RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

GUIDE DE SÉLECTION DU NIVEAU DES SIGNATURES ET DES CACHETS ÉLECTRONIQUES

TABLE DES MATIÈRES

1. INTRODUCTION

Objectif du guide

Ce guide a vocation à accompagner les lecteurs dans la sélection du niveau de signature ou cachet électronique le plus adapté à leurs besoins en fonction, notamment, des risques identifiés et des contraintes réglementaires applicables.

Contexte

Le règlement européen n°910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS », a pour objectif de mettre en place un cadre juridique propre à susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur.

Ce règlement formalise notamment des exigences relatives à la délivrance de certificats de signature et de cachet électroniques, ainsi qu'à la sécurité des dispositifs permettant de créer ces signatures et cachets électroniques. Il prévoit quatre niveaux distincts de signature et cachet électroniques, ayant chacun des caractéristiques, usages et effets juridiques différents, qui sont présentés dans ce guide afin d'aiguiller lors de la sélection du niveau le plus adapté.

Organisation du guide

Tout d'abord, le guide explicite la différence entre un cachet électronique et une signature électronique.

Une fois cette distinction établie, le document s'applique à présenter les quatre niveaux prévus par le règlement eIDAS pour les signatures

et cachets électroniques, en précisant leurs caractéristiques, effets juridiques et usages.

Ensuite, le guide présente une démarche d'analyse des risques permettant d'identifier les besoins en matière d'utilisation de signature/cachet électronique, en l'illustrant avec des exemples.

En conclusion, le document présente un schéma récapitulatif du mécanisme de sélection du niveau adapté, et explicite l'articulation avec les niveaux prévus par le référentiel général de sécurité.

Enfin, pour aller plus loin, une annexe technique vient préciser les mécanismes sous-jacents à la création d'une signature ou d'un cachet électronique.

2. QUELLE DISTINCTION ENTRE LA SIGNATURE ET LE CACHET ÉLECTRONIQUE

Le règlement eIDAS prévoit deux notions reposant sur un même principe technologique, mais aux cas d'usage et effets juridiques distincts : la signature électronique et le cachet électronique.

En effet, tandis que la signature électronique permet, tout comme la signature manuscrite traditionnelle, d'attester du consentement d'une personne physique signataire, le cachet électronique est utilisable par les personnes morales tel un tampon électronique permettant d'attester de l'intégrité et l'authenticité des données.

Le tableau ci-dessous reprend les définitions du règlement eIDAS applicables à la signature et au cachet électroniques.

Signature électronique	**Cachet électronique**
Définie par *Article 3.10 du règlement eIDAS ;* *Article 1367 du code civil.*	*Défini par* *Article 3.25 du règlement eIDAS.*
Créée par *Personne physique.*	*Créé par* *Personne morale.*
Créée via *Action manuelle réalisée par un humain.*	*Créé via* *Action automatisée réalisée par un service applicatif, ou action manuelle réalisée par un humain.*

A pour objectif *D'attester du consentement du signataire.*	*A pour objectif* *D'attester que le créateur de cachet est bien à l'origine du document.*
Effet juridique de la signature électronique qualifiée *Assimilable à celui de la signature manuscrite[1], et présomption de fiabilité jusqu'à preuve du contraire[2].*	*Effet juridique du cachet électronique qualifié* *Présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet est lié.*

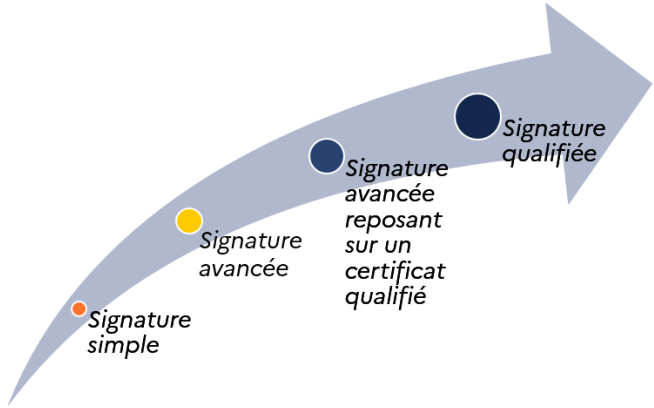
Tout document électronique signé électroniquement ne conserve sa qualité d'original que lorsque celui-ci est conservé sous format électronique. Toute impression et transmission au format « papier » d'un acte signé électroniquement lui enlève sa qualité d'original, et affecte la fiabilité de la signature ou cachet électronique.

[1] La signature manuscrite est une forme graphique personnelle à une personne permettant d'authentifier un document et d'attester du consentement de la personne l'ayant apposée. Il s'agit de la forme traditionnelle de la signature. Dans le domaine du numérique, elle a pour seul équivalent la signature électronique qualifiée.

[2] Prévu par l'article 1367 du code civil et le décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique.

3. QUELS SONT LES NIVEAUX DE SÉCURITÉ DE SIGNATURE ÉLECTRONIQUE PRÉVUS PAR LE RÉGLEMENT EIDAS ?

<u>Convention de lecture</u> : Pour des raisons de simplicité, dans la suite de ce guide, le terme « signature » sera retenu pour parler autant de signature électronique que de cachet électronique. En cas de différenciation, une précision sera apportée. Dans le cas du cachet électronique, le terme « signataire » désigne le créateur du cachet.



La signature électronique « simple »

La signature électronique « simple »[3] correspond au niveau le plus couramment utilisé en raison de son accessibilité et de sa simplicité. En effet, il peut s'agir du niveau s'approchant le plus de l'idée que l'on peut se faire d'une signature sous format électronique à destination du grand public. Il peut s'agir par exemple d'une signature réalisée sur tablette avec un stylet.

