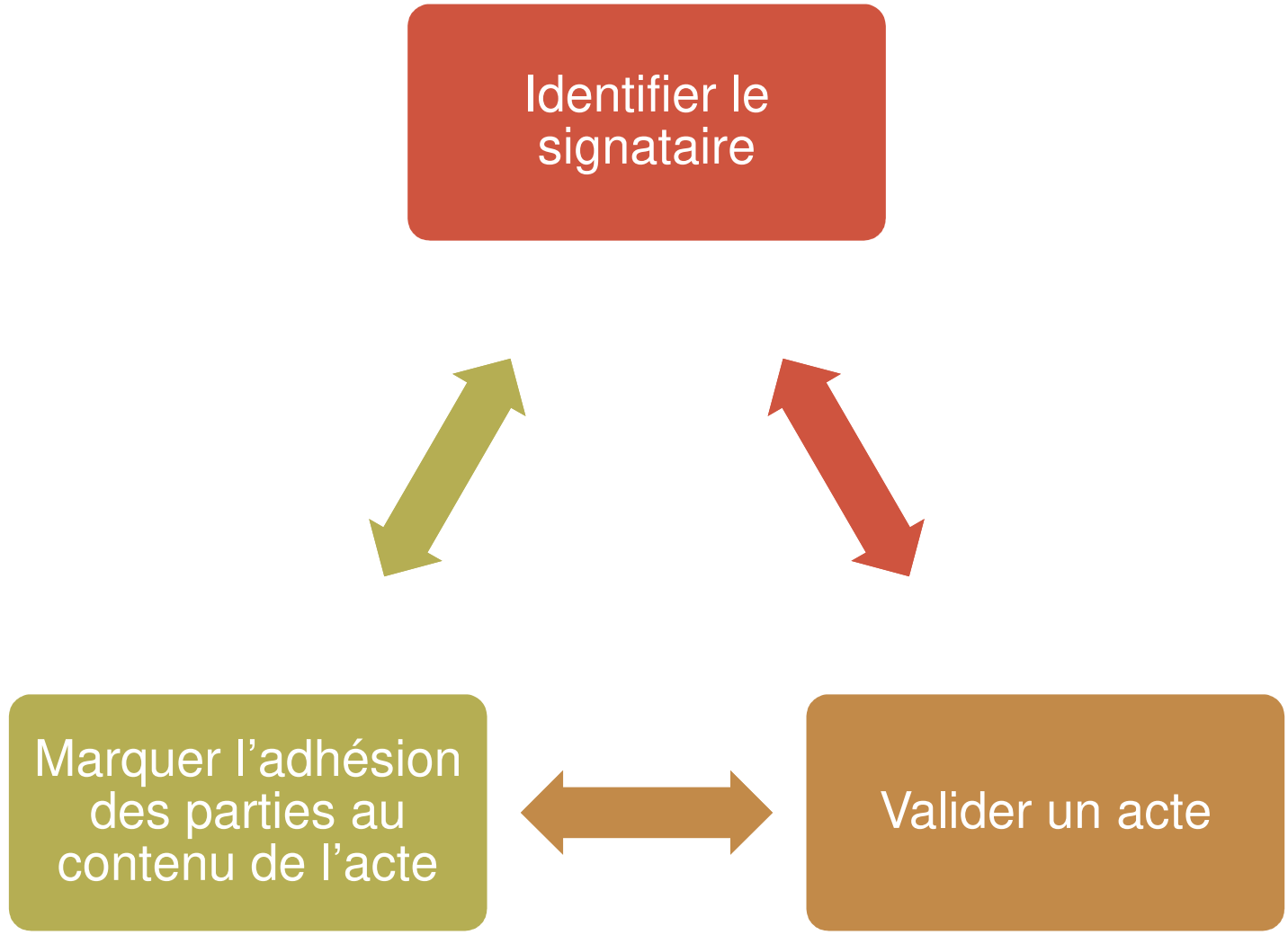
Contexte

- La signature manuscrite est devenue un acte banalisé au point de ne plus vraiment apprécier sa fonction
- La signature résulte d'un long processus historique qui commence au VIIe siècle et s'achève au XVIe siècle lorsqu'elle devient obligatoire, en 1554

- La signature est un signe de validation, c'est-à-dire qu'elle authentifie un acte : elle transforme un document en instrument juridique

- Les signes de validation existent depuis plusieurs millénaires (ex. les sceaux)

A quoi sert une signature ?



