



Titre du document

Tâche 1.7 Elaboration du système de signature électronique

Livrable : Tâches 1.7.1 : Publication résultats de recherche de méthode d'authentification et de cryptographie autonome

Objet du document

L'objectif de ce document est de prendre connaissance des moyens à mettre en œuvre sur les plans techniques, juridiques, organisationnels en matière de sécurisation de la signature électronique.

Informations sur le document

Responsable	Référence	Description	Date livraison
CHONOSERVICES	T1.7.1	Version 1.0	18/04/2013
CHONOSERVICES	T1.7.1	Version 2.0	15/07/2013

Contributions

Contributeurs	Pourcentage
CHONOSERVICES	100 %


Table des matières

1	Principes cryptographiques	4
1.1	Cryptographie symétrique – Un aperçu	4
1.2	Cryptographie asymétrique – les secrets	4
1.3	Principes de cryptographie asymétrique – Chiffrement	5
1.4	Principes de cryptographie asymétrique – La signature	5
1.5	Certificats et acteurs	5
1.6	Cryptographie à clé publique – Remarques	7
1.7	Signature électronique : les étapes du cycle de vie	7
1.8	Idée reçue.....	7
1.9	Outils cryptographiques.....	8
2	Le certificat	9
2.1	Le certificat : principe.....	9
2.2	Le certificat : son format	10
2.3	Le certificat : délivrance (vue simplifiée).....	11
2.4	Le certificat : organisation des classes de certificats	11
2.5	Le certificat : conclusion	12
3	La signature électronique	13
3.1	La signature électronique : principe	13
3.2	La signature électronique ne se voit pas !.....	13
3.3	Les étapes de la signature électronique	14
3.4	La signature électronique : les moyens.....	14
3.5	La signature électronique : les formats.....	15
4	L'horodatage	16
4.1	L'horodatage : principe	16
4.2	L'horodatage : valeur.....	16
4.3	L'horodatage : demande de jeton	17
5	L'archivage électronique.....	18
5.1	L'archivage électronique : principe	18
5.2	L'archivage électronique : rappel des normes	18
5.3	L'archivage électronique : Avantages et réduction des risques	18

5.4	L'archivage électronique à valeur probatoire	19
5.5	Archivage : dépôt.....	20
5.6	Archivage : consultation	21
6	Moyens juridiques	21
6.1	Le référentiel documentaire.....	21
6.2	Conditions Générales de Vente et Conditions Générales d'Utilisation.....	21
6.3	Convention de preuve	22
6.4	Politique de signature	22
6.5	Politique de gestion des preuves.....	23
6.6	Conclusion	23
6.7	Les « niveaux » de sécurité.....	24
7	Acteurs du marché et ROI.....	25
7.1	Les éléments dimensionnants	25
7.2	Les éléments secondaires.....	26
7.3	Acteurs du marché pour la signature et l'horodatage	26
7.4	Acteurs du marché pour l'archivage.....	27
7.5	ROI	27
8	Retours d'expériences sur des exemples concrets et bonnes pratiques à favoriser.....	29
8.1	Dans un contexte marchand en ligne : sur internet.....	29
8.2	Dans le monde de la téléphonie mobile : en agence.....	30
8.3	Dans le monde des assurances : sur tablette	31

1 Principes cryptographiques

1.1 Cryptographie symétrique – Un aperçu

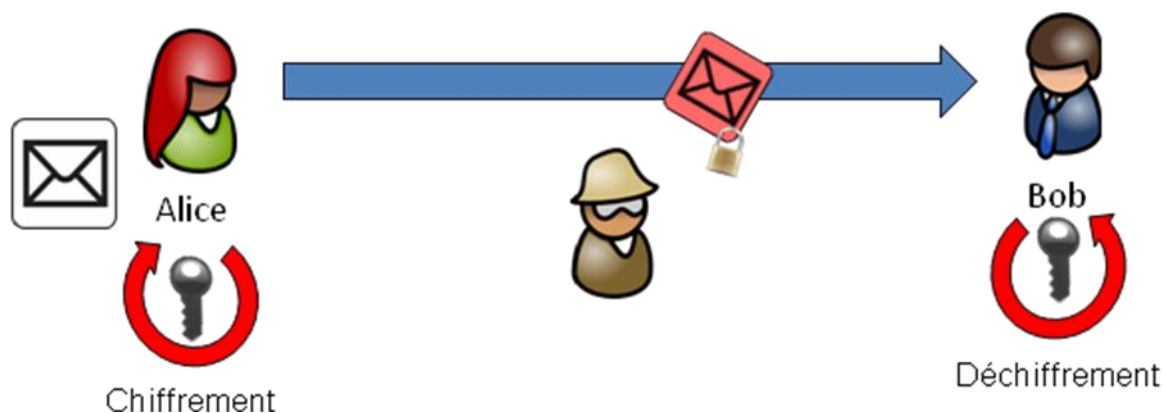
Les utilisateurs partagent une clé secrète 

Chiffrement et déchiffrement sont deux opérations symétriques


- La même clé est utilisée « dans un sens » et « dans l'autre »

Principale difficulté : la distribution des clés

Limitation : ne permet pas réellement la non-répudiation (puisque les clés sont partagées)



1.2 Cryptographie asymétrique – les secrets

Chaque utilisateur dispose d'un bi-clé 

- Une clé publique
- Une clé privée

La clé publique peut être librement diffusée

Les deux clés sont fortement liées (mathématiquement)

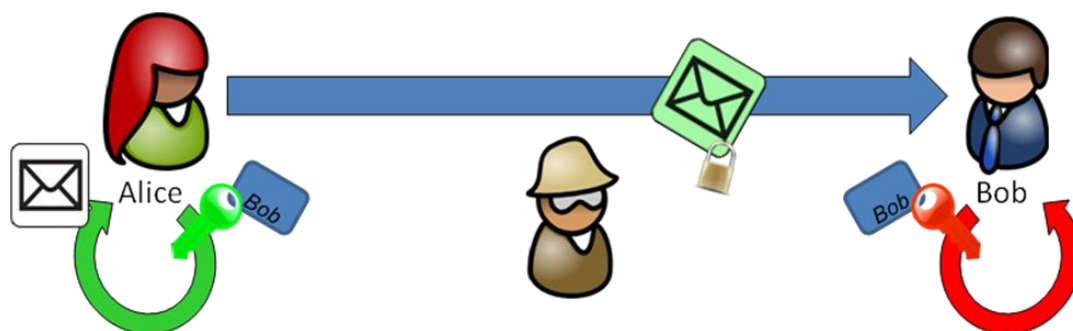
On ne peut pas déduire l'une de l'autre

Ce que fait l'une, l'autre seule permet de le défaire

- Ce que je *chiffre* avec la clé publique, la clé privée permet de le *déchiffrer*
- Ce que je *chiffre* avec la clé privée, la clé publique permet de le *déchiffrer*

Il y a asymétrie des *opérations*

1.3 Principes de cryptographie asymétrique – Chiffrement



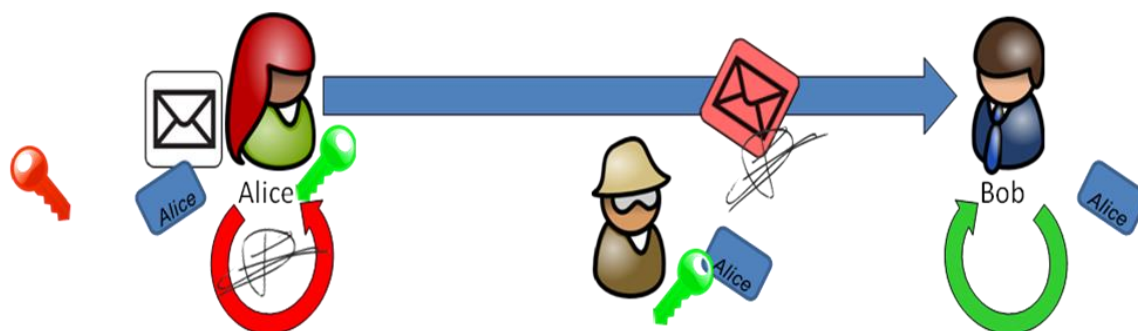
Alice souhaite transmettre un message à Bob...