Toutefois, **en contrepartie de sa simplicité, cette signature présente un niveau de sécurité faible**, l'identité du signataire peut difficilement être garantie et la signature ne permet pas de garantir la non-répudiation du document. La conformité des dispositifs concourant à la signature électronique simple ne fait pas l'objet d'audit par un tiers compétent et indépendant ni d'une décision par l'organe de contrôle[4].

Ainsi, les éventuelles garanties affichées par un offreur de solution de signature simple sont généralement déclaratives et peuvent varier entre différentes solutions. **La signature électronique simple peut donc être utilisée, par exemple, lorsqu'il n'existe pas de risque substantiel de litige, ni d'obligation légale imposant un niveau particulier de signature électronique**.

Article eIDAS	*Articles 3(10) et 25.*
Définition	*Des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer.*

[3] On appelle signature électronique « simple » la signature électronique définie sans autre précision dans le règlement eIDAS.

[4] Dans le cadre du règlement eIDAS, l'organe de contrôle a la charge de contrôler le respect des exigences du règlement par les prestataires de service de confiance qualifiés et la conformité des services de confiance qualifiés qu'ils fournissent. Chaque État membre de l'Union européenne a désigné un organe de contrôle qui lui est propre. En France, il s'agit de l'ANSSI.

Exemples de solutions techniques	• *Signature sur tablette électronique ;* • *Signature avec confirmation par code reçu à une adresse courriel déclarée par le signataire ;* • *Signature avec confirmation par code reçu par sms sur un numéro de téléphone déclaré par le signataire.*
Force probante	*Le juge ne peut pas la refuser au seul motif qu'elle est électronique*[5]*. Toutefois, elle nécessite d'apporter la preuve de sa fiabilité via un dossier de preuve (intégrité des données, horodatage, identité du signataire).*
Reconnaissance par les organismes publics	*Aucun mécanisme de reconnaissance prévu.*
Accessibilité/Mise en œuvre	*Peu de contraintes. Accessible au grand public. Faible coût. Nombreuses solutions disponibles.*
Niveau de fiabilité de l'identité du signataire	• *Aucune exigence précise formalisée ;* • *Aucune vérification par un tiers indépendant et compétent, ni par l'organe de contrôle national.*
Niveau de sécurité du dispositif de création de signature électronique	• *Aucune exigence précise formalisée ;* • *Aucune vérification par un tiers indépendant et compétent ni par l'organe de contrôle national.*

[5] Article 25 1, Règlement eIDAS : « L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique».

La signature électronique avancée

La signature électronique avancée correspond au deuxième niveau prévu par le règlement eIDAS. Comme pour la signature électronique simple, la conformité des dispositifs concourant à la signature électronique avancée ne fait pas l'objet d'audit par un tiers compétent et indépendant ni d'une décision par l'organe de contrôle[6]

Ainsi, **toutes les garanties apportées par le prestataire sont là encore généralement déclaratives** et peuvent varier entre les différentes solutions. **Toutefois, les signatures avancées répondent à des exigences spécifiques formalisées dans la réglementation** et doivent, en principe, permettre d'identifier le signataire. Cette identification est un élément de preuve supplémentaire en justice devant apparaître dans le dossier de preuve accompagnant la présentation d'une signature avancée lors d'un litige.

Article eIDAS	*Articles 3(11) et 25 à 27.*
Définition	*Signature électronique qui :* • *Est liée au signataire de manière univoque ;* • *Permet d'identifier le signataire ;* • *Est créée à l'aide de données que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ;* • *Permet de détecter toute modification ultérieure du document signé électroniquement.*
Exemples de solutions techniques	• *Signature avec confirmation par code reçu par SMS sur un numéro de téléphone enregistré et lié de façon procédurale à l'identité du signataire ;*

[6] Dans le cadre du règlement eIDAS, l'organe de contrôle a la charge de contrôler le respect des exigences du règlement par les prestataires de service de confiance qualifiés et la conformité des services de confiance qualifiés qu'ils fournissent. Chaque État membre de l'Union européenne a désigné un organe de contrôle qui lui est propre. En France, il s'agit de l'ANSSI.

	• *Signature avec vérification de l'identité du signataire via l'envoi d'une copie de document d'identité.*
Force probante	*Le juge ne peut pas la refuser au seul motif qu'elle est électronique. Toutefois, elle nécessite d'apporter la preuve de sa fiabilité via un dossier de preuve (intégrité des données, horodatage, identité du signataire).*
Reconnaissance par les organismes publics	*Doit être acceptée par les services en ligne des organismes publics des États membres de l'UE exigeant ou utilisant une signature électronique avancée.*
Accessibilité/Mise en œuvre	• *Contrainte variable pour l'utilisateur en fonction des dispositifs et procédures de collecte et vérification d'identité du signataire ;* • *Généralement peu coûteuse pour l'utilisateur ;* • *Contrainte et coût variables pour le prestataire en fonction des certifications passées.*
Niveau de fiabilité de l'identité du signataire	• *Dépend des dispositifs et procédures de collecte et vérification d'identité mis en place par le prestataire ;* • *Aucune vérification obligatoire par un tiers compétent et indépendant, mais de nombreux prestataires font certifier leurs services au regard de standards reconnus[7] par un auditeur indépendant ;* • *En l'absence de certification : nécessité pour l'utilisateur de s'assurer auprès du prestataire du niveau de sécurité des dispositifs et procédures de collecte de collecte et vérification d'identité.*

[7] L'*European Telecommunications Standard Institute* (ETSI) publie la norme ETSI 319 411-1, prévoyant plusieurs niveaux de certification selon le niveau de fiabilité revendiqué par le service.

