Agence Régionale de Santé Nouvelle-Aquitaine

Agir pour la santé de tous

PRESCRIPTION DES PSL : la signature électronique

Réunion d'hémovigilance et de sécurité transfusionnelle
CHU de Bordeaux
30 janvier 2020

Dr Farah HATIRA
CRHST NA

La signature électronique :
le cadre règlementaire

LIGNE DIRECTRICE RELATIVE AUX ACTIVITÉS DE DÉLIVRANCE ET DE DISTRIBUTION (BPT du 10 juillet 2018)

……..

I. – Délivrance

3.1. Généralités.

3.1.1. L'ordonnance.

Quel que soit le type de produit, l'ordonnance est remplie avec précision sur un support papier ou électronique et comporte notamment :

- l'identification de l'établissement de santé demandeur et du service ;

- l'identification du médecin prescripteur : cette identification sera complétée par sa signature si elle est **remplie manuellement ou par son identification dans le système d'information de l'Etablissement de santé pour la prescription informatisée…**

La signature électronique :
intérêts

La signature électronique présente de nombreux avantages :

1- Garanties théoriques de la signature électronique

La signature numérique est **authentique et infalsifiable**. L'identité du signataire doit pourvoir être retrouvée de manière certaine, et personne ne peut se faire passer pour le signataire.

En outre, elle **garantit l'intégrité** du document. Le document, une fois signé, ne peut plus être modifié.

Enfin, elle est **irrévocable.** La personne qui a signé ne peut pas nier sa signature (on parle aussi de garantie de « non-répudiation »).

La signature électronique :
avantages pratiques

2- Avantages pratiques de la signature électronique

La signature électronique permet de signer un document sans avoir à prévoir de rendez-vous physique (ce **gain de temps** pour les entreprises est considérable) ;

Elle est également plus **économique et écologique**, puisqu'elle ne nécessite pas d'être imprimée et permet un envoi par mail du document.

Enfin, elle peut être conservée sous forme numérique.

La signature électronique :
procédés techniques

Pour une signature électronique, l'outil utilisé est complexe. La difficulté technique principale est **l'authentification de l'auteur.**

La signature électronique correspond à une suite de caractères (elle n'est pas visuelle). La technique est fondée sur la **cryptographie asymétrique**.

Pour signer électroniquement, vous avez besoin :

- d'un **document numérique** (quel que soit son format, mais généralement en pdf) ;
- d'un **logiciel de signature électronique** ;
- d'une **identité numérique** vérifiée par un **certificat électronique**, simple ou qualifié (selon le niveau de sécurité recherché).

Le certificat numérique est une sorte de carte d'identité numérique qui atteste avec certitude de l'identité de l'utilisateur. Il est délivré par une autorité de certification. Cette démarche nécessite un déplacement physique auprès de l'autorité, qui vérifie votre identité sur présentation d'une pièce d'identité.

La signature électronique :
valeur légale

A. La même valeur juridique que la signature manuscrite

Dans l'Union Européenne, la signature électronique est introduite par une directive de 1999, puis par **le règlement eIDAS** (identification électronique et services de confiance) **de 2014, mis en application le 1er juillet 2016.**

La signature électronique présumée fiable (ou qualifiée) bénéficie des mêmes effets juridiques que la signature manuscrite. Pour cela, elle doit être basée sur un certificat qualifié (par une autorité de confiance).

En France, depuis la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, ainsi que son **décret d'application du 30 mars 2001, la signature électronique a la même valeur juridique que la signature manuscrite**.

Au surplus, la preuve électronique est reconnue au même titre que la preuve 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 » (article 1366 du Code civil).

La signature électronique :
valeur légale

L'article 1367 du Code civil définit la signature électronique comme celle consistant « en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ».

La signature électronique :
valeur légale

B. Fiabilité de la signature électronique

L'article 1367 du Code civil précise ensuite que : « La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d' État ».

Ce décret du Conseil d'État n° 2017-1416 du 28 septembre 2017 exige une signature qualifiée, c'est-à-dire qui repose sur un certificat qualifié de signature électronique répondant aux exigences du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014.