- Sans être écoutée
- Sans que son message ne soit modifié

Alice *chiffre* avec la clé publique de Bob

Bob *déchiffre* avec sa clé privée

1.4 Principes de cryptographie asymétrique – La signature



Bob souhaite...

- Être sûr que le message qu'il reçoit provient bien d'Alice

Alice *chiffre* avec sa clé privée

Bob *déchiffre* avec la clé publique d'Alice

Tout le monde peut s'assurer que le message provient bien d'Alice

1.5 Certificats et acteurs

- **Autorité de certification (A.C.)**

Au sein d'un prestataire de services de certification électronique (P.S.C.E.), une A.C. a en charge, au nom de et sous la responsabilité de ce P.S.C.E., l'application d'au moins une

politique de certification (P.C.). Elle est identifiée en tant qu'émetteur dans les certificats émis selon cette P.C.

- **Chaîne de certification**

Ensemble d'A.C. au sein duquel chaque A.C. est certifiée par une A.C. d'échelon supérieur.

- **Certificat électronique**

Fichier électronique attestant qu'une bi-clé appartient à une personne physique, une personne morale, un élément matériel ou un logiciel identifié, directement ou indirectement (pseudonyme). Il est délivré par un P.S.C.E. En signant le certificat, l'A.C. valide le lien entre l'identité de la personne ou de l'élément considéré avec la clé publique.

- **Politique de certification (P.C.)**

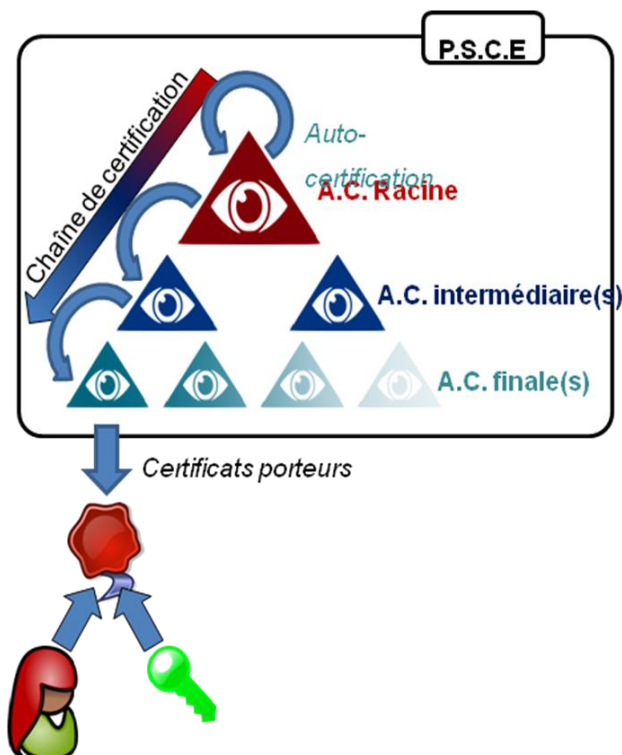
Document décrivant les exigences de sécurité et les procédures mises en œuvre par une A.C. et qui précise l'applicabilité d'un certificat électronique délivré selon ladite P.C.

- **Infrastructure de gestion de clés (I.G.C. / P.K.I.)**

Ensemble de composants, fonctions et procédures dédiés à la gestion de clés cryptographiques asymétriques et des certificats associés.

- **Prestataire de certification électronique (P.S.C.E.)**

Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un P.S.C.E. comporte au moins une A.C.



1.6 Cryptographie à clé publique – Remarques

- Les bi-clés de chiffrement et de signature sont distincts
- Performances

Les opérations asymétriques sont plus coûteuses (temps et espace) que les opérations symétriques

On utilise donc souvent du chiffrement hybride (clé secrète chiffrée asymétriquement)

On signe un condensé du message (empreinte, hash) plutôt que le message lui-même

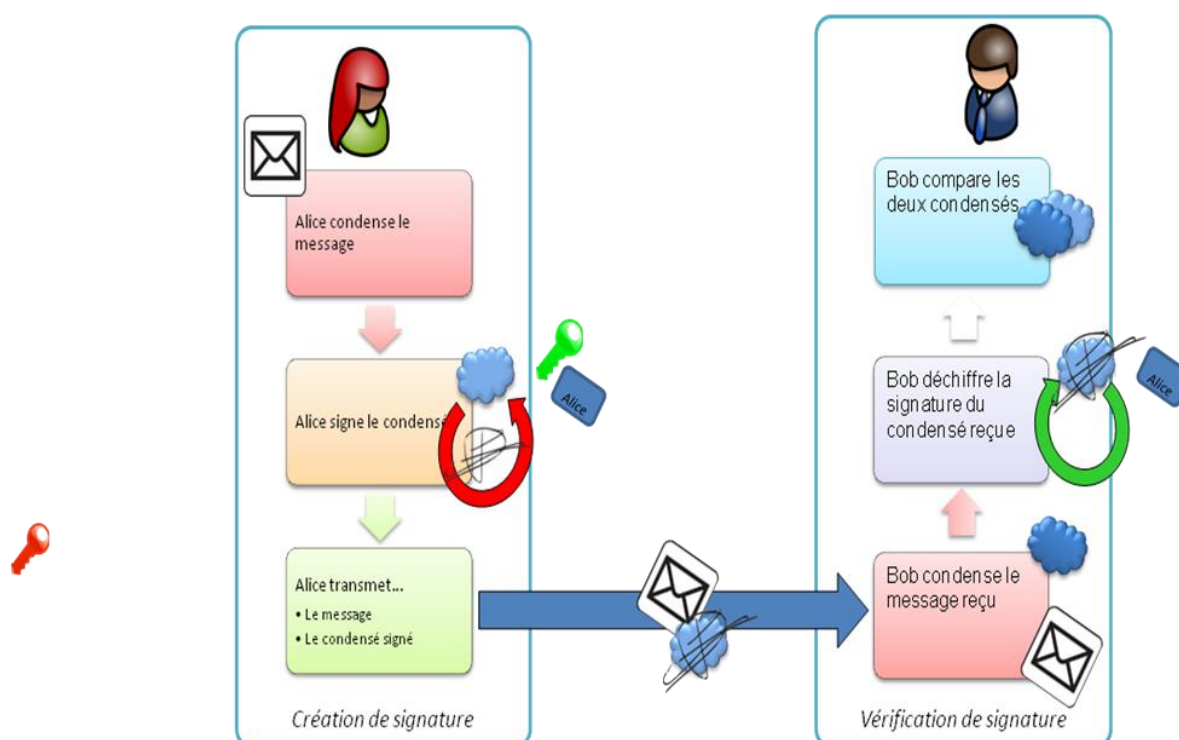
- Algorithmes de hachage/condensation/empreinte

○ ~~MD5, SHA-1, SHA-224~~

○ SHA-256, SHA-384, SHA-512

○ ...

1.7 Signature électronique : les étapes du cycle de vie



1.8 Idée reçue

Récapitulatif des risques principaux à éviter après la signature d'un contrat :

- Que le contractant conteste avoir signé le contrat,
- Que le contractant conteste le contenu du contrat,

- Que le contractant conteste la date d'exécution du contrat,

La démarche naturelle serait d'ajouter une « signature manuscrite numérisée » :

- Le principe étant de numériser la signature manuscrite du contractant et de l'apposer sur le document électronique.

La « signature manuscrite numérisée » ne permet de garantir ni l'identité du signataire ni l'intégrité du contrat. Elle est considérée comme une simple copie de la « signature manuscrite ».

En revanche, elle permet de conserver les habitudes du contractant. Elle pourrait être un élément prépondérant dans le déploiement d'une solution de contractualisation électronique.

