FAQ – La signature électronique

Les niveaux de signature

Comment déterminer le niveau de signature pour un type de document ?

Le niveau de signature doit être établi en fonction du type de document à signer et plus précisément du risque que celui-ci représente pour l'entreprise. Ce risque porte notamment sur la relation préalable entre les signataires. Une analyse de risque peut donc être réalisée. Lorsque le signataire est connu, un niveau simple ou avancé peut être suffisant (dans la mesure où la solution de signature compose un dossier de preuve suffisant).

Le premier fascicule sur la signature électronique, réalisé par la FnTC et le CR2PA, vous propose un schéma vous permettant de définir le niveau de signature à mettre en place ainsi que des cas d'usages.

Les preuves à fournir pour renforcer la valeur d'une signature électronique diffèrent-elles de celles qu'il faudrait produire pour justifier de la validité d'une signature auparavant manuscrite. Et pourquoi ?

Les preuves pouvant justifier la validité d'une signature manuscrite portent sur l'identification des signataires, l'authenticité de la signature et l'intégrité du document.

En ce sens, elles ne diffèrent pas de celles de la signature électronique.

Toutefois dans le cadre d'une signature électronique un tiers intervient très fréquemment : le prestataire de signature. Ce dernier dispose normalement d'éléments permettant de rapporter la fiabilité de la signature. Ces éléments pourront être présentés au juge en cas de litige.

Voici le tableau récapitulant les besoins de preuve, figurant dans le deuxième fascicule sur la signature électronique.

Ce que l'on doit prouver	Comment le prouver
Que le signataire est bien qui il prétend.	Grâce au processus d'enrôlement avant la signature et d'authentification au moment de la signature.
Que le processus de signature a permis de recueillir le consentement.	Grâce au processus de consentement au moment de la signature, dont les traces se retrouvent dans les éléments de preuves.
Que le document n'a pas été modifié et que la signature est bien liée au document.	Grâce aux processus de garantie de l'intégrité du document signé : • Le rapport de validation permet de démontrer la validité de la signature et l'intégrité du document. • Une des fonctionnalités d'un système d'archivage électronique ou d'un coffre-fort numérique est de pouvoir produire un rapport intelligible à partir de ses différents journaux démontrant l'intégrité des archives tout au long de leur vie.
Que le document a été conservé dans des conditions qui font foi et qu'il est toujours lisible.	Grâce à la capacité de maintenir la lisibilité du document via, par exemple, un logiciel de visualisation interne ou externe à la solution d'archivage.

Dans le marché de la signature, il existe souvent 2 niveaux de signature avancée ; l'un basé sur un certificat normal + de l'OTP ("one time password") et l'autre basé sur un certificat qualifié + de l'OTP. Ces deux niveaux sont- ils valides et équivalents du point de vue eIDAS ?

Les 2 procédés sont valides puisque on ne peut pas refuser une signature sous prétexte qu'elle n'est pas qualifiée. Ces 2 signatures avancées possèdent le même effet juridique : leur fiabilité devra être prouvée en cas de litiges. Les preuves à rapporter ne seront en revanche pas tout à fait les mêmes, notamment sur l'identification du signataire du fait que l'une repose sur un certificat qualifié, et l'autre non.

Archivage des documents signés

Pourquoi archiver des documents dont la sécurité et l'intégrité sont déjà assurées par des opérations de scellement (certificats de signature, horodatage) ?

Pour répondre à la règlementation en vigueur (notamment l'article 1366 du Code civil). En effet, l'archivage permet de garantir l'intégrité des documents électroniques tout au long de leur durée de conservation légale. Les moyens techniques utilisés pour signer garantissent l'intégrité du document, quel que soit son format, mais ne sauraient se substituer au maintien de celle-ci dans le temps apporté par un Système d'archivage électronique (SAE) qui génère un journal des évènements garantissant la traçabilité de l'archive et du système d'archivage. Le SAE prémunit les parties contre l'obsolescence technologique des mécanismes de signature.

Est-ce déjà arrivé qu'un juge rejette la validité d'un document signé électroniquement parce qu'il était conservé sur un lecteur réseau ou une GED au lieu d'un CFN ou SAE ?

La jurisprudence actuelle ne s'exprime pas en ces termes techniques de GED, lecteur réseau, de Système d'Archivage électronique ou de Coffre-Fort Numérique. La jurisprudence s'intéresse à la fiabilité de l'archivage pour mener la conservation intègre dans le temps. Les juges s'appuient, entre autres, sur l'attestation d'archivage qui permettra de prouver la fiabilité du système utilisé. La production de cette attestation est notamment assurée par les systèmes dit d'archivage électroniques (SAE) lorsqu'ils possèdent la certification NF 461. L'attestation est en général disponible dans le rapport de conservation. Pour en savoir plus sur ce rapport, ainsi que sur les différents éléments qu'il doit contenir, ce sujet est développé dans le deuxième guide sur la signature électronique.