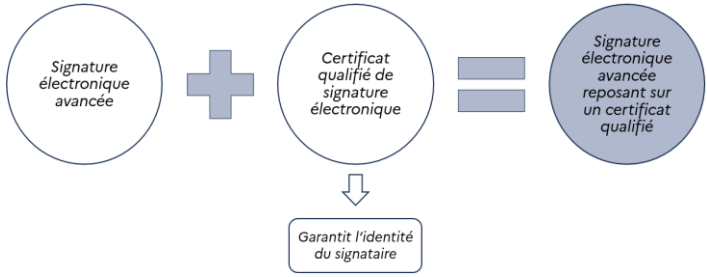
Niveau de sécurité du dispositif de création de signature électronique	• *Aucune exigence précise formalisée ;* • *Aucune obligation de vérification par un tiers compétent et indépendant.*

La signature électronique avancée reposant sur un certificat qualifié

La signature électronique avancée reposant sur un certificat qualifié de signature électronique correspond au troisième niveau et un service délivrant **ce niveau de signature électronique doit faire l'objet d'un audit par un tiers compétent et indépendant ainsi que d'une décision par l'organe de contrôle**. En effet, le certificat de signature électronique devant être qualifié, il permet de s'assurer de façon fiable de l'identité du signataire. Grâce à celui-ci, **la preuve de la fiabilité de la signature est simplifiée dans le cas d'un litige.**

Un certificat qualifié de signature électronique est une attestation de l'identité du signataire délivrée par un processus répondant à des exigences garantissant la validité de la signature, l'identité de son signataire, a minima son nom, son pseudonyme ou son numéro d'immatriculation dans le cas d'une entreprise.

La vérification de l'identité peut alors se faire lors d'un face-à-face physique avec un agent qualifié, via l'utilisation d'un service de vérification d'identité à distance certifié[8] ou encore via la présentation d'une identité électronique préalablement établie suite à un face-à-face physique. Le prestataire délivrant un certificat qualifié de signature électronique fait l'objet de contrôles permettant d'attester de son niveau de fiabilité.



[8] Au titre du référentiel PVID : https://www.ssi.gouv.fr/actualite/publication-du-referentiel-dexigences-applicables-aux-prestataires-de-verification-didentite-a-distance-pvid/

Articles eIDAS	*Article 3(11) et articles 24 à 28*
Définition	*Signature électronique avancée qui repose sur un certificat qualifié de signature électronique.* *Un certificat qualifié de signature électronique est délivré par un prestataire de services de confiance qualifié et satisfait aux exigences fixées à l'annexe I du règlement.* *La signature électronique avancée :* • *Est liée au signataire de manière univoque ;* • *Permet d'identifier le signataire ;* • *Est créée à l'aide de données que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ;* • *Permet de détecter toute modification ultérieure du document signé électroniquement.*
Exemples de solutions techniques	• *Signature via l'utilisation d'un logiciel de signature électronique exigeant la présentation d'un certificat qualifié préalablement délivré au signataire lors d'un face-à-face physique ;* • *Signature avec confirmation par code reçu par SMS sur un numéro de téléphone ou sur une application mobile, enregistré et lié à l'identité du signataire à l'occasion d'un face-à-face physique ou d'une vérification d'identité à distance couplé à l'utilisation d'un certificat qualifié de signature électronique.*
Force probante	*Le juge ne peut pas la refuser au seul motif qu'elle est électronique.*[9] *Elle nécessite d'apporter la preuve de sa fiabilité via un dossier de preuve (intégrité des données, horodatage, identité du signataire), toutefois, la preuve de l'identité du signataire est simplifiée par l'utilisation d'un certificat qualifié.*

[9] Article 25 1, Règlement eIDAS : « L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique».

Reconnaissance par les organismes publics	*Doit être acceptée par les services en ligne des organismes publics des États membres de l'UE exigeant ou utilisant une signature électronique avancée, ou une signature électronique avancée reposant sur un certificat qualifié.*
Accessibilité/Mise en œuvre	*Contraintes fortes sur la vérification de l'identité du signataire, qui doit alors se faire lors d'un face-à-face physique avec un agent qualifié, via l'utilisation d'un service de vérification d'identité à distance certifié ou via la présentation d'une identité électronique préalablement établie.*
Niveau de fiabilité de l'identité du signataire	• *Identité garantie ;* • *Exigences formalisées ;* • *Fait l'objet de vérification par un tiers indépendant et compétent donnant lieu à une décision de qualification par l'organe de contrôle.*[10]
Niveau de sécurité du dispositif de création de signature électronique	• *Aucune exigence précise formalisée ;* • *Aucune obligation de vérification par un tiers indépendant et compétent.*

[10] Tous les services de confiance qualifiés dans le cadre du règlement eIDAS par l'ANSSI sont inscrits dans la liste nationale de confiance. Cf VIII. Liens utiles

La signature électronique qualifiée

La signature électronique qualifiée correspond au **niveau le plus élevé** permettant à la fois de s'assurer de façon fiable de l'identité du signataire en se reposant sur un **certificat qualifié de signature électronique** et de s'assurer de la sécurité des données contenues dans le document signé grâce à l'utilisation d'un **dispositif de création de signature électronique qualifié**.

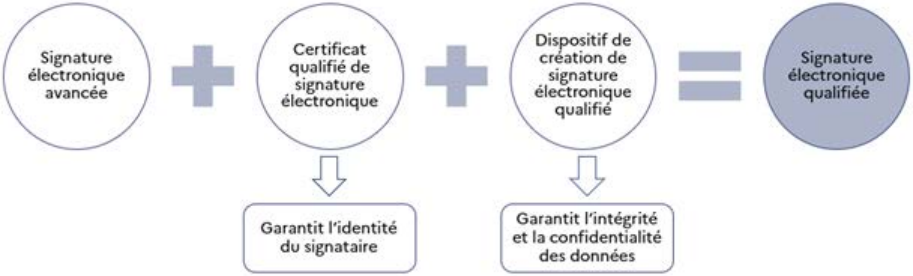
En France, cela permet à la signature électronique qualifiée de jouir d'une **présomption de fiabilité** induisant un renversement de la charge de la preuve. De plus, la signature électronique qualifiée est considérée comme **équivalente à une signature manuscrite**, et est reconnue dans tous les États membres de l'Union européenne. Celle-ci est donc fortement conseillée lors d'une utilisation dans un contexte européen ou en cas de risque important de litige (volume, impact).

