Comprendre le règlement eIDAS

Volume 2 - Les services de confiance

fntc

Fédération des Tiers de Confiance du Numérique

Créée en 2001, la Fédération des Tiers de Confiance du Numérique (FnTC) est aujourd'hui l'une des organisations les plus visibles de l'écosystème numérique.

La Fédération regroupe plus de 160 adhérents qui prennent une part active dans la définition, la mise en œuvre et la promotion de la confiance dans l'économie numérique : des éditeurs de logiciels, des prestataires de services numériques, des experts, des professionnels réglementés, des start-up, des institutions et des utilisateurs des services de confiance. Cette hétérogénéité des acteurs offre à la Fédération un inestimable gisement de compétences pour favoriser une digitalisation fiable et sécurisée.

Avec un souci constant d'éthique, la FnTC œuvre depuis plus de vingt ans dans les domaines historiques de la dématérialisation (signature électronique, archivage électronique, facture électronique, vote électronique, e-finance). La Fédération agit aujourd'hui également dans les secteurs montants de la digitalisation : Blockchain, KYC, Cachet électronique visible (CEV), e-santé, identité numérique,...

SOMMAIRE

INTRODUCTION

Un peu d'étymologie pour débuter : le terme confiance vient du latin confidentia ; la confiance, se définit comme le « Sentiment de quelqu'un qui se fie entièrement à quelqu'un d'autre, à quelque chose[1] ». En droit, elle se traduit par la « croyance en la bonne foi, loyauté, sincérité et fidélité d'autrui (un tiers, un cocontractant) ou en ses capacités, compétences et qualifications professionnelles[2] » (ex : la confiance en un professionnel du droit ou envers un médecin), par l' «action de se fier à autrui, ou plus précisément de lui confier une mission (mandat, dépôt[3], ...) ». Or, souvent le droit appréhende cette notion de manière négative (abus de confiance en droit pénal et licenciement pour perte de confiance) ou encore par la manifestation de cette confiance (engagement de la responsabilité du gouvernement avec le fameux article 49-3 de la Constitution de 1958).

(1) Définition du Dictionnaire Larousse https://www.larousse.fr/dictionnaires/francais/confiance/18082.
(2) Gérard Cornu, Association Henri Capitant, Vocabulaire juridique, P.U.F., 2011, V° Confiance.
(3) Gérard Cornu, op. Cit.
(4) JO du 22 juin 2004. 5 JOUE L.257/73 du 28 août 2014.
(5) JOUE L.257/73 du 28 août 2014.
(6) Ce fascicule a été élaboré avant la publication du Règlement.

Le Droit s'est emparé de cette notion. Le cadre juridique de la confiance associe l'exigence du respect de normes (souvent techniques) à celui d'exigences plus classiques du domaine de la loi (responsabilités civile et pénale). D'ailleurs, le terme « confiance » peut être mentionné de manière explicite comme c'est le cas pour la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004[4], ou encore le règlement n°910/2014 le 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit « eIDAS[5] »

Ce règlement constitue la colonne vertébrale du marché de la confiance numérique. Il touche à des domaines aussi variés que l'identification électronique régalienne, les signatures, les cachets, l'horodatage, les certificats d'authentification de site, les documents ou les services d'envois recommandés électroniques, éléments constitutifs de la confiance électronique sur le marché intérieur...

A l'heure où une nouvelle version du règlement eIDAS a été validée par les différentes instances européennes[6], il était urgent de se pencher sur les différents services de confiance, d'autant que ces services perdureront, certains modifiés - après l'entrée en vigueur du règlement eIDAS 2.

1

Définition des services de confiance

Qu'est-ce qu'un service de confiance ?