1.9 Outils cryptographiques

La sécurisation d'une solution de « contractualisation électronique » devra s'appuyer sur la cryptologie et les mécanismes qui en découlent :

L'identification,

Le contractant devra se munir d'un « certificat électronique » (pièce d'identité électronique),

L'authentification,

Mécanisme permettant de vérifier l'identité d'un contractant,

La signature électronique,

Mécanisme permettant de garantir l'intégrité du document et la non-répudiation par le signataire du document signé, et d'authentifier l'auteur,

L'horodatage,

Mécanisme consistant à ajouter une date et une heure à un évènement,

L'archivage,

Mécanisme de conservation de données électroniques (preuves) considérées comme « figées ». Ce mécanisme met en œuvre des moyens pour stocker, sécuriser, pérenniser, restituer, tracer et détruire les données électroniques archivées.

2 Le certificat

2.1 Le certificat : principe

La « signature électronique » d'un document nécessite l'utilisation d'un « certificat électronique » (appellation vulgaire).

Ce certificat est un fichier électronique assimilable à une pièce d'**identité** électronique. Il contient notamment :

- des informations personnelles :
 - Nom, prénom,
 - SIREN,
 - @ email,
 - ...
- Une clé privée permettant de réaliser des opérations cryptographiques (signature électronique)

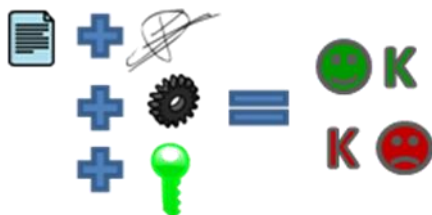
Le certificat permet de signer des documents électroniques en ayant la garantie de l'**identité** du signataire.

Techniquement,

- Le signataire n'utilise qu'une **clé privée** pour **créer** une signature



- Le destinataire n'a besoin que d'une **clé publique** pour **vérifier** une signature



Le bi-clé ne contient pas l'**identité** du signataire

Un **certificat** est une donnée assurant le lien entre

- une clé publique
- une personne (morale ou physique)



2.2 Le certificat : son format

Le « certificat électronique » peut être délivré sous plusieurs formes :

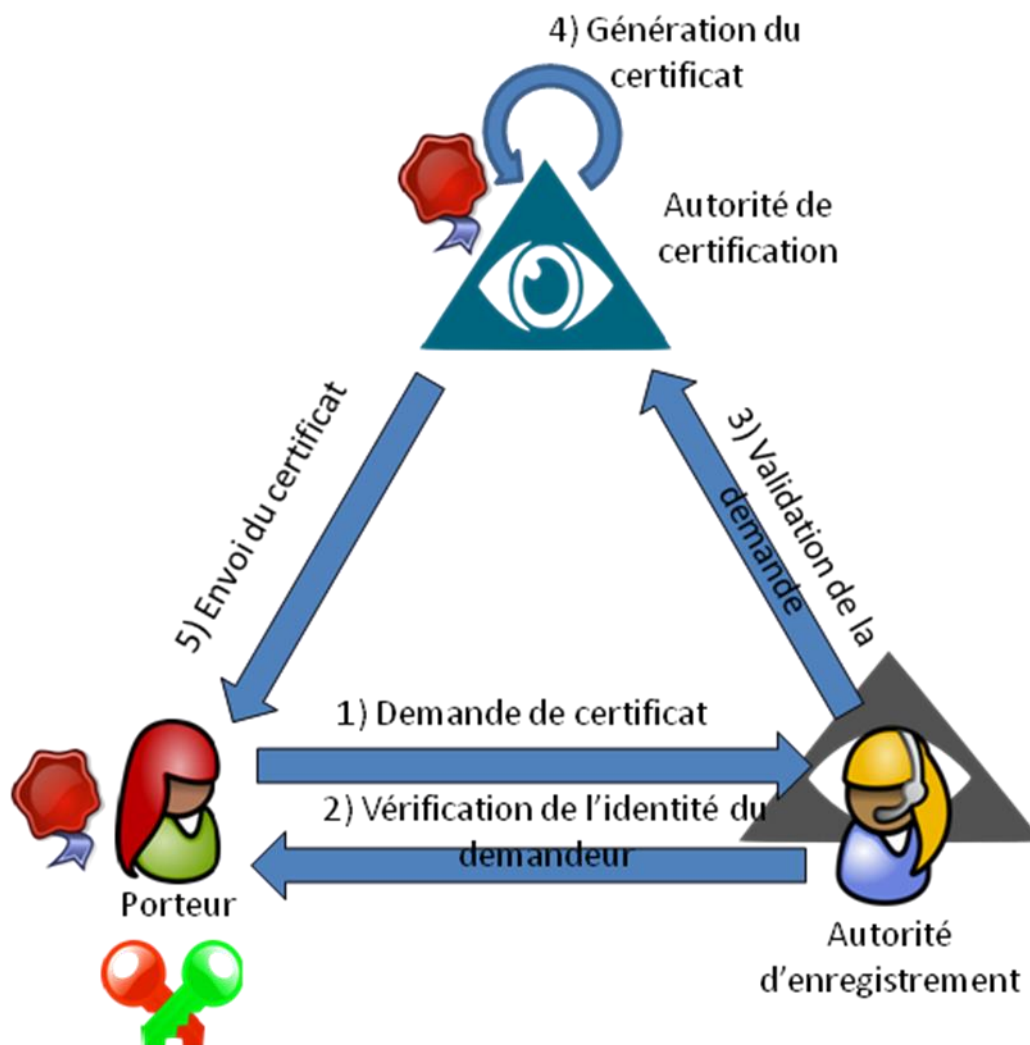
Logiciel : certificat logiciel (.pfx, p12, etc ...)

- Niveau de sécurité minimum,
- Comme tout fichier électronique, le certificat logiciel peut être dupliqué. Par conséquent, l'appartenance exclusive de la clé privée au signataire n'est pas garantie.

Matériel : sur support cryptographique (carte à puce, carte SIM, clé USB cryptographique, ...),

- Niveau de sécurité maximum,
- Aussi appelé SSCD (*Secure Signature Creation Device* en anglais), le support cryptographique permet de sécuriser la clé privée et par conséquent l'empêche d'être copiée ou volée. L'accès à la clé privée est protégé par un mot de passe (ou code PIN) connu exclusivement par le signataire.

2.3 Le certificat : délivrance (vue simplifiée)



2.4 Le certificat : organisation des classes de certificats

L'Autorité de Certification peut définir plusieurs politiques de certification en fonction...

- Du mode d'enregistrement (face-à-face ou pas, par exemple...)
- De l'utilisation du certificat (authentification, signature, chiffrement...)
- Du type de porteur (personne physique, serveur, ...)
- Du mode de stockage de la clé privée (H.S.M., clé USB ou carte à puce, certificat logiciel)

Elle distingue alors des classes de certificats et définit en même temps les conditions et le **niveau de son engagement**.

2.5 Le certificat : conclusion

Le « certificat électronique » est délivré par une AC (Autorité de Certification) dont le rôle est de vérifier l'**identité** et de faire le lien entre la clé privée et l'identité du signataire.

La délivrance de certificat repose sur une vérification de l'**identité**. Cette vérification est plus ou moins lourde selon le niveau de certificat souhaité :

- À minima, une photocopie des pièces d'**identité** peut satisfaire. Dans ce cas, le certificat est souvent délivré sous forme logiciel.
- Un déplacement physique du demandeur de certificat auprès de l'AC et une vérification de l'**identité** en face-à-face peut être envisagés. Dans ce cas, le certificat est souvent livré sous forme de SSCD.

Conclusion : plus la démarche de vérification de l'identité sera lourde, plus la « qualité » du certificat et des signatures produites sera élevé.

3 La signature électronique

3.1 La signature électronique : principe

La production d'une signature électronique nécessite l'usage d'un **certificat électronique** (identité électronique remise par une « Autorité de Certification »)



La signature électronique permet...

- De garantir **l'intégrité** d'un message électronique
- D'**authentifier** son émetteur de façon « certaine »

Comme une signature papier, la création d'une signature électronique a pour seul objectif de démontrer à un tiers que le document a été approuvé par une personne identifiée.