L'identité : la base de la signature électronique

- **Identification du signataire**
  - Identité de la personne physique qui signe en son nom propre
  - Identité de la personne physique agissant dans son cadre professionnel
  - Identité d'une personne morale
  - L'identité utilisée pour réaliser une signature électronique est fonction du contexte dans lequel la signature est réalisée :

- **Niveau de fiabilité de l'identité**
  - Certification de l'identité (Identité déclarative/Identité fiable)
  - Adapter le niveau de fiabilité aux besoins = au contexte de l'application dans laquelle cette identité est requise pour la réalisation de la signature électronique

L'identité : la base de la signature électronique

- **Fiabilité de l'identité**
  - 3 niveaux de fiabilité
  - **classe 1** : certification de l'identité d'un signataire sans autre contrôle que la validité de son adresse mail
  - **classe 2** : certification de l'identité d'un signataire à distance, sur la base de copies de ses papiers d'identité
  - **classe 3** : certification de l'identité d'un signataire suite à une rencontre en face à face, et sur présentation des papiers d'identité originaux
- Déclinaison dans le RGS (Référentiel général de sécurité)
  - **Une étoile (*)** correspond à la classe 2
  - **Deux étoiles (**)** correspond à la classe 3+
  - **Trois étoiles (***)** correspond à l'émission d'un certificat qualifié de classe 3+
  - Le symbole « + » signifie que le certificat d'identité délivré est hébergé sur un support cryptographique physique : carte à puce ou clef USB

Le certificat : pièces d'identité électronique

- Le certificat est délivré par une **Autorité de certification**
- **L'enregistrement** (ou enrôlement) du futur porteur
  - Le demandeur du certificat prouve son identité en respectant le processus défini en fonction du niveau du certificat qu'il souhaite acquérir (cf. 3 classes de certificats)
  - L'enregistrement est réalisé par **l'Autorité d'Enregistrement**
- **La fabrication du certificat**
  - Une paire de clefs cryptographiques, appelées « clef privée » et « clef publique » est générée
  - L'identité du signataire et sa clef publique sont liées entre elles dans un fichier appelé le certificat, qui est scellé par l'Autorité de Certification de manière à garantir sa provenance (c'est-à-dire l'Autorité de Certification émettrice), son intégrité (il est impossible de modifier un certificat sans en rendre le scellement invalide), son niveau de sécurité (le certificat mentionne la Politique de Certification définissant les règles appliquées lors de sa délivrance)
  - Le certificat est fabriqué par **l'Opérateur de Certification**

Le certificat : pièces d'identité électronique

- **La délivrance du certificat**
  - Le certificat et la clef privée correspondante (appelée également le « moyen de création de signature électronique ») sont remis à leur porteur selon le mode de délivrance défini dans la Politique de Certification. Ainsi, si le niveau de sécurité impose un support physique, une carte à puce ou une clef USB cryptographique sera remise au porteur ainsi qu'un code PIN, équivalent du code des cartes bancaires, qui permettra au seul porteur l'usage de sa clef privée pour réaliser des signatures électroniques
- **Cycle de vie du certificat**
  - Durée de vie limitée
  - Révocation du certificat