Les services de confiance sont définis comme suit dans le règlement eIDAS: « service électronique normalement fourni contre rémunération qui consiste:

a) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou

d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services; ou

b) en la création, en la vérification et en la validation de certificats pour l'authentification de site internet; ou

c) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services » (article 3.16)

Comme son nom l'indique, un tel service a pour objectif d'assurer la confiance dans le prestataire qui le réalise. Cette confiance s'applique ici dans le cadre d'activités liées au numérique comme l'établissement et l'échange de documents dématérialisés.

Un peu d'histoire :

La confiance numérique est un terme qui apparait dès les années 2000 (notamment avec la Loi du 13 Mars 2000) et propose ainsi aux utilisateurs de services numériques une référence leur permettant d'avoir un choix éclairé sur les services qu'ils utilisent.

C'est donc tout naturellement que ce terme s'est ancré dans le secteur du numérique au fil des années et que nous le retrouvons pleinement défini dans le règlement eIDAS

Quels sont les services de confiance définis par le règlement eIDAS ?

Le règlement eIDAS définit 5 services de confiance :

- La délivrance de certificats de signature et cachets électroniques et d'authentification des sites web
- La validation de cachets et signatures électroniques
- La conservation de cachets et signatures électroniques
- L'horodatage électronique
- L'envoi recommandé électronique

Ces services de confiance sont utilisés dans l'implémentation de solutions et de logiciels par les professionnels du secteur du numérique (éditeurs, opérateurs et prestataires de services). Ces solutions seront utilisées directement ou indirectement par les entreprises et/ou les citoyens (archivage électronique, blockchain, signature électronique, etc.)

Les évolutions constantes technologiques observées dans le secteur du numérique conduisent à l'émergence de nouveaux services de confiance que les pouvoirs règlementaires européens saisissent dans une modification du règlement eIDAS (ledger, archivage électronique, remote signature, délivrance d'attestations d'attributs) qui seront étudiés dans un prochain fascicule.

2

La valeur juridique des différents niveaux de services de confiance

Quels sont les différents niveaux des services de confiance ?

Le règlement eIDAS définit différents niveaux de fiabilité. Ceux-ci apportent des présomptions juridiques distinctes.

L'horodatage, l'envoi recommandé électroniques et l'authentification de site web peuvent avoir un niveau de fiabilité non qualifié ou qualifié.

La signature et le cachet électroniques ont eux 4 niveaux de fiabilité : simple, avancé, avancé avec certificat qualifié et qualifié.

Présomptions juridiques des niveaux de fiabilité (tableau 1)

Service de confiance	Non qualifié	Qualifié
Horodatage	Exactitude de la date et de l'heure à démontrer, le cas échéant, devant le juge.	Présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure.
Envoi recommandé electronique	Intégrité des données, identification de l'expéditeur et du destinataire, date et heure de l'envoi et de la réception à démontrer, le cas échéant, devant un juge.	Présomption relative à l'intégrité des données par l'expéditeur identifié, à leur réception par le destinataire identifié et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées.
Authentification du site web	Lien entre l'authentification du site et de la personne phydique ou morale à démontrer, le cas échéant devant le juge.	Pas de présomption juridique directe mais une authentification du site et un lien entre le dit site et une personne physique ou morale (imputabilité des éléments contenus par le site)

Présomptions juridiques des niveaux de fiabilité de la signature et du cachet électroniques. (tableau 2)