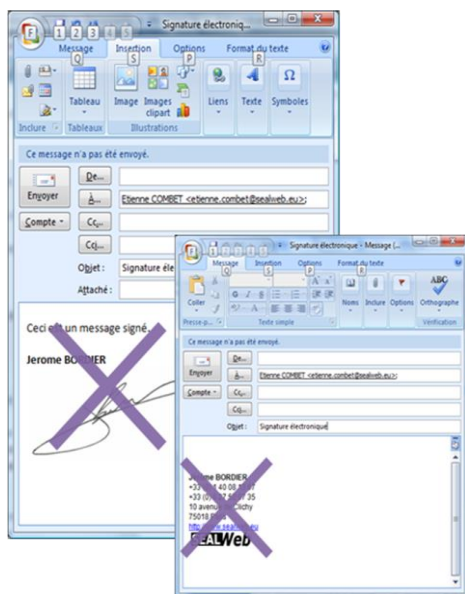
En plus de la signature papier, la signature électronique permet de démontrer que le document n'a pas été modifié.

3.2 La signature électronique ne se voit pas !

La signature électronique est utilisée pour des échanges présentant des enjeux juridiques, utilisant assez rarement le canal *mail*

La signature électronique est généralement intégrée dans une logique applicative ou métier

- Logiciel de *workflow* métier
- Logiciel vertical spécifique à un métier
- Parapheur de signature électronique



3.3 Les étapes de la signature électronique

Je visualise le document que je vais signer

Je clique sur le bouton « signer »

Le contrat est sécurisé.



3.4 La signature électronique : les moyens

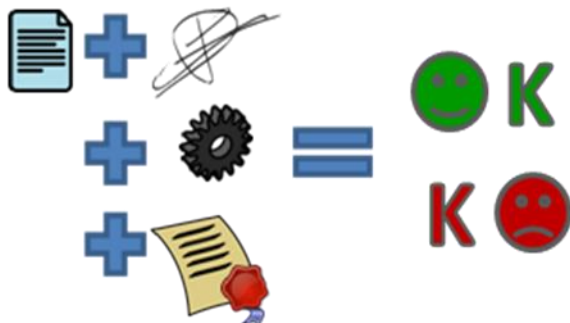
Pour **créer** une signature électronique, il faut...

- Le ou les documents à signer
- Un logiciel de signature
- Un certificat électronique
 - Fichier logiciel
 - Support physique (clé USB, carte à puce)



Pour **vérifier** une signature électronique , il faut...

- Le ou les documents signés
- La signature électronique (fichier)
- Un logiciel spécifique
- Des données de certification



3.5 La signature électronique : les formats

Trois grandes familles

Binaires

- PKCS #7
- CMS, S/MIME
- CAdES



Signature enveloppante :
Les données signées sont contenues dans la structure de la signature

XML

- XML-Dsig
- XAdES



Signature enveloppée :
La signature est contenue dans la structure des données signées

PDF (enveloppée)

- Signature PDF (PKCS #7)
- PAdES



Signature détachée :
La signature et les données signées sont contenues dans deux structures distinctes (deux fichiers ou au sein d'un même fichier)

4 L'horodatage

4.1 L'horodatage : principe

L'horodatage ?

L'horodatage est un mécanisme consistant à apposer une date et une heure à un évènement sous forme de jeton d'horodatage.

Le jeton d'horodatage ?

Le jeton d'horodatage est un fichier résultant de l'association de l'empreinte des données horodatées (hash) et d'une date et une heure provenant d'une source de temps fiable, le tout étant signé électroniquement par l'Autorité d'Horodatage.

Que vérifie t-on avec un jeton ?

L'empreinte de chaque document étant unique, la comparaison d'un fichier avec un « hash » permet de vérifier qu'ils se correspondent fidèlement et par conséquent que le fichier existait dans sa forme actuelle à la date du jeton. La signature électronique de l'Autorité d'Horodatage scelle le jeton, empêchant sa modification intentionnelle.

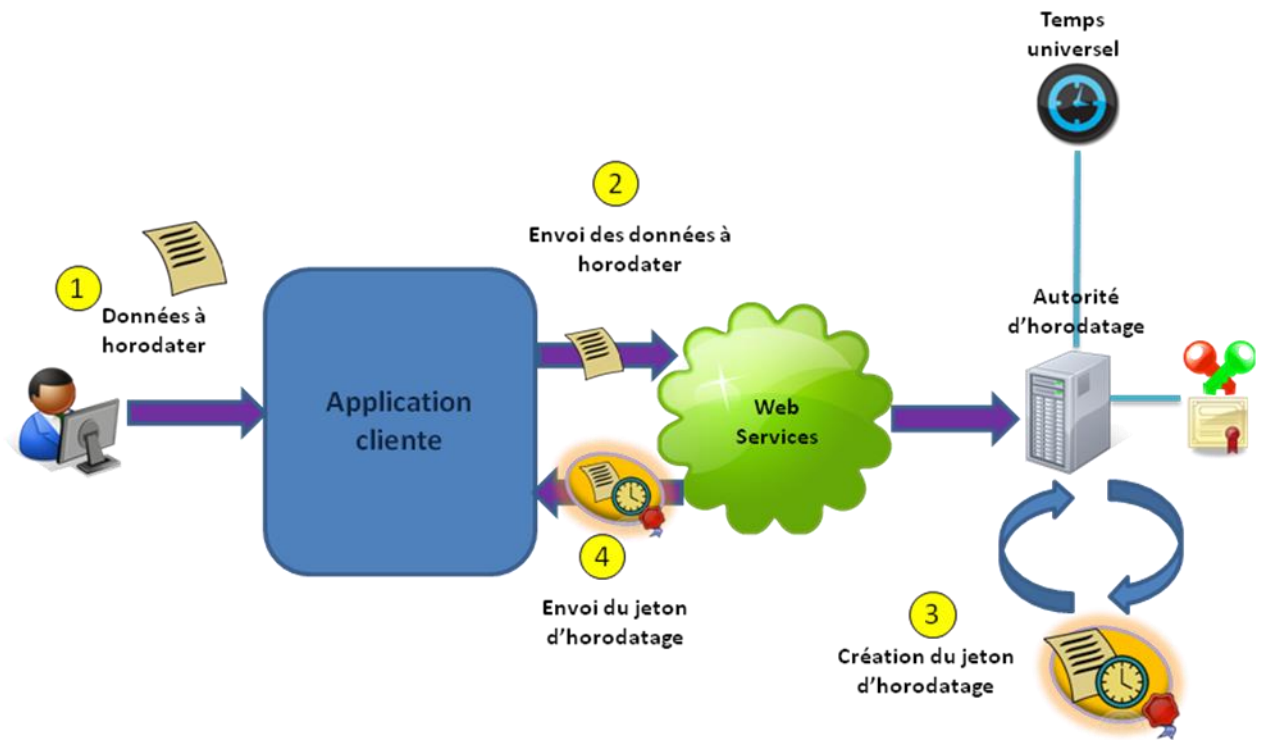
4.2 L'horodatage : valeur

L'horodatage garantit :

- L'**intégrité** par la délivrance d'un jeton d'horodatage qui permet de sceller des données électroniques puisque toute modification des données horodatées romprait la correspondance entre elles et le jeton d'horodatage.
- L'**antériorité** par la datation des données électroniques qui permet de démontrer qu'elles existaient à partir de la date et de l'heure certifiées.

Pour avoir valeur probante, le **jeton d'horodatage** doit être délivré par une organisation respectant la réglementation concernant les services d'horodatage.

4.3 L'horodatage : demande de jeton



5 L'archivage électronique

5.1 L'archivage électronique : principe

Qu'est-ce qu'une archive ?

Une archive n'est pas forcément un document ancien. Un document dit « figé », qui n'est plus amené à évoluer, doit être considéré comme une archive.

Qu'est-ce que l'archivage ?

- L'archivage consiste à conserver une information (documents, images, ...) :
 - qui n'a plus nécessairement d'utilité immédiate,
 - en vue d'un éventuel usage ultérieur,
- La conservation peut être volontaire, organisée ou encore sécurisée pour une période relativement longue.