Pour rappel, un certificat qualifié de signature électronique qualifié est une attestation de l'identité du signataire délivré par un processus répondant à des exigences garantissant la validité de la signature, l'identité de son signataire, a minima son nom, son pseudonyme ou son numéro d'immatriculation dans le cas d'une entreprise. La vérification de l'identité peut notamment se faire lors d'un face-à-face physique avec un agent qualifié, via l'utilisation d'un service de vérification d'identité à distance certifié ou via la présentation d'une identité électronique préalablement établie suite à un face-à-face physique.

Le prestataire délivrant un certificat qualifié de signature électronique fait l'objet de contrôles par un tiers compétent et indépendant permettant d'attester de son niveau de fiabilité.

Le dispositif de création de signature électronique qualifié est un dispositif combinant un logiciel et un élément matériel permettant de créer une signature électronique tout en garantissant l'intégrité et la confidentialité des données de création, ainsi que la sécurité de la signature.

En pratique, il s'agit souvent d'une carte à puce certifiée ou d'une clé d'authentification certifiée, et plus récemment, d'équipements cryptographiques certifiés installés dans l'environnement du prestataire qualifié, et dont l'accès est sécurisé pour garantir la qualité de l'authentification du signataire.



Articles eIDAS	*Articles 3(12) et 24 à 30.*
Définition	*Signature électronique avancée créée à l'aide d'un dispositif de création de signature électronique qualifié et qui repose sur un certificat qualifié de signature électronique.* *La signature électronique qualifiée* : • *Est liée au signataire de manière univoque ;* • *Permet d'identifier le signataire ;* • *Est créée à l'aide de données que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ;* • *Permet de détecter toute modification ultérieure du document signé électroniquement.* *Le dispositif de création de signature électronique qualifié garantit que :* • *La confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée ;*

	• *Les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être pratiquement établies d'une seule fois ;* • *L'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles ;* • *Les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.*
Exemples de solutions techniques	• *Signature via l'utilisation d'un logiciel de signature électronique exigeant la présentation d'un certificat qualifié préalablement délivré au signataire lors d'un face-à-face physique, sur une carte à puce ou une clé d'authentification cryptographique ;* • *Signature au moyen d'une application mobile garantissant une identification et une authentification forte du signataire (permettant de manifester son consentement) auprès d'un matériel cryptographique géré par un prestataire qualifié.*
Force probante	• *Effet juridique équivalent à celui d'une signature manuscrite ;* • *Présomption de fiabilité induisant un renversement de la charge de la preuve. La preuve de la non-fiabilité de la signature électronique qualifiée devra être apportée par celui qui conteste la signature, et non l'inverse (cf. article 1367 du code civil).*

Reconnaissance par les organismes publics	*Doit être acceptée par les services en ligne des organismes publics des États membres de l'UE exigeant ou utilisant une signature électronique avancée, une signature électronique avancée reposant sur un certificat qualifié, ou une signature électronique qualifiée.* *Les organismes publics ne peuvent exiger, pour une utilisation transfrontalière dans un service en ligne, de signature d'un niveau de sécurité supérieur à la signature électronique qualifiée.*
Accessibilité/Mise en œuvre	*Contraintes techniques et procédurales pour l'identification du signataire et la réalisation de la signature. Coûts de mise en œuvre généralement élevés.*
Niveau de fiabilité de l'identité du signataire	• *Identité garantie ;* • *Exigences formalisées ;* • *Fait l'objet de vérification par un tiers compétent et indépendant confirmée par la qualification délivrée par l'organe de contrôle.*[11]
Niveau de sécurité du dispositif de création de signature électronique	• *Haut niveau de garantie ;* • *Exigences formalisées ;* • *Fait l'objet de vérification (certification) par un tiers compétent et indépendant confirmée par une certification d'un organisme de certification.*[12] *et compétent.*

[11] Tous les services de confiance qualifiés dans le cadre du règlement eIDAS par l'ANSSI sont inscrits dans la liste nationale de confiance. Cf VIII Liens utiles

[12] En France, l'ANSSI assure la certification des dispositifs de création de signature électronique qualifiés.

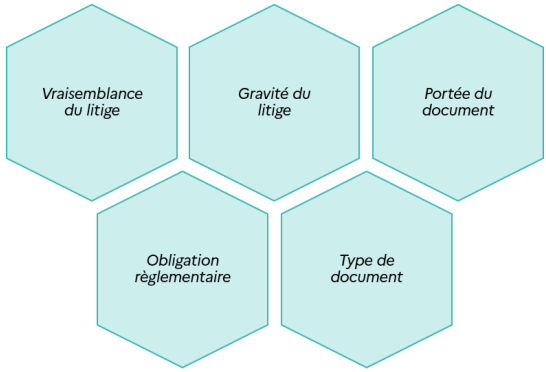
En bref, que faut-il retenir ?

Le tableau ci-dessous reprend les principales caractéristiques des différents niveaux de signature électronique selon le règlement eIDAS.

	Simple	Avancée	Avancée reposant sur un certificat qualifié	Qualifiée
Accessibilité et coûts				
Degré de preuve de la fiabilité				
Reconnue au sein de l'Union européenne				
Niveau de fiabilité de l'identité du signataire				
Niveau de sécurité du dispositif de signature électronique				

4. COMMENT SAVOIR QUEL NIVEAU CHOISIR ?

Afin de déterminer le niveau de signature électronique adapté, il est recommandé de réaliser une analyse des risques prenant en compte différents éléments détaillés ci-après :



Celle-ci peut être réalisée pour chaque typologie de document devant être signé électroniquement.

En phase initiale de l'analyse, la caractérisation de la **portée du document** à signer (nationale, européenne, internationale…) et **son type** (acte sous-seing privé, acte notarié, décision administrative…) permettent d'identifier les besoins de reconnaissance extranationale, les contraintes de moyens liées à la population utilisatrice, ainsi que d'éventuelles obligations réglementaires générales.