Service de confiance	Simple	Avancé	Avancé sur certificat qualifié	Qualifié
Signature électronique	Elle ne peut pas être refusée par le juge au seul motif qu'elle n'est pas qualifiée (art. 25.1 du Règlt eIDAS) Il faut démontrer sa fiabilité devant le tribunal en cas de remise en cause. Ce sera à la personne qui s'en prévaut de rapporter la preuve.	Elle ne peut pas être refusée par le juge au seul motif qu'elle n'est pas qualifiée (art. 25.1 du Règlt eIDAS) Il faut démontrer sa fiabilité devant le tribunal en cas de remise en cause. Ce sera à la personne qui s'en prévaut de rapporter la preuve.	Dans le domaine privé, elle ne peut pas être refusée par le juge au seul motif qu'elle n'est pas qualifiée (art.25.1 du Règlt eIDAS) . Il faut démontrer sa fiabilité devant le tribunal en cas de remise en cause. Ce sera à la personne qui s'en prévaut de rapporter la preuve. Dans le domaine public (art. 27 Règlt eIDAS) et selon la réglementation nationale en vigueur (c'est-à-dire si un Etat membre exige une SEA* avec certificat qualifié pour accéder à un téléservice public) , toutes les SEA avec certificat qualifié sont reconnues par les autres Etat membres. *Signature electronique Avancée	La signature électronique qualifiée est équivalence avec la signature manuscrite (art. 25.2 Règlt eIDAS) Elle est reconnue dans les autres Etats membrres (art. 25 Réglt eIDAS). La fiabilité de la signature est présumée. Ca sera à la personne qui la conteste de rapporter la preuve de son absence de fiabilité.
Cachet électronique	Il ne peut pas être refusé par le juge au seul motif qu'il n'est pas qualifié (art.35.1 du Règlt eIDAS). Il faut démontrer sa fiabilité devant le tribunal en cas de remise en cause. Ce sera à la personne qui s'en prévaut de rapporter la preuve.	Il ne peut pas être refusé par le juge au seul motif qu'il n'est pas qualifié (art.35.1 du Règlt eIDAS). Il faut démontrer sa fiabilité devant le tribunal en cas de remise en cause. Ce sera à la personne qui s'en prévaut de rapporter la preuve.	Dans le domaine privé, elle ne peut pas être refusée par le juge au seul motif qu'elle n'est pas qualifiée (art.35.1 du Règlt eIDAS) Il faut démontrer sa fiabilité devant le tribunal en cas de remise en cause. Ce sera à la personne qui s'en prévaut de rapporter la preuve. Dans le domaine public (art. 37 du règlement eIDAS) et selon la réglementation nationale en vigueur, c'est à dire si un Etat membre exige un cachet électronique qualifié (CEA) avec certificat qualifié pour accéder à un téléservice public, tous les CEA avec certificat qualifié sont reconnus par les autres Etats membres.	L'intégrité des données et l'exactitude de l'origine des données sont présumées. (art 35.2). Il est reconnu dans les autres Etats membres (art. 35.3 Règlt eIDAS).

Pourquoi y a-t-il différents « niveaux » de services de confiance ?

Il existe différents niveaux, au minimum deux : non-qualifié et qualifié.
Le règlement eIDAS dispose qu'un service de confiance ne peut pas être rejeté au seul titre qu'il n'est pas qualifié. Cela induit donc une reconnaissance de ces deux niveaux.

Autrement dit, ce n'est pas parce qu'un service de confiance n'est pas qualifié qu'il n'est pas fiable. En revanche cette démonstration devra être faite devant le juge.

Les différents niveaux de fiabilité permettent de ne pas confondre les bonnes pratiques techniques avec les présomptions juridiques qu'elles induisent.

De ce fait, plus le niveau est fiable (avancé, qualifié par exemple) plus les exigences techniques et procédurales déployées sont strictes et souvent onéreuses mais plus la recevabilité juridique du service de confiance sera facile à rapporter. Les différents niveaux, leur recevabilité et donc leur acceptabilité permettent une utilisation par et pour le plus grand nombre.

.

Cette utilisation généralisée (surtout du service de signature électronique) s'applique aujourd'hui à des usages quotidiens excédant le périmètre B2B

La confiance naît du fait que la qualification d'un service de confiance résulte d'un audit mené par un organe de contrôle étatique, ayant pu attester de la conformité dudit service et dudit prestataire avec un référentiel issu du règlement eIDAS. Le client peut donc souscrire audit service de manière sereine et confiante.