5.2 L'archivage électronique : rappel des normes

L'archivage électronique à valeur probatoire correspond à un nouveau défi pour toutes les entreprises :

- ⇒ assurer aux documents numériques une valeur légale comme c'est le cas pour les documents papiers.

Dans ce contexte précis, plusieurs normes doivent être appliquées parmi lesquelles nous retrouvons :

- NF Z 42-013
Relative aux mesures à mettre en œuvre pour l'archivage de documents,
- NF Z 42-020
Relative aux mesures pour la mise en œuvre d'un coffre-fort électronique,
- ETSI TS 101 533
Relative aux exigences applicables pour la mise en œuvre d'un système d'archivage sécurisé,
- NF 461
Relative à la certification de système d'archivage électronique,

5.3 L'archivage électronique : Avantages et réduction des risques

Aujourd'hui, l'archivage électronique permet de réduire des risques jusqu'ici non négligeables avec l'archivage traditionnel (archivage papier) :

- **La confidentialité** : archivage électronique permet de mettre en place un contrôle strict et une traçabilité complète des accès aux archives.
- **La perte** : Les risques de perte de documents archivés lors de leur consultation, ou suite à une erreur de reclassement, sont également éliminés.
- **Le sinistre** : tous les moyens techniques nécessaires (backup, réplication, etc.), permettent de sécuriser de manière satisfaisante un système d'archivage électronique.

5.4 L'archivage électronique à valeur probatoire

Seul le Juge peut décider de la valeur probante d'un document archivé. Cependant, sa décision sera fondée sur des éléments d'appréciations qui seront portés à sa connaissance.

Ces éléments « **probatoires** » ou aussi appelés « **preuves** » doivent également être archivés et pourront, le moment venu, venir appuyer la validité du document archivé.

Dans ce cas précis, nous parlons d' « **archivage électronique à valeur probatoire** ».

L'archivage électronique à valeur probatoire doit prendre en compte :

- Le **cadre réglementaire**,
- Une **approche métier**
 - Basée sur des processus administratifs/commerciaux,
 - Intégrant des contraintes/directives sectorielles,

L'archivage électronique à valeur probatoire doit garantir dès l'origine et jusqu'à la fin de la période de conservation :

- **L'authenticité** : identifier la personne physique liée au document archivé.

L'authentification repose sur la « **signature électronique** ».

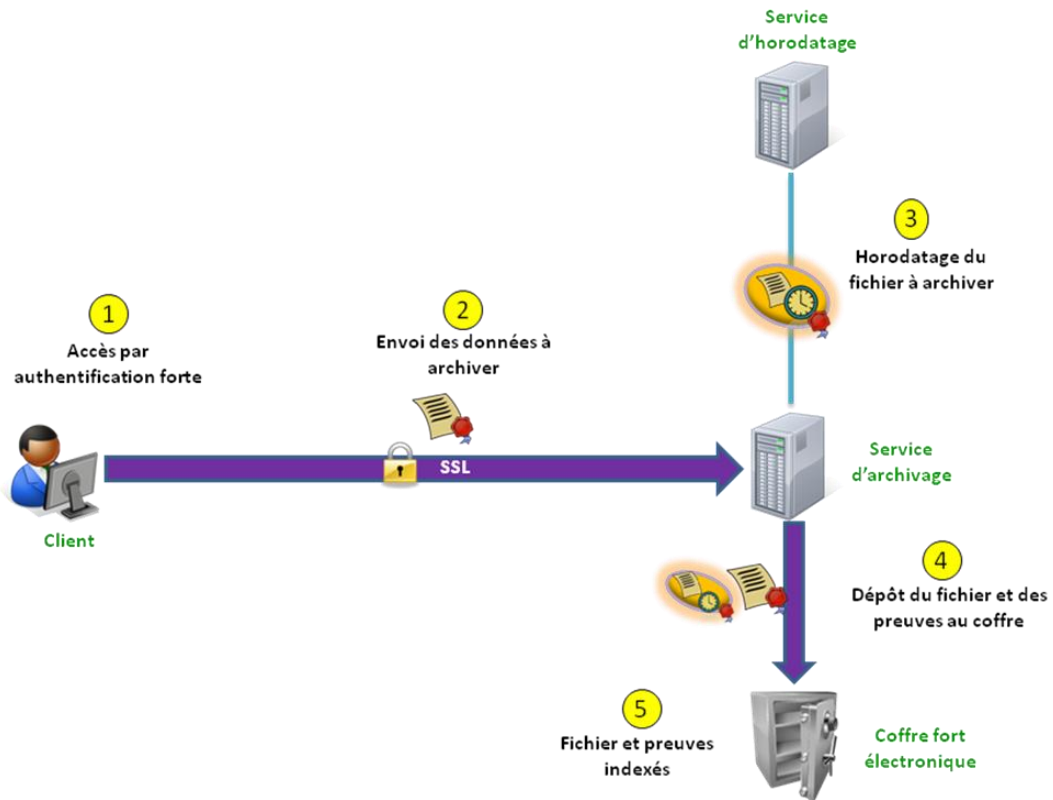
- **L'intégrité** : pour accorder une valeur probante à une archive, le Juge doit être certain que l'objet présenté n'a pu être modifié depuis qu'il a été créé.

La protection contre la modification/altération repose sur la « signature électronique ».

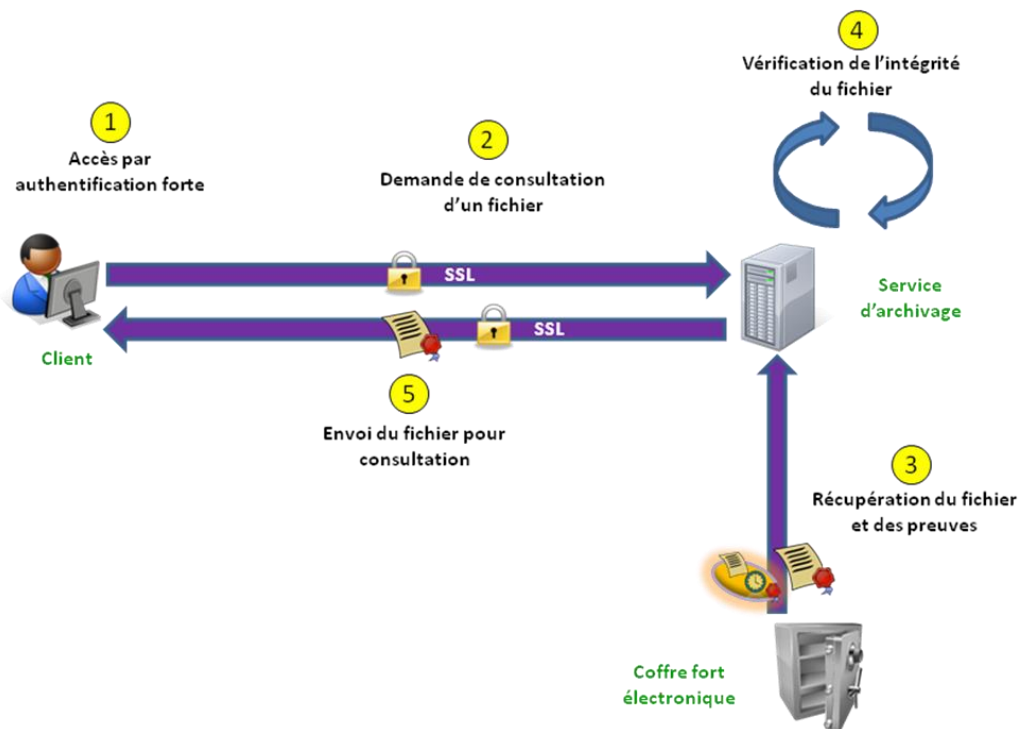
- **L'intelligibilité** : l'archive doit être **disponible/accessible/lisible** durant toute sa période de conservation pour qu'elle puisse être exploitée par un Juge. Tout objet doit être archivé dans un format normalisé (TIFF, XML, PDF/A, ...).