Le support du certificat

La signature électronique : une chaine de confiance

- Un tiers (l'Autorité de certification) se porte garant de l'identité du signataire
- La confiance dans l'identité du signataire découle de la confiance dans l'Autorité de certification
- Cette confiance repose sur le contrôle des Autorités de certification
- Ce contrôle se manifeste par la qualification des Autorités de certification
  - Les conditions de qualification sont définies par l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation
  - Les Autorités de Certification auditées et reconnues conformes à l'arrêté du 26 juillet 2004 sont aptes à émettre des Certificats dits Qualifiés
  - Qualification des autorités de certification (http://www.lsti-certification.fr/images/liste_entreprise/Liste%20PSCe.pdf

Les autres éléments de confiance

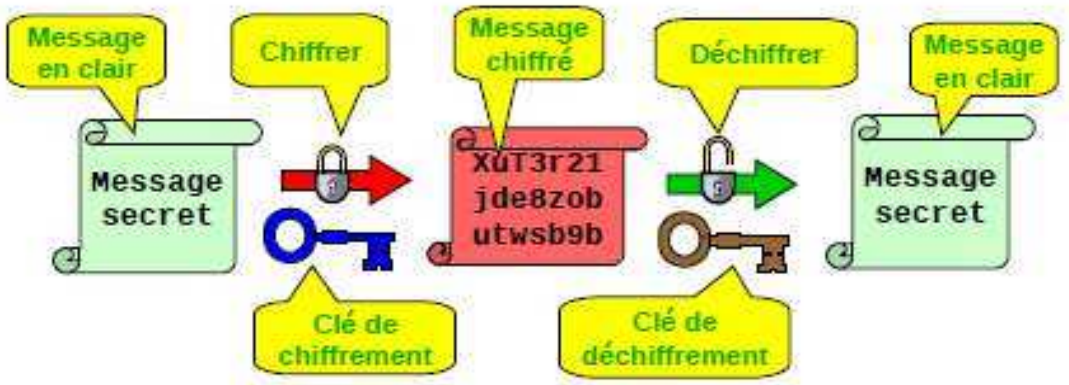
- Le jeton d'horodatage
  - Connaître avec certitude la date et l'heure de réalisation de la signature
  - Contrôler que le certificat du signataire n'était pas révoqué au moment de la signature
- Une preuve de validité du certificat au moment de la réalisation de la signature
  - Sous la forme d'une liste de certificats révoqués ou d'un jeton OCSP (Online Certificate Status Protocol) garantissant que le certificat n'est ni périmé, ni révoqué

La signature électronique côté technique

Concrètement comment ça marche ?