2

Les efforts de preuve en fonction des niveaux de fiabilité

Vu la possibilité de disposer d'une présomption ou non selon le niveau de fiabilité des services de confiance, notamment pour la signature et le cachet électroniques, les utilisateurs doivent fournir un effort de preuve différent.

Les preuves à présenter à un juge sont multiples. Vous pouvez les retrouver dans le guide signature électronique II : validation et conservation.

Exemple des efforts de preuves pour la signature électronique

Service de confiance	Simple	Avancé	Avancé sur certificat qualifié	Qualifié
Signature électronique	Preuve de l'identification avec des éléments extrinsèques. Fourniture d'un fichier de preuve, attestation de preuve, etc.	Fournir la preuve de l'identification et la preuve sur le contrôle exclusif du dispositif de création de signature : il faudra prouver qu'il n'y a que la signataire qui peut activer le dispositif de signature.	L'effort de preuve devra porter sur le contrôle exclusif.	Equivalence avec la signature manuscrite et application des règles figurant dans le Code de procédure civile.

Pourquoi y a-t-il deux niveaux avancés pour la signature électronique ?

Le règlement définit trois niveaux : simple, avancé et qualifié.

Le niveau avancé est défini comme suit :

« Une signature électronique avancée satisfait aux exigences suivantes:

a) être liée au signataire de manière univoque;

b) permettre d'identifier le signataire;

c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif; et

d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable. »

Il est également possible de répondre à l'exigence d'identification via l'utilisation d'un certificat qualifié tel que précisé à l'article 28 du règlement eIDAS.

Cela a donc l'effet de deux niveaux avancés dans les pratiques actuelles.

Petit rappel : La différence entre signature et cachet électronique

	Signature électronique	Cachet électronique
Qui est identifié ?	Le certificat généré pour établir une signature électronique identifie une personne physique ou une personne physique représentant une personne morale.	Le certificat généré identifie une personne nmorale.
Quel est son usage ?	Identifier le signataire, consentir au contenu d'un document et en garantir l'intégrité.	Identifier la personne morale dont il émane et en garantir l'intégrité. Il n'engage pas sur le consentement au contenu du document.
Existe-t-il une équivalence manuscrite ?	La signature électronique qualifiée équivaut à une signature manuscrite.	Le cachet électronique qualifié n'a pas d'équivalence manuscrite.

Et le cachet serveur, qu'est-ce que c'est ?

Il s'agit d'un cachet électronique dont l'utilisation est automatisée via un serveur : on peut alors cacheter des documents de manière automatique et en masse.

Les obligations en termes de niveaux de services de confiance

Certains textes imposent l'utilisation d'un niveau spécifique des services de confiance, notamment du niveau qualifié. Il est primordial lors de la mise en place de services de confiance de vérifier la règlementation en vigueur.

Textes	Validation sur niveau de signature particulier	Validation sur une typologie de document
eIDAS (article 32 et 33)	Signature électronique qualifiée	
Articles 96F bis du CGI		Facture électronique signée
Article 5 de l'arrêté du 22 mars 2019 relatif à la signature électronique des contrats de la commande publique	Signature électronique qualifiée	

Source : La signature électronique II Validation et archivage, FnTC

A quoi servent les obligations en termes de niveau de services de confiance ?

Le niveau de fiabilité du service de confiance induit des obligations différentes à respecter par les Prestataires de services de confiance mais aussi par leurs utilisateurs (ex : renforcement des exigences relatives à l'identification). Cela permet de garantir la fiabilité et la sécurité d'un document en fonction des besoins et exigences d'une situation donnée.

Par exemple, les factures électroniques doivent garantir, entre autres, l'authenticité de leur origine c'est à dire de l'identité de la personne dont elle émane. L'authenticité des factures peut être apportée par 4 moyens dont la signature électronique qualifiée ou le cachet électronique qualifié.

Tous les niveaux de services de confiances sont-ils interopérables en Europe ?