Pour que la signature soit présumée **fiable**, trois conditions doivent être remplies :

- la signature électronique doit être **sécurisée** ;
- elle doit être créée **par un dispositif sécurisé** de création de signature, certifié conforme ;
- elle doit être **vérifiée** par utilisation d'un **certificat électronique qualifié.**

L'article R. 249-11 du Code de procédure pénale définit la signature numérique comme :

« la conservation sous forme numérique d'une signature manuscrite produite via un écran tactile ».

La signature électronique :
référentiel général de sécurité (RGS)

Signatures Électroniques RGS

Référentiel Général de Sécurité

Est le résultat d'un travail conjoint entre la Direction générale de la modernisation de l'État (DGME) et l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

« Décret RGS »

Le référentiel général de sécurité est pris en application du décret n° 2010-112 du **2 février 2010** pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives. Dans le cadre du développement des téléservices et des ***échanges électroniques entre l'administration et les usagers***, les autorités administratives doivent garantir la sécurité de leurs systèmes d'information...

- Les **signatures électroniques RGS** se présentent sous **forme de clé USB cryptographique,** et ont trois fonctions :

La signature électronique :
référentiel général de sécurité

1. Authentifier l'auteur du contenu d'un document

Tout document signé électroniquement possède la **même valeur légale qu'un document signé à la main**.
Le certificat de signature électronique RGS garantit donc également aux destinataires du document que son contenu n'a pas été altéré depuis sa signature.

Vous pouvez également signer vos e-mails (message S/MIME) pour prouver que vous en êtes l'auteur. Si le destinataire de votre e-mail possède également un certificat de signature électronique, vous serez alors en mesure de crypter vos e-mails échangés avec ce dernier pour un maximum de confidentialité.

La signature électronique :
référentiel général de sécurité

2. Afficher la date et l'heure à laquelle un document a été signé

Il s'agit de la fonction horodatage : la signature électronique laisse dans son empreinte la date et l'heure exacte à laquelle le document a été signé.
Non seulement le document a une vraie valeur juridique, mais il garantit en plus que ce dernier existait bien à la date et l'heure précise à laquelle il a été signé.

La signature électronique :
référentiel général de sécurité

3. Se connecter aux plateformes publiques des administrations Françaises

La plupart des administrations Françaises exigent une authentification par signature électronique sur leurs plateformes publiques. Un certificat de Signature Électronique RGS vous **garantit l'accès à l'ensemble de ces plateformes, sans restriction.**

Bien qu'il s'agisse de plateformes Françaises, et donc liées au territoire Français, certaines d'entre elles sont également utilisées à l'étranger, notamment pour répondre à des appels d'offres internationaux (construction de bâtiment, par exemple).

La signature électronique :
référentiel général de sécurité : 3 niveaux

Signature RGS * (une étoile)

Il s'agit du premier niveau d'authentification. Une fois votre dossier reçu et validé, une clé USB vous est **envoyée par la Poste**, et vous permettra de signer des documents et vous authentifier sur les plateformes publiques.

Signature RGS ** (deux étoiles) EUROPE

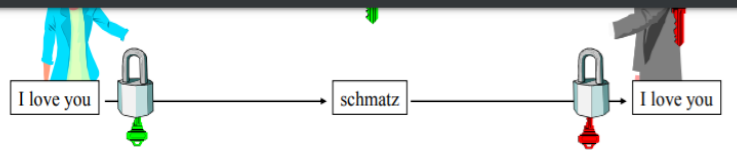
Ces signatures RGS nécessitent la **remise en mains propres de la clé USB** qui vous servira à signer et vous authentifier.

Signature RGS *** (trois étoiles)

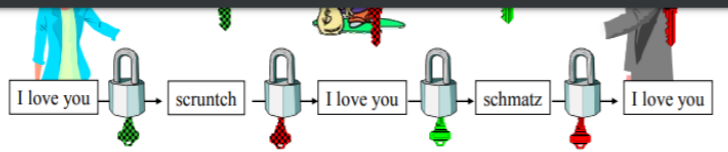
Il s'agit du niveau maximum d'authentification. La clé USB servant à signer et vous authentifier doit être remise en mains propres. Tous les documents à fournir pour son obtention doivent être signés à la main et envoyés par la Poste. Ils feront l'objet d'une vérification rigoureuse.