En second lieu, le recensement des **obligations réglementaires** spécifiques au cas d'usage considéré peut permettre de déterminer un niveau minimal de signature électronique obligatoire. Un niveau supérieur peut cependant être retenu en fonction du résultat de l'analyse des risques.

Enfin, l'estimation de la **vraisemblance du litige** (probabilité de survenue d'un litige sur une période donnée) et de la **gravité du litige**

(impacts liés à l'annulation de l'acte signé électroniquement) permet de raffiner l'analyse. Plus la vraisemblance et la gravité estimées d'un litige sont importantes, plus la sélection d'un niveau de signature disposant d'une force probante élevée est recommandée.

Il est à noter que le niveau de gravité et la vraisemblance d'un litige peuvent également être réduits par d'autres moyens techniques et/ou fonctionnels (par exemple, le maintien d'une signature manuscrite sur les actes les plus sensibles, ou la mise en place d'un système permettant de générer des preuves complémentaires à la signature électronique).

Différents exemples du niveau de signature électronique conseillé selon les résultats d'une analyse de risques sont présentés ci-dessous.

Exemple 1 :

> Dans le cas d'un acte dont la nullité aurait des impacts juridiques et/ou financiers importants, l'utilisation d'une signature électronique de niveau avancé reposant sur un certificat qualifié ou une signature électronique qualifiée est recommandée. En effet, la signature avancée reposant sur un certificat qualifié permettant de prouver de façon fiable l'identité du signataire, celle-ci facilite l'élaboration d'un dossier de preuve. Tandis que la signature électronique qualifiée étant présumée fiable jusqu'à preuve du contraire, attestant à la fois de l'identité du signataire et de l'intégrité des données, elle est la preuve ultime en matière de litige.

Exemple 2 :

> Dans le cas d'un document à portée européenne, une signature électronique qualifiée est recommandée. En effet, celle-ci jouissant d'une reconnaissance mutuelle dans les États membres de l'Union européenne, elle constituera une preuve devant toute instance nationale.

Exemple 3 :

> Dans le cas d'un document interne n'ayant que peu ou pas d'impact sur des tiers, et ne présentant aucun risque particulier (fraude…), une signature électronique simple ou avancée peut être utilisée. En effet,

ces deux niveaux de signature étant plus accessibles, ils sont recommandés pour les usages courants.

Exemple 4 :

Dans le cas d'un document permettant de signer un appel d'offre dans le cadre d'un marché public, l'arrêté[13] relatif à la signature électronique dans la commande publique imposant un niveau de signature électronique avancé reposant sur un certificat qualifié, il est obligatoire de respecter a minima ce niveau. En l'absence de risque spécifique identifié pour le marché public considéré, le niveau minimal imposé par la réglementation peut être retenu. En cas de risque important, l'usage d'une signature qualifiée peut être recommandé.

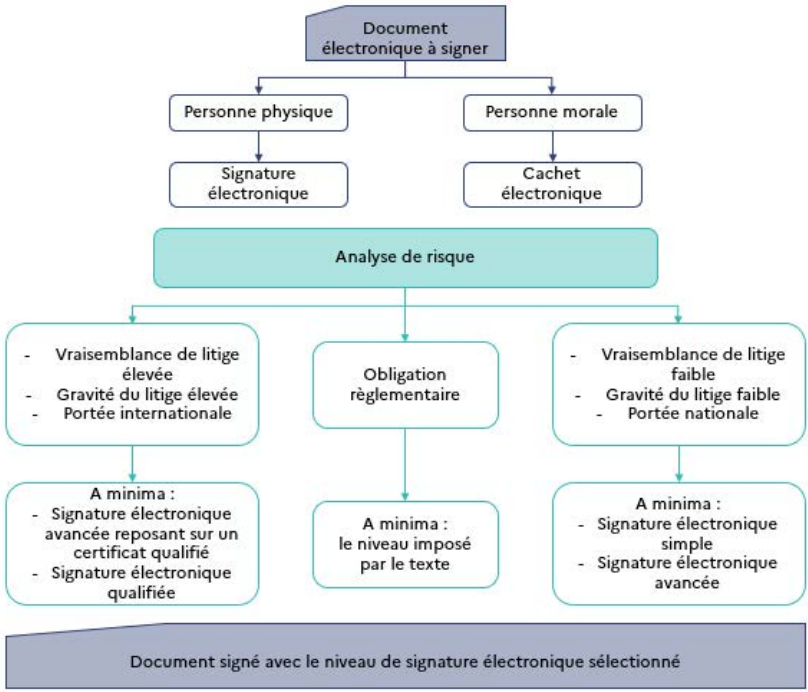
La fiabilité de l'environnement de signature électronique doit également être prise en compte. Un environnement sécurisé permet, par exemple, de garantir que l'utilisateur signe bien ce qu'il voit sur son écran, et non un autre document. Il est donc important au moment de la signature électronique de se questionner sur l'environnement de celle-ci.

La durée d'opposabilité de la signature électronique peut être prolongée via deux procédés : l'archivage électronique à valeur probatoire et la sur-signature. Lorsqu'on parle d'archivage électronique à valeur probatoire, cela signifie que c'est l'environnement de conservation de la signature électronique qui permet d'en garantir la validité et l'intégrité. Tandis que la sur-signature consiste à garantir la validité et l'intégrité de la signature en apposant régulièrement une nouvelle signature ou nouveau cachet d'horodatage par-dessus celles ou ceux déjà existants.

[13] Arrêté du 22 mars 2019 relatif à la signature électronique des contrats de la commande publique

5. QUEL EST LE PROCESSUS RECOMMANDÉ DE SÉLECTION D'UN NIVEAU DE SIGNATURE ÉLECTRONIQUE ?

Dans l'objectif de synthétiser le chemin de réflexion nécessaire au choix d'un niveau de signature électronique adapté à vos besoins, le schéma suivant synthétiste les différentes étapes précédemment vues.