Exemple : un document WORD devra être converti en PDF/A avant d'être signé puis archivé.

5.5 Archivage : dépôt



5.6 Archivage : consultation



6 Moyens juridiques

6.1 Le référentiel documentaire

Dans le cadre de la mise en œuvre d'une contractualisation électronique sécurisée, plusieurs documents sont requis afin de sécuriser la relation contractuelle :

- Conditions générales de vente
- Convention de preuve
- Politique de signature
- Politique de gestion des preuves

6.2 Conditions Générales de Vente et Conditions Générales d'Utilisation

Les Conditions générales de vente (CGV) régissent les modalités, droits et limites liées à toute opération de vente/contractualisation effectuée à travers un site/service. Elles ne sont nécessaires que lorsque le site/service exerce une activité de commerce en ligne et doivent présenter toutes les modalités, opération et méthodologies appliquées par le site lors d'une vente.

- Dans le cadre de la contractualisation électronique sécurisée, ces CGV peuvent être assimilées à la Politique de Signature électronique.

- Les CGV doivent être affichées et acceptées par le contractant avant la conclusion définitive du contrat/vente. Ainsi, le contractant doit obligatoirement, volontairement et expressément accepter les CGV en cochant une case intitulée « Acceptation des CGV » (ou une formulation approchante).
- Exemple : un encadré déroulant peut suffire.

Les Conditions Générales d'Utilisation (CGU) service régissent les modalités, droits et limites d'utilisation du site/service. Elles s'adressent à tout contractant qui accède et utilise le service.

- Ces conditions sont acceptées par le contractant utilisateur du service du seul fait de son accès au site/service et de son utilisation.
- Elles peuvent contenir et reprendre les mentions légales du site ou contenir un lien direct vers elles.
- Les CGU ne concernent que l'utilisation du site/service, elles ne sont pas relatives aux conditions de ventes. Il est tout de même conseillé d'y insérer certains éléments relatifs au CGV.

6.3 Convention de preuve

La convention de preuve est un contrat conclu entre entreprises ou entre entreprises et particuliers qui a pour objet de définir les modes de preuve admissibles entre les parties, la charge de la preuve et les modalités de règlement des conflits de preuve.

Ce qu'apporte une « Convention de preuve » :

- Elle permet de garantir la force probante des documents produits par une solution de signature électronique,
- Elle permet d'organiser un renversement de la charge de la preuve.

Les parties peuvent ainsi s'accorder conventionnellement pour reconnaître la valeur probante des contrats conclus au moyen de celui-ci et pour prévenir toute contestation autour de sa fiabilité.

Selon les termes de *l'article 1316-2 du Code civil*, à défaut de convention de preuve valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens, le titre le plus vraisemblable. Mais lorsqu'une convention de preuve a été valablement conclue entre les parties, le juge doit l'appliquer. Cela peut permettre d'organiser par avance la façon dont lesdits conflits pourront être résolus et donc d'en prévoir l'issue.

6.4 Politique de signature

Objet : expliquer le sens et la portée de la signature électronique au signataire

La politique de signature...

- Décrit l'engagement et les conditions de mise en œuvre de la signature
 - Le contexte d'utilisation de la signature électronique

- Les limites de responsabilité
- Précise les paramètres techniques de la mise en œuvre
 - Formats de signature
 - Moyens de signature
 - Certificats utilisés
 - Etc.
- Est identifiée par un OID apparaissant dans la signature électronique

Le contenu de la politique de signature est « normalisé » (RFC, ETSI)

6.5 Politique de gestion des preuves

Objet : décrire les règles suivies pour constituer et conserver les éléments de preuve aux différentes parties concernées par les documents signés

Conformément au *Code civil (art. 1316-1)*, la force probatoire de l'écrit sous forme électronique *est admise sous réserve [...]*

- *Que puisse être dûment identifiée la personne dont il émane* (c'est le rôle de la signature électronique)
- *Qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* (c'est le rôle de la conservation)

C'est un document technique décrivant...

- Le processus de constitution des données considérées comme probatoires
- Les conditions de conservation (forme, durée de conservation, protection) de ces données
 - Éventuellement, leur destruction et les procédures d'accès à ces données

6.6 Conclusion

La signature électronique, l'horodatage, l'archivage électronique répondent à des objectifs...

- De traçabilité : des faits, des transactions, de leur historique
- D'imputabilité : des personnes ayant participé à la réalisation de ces faits, de ces transactions
- D'intégrité : des documents, des transactions, des échanges
- De datation : des faits, des échanges, des validations
- De pérennité : des contenus, de leur contexte, de leur histoire
- D'autonomie : se mettre en capacité de restituer le contenu de ces informations et des « preuves associées » dans le temps

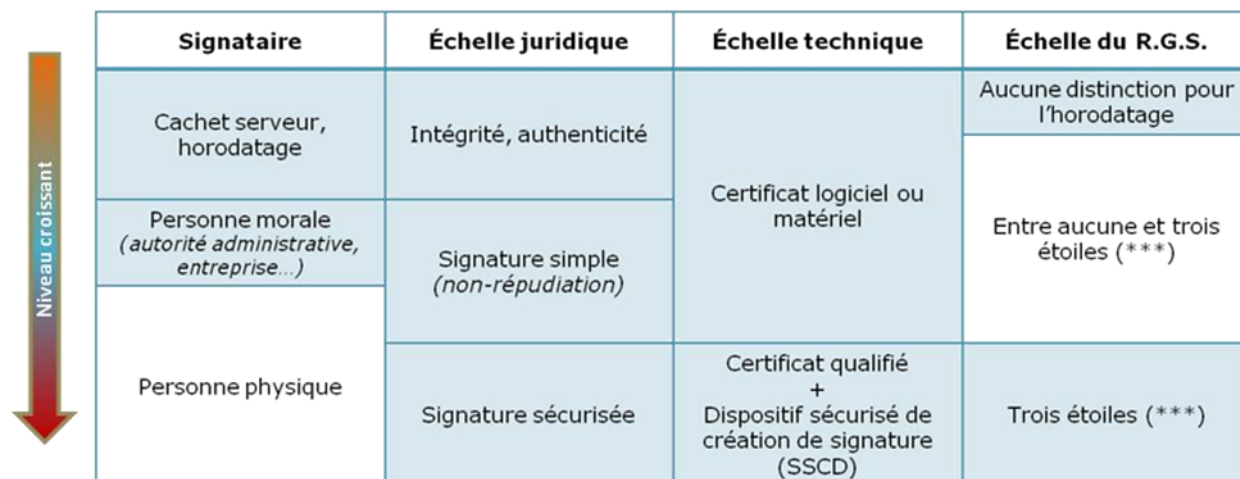
Ces mécanismes peuvent prendre différentes formes plus ou moins complexes suivant le niveau de « qualité » attendue, en fonction...