La signature électronique côté technique

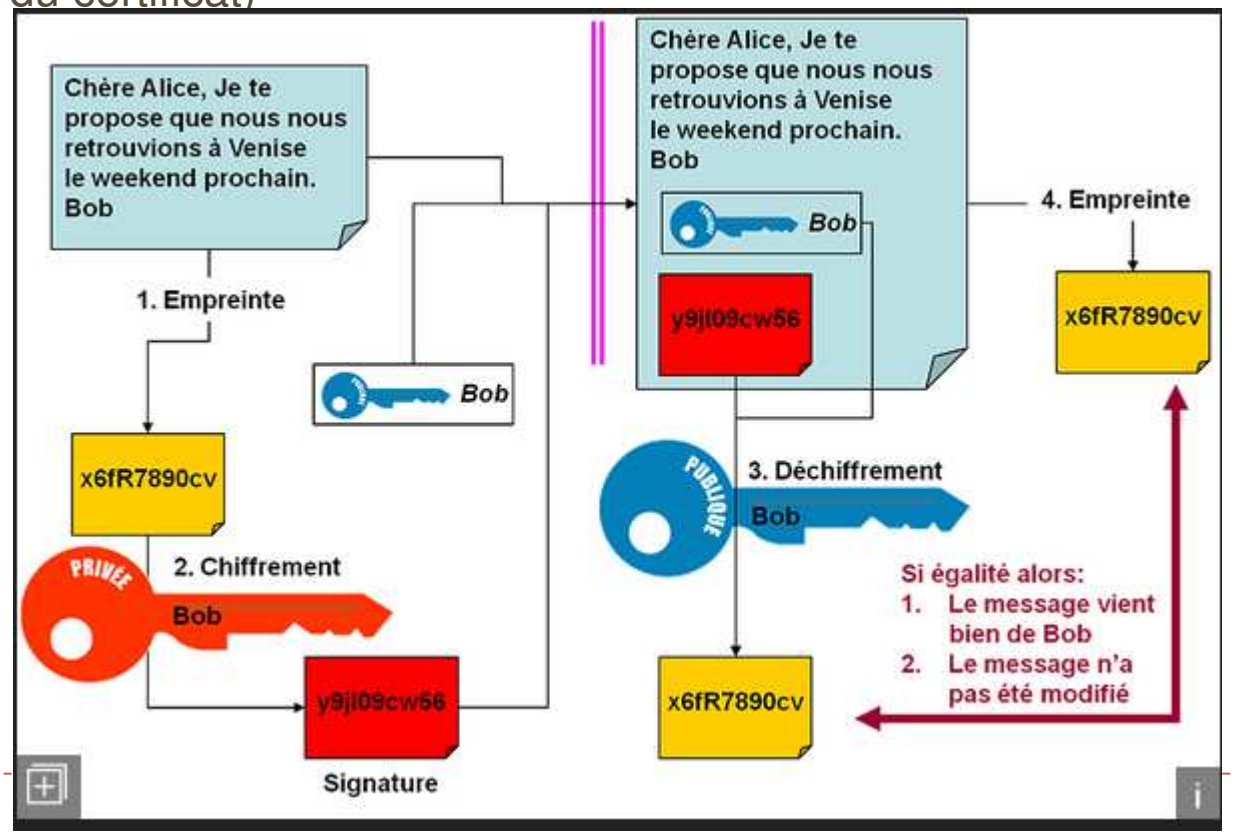
- Prend sa source dans le domaine de la cryptographie



- Le mécanisme est fondé sur la séparation de la clé unique en deux clés distinctes
  - La clé privée est utilisée pour la signature (chiffrement)
  - La clé publique est utilisée pour la vérification de la signature (déchiffrement)