Au niveau européen le règlement eIDAS étant d'application directe, ses dispositions sont reconnues dans tous les Etats membres de l'Union. L'interopérabilité des services de confiance qualifiés est donc assurée par le respect du règlement eIDAS.

La réception d'un service de confiance non qualifié dépendra de la démonstration qui pourra être effectuée devant le tribunal d'un autre pays. De la pédagogie et des explications claires seront à ce titre nécessaires.

Pour une utilisation de services de confiance dans un pays autre que celui du prestataire de service de confiance, il est recommandé de s'assurer que le prestataire soit reconnu comme un prestataire de service de confiance qualifié (PSCQ) inscrit dans la liste européenne de confiance.

De même si une solution non qualifiée est mise en œuvre, il est recommandé de s'assurer que le prestataire aura la capacité de produire les preuves suffisantes et recevables dans le pays visé.

Le fait de respecter certaines normes (en particulier EN et ETSI) permettra de faciliter cette démonstration.

Flash info : Un acte d'exécution prévu dans le nouveau règlement eIDAs devrait prévoir un cadre juridique pour la signature avancée dans les différents Etats membres de l'Union européenne.

3

Pourquoi et comment mettre en place un service de confiance ?

Pour quelles raisons mettre en place un service de confiance ?

Il existe différentes raisons poussant les entreprises à mettre en place des services de confiance :

- Être en conformité avec les règlementations sur des process dématérialisés.
- Améliorer l'image de l'entreprise : le service de confiance optimise l'image de l'entreprise et limite les litiges et leur publicité négative.
- Assurer la fiabilité et la validité du service mais aussi fluidifier l'expérience de vente (signature électronique), l'expérience de l'utilisateur (Envoi recommandé) tout en apportant les mêmes effets juridiques vus précédemment.
- Permettre de tracer et conserver les échanges et engagements de manière opposable.

Exemple de cas d'usages (non exhaustifs)

Cas d'usage	Service de confiance	Règlementation	Objectifs
Contrats entre client et fournisseur	Signature électronique	Article 25 et suivants du règlement eIDAS Article 1366 et 1367 du Code Civil	Disposer d'un contrat électronique signé fiable à des fins probatoires
Envoi d'une lettre recommandée	Envoi recommandé électronique	Article 43 et suivants du règlement eIDAS Article L100 du Code des postes et télécommunications électroniques	Disposer d'une lettre électronique fiable à des fins probatoires et de validité d'un acte.
Facture électronique	Signature ou cachet électronique	Article 25 et suivants et 35 et suivants du règlement eIDAS Article 289 du CGI	Disposer d'une facture électronique fiable et recevrable par l'administration fiscale en cas de contrôle.
Cachet de la poste faisant foi	Horodatage électronique	Article 41 et suivants du règlement eIDAS. (différents textes nationaux font référence à ce cachet de la poste)	Prouver la date d'envoi d'un message

L'analyse de risque dans le B2B : est-elle indispensable ?

Qu'est-ce qu'une analyse de risque ?

L'analyse de risque vise à identifier et évaluer les risques, menaces et vulnérabilités qui pèsent sur une organisation dans un contexte précis afin de déterminer les moyens de couverture de ces risques.

De quels risques parle-t-on ?

Concrètement : une atteinte à l'intégrité, à la confidentialité et à la disponibilité d'un service pouvant entraîner des conséquences juridiques et financières.

Le but étant de définir quels sont les biens essentiels de mon entreprise afin d'analyser les risques qui peuvent toucher ces biens et les conséquences juridiques et financières pour mon entreprise : divulgation de données personnelles ou stratégiques au grand public, perte d'un contrat d'un montant important, désaccord sur les termes d'un contrat préalablement signé ou encore la perte de preuve d'antériorité, etc

Qui doit ou peut faire une analyse de risque ?

Les PSCQ sont obligés de la mener pour répondre à la règlementation eIDAS et obtenir leur qualification.