- Du niveau de risque
- Des enjeux politiques, juridiques, financiers et patrimoniaux associés

Il faut adapter les moyens en fonction des risques, des objectifs de sécurité

Il est néanmoins possible d'avoir une approche « générique » pour traiter ces sujets

6.7 Les « niveaux » de sécurité



	Signataire	Échelle juridique	Échelle technique	Échelle du R.G.S.
 Niveau croissant	Cachet serveur, horodatage	Intégrité, authenticité	Certificat logiciel ou matériel	Aucune distinction pour l'horodatage
	Personne morale (autorité administrative, entreprise...)	Signature simple (non-répudiation)		Entre aucune et trois étoiles (***)
	Personne physique	Signature sécurisée	Certificat qualifié + Dispositif sécurisé de création de signature (SSCD)	Trois étoiles (***)

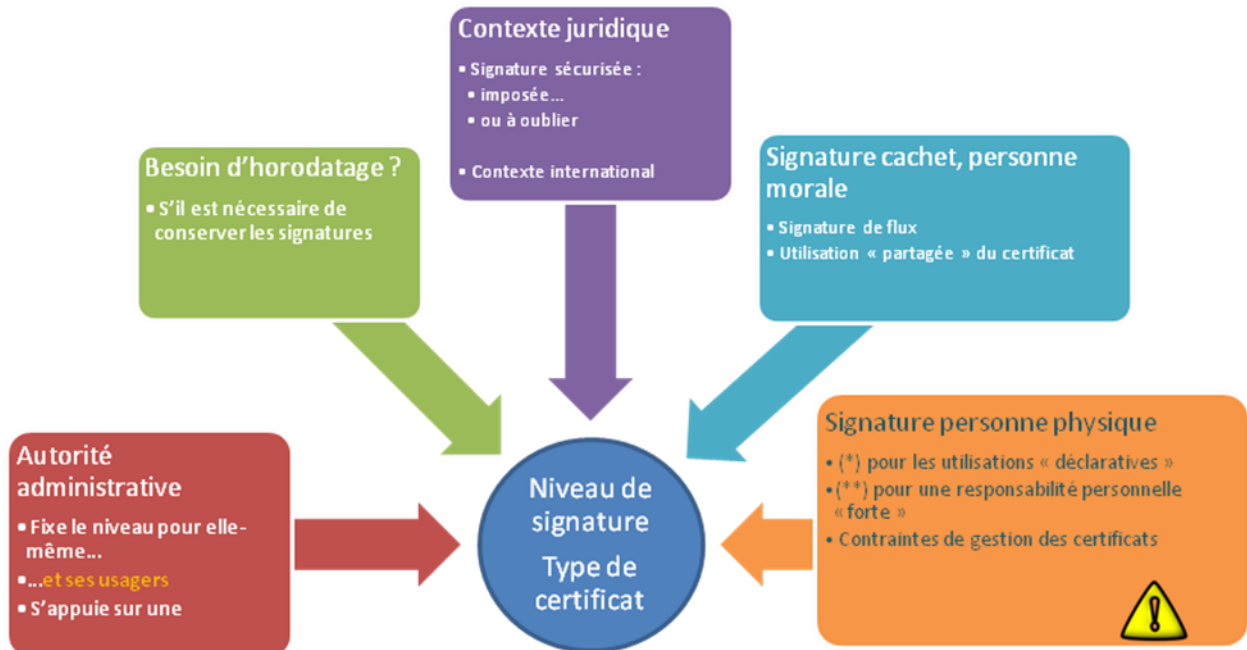
Déterminer « le » niveau de sécurité adapté nécessite de déterminer **un ou plusieurs de ces éléments** (rarement un seul)

La robustesse cryptographique (taille des clés, algorithmes) n'est *pas* le facteur discriminant

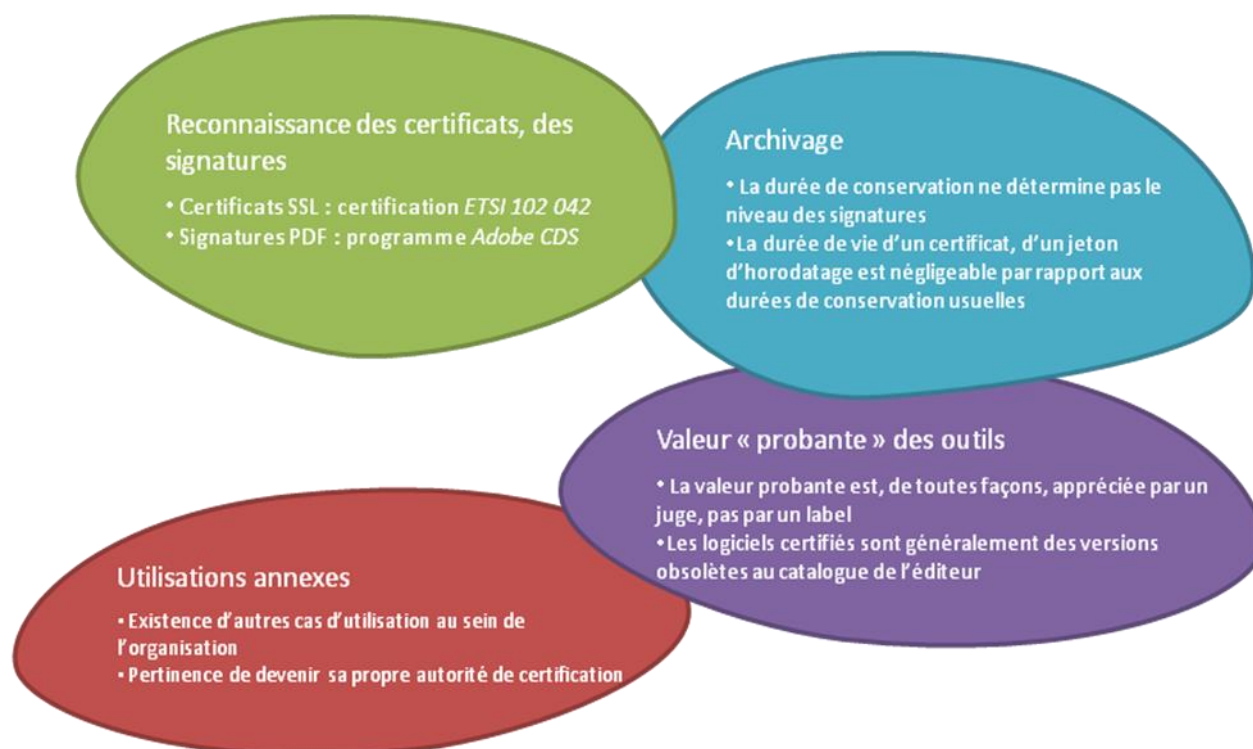
La granularité du R.G.S. est un repère mais *n'est pas* un guide

7 Acteurs du marché et ROI

7.1 Les éléments dimensionnants



7.2 Les éléments secondaires



7.3 Acteurs du marché pour la signature et l'horodatage

Société	Signature	Horodatage	Remarques
Cryptolog	SAAS/licence	SAAS	Éditeur uniquement
Dictao	SAAS/licence	SAAS/licence	Principalement éditeur Logiciels qualifiés (**)
Keynectis	SAAS	SAAS	Spécialisé en signature PDF Service OCSP en mode SAAS
Lex Persona	SAAS/licence	Gratuit/licence	
CertEurope	SAAS	SAAS	
Docapost	SAAS	SAAS	
ATOS Worldline	SAAS	SAAS	

L'offre technique est très différente d'un acteur à l'autre

- « brique logicielle » de signature à intégrer au S.I. du client
- Service « tout-en-un » utilisé par le S.I. du client
- Grande disparité dans l'ergonomie et les possibilités de personnalisation
- Existence ou absence d'une interface utilisateur
- Types de certificat utilisés, gestion de la preuve
- ...

L'offre commerciale (modèle économique) aussi...

7.4 Acteurs du marché pour l'archivage

Société	Internalisation	Externalisation
Cecurity.Com	X	
Arcsys software	X	
Dictao	X	X
CDC Arkhinéo		X
Locarchives		X
Docapost		X

L'offre technique est très différente d'un acteur à l'autre

- « brique logicielle » à intégrer au S.I. du client
- Service « tout-en-un » utilisé par le S.I. du client
- ...

L'offre commerciale (modèle économique) aussi ...