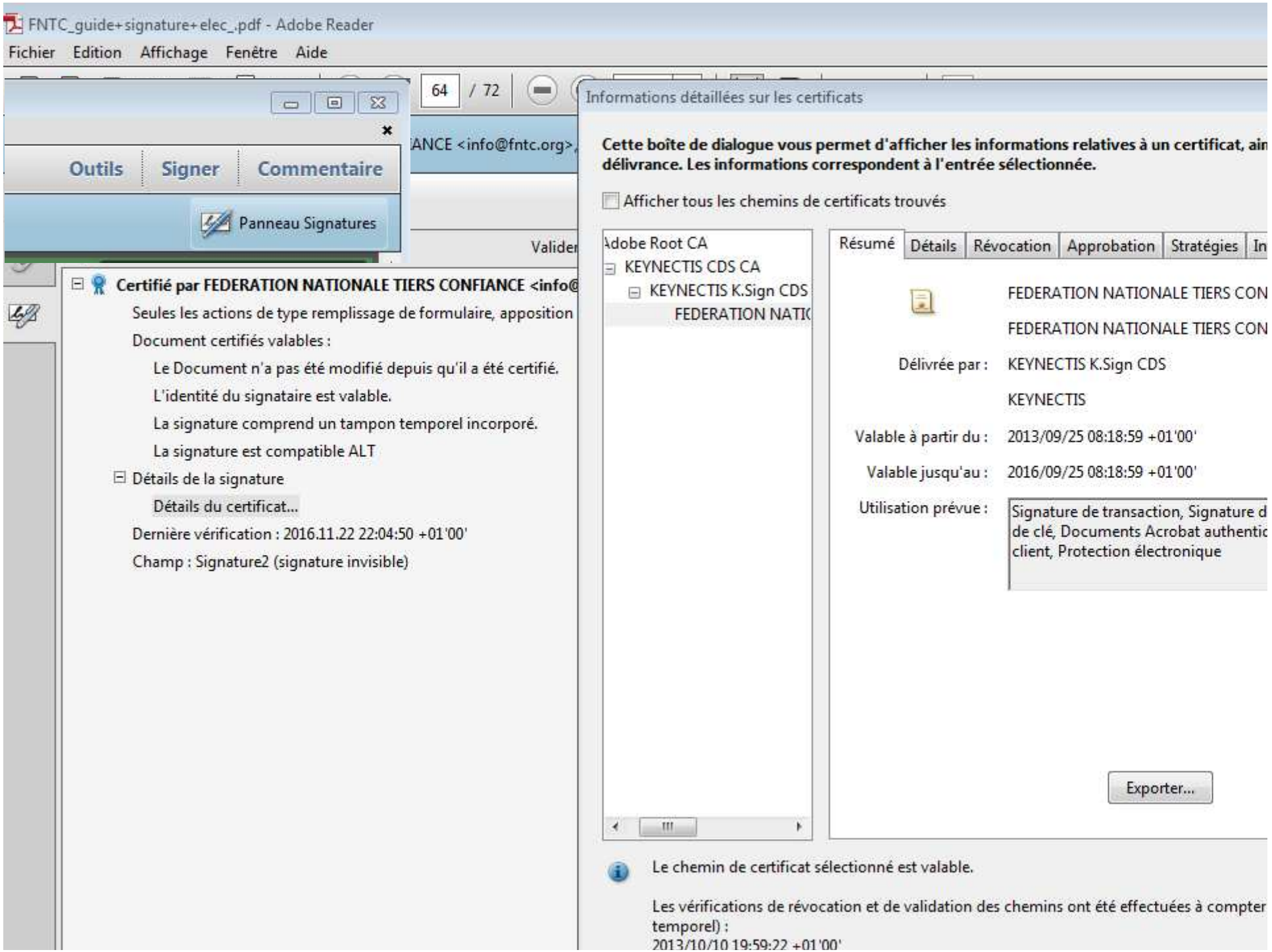
La signature électronique côté technique

- La réalisation technique d'une signature électronique consiste en un calcul mathématique réalisé à partir
  - Du document à signer (ce qui garantira son intégrité)
  - De la clef privée du signataire (ce qui garantira le lien avec son identité au travers du certificat)



La signature électronique côté technique

- Génération d'une empreinte (ou condensat) à partir du document grâce à une fonction mathématique dite fonction de hachage (algorithmes)
  - L'empreinte est indissociable du document dont elle est extraite
- Chiffrement de l'empreinte avec la clé privée (secrète)
  - Etablissement du lien entre la clé privée et son propriétaire (certificat)
- Vérification de l'empreinte à l'arrivée avec la clé publique de l'auteur du document
  - La clé publique correspond à la clé privée
  - Elle est destinée à être communiquée à quiconque veut vérifier la signature
- Confrontation des deux empreintes
  - La signature permet de certifier la provenance du document
  - On parle alors de « non-répudiation » : l'auteur ne peut pas ne pas reconnaître être l'auteur de l'acte dans la mesure où la clé publique ne peut vérifier positivement que ce qui a été signé par la clé privée correspondante