ANNEXE 1

COMMENT S'ARTICULENT LES NIVEAUX DU RÈGLEMENT EIDAS AVEC CEUX PRÉVUS PAR LE RGS ?

Le référentiel général de sécurité (RGS), publié dans sa première version en 2010, est un texte réglementaire français, appelé par l'ordonnance n° 2005-1516, s'adressant aux administrations dans leurs relations entres elles ainsi qu'avec leurs usagers. Il a pour objet de renforcer la confiance des usagers dans les services électroniques mis à disposition par les administrations et s'impose à elles comme un cadre contraignant tout en étant adaptable selon leurs enjeux et besoins.

Le RGS impose l'usage de signatures et cachets électroniques conformes à ses prescriptions par les administrations pour leurs échanges entre elles ou avec les usagers, dès lors qu'un risque identifié nécessite la mise en œuvre d'une signature ou d'un cachet.

Les organismes du secteur public doivent, préalablement à l'ouverture d'un service en ligne, mener une analyse de risques et estimer le cas échéant, le niveau de fiabilité requis pour les signatures électroniques.

Les signatures et cachets électroniques peuvent être qualifiés selon trois niveaux de sécurité croissants : 1 (*), 2 (**) ou 3 étoiles (***) correspondant à des exigences de sécurité distinctes.

La qualification, délivrée par l'ANSSI, permet d'obtenir une présomption de conformité aux exigences du référentiel général de sécurité.

Il n'existe pas d'équivalence parfaite entre les niveaux prévus par le règlement eIDAS et ceux prévus par le RGS, les critères de distinction des niveaux n'étant pas équivalents.

On peut néanmoins distinguer deux grandes catégories :

- Les niveaux 2 ou 3 étoiles prévus par le RGS, appropriés en cas de besoin de sécurité important, présentent un degré de fiabilité proche de la signature électronique qualifiée.
- Le niveau 1 étoile prévu par le RGS, approprié en cas de besoin de sécurité limité, présente un degré de fiabilité de l'ordre d'une signature électronique avancée.

Le règlement eIDAS et le RGS peuvent être appliqués conjointement lorsque, par exemple, une administration française signe des actes pour lesquels une reconnaissance à l'échelle européenne est nécessaire.

Toutefois, il n'existe aucune équivalence juridique exacte entre ces deux réglementations. Une qualification au titre du RGS ne vaut pas conformité au règlement eIDAS et inversement.

Il est dans ce cas nécessaire de vérifier que le certificat de signature utilisé est bien conforme à la fois au RGS et au règlement eIDAS.

ANNEXE 2

QUELS SONT LES PRINCIPES TECHNIQUES DE LA SIGNATURE ÉLECTRONIQUE ?

Pourquoi associe-t-on la signature électronique et la cryptologie ?

Étymologiquement, la cryptologie est la « **science du secret** » ; elle est composée de la cryptographie et de la cryptanalyse. La cryptographie porte sur des techniques permettant, notamment à l'aide de codes secrets et de clés cryptographique, de s'assurer de l'intégrité, l'authenticité et de la confidentialité d'un message. Tandis que la cryptanalyse, au contraire, est la composante de la cryptologie relative au décryptage du message secret sans la connaissance du code secret ou de la clé cryptographique.

La signature électronique étant un procédé cryptographique, il est tout d'abord nécessaire de présenter la cryptographie afin de pouvoir, par la suite, préciser le fonctionnement technique d'une signature électronique. Pour finir, le hachage étant un procédé cryptographique pouvant être utilisé dans le cadre d'une signature électronique, ce cas d'usage est spécifié.

Qu'est-ce que la cryptographie ?

Le grand public connaît la cryptographie via son cas d'usage le plus courant qui est de transmettre des messages confidentiels. Toutefois, son champ d'application dépasse depuis bien longtemps celui-ci. En effet, des mécanismes cryptographiques permettent d'assurer que des messages ne sont pas modifiés pendant leur transit, à authentifier des utilisateurs etc. Ainsi, les cas d'usages de la cryptographie se sont étendus à la protection en intégrité et en authenticité des données échangées, via notamment le développement de la signature électronique.

Dans le cadre d'une signature électronique, la **clé cryptographique** correspond aux paramètres utilisés pour signer la donnée et vérifier la signature. Il s'agit d'un grand nombre utilisé dans une série de calculs mathématiques (« l'algorithme ») effectués sur la donnée.

Il existe deux principaux types de cryptographie, la cryptographie symétrique et la cryptographie asymétrique. Dans le cadre de la signature électronique, la cryptographie asymétrique, présentée ci-après, est généralement employée.

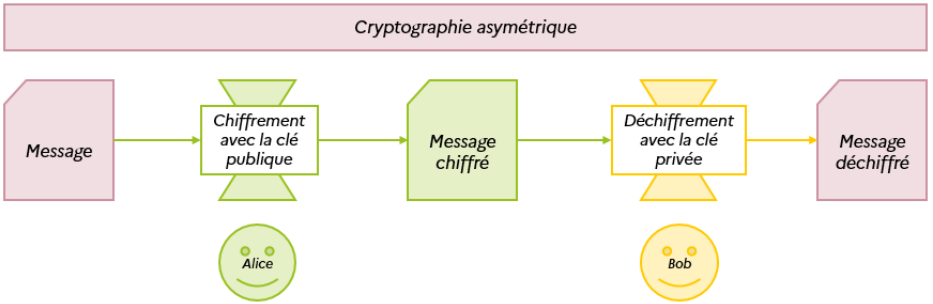
Quelles sont les spécificités de la cryptographie asymétrique ?

La cryptographie asymétrique consiste en l'utilisation d'un couple de clés, l'une dite « privée » et l'autre dite « publique ». La **clé privée** est **confidentielle** et doit être détenue uniquement par le signataire du document. La **clé publique** est **connue** et utilisable par toutes les personnes désirant vérifier la signature du document.