7.5 ROI

R.O.I. économique

- Économies de consommables

-
- Économies d'acheminement
 - Gains de productivité
 - Possibilités de croiser des informations externes pour faciliter ses traitements

R.O.I. social

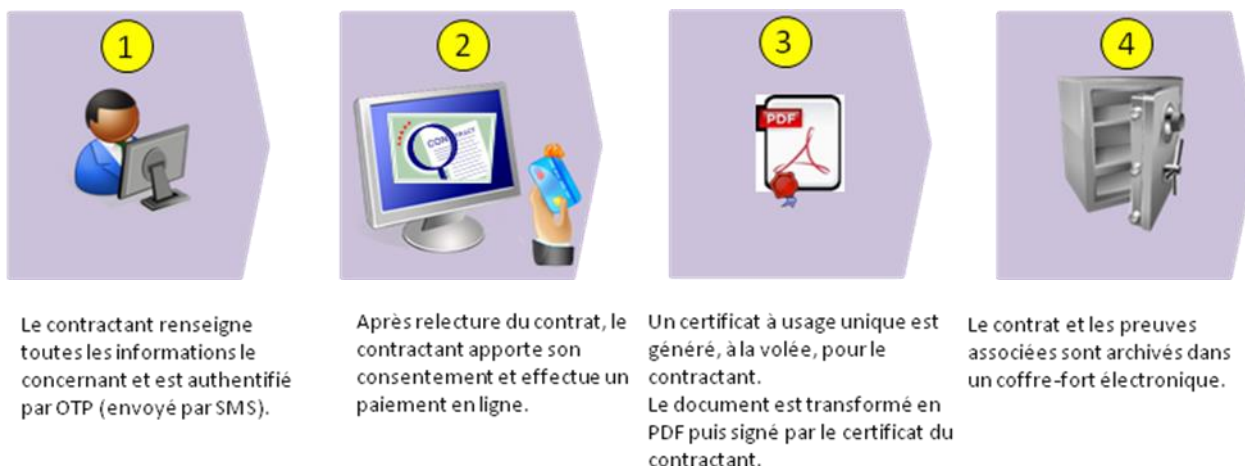
- Amélioration de la valeur ajoutée et meilleure implication des utilisateurs
- Meilleure réactivité perçue par les clients et partenaires
- Traitement plus précis des dossiers (moins d'erreurs, moins de dépenses en conséquence, plus de moyens pour agir)
- Possibilité de développer les services en ligne (enquêtes publiques, forums, informations échanges, ...)
- Transparence et modernité de l'activité de l'organisation

8 Retours d'expériences sur des exemples concrets et bonnes pratiques à favoriser

8.1 Dans un contexte marchand en ligne : sur internet

Description du contexte du cas d'usage :

Un site marchand a mis en place une solution de contractualisation électronique permettant de signer en ligne des contrats commerciaux.



Sécurité apportée au dispositif :

- Utilisation d'un certificat à usage unique. Certificat généré à la volée.
- Signature du contrat avec le certificat à usage unique du contractant,
- Le contrat ainsi que toutes les preuves associées sont archivés électroniquement.

Les bonnes pratiques :

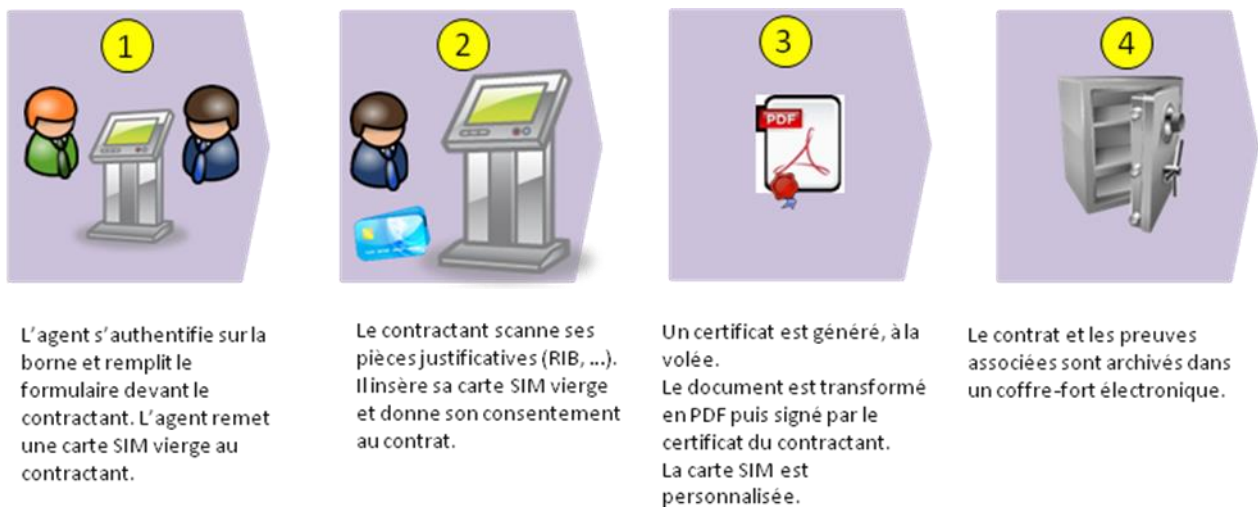
- Constitution d'un chemin de preuve
 - Réaliser une identification la plus fiable possible du contractant,
Exemple : collecte d'un maximum de données d'identification (formulaire de renseignements, adresse IP, paiement en ligne, ...),
 - Collecter un maximum d'éléments de preuve pouvant être utilisés en cas de contestation ultérieure,
Exemple : identification par email ou SMS : envoi d'un OTP pour validation de l'adresse email ou du n° de mobile renseignés.
 - durcir le mécanisme de contractualisation en ligne afin de dissuader la souscription de visiteurs peu intéressés par le service proposé,
Exemple : la vérification de l'engagement contractuel (acceptation via le système de case à cocher, affichage du contrat).

- Conditions Générales de Vente
 - Ajouter une clause ad hoc permettant de donner une valeur juridique pleine et entière à l'ensemble des moyens de preuve électronique.

8.2 Dans le monde de la téléphonie mobile : en agence

Description du contexte du cas d'usage :

Un opérateur de téléphonie mobile a mis en place une solution de dématérialisation dans le cadre des opérations de souscription et de gestion des actes dématérialisés en agence (point de vente). Ces actes sont réalisés en agence sur des « bornes ».



Sécurité apportée au dispositif :

- L'identité du contractant est vérifiée en face-à-face,
- Un certificat est généré, à la volée, sur le module cryptographique du contractant,
- Le contrat est signé par le certificat du contractant,
- Le contrat ainsi que toutes les preuves associées sont archivés électroniquement,

Les bonnes pratiques :

- Établissement d'une Convention de preuve

Dans le cas où des certificats non qualifiés sont utilisés, il est judicieux de mettre en œuvre une « Convention de preuve » : contrat définissant les modes de preuve admissibles entre les parties.

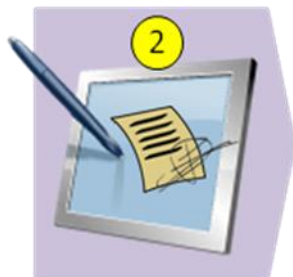
8.3 Dans le monde des assurances : sur tablette

Description du contexte du cas d'usage :

un groupe d'assurance a mis en place une solution de dématérialisation de son processus de souscription de certains de ses contrats, en dotant les conseillers de tablettes mobiles, leur permettant de remplir les formulaires d'adhésion et de recueillir le consentement de l'assuré.



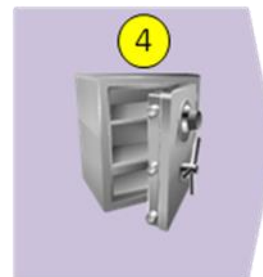
L'agent d'assurance remplit le formulaire devant le contractant



Après relecture du contrat, le contractant apporte son consentement via une signature graphique.



Le document est transformé en PDF puis signé par les certificats du Groupe d'assurance et du contractant.



Le contrat et les preuves associées sont archivés dans un coffre-fort électronique.

Sécurité apportée au dispositif :

- L'identité du contractant est vérifiée en face-à-face,
- Le service de contractualisation électronique est doté d'un certificat de type « cachet serveur »,
- Un certificat est généré, à la volée, pour le contractant,
- Le contrat est co-signé par le certificat du groupe d'assurance (certificat de cachet serveur) et celui du contractant,
- Le contrat ainsi que toutes les preuves associées sont archivés électroniquement,

Les bonnes pratiques :

- L'ajout de la signature graphique donne la possibilité, au contractant, de visualiser dans les documents signés sa signature graphique.

Cette pratique est un atout précieux pour convaincre les utilisateurs attachés à leur signature et potentiellement hostiles à la mise en œuvre de la contractualisation électronique