# Comprendre le règlement eIDAS


## Volume 1 - Qu'est-ce que le règlement eIDAS ?

fntc

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


## 1. Qu'est-ce que le règlement eIDAS ?

Champ d'application

L'application nationale : obligations et champ libre vis à vis du règlement

La différence entre Prestataire de service de confiance et Prestataire de service de confiance qualifié

## 2. Comment est-il mis en application ?

Organes de contrôles

## Conclusion

1

# Qu'est-ce que le règlement eIDAS ?

Il s'agit du règlement européen n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, et abrogeant la directive 1999/93/CE.

Comme tout règlement, il est d'application directe dans les droits nationaux, sans que des actes de transposition ne soient nécessaires par les Etats membres. Une transposition consiste à adapter le droit national aux exigences du droit européen, comme pour les directives européennes. Ce règlement est applicable pour la majorité de ses dispositions depuis 2016.

## Qu'est-ce que l'identification électronique ?

L'identification électronique est définie par le réglement eIDAS comme *« le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale. »* (article 3.1 du règlement eIDAS).

En d'autres termes, l'identification électronique sert à prouver l'identité d'une personne dans l'espace numérique (plateforme internet, carte d'identité électronique, etc.)

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

Le règlement introduit et définit des services de confiance : « un 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

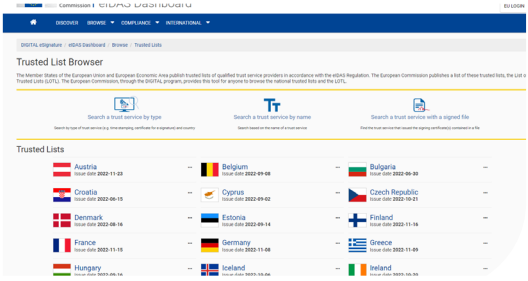
c) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services; » (article 3.16 du règlement eIDAS)

## Qu'est ce qu'un service de confiance qualifié ?

Un service qualifié de confiance répond à des exigences techniques complémentaires à respecter en amont pour garantir sa fiabilité.
De ce fait il offre :

- une présomption de fiabilité : celui qui conteste la valeur d'un service de confiance qualifié doit en rapporter la preuve.
- une reconnaissance mutuelle des services qualifiés et leur interopérabilité au sein de l'Union européenne.
- une publicité pour le prestataire et la qualité de ses services qualifiés. Cette publicité prend la forme de la trustmark, mais aussi de sa présence dans la liste de confiance (EUTL).

Il existe également différents niveaux pour les services de confiance. Ce point sera traité dans le 2e fascicule de cette série.




**Le renversement de la charge de la preuve**: dans le cas d'un service de confiance non qualifié, c'est la personne qui se prévaut du service de confiance qui doit en prouver la fiabilité. Dans le cas d'un service de confiance qualifié c'est à celui qui conteste le service de confiance de rapporter la preuve de cette absence de fiabilité.

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

*Un «prestataire de services de confiance» (PSCO) est «une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié; » (article 3.19 du règlement eIDAS).*

*«Un «prestataire de services de confiances qualifié (PSCQ) est «un prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut qualifié; » (article 3.20 du règlement eIDAS).*

**Quelle différence entre un PSCQ et un PSCO ?**
Le PSCQ est un Prestataire de Service de Confiance Qualifié tel que défini dans le règlement européen eIDAS. Il est évalué selon des critères nationaux découlant du règlement et de ses actes d'exécution, et qui ne peuvent pas y être contraires.

## Comment devenir un prestataire de services de confiance qualifié?

Le PSCQ doit répondre à un référentiel de certification élaboré par chaque organe de contrôle national. Il est soumis tous les 24 mois à des audits de contrôle, à sa charge. Il doit notamment satisfaire aux exigences suivantes:

- «A en charge de vérifier l'identité des personnes physique ou morale auxquelles il délivre un certificat qualifié ;
- Utilise des systèmes fiables protégés contre les modifications et assure la