La cryptographie asymétrique permet d'éviter la transmission d'une clé secrète unique (comme dans la cryptographie symétrique), dont la possible interception lors de sa transmission crée un risque pour la confidentialité de la donnée signée, et de garantir l'unicité du signataire.

Exemple :

> Si Alice veut envoyer un message signé à Bob, elle doit utiliser sa clé privée pour signer celui-ci. Une fois le message signé, elle le transmet à Bob qui utilisera sa clé publique afin d'en vérifier le signataire.



De plus, tous les algorithmes cryptographiques ne sont pas du même niveau de qualité. Pour expliquer ces différences de niveau de qualité, il est nécessaire de présenter les critères sur lesquels ce niveau de qualité est appréciable.

Comment apprécier la qualité d'un algorithme cryptographique ?

Il existe différents algorithmes cryptographiques de qualité variable. La qualité d'un algorithme cryptographique est appréciée en fonction de plusieurs critères :

- La **difficulté de produire une signature sans possession de la clé** : un algorithme cryptographique robuste doit réduire les probabilités de création d'une signature valide sans connaissance de la clé ;
- La **difficulté d'obtention de la clé à partir des données signées** : Un algorithme cryptographique robuste doit réduire les probabilités d'obtention de la clé à partir des données signées ;
- La **performance des opérations cryptographiques**: un algorithme performant doit permettre d'optimiser la puissance de calcul nécessaire pour réaliser la signature.

Ainsi, un algorithme cryptographique robuste et performant doit permettre d'atteindre un bon équilibre entre la sécurité des clés, la taille des clés, la protection du message, la facilité d'utilisation et la vitesse de réalisation des opérations cryptographiques.

Le guide de sélection d'algorithmes cryptographiques publié par l'ANSSI fournit une liste d'algorithmes de signature à l'état de l'art[14].

Un autre procédé cryptographique qu'il faut désormais présenté est couramment utilisé par la signature électronique : le hachage.

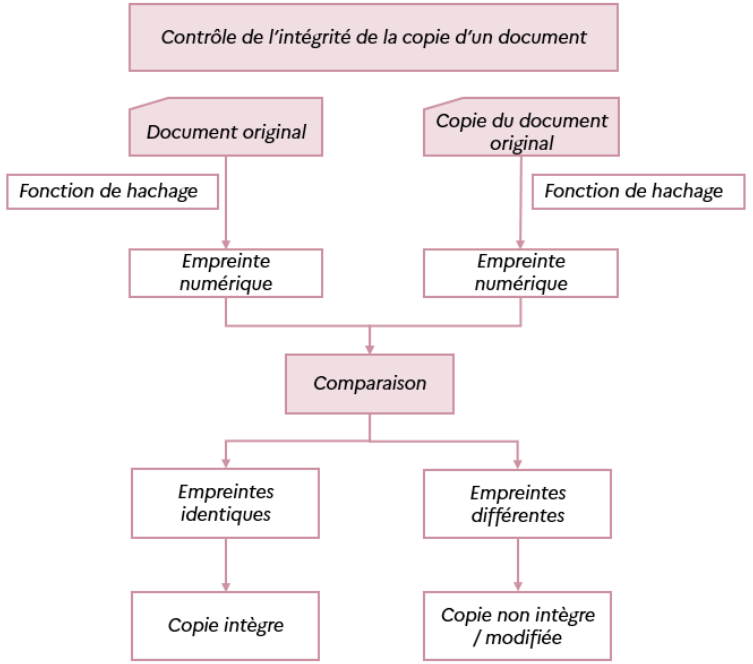
Qu'est-ce que le hachage ?

Le hachage est une technique cryptographique ayant pour objectif de garantir l'**intégrité** d'un document. Pour cela, à partir d'un document, on calcule, via une fonction de hachage, une **empreinte numérique unique** (« *hash* » en anglais) ayant pour caractéristiques d'être beaucoup plus petite que la donnée originelle, et d'être liée à cette donnée précise uniquement.

L'utilisation d'une fonction de hachage sur un document permet d'en obtenir une empreinte unique : si le document est modifié, ne serait-ce qu'une modification minime telle que l'ajout d'un espace entre deux lettres, l'empreinte associée au document sera différente. Le hachage permet donc de garantir l'intégrité d'une donnée puisque toute modification apportée à celle-ci en modifiera l'empreinte et sera donc visible.

Ainsi, en comparant l'empreinte du document original et l'empreinte de la copie du document, on peut contrôler l'intégrité du document. Si les deux empreintes sont identiques, la copie du document n'a pas été modifiée donc celle-ci est intègre. Au contraire, si les deux empreintes sont différentes, alors la copie du document a bel et bien été modifiée, et n'est donc pas intègre.

[14] https://www.ssi.gouv.fr/entreprise/guide/mecanismes-cryptographiques/



Tout comme vu précédemment pour la cryptographie, tous les algorithmes de hachage ne sont pas du même niveau de qualité. Les différents critères permettant d'évaluer le niveau de qualité d'un algorithme de hachage sont donc présentés ci-dessous.

Comment apprécier la qualité d'un algorithme de hachage ?

Il existe différents algorithmes de hachage de qualité variable. La qualité d'une fonction de hachage est appréciée en fonction de différents critères :

- La **résistance aux collisions** : on parle de collision lorsque deux données distinctes donnent une même empreinte. Celles-ci sont indésirables mais inévitables. Une collision peut avoir des impacts très important dans le cas d'une signature électronique. En effet, celle-ci pourrait conduire à une usurpation d'identité du signataire, porter atteinte à l'intégrité et/ou à l'authenticité du document électronique

signé. Ainsi, plus un algorithme de hachage réduit les risques de collisions, plus il sera de bonne qualité ;

- La **longueur des empreintes** : l'objectif du hachage est d'obtenir une empreinte plus petite que la donnée hachée, afin notamment, d'en faciliter le stockage dans un espace réduit, ou de limiter le coût des opérations (ex. signature) réalisées sur cette empreinte ;
- La **résistance à la découverte** de la donnée hachée : un algorithme de hachage performant doit réduire les probabilités de découvrir une donnée à partir de son empreinte.