La signature électronique :
cryptages symétrique (pas de signature) et asymétrique

Cryptographie Symetrique Asymetrique.pdf 5 / 5



LASEC Ph. Oechslin, Sécurité des Réseaux, 2009 17



LASEC Ph. Oechslin, Sécurité des Réseaux, 2009 18

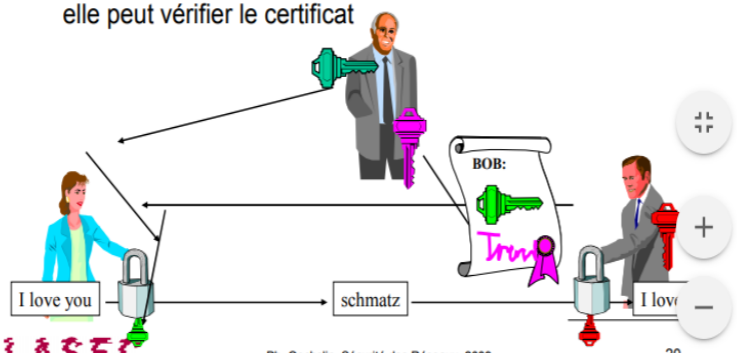
Le Certificat

- Un certificat est un document qui sert à prouver qu'une clé appartient bien à qui de droit.
- Le certificat est signé par un tiers dont on connaît la clé publique (notez la récursion)
- Un certificat contient au moins les informations suivantes:
  - Identité (Nom et adresse e-mail de la personne)
  - Clé publique
  - Date d'expiration
  - Signature du certificat
- Il existe deux types de certificats prévalents: (Open)PGP et X.509

LASEC Ph. Oechslin, Sécurité des Réseaux, 2009 19

Certificat: Exemple

- Un tiers de confiance (Trent) à signé un certificat liant la clé de Bob à son nom
- Si Alice est en possession de la clé publique de Trent elle peut vérifier le certificat