Les entreprises ensuite peuvent mener ce type d'analyse dans une procédure de prise de décision sur un projet de dématérialisation. Dans ce cas, l'analyse de risque permet de s'assurer que la solution choisie couvre les risques identifiés.

Le périmètre de l'analyse de risque est donc primordial.

Des méthodes existent pour les mener :

-https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/

-Guide de sélection du niveau des signatures et des cachets électroniques | Agence nationale de la sécurité des systèmes d'information

Elle est obligatoire pour les PSCQ mais peut s'appliquer à tout le monde de manière volontaire.

L'analyse de risque dans le B2B semble donc indispensable, c'est un vecteur de confiance.

Quels sont les critères pour choisir un prestataire de service de confiance (PSCQ) ?

Les critères suivants, au minimum, devraient être pris en compte pendant la phase de sélection du prestataire :

- S'assurer que le prestataire répond aux exigences de l'analyse de risque et de la règlementation sur les niveaux de services à mettre en œuvre.
- S'assurer de la responsabilité du prestataire et de ses garanties : clause de limitation de responsabilité, montant de la responsabilité, assurance, etc.
- S'assurer qu'il répond à la politique sécurité de l'organisation.

CONCLUSION

Comprendre et mettre en œuvre les services de confiance dans l'environnement numérique actuel est une étape cruciale pour toute entreprise souhaitant sécuriser ses transactions et interactions électroniques. Ces services, encadrés par le règlement eIDAS, offrent une base solide pour établir une confiance numérique, essentielle à la croissance et à la compétitivité dans le marché unique numérique européen.

En définissant les différents services de confiance et en explorant la valeur juridique des niveaux de fiabilité, nous avons vu comment chaque service joue un rôle spécifique dans la protection des interactions numériques, en garantissant leur intégrité, leur authenticité et leur confidentialité. Les efforts de preuve et la notion de présomption de fiabilité sont des concepts clés qui renforcent cette infrastructure de confiance, en offrant des garanties solides sur la fiabilité des transactions électroniques.

L'interopérabilité des services qualifiés au sein de l'Europe est un pilier de ce système, assurant que les services de confiance déployés dans un État membre soient reconnus et acceptés à travers tous les autres, facilitant ainsi les affaires et la communication dans un cadre transfrontalier. Cette harmonisation est fondamentale pour les entreprises qui cherchent à étendre leur présence et à opérer efficacement dans l'UE.

Pour les entreprises prêtes à adopter ces services, la décision ne doit pas être source d'anxiété mais vue comme une opportunité d'améliorer la sécurité, la confiance et l'efficacité des processus numériques. L'analyse de risque et le choix d'un prestataire de service de confiance compétent sont des étapes importantes de ce processus, guidant vers des solutions adaptées aux besoins spécifiques de l'entreprise et conformes aux standards réglementaires.

En conclusion, l'adoption des services de confiance n'est pas seulement une exigence réglementaire mais une démarche stratégique vers une digitalisation sécurisée et efficace.

A l'approche de l'adoption d'eIDAS v2, il est essentiel de reconnaître que l'objectif reste inchangé : renforcer la confiance dans le numérique. Pour les entreprises qui souhaitent déployer des services de confiance, cette évolution réglementaire représente une opportunité de se positionner à l'avant-garde de la sécurité numérique, tout en assurant une transition fluide et sans heurts.

NOTES

REMERCIEMENTS :

- Vincent Jamin, Vjamin Conseil
- Pascal Agosti, Cabinet Caprioli et associés
- Sebastien Passelergue, Be-ys
- Noémie Boris, Be-ys
- Amelie Frezier, Cecurity.com
- Marie Christine Baldy, Société Générale

fntc
Fédération des Tiers de Confiance du Numérique

Délégation Générale
14 rue de Bruxelles
75009 Paris
infos@fntc-numerique.com
fntc-numerique.com

AVRIL 2024