Utiliser un service qualifié de conservation des signatures ou cachets électroniques qualifiés est-il obligatoire ?

Ce service qualifié n'est pas obligatoire mais simplifie la recevabilité probatoire en cas de litiges. Pour en savoir plus, n'hésitez pas à consulter le troisième fascicule sur la signature électronique, notamment la partie « *Quels sont les enjeux et les risques juridiques d'une 1 conservation à long terme ?* ».

En cas de signature PAdES avec des signatures à la volée, il est parfois indiqué que la signature n'est pas compatible avec de l'archivage à long terme. Que cela implique-t-il ?

Il est important de se ménager la preuve de la vérification de la signature à la volée (et du certificat, surtout si celui-ci n'est pas qualifié) au moment de son établissement. Cette preuve est fréquemment conservée avec le document signé et la signature dans un dossier de preuve qu'il convient d'archiver au même titre que le document signé. Cette question est notamment évoquée en profondeur dans le deuxième fascicule.

Quelle est la valeur juridique d'avoir l'image (sceau) du tiers de confiance sur le document signé ? Est-ce une obligation ?

Le sceau du Tiers de confiance fait intervenir un tiers qui atteste que les signataires ont bien suivi le processus de consentement et appose pour ce faire un cachet électronique parfois qualifié. Ce n'est pas une obligation et sa valeur juridique n'a pas été avérée à ce jour. La signature avec cachet électronique qualifié n'est pas un standard du droit. Il est important de rapporter la preuve au juge que les exigences de l'article 1367 du code civil alinea 2 sont respectées.

Que dois-je archiver dans le cas de la facture électronique signée ?

Dans le cas d'une facture électronique signée, il faut archiver la facture et sa signature ainsi que les preuves comme pour tout autre document signé.

Attention, dans le cas d'une facture qui ne serait pas signée avec une signature ou un cachet électronique qualifié, il faudra aussi conserver les éléments de la piste d'audit fiable pour répondre aux exigences de l'article 289 du Code général des impôts.

Pour en savoir plus, la FnTC et le CR2PA ont notamment organisé un webinaire, « Archivage des factures électroniques : tout ce qu'il faut savoir pour conserver la valeur probatoire », disponible ici. Un article « L'archivage des factures électroniques en 8 questions » est également consultable sur le site de la FnTC.

En tant que particulier on me demande de signer un document électroniquement. Que dois-je faire avec ma version signée reçue par mail ?

D'abord vérifier que la signature est correcte. Ensuite, dans le but de faire valoir vos droits sur ce document, il serait préférable d'archiver ce document signé dans un outil sécurisé et garantissant l'intégrité. Pour les particuliers, des services de coffres-forts numériques s'adaptent tout à fait à ces usages. Si vos bulletins de salaires sont dématérialisés, vous bénéficiez peut-être d'un coffre-fort numérique dans lequel vos documents signés électroniquement ou tout autre document électronique peuvent être conservés.

Cependant, si vous n'avez accès à ce type d'outils, les juges ont une tolérance accrue dans les pièces fournies par un particulier.

Preuves

Quels sont les éléments de preuve qui doivent accompagner un document ?

A minima, il faut produire les preuves ci-dessous. Pour plus d'informations consultez le deuxième fascicule sur la signature électronique.

Contenu du journal de preuve accompagnant le document signé
Langue du journal
Désignation du tiers horodateur
Description de la méthode d'enrôlement avant signature
Niveau des certificats utilisés
Description de la méthode d'authentification au moment de la signature
Mode de consentement au moment de la signature
Détail chronologique des événements
Mode d'archivage

Comment apporter les preuves en 2021 d'un document signé en 2013 ?

La question a été abordée dans le deuxième guide sur la signature électronique via un schéma :

Les constituants de la preuve peuvent être générés, soit lors de l'établissement de la signature et conservés par la suite, afin de pouvoir les restituer à n'importe quel moment, soit à la demande de l'utilisateur. Dans ce dernier cas, et si la signature n'est pas qualifiée, il faudra prêter une attention particulière aux risques d'une génération a posteriori des preuves. Cette problématique est notamment abordée dans le deuxième guide sur la signature électronique.

Faut-il archiver les éléments de preuve de la signature électronique ?

Les éléments de preuves liés aux documents signés électroniquement ne possèdent aucun système intégré de garantie de leur fiabilité et de leur intégrité. Il est donc primordial de les archiver dans un Système d'archivage électronique (SAE) ou un coffre-fort numérique (CFN). Le versement dans un CFN ou un SAE ne confère pas de valeur juridique supplémentaire, mais maintient une vocation probatoire à la fiabilité et l'intégrité des éléments de preuve en cas de litige.

Pour mieux comprendre cette vaste problématique, nous vous invitons à consulter nos trois guides sur la signature électronique : le premier est disponible là, le deuxième est consultable avec ce lien, et vous pouvez retrouver le troisième ici.