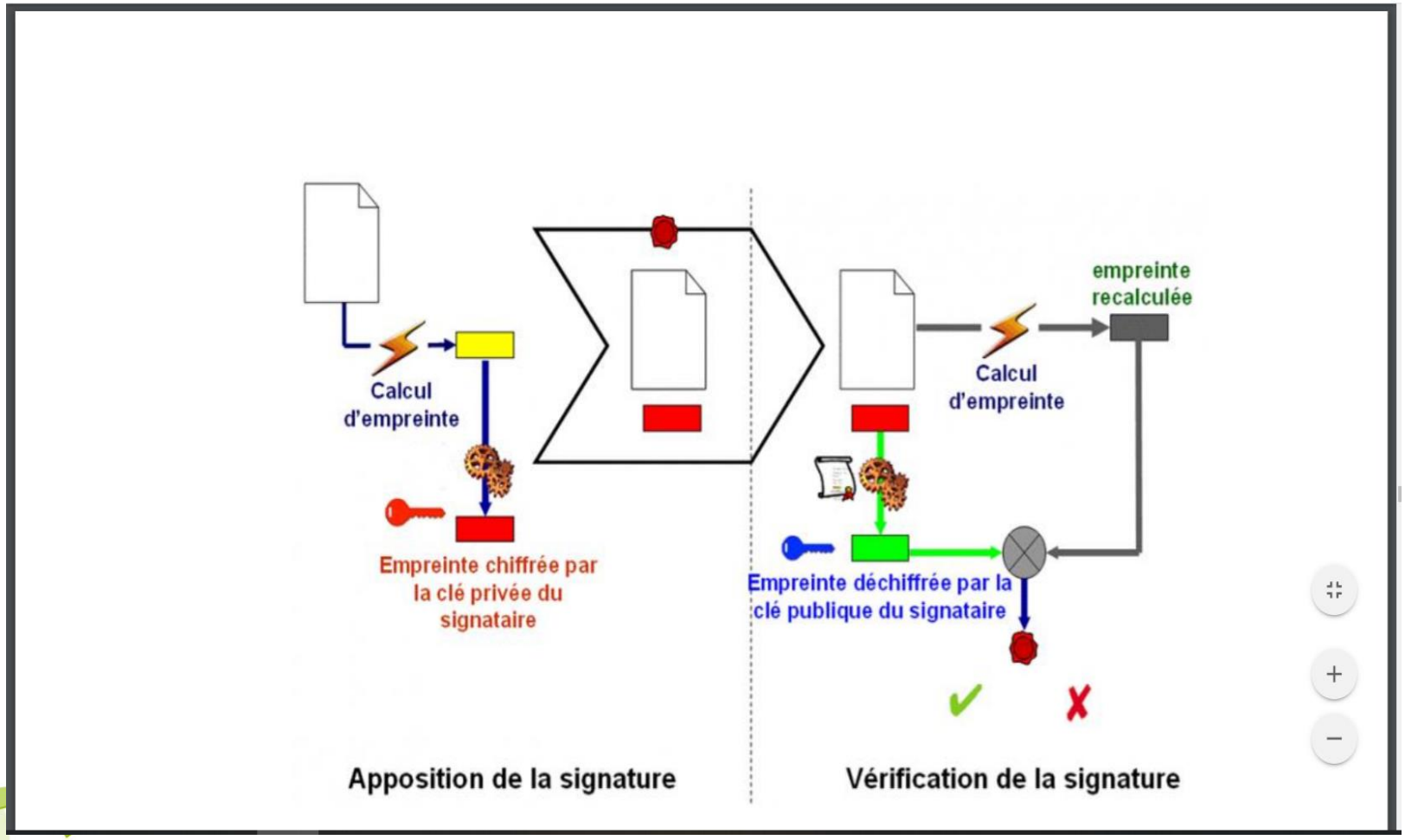


LASEC Ph. Oechslin, Sécurité des Réseaux, 2009 20

La signature électronique :
principe de fonctionnement du RGS** avancé

Cryptage asymétrique : 2 clés (1 publique et 1 privée) + un certificat

-



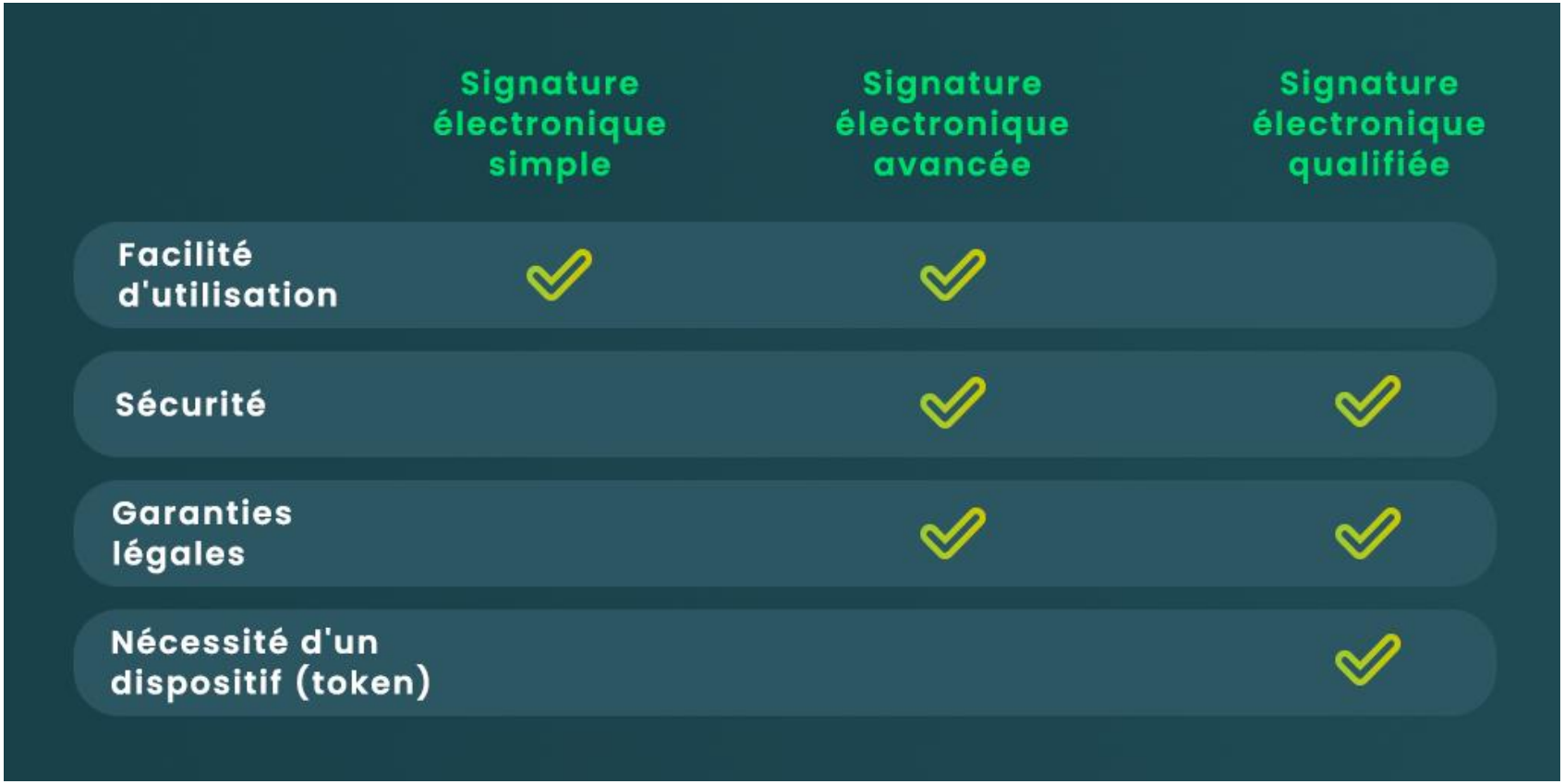
La signature électronique

LES 3 DEGRÉS DE FIABILITÉ DE LA SIGNATURE ÉLECTRONIQUE

- signature électronique simple,
- signature électronique avancée,
- signature électronique qualifiée.

-

La signature électronique



La signature électronique :
exemples d'établissement

- CHU de Saint-Etienne, CHU de Clermont-Ferrand : EDITAL (Medinfo)

Cet outil est utilisé aux USA, Canada, Angleterre, Belgique, Australie, N-Z, EAU, KSA,…

La prescription se fait d'une façon électronique par le biais **d'un mot de passe alphanumérique**, mais les établissements **continuent à imprimer l'ordonnance, à la signer manuellement et à la faxer à l'EFS**.

- CHU de Lille : TRACELINE (Mak-system)

La sécurisation se fait par le biais de clé USB utilisant le RGS, mais **50 % des prescriptions sont signées manuellement** en raison des pertes récurrentes des clés USB et la difficulté d'en avoir d'autres (envoi par la Poste, remise en main propre).

- CHU de Nîmes : CURSUS (Guyot-Walser)

Actuellement**, les prescripteurs impriment l'ordonnance, la signent de façon manuscrite** et font parvenir leur prescription à l'EFS, par fax pour la majorité des prescriptions.