Ainsi, un algorithme de hachage performant doit permettre d'obtenir une empreinte de taille raisonnable/réduite tout en minimisant le risque de collisions et le risque de découvrir la donnée hachée à partir de son empreinte.

Le guide de sélection d'algorithmes cryptographiques publié par l'ANSSI fournit une liste d'algorithmes de hachage à l'état de l'art[15].

Désormais, il est nécessaire de voir l'utilisation qui est faite de la cryptographie et du hachage dans le mécanisme de la signature électronique et les garanties que celle-ci apporte.

[15] https://www.ssi.gouv.fr/entreprise/guide/mecanismes-cryptographiques/

Comment fonctionne une signature électronique ?

La signature électronique est un mécanisme cryptographique permettant de garantir l'identité du signataire d'un document électronique et l'intégrité de celui-ci via notamment l'usage d'un procédé fiable d'identification garantissant le lien entre la signature et le document électronique auquel elle se rattache.

Ainsi, elle doit permettre de **garantir** :

- L'**intégrité** du document ;
- L'**authenticité** de l'émetteur ;
- La **non-répudiation.**[16]

Lorsque la signature électronique s'appuie sur les mécanismes de cryptographie asymétrique présentés précédemment, la donnée à signer est hachée afin d'obtenir son empreinte numérique. Ainsi dans le cas de document volumineux, il est conseillé de hacher préalablement le document afin d'en signer seulement l'empreinte afin de réduire la puissance de calcul nécessaire. Cette empreinte est alors signée avec la clé privée du signataire. Cette empreinte numérique signée correspond à la signature électronique du signataire. La donnée « signée » est donc la combinaison de la donnée initiale et de cette signature électronique sur l'empreinte.

Afin de vérifier que la signature électronique est valide, le destinataire de la donnée signée doit vérifier la signature à l'aide de la clé publique du signataire.

Il est important de souligner que toutes les signatures électroniques ne sont pas du même niveau de qualité. Pour expliquer ces différences de niveau de qualité, il est nécessaire de présenter les critères sur lesquels le niveau de qualité est appréciable.

[16] Le fait que le document électronique soit signé ne peut être renié. Toutefois, l'identité du signataire peut être remise en cause si l'absence de fiabilité du procédé utilisé est démontrée.

Comment apprécier la qualité d'une signature électronique ?

La qualité d'une signature électronique est appréciée en fonction de différents critères :

- La **fiabilité de l'identité du signataire** : L'identité du signataire doit être garantie. Pour cela, et afin d'associer la clé publique à l'identité du signataire, celle-ci peut être associée à un certificat émis par une **infrastructure de gestion des clés** (IGC). Un certificat de clé publique peut ainsi être assimilé à une carte d'identité numérique, signée par une autorité de confiance.
- La **protection de la clé privée** : Il est recommandé d'utiliser un **dispositif de création de signature électronique qualifié** (QSCD). Il s'agit d'un dispositif cryptographique (par exemple une clé d'authentification USB ou une carte à puce) permettant de créer une signature électronique tout en garantissant l'intégrité et la confidentialité des données de création (c'est-à-dire la clé privée du signataire), ainsi que la sécurité de la signature. Le règlement eIDAS prévoit la certification des QSCD par les organismes certificateurs nationaux[17].
- La **fiabilité de l'application/environnement de signature électronique** : L'utilisation d'un QSCD et d'un certificat qualifié ne garantit pas la fiabilité de l'application/environnement de signature électronique. Il est donc nécessaire de se poser la question de la fiabilité de celle-ci.

[17] La liste des QSCD certifiés selon le règlement eIDAS est disponible à cette adresse :
https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD

ANNEXE 3

OÙ RETROUVER CES INFORMATIONS ET BIEN PLUS ENCORE ?

- Page Internet sur le règlement eIDAS sur le site de l'ANSSI : https://www.ssi.gouv.fr/eidas/

- Foire aux questions sur le règlement eIDAS : https://www.ssi.gouv.fr/uploads/2017/01/eidas_faq_anssi.pdf

- Référentiel « Prestataires de service de confiance qualifiés » : https://www.ssi.gouv.fr/uploads/2017/01/eidas_psc-qualifies_v1.2_anssi.pdf

- Référentiel « Services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés » : https://www.ssi.gouv.fr/uploads/2016/06/eidas_validation-signatures-cachets-qualifies_v1.0_anssi.pdf

- Référentiel « Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet » : https://www.ssi.gouv.fr/uploads/2017/01/eidas_delivrance-certificats-qualifies_v1.2.pdf

- Référentiel « Dispositifs de création de signature / cachet électronique qualifiés » : https://www.ssi.gouv.fr/uploads/2017/01/eidas-certificationconformiteqscd_v1.0_anssi.pdf

- Liste des organismes accrédités, en France, pour l'évaluation de la conformité aux exigences du règlement eIDAS : https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/centres-evaluation/

- Liste nationale de confiance : https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/liste-nationale-de-confiance/

- Guide de sélection des algorithmes cryptographiques : https://www.ssi.gouv.fr/entreprise/guide/mecanismes-cryptographiques/

ANNEXE 4

QUELS TEXTES RÉGLEMENTAIRES CONNAÎTRE ?

- Règlement n°910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=hr

- Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives disponible sur : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000636232/

- Référentiel général de sécurité (RGS) disponible sur : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/liste-des-documents-constitutifs-du-rgs-v-2-0/

- Article 1367 du code civil : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032042456/

- Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035676246/

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION

SGDSN/ANSSI

51 BOULEVARD DE LA TOUR-MAUBOURG

75700 PARIS 07 SP

SUPERVISION-EIDAS@SSI.GOUV.FR