Dans un cadre international, que se passe-t-il quand on utilise une signature électronique ?

Le règlement eIDAS dans son article 14 traite l'équivalence entre les services de confiance qualifiés en UE et hors UE sous la forme d'un accord entre l'UE et le pays tiers.

Dans le cadre d'une signature à l'internationale, la convention de preuve comprise dans le contrat permet de traiter la question de la recevabilité de la signature électronique.

Qu'est-ce que la validation ?

La validation est le processus de vérification et de confirmation de la validité d'une signature ou d'un cachet électronique. Elle doit s'effectuer le plus tôt possible, notamment avant l'expiration de la validité du certificat électronique de signature ou de cachet électronique. Cette thématique est abordée dans le deuxième fascicule sur la signature électronique, notamment dans la première partie « La validation des signatures ».

Comment savoir si un document PDF est signé électroniquement ?

Pour savoir si un document PDF est signé électroniquement selon un parcours de consentement électronique (à ne pas confondre avec une signature scannée ou dessinée sur le document ou même un copié collé d'un pavé de signature), on peut ouvrir le document dans le lecteur PDF Adobe qui indiquera automatiquement que le document comporte une signature électronique ainsi que des informations sur celle-ci, et sur le certificat utilisé.

A quoi ressemble une signature valide ou invalide ?

Afin de savoir si une signature est valide ou non différentes solutions s'offrent à nous :

- Vérifier la validité sur un lecteur PDF : lorsque l'on ouvre un document signé dans un lecteur PDF, des informations sur la validité de la signature et du certificat nous sont proposées. Attention, il faut tenir compte que ces lecteurs peuvent indiquer une signature comme invalide lorsqu'ils ne reconnaissent pas l'Autorité de Certification dont elle émane. A savoir que cette reconnaissance est un service payant auxquels peuvent souscrire les AC.
- Vérifier la signature via le site : Accueil | e-Signature (chorus-pro.gouv.fr)
- Vérifier la signature via : https://ec.europa.eu/cefdigital/DSS/webapp-demo/validation
- Vérifier la validité de la signature et de son certificat dans les éléments de preuve du document signé.

La FNTC et le CR2PA recommandent de toujours demander les éléments de preuves associés au document signé, afin de pouvoir démontrer sa validité sans dépendre de solution de vérification.

La validation est-elle obligatoire ?

Pour répondre, le tableau ci-dessous est tiré du deuxième fascicule, qui comprend toute une partie dédiée à la question : « *Quand doit-on procéder à la validation ?* ».

Niveau de signature/ cachet	Validation encadrée par l'eIDAS	Qui peut procéder à la validation ?	Avec quel outil valider ?	Quand procéder à la validation ?
Qualifié	Oui	PSCQ	-	Au besoin
Avancé ou Simple	-	Tout le monde	La solution de signature ou un outil en ligne ou la solution de conservation (si la fonctionnalité existe)	Au plus tôt après la signature

Un document signé électroniquement d'une part et manuscritement de l'autre est-il valide ?

Ces signatures hybrides (une des parties signe électroniquement, l'autre manuscritement etc.) sont à proscrire. En tout état de cause si des documents ont été signés de cette façon, chacune des parties doit avoir accès aux originaux de l'autre partie. La partie qui a signé le document électroniquement doit envoyer l'original électronique à l'autre partie (i.e., le contrat dématérialisé et non une copie ou un scan), accompagné du certificat de signature électronique. Quant à la partie ayant signé le contrat manuscritement, elle doit faire parvenir un exemplaire papier signé à la contrepartie. Le premier guide sur la signature électronique peut vous aider à mieux comprendre ce processus.

Est-il possible de signer un document dans son format natif, même si celui-ci n'est pas convertible dans un format lisible de type PDF ?
Oui, ceci est possible. Et les conditions de garantie de l'intégrité, de la pérennité dans le temps du document et de sa vocation probatoire restent les mêmes que pour un document PDF. Cependant, ce qui peut poser un problème dans le temps est sa lisibilité. Il est impératif de mettre en œuvre les moyens nécessaires pour garantir cette lisibilité sur toute la durée de conservation du document en question. Le premier fascicule sur la signature électronique analyse en profondeur ces exigences.

Comment signer un document sensible lorsque le SaaS n'est pas envisageable ?

Il faut distinguer la signature d'un document dont la simple visualisation ne peut être envisagée à l'extérieur de l'entité, de la signature en SaaS sans externaliser le document à l'entreprise et pour laquelle il existe des solutions protégeant toute copie du document. Pour la première obligation il est possible de signer avec une solution de signature électronique en interne. Dans ce cas, la convention de preuves en annexe du contrat devra décrire la technologie utilisée. L'entreprise peut fournir l'outil maison qui permettra de signer (ex un badge avec une PKI).

Sinon, il reste le recours à une signature manuscrite.