Des tests de prescription connectée de PSL sont en cours. La mise en production est prévue dans quelques mois.

Le prescripteur se connecte sur CURSUS à partir du dossier du patient dans le DPI avec son **matricule et son mot de passe**, y compris les internes qui ont été paramétrés dans CURSUS par le SIH.

La signature électronique :
Conclusion

1-la signature électronique est possible :BPT du 10 juillet 2018,

2-Elle a la même valeur que la signature manuscrite : règlement eIDAS du 1er juillet 2016,

3-doit utiliser un procédé fiable (art, 1367 du code civil + art R.249-11 du code pénal) : → décret…

4-Décret RGS : référentiel général de sécurité (décret RGS du 2 février 2010),

5-basé sur la cryptographie asymétrique, car la cryptogr. symétrique ne permet pas la signature,

6-trois niveaux de RGS ,*, et ***, il faut au moins le ** : 2 clés + un certificat fiable.**

7-L'arrêté du 22 mars 2019 relatif à la signature électronique fixe les modalités d'utilisation de la signature électronique lorsqu'elle est requise pour tout document électronique d'un marché public.

8-Dans l'attente de la publication d'un référentiel national définissant les exigences de sécurité nécessaires aux échanges de documents dématérialisés dans le domaine médical et transfusionnel en particulier, l'utilisation d'un système fiable est de mise.

Merci pour votre attention