FNTC_guide+signature+elec_.pdf - Adobe Reader
Fichier Edition Affichage Fenêtre Aide
64 / 72
Outils
Signer
Commentaire
Panneau Signatures
ANCE <info@fntc.org>
Valider
Certifié par FEDERATION NATIONALE TIERS CONFIANCE <info@
Seules les actions de type remplissage de formulaire, apposition
Document certifiés valables :
Le Document n'a pas été modifié depuis qu'il a été certifié.
L'identité du signataire est valable.
La signature comprend un tampon temporel incorporé.
La signature est compatible ALT
Détails de la signature
Détails du certificat...
Dernière vérification : 2016.11.22 22:04:50 +01'00'
Champ : Signature2 (signature invisible)
Informations détaillées sur les certificats
Cette boîte de dialogue vous permet d'afficher les informations relatives à un certificat, ain
délivrance. Les informations correspondent à l'entrée sélectionnée.
Afficher tous les chemins de certificats trouvés
dobe Root CA
KEYNECTIS CDS CA
KEYNECTIS K.Sign CDS
FEDERATION NATI(
Résumé
Détails
Révocation
Approbation
Stratégies
In
FEDERATION NATIONALE TIERS CON
FEDERATION NATIONALE TIERS CON
Délivrée par :
KEYNECTIS K.Sign CDS
KEYNECTIS
Valable à partir du :
2013/09/25 08:18:59 +01'00'
Valable jusqu'au :
2016/09/25 08:18:59 +01'00'
Utilisation prévue :
Signature de transaction, Signature d
de clé, Documents Acrobat authentic
client, Protection électronique
Exporter...
Le chemin de certificat sélectionné est valable.
Les vérifications de révocation et de validation des chemins ont été effectuées à compter
temporel) :
2013/10/10 19:59:22 +01'00'

Les différents modes de réalisation d'une signature électronique

- En fonction des contraintes liées au projet et aux signataires, on peut envisager des manières différentes de réaliser une signature électroniques
- La signature électronique autonome
  - Le signataire dispose d'un logiciel de signature + d'un certificat
- La signature électronique à la volée
  - Le signataire fait l'acquisition d'un certificat pour un usage unique
  - Le signataire va s'authentifier à une plateforme
  - Le niveau de confiance sera fonction des conditions d'authentification
- La signature sur tablette
  - Le client appose sa signature manuscrite sur la tablette
  - Une signature électronique à la volée est réalisée en plus de la signature manuscrite
- Les différents types de signature
  - Signature individuelle
  - Signature serveur (cachet) = signature personne morale

Les différents formats de signature électronique

- Tous types de fichiers peuvent être signé**s**
- XAdES : signature électronique XML.
  - Il s'agit d'un format de stockage des signatures électroniques qui peut être indépendant des données signées (la signature constitue alors un fichier XML à part du document signé, qui peut être à n'importe quel format), ou inclus dans le document signé si ce document est lui-même au format XML.
  - Le format XAdES permet la signature multiple du même document par plusieurs signataires
- PAdES : signature électronique PDF.
  - Le format PAdES (PDF Advanced Electronic Signature) est le format des signatures électroniques incluses dans les documents PDF.
  - Il permet la signature multiple du même document par plusieurs signataires, sous la forme de sur-signatures : chaque signataire signe non seulement le document, mais aussi les signatures déjà apposées par les signataires précédents.
- CAdES : aussi appelé PKCS#7 ou CMS

Signature simple et signature sécurisée ou qualifiée

- Toutes les signatures électroniques ont la même valeur juridique
- La signature électronique sécurisée emporte présomption de fiabilité
- Les exigences relatives à la signature sécurisée sont contraignantes à mettre en œuvre et ne concernent dans la pratique qu'une population très réduite, principalement les professions réglementées pour la perfection des actes authentiques

Signature électronique et signature sécurisée

- Le procédé utilisé pour la signature doit mettre en œuvre « *une **signature électronique sécurisée**, établie grâce à un **dispositif sécurisé** de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un **certificat électronique qualifié** »*, décret du 30 mars 2001
- **Dispositif sécurisé** de création de signature électronique : dispositif conforme aux exigences définies dans à l'article 3 du décret du 30 mars 2001 **ET** qui a été certifié conformément à ces exigences
- **Certificat électronique qualifié** : conforme aux exigences de l'article 6 du décret du 30 mars 2001 ; les prestataires de certification peuvent demander à être reconnus comme qualifiés (un certificat peut être qualifié sans que le prestataire soit qualifié)

La signature électronique : ce qu'il faut retenir

- Etre propre au signataire
- Etre créée par des moyens que le signataire puisse garder sous son contrôle exclusif
- Garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable

Fonctions de la signature électronique

- **Authenticité**
- Donner au destinataire la certitude de l'identité de du signataire
  - Identification du signataire
  - Garantie de la provenance du contenu signé
  - Non répudiation
- **Intégrité**
- Donner au destinataire l'assurance que le contenu n'a pas été modifié
  - Garantie de l'intégrité du contenu signé
  - Adhésion au contenu de l'acte

Signature manuscrite et signature électronique

- Le parallèle entre les deux formes de signatures peut être réalisé assez simplement
  - Un individu, le signataire, qui marque son engagement sur les termes du document à signer
  - Un document
    - un papier
    - un fichier informatique
  - La signature est réalisée à l'aide d'un instrument
    - le stylo dans le cas de la signature manuscrite
    - Un logiciel appelé «outil de signature» et un certificat dans le cas de la signature électronique
  - Il y a un secret détenu par le signataire
    - le geste qu'il est le seul à pouvoir réaliser, dans le cas de la signature manuscrite,
    - le code d'utilisation de son certificat dans le cas de la signature électronique
  - L'encre marque le papier, la cryptographie garantit le lien entre le signataire et le document

Signature électronique et signature scannée

- Une signature scannée n'est pas une signature électronique
- Décision de la Cour d'appel de Fort-de-France du 14 décembre 2012
- Les juges ont estimé que, en l'absence de production d'un certificat, la signature en question ne saurait être considérée comme une signature électronique. D'autre part, la signature scannée « *est insuffisante pour s'assurer de l'authenticité de son engagement juridique comme ne permettant pas une parfaite identification du signataire* »

Déployer la signature électronique

Points d’attention et de vigilance

Conserver des documents signés électroniquement

- Conditions de conservation des écrits numériques sont définies dans le code civil, article 1366
- « L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »
- Un projet de déploiement de la signature électronique doit s'accompagner du déploiement d'un système d'archivage électronique

La conservation de la signature électronique dans le temps

- Les obstacles
  - Impossibilité de « rejouer » une signature électronique…dans le temps
  - La conservation à moyen et long terme peut imposer des migrations de format… qui affectent la structure du document et modifient son train de bits électronique…donc son empreinte….et son intégrité ?
- Les réponses
- Juridiques
  - Les opérations de migration pour la conservation n'enlèvent pas au document son caractère juridique ni son caractère d'original (cf. décrets n°2005-972 et 973 du 10 août 2005 relatifs aux actes authentiques des huissiers et des notaires)
- Organisationnelles
  - Conserver la trace des opérations de vérification de la validité de la signature électronique
  - Etablir un cadre de confiance de l'archivage électronique

Mettre en place une signature électronique

- Les projets qui incluent l'usage de la signature électronique doivent être menés du point de vue métier et organisationnel, de même que tout autre projet de l'entreprise ou de l'organisation

- Un projet structurant
  - Implications juridiques
  - Dimension humaine
  - Aspects économiques
  - Implications à long terme sur le SI

- Adapter les exigences et le niveau de sécurité en fonction des besoins

Les caractéristiques du projet

- Volet outils
  - Le parapheur électronique
- Volet organisation
  - Déployer un parc de certificats
  - Adapter le niveau de sécurité aux besoins
  - Former et sensibiliser les utilisateurs
- Volet procédure
  - Délégations de signature
  - Politique de signature, Convention de preuve
- Volet archivage
  - Conserver les documents signés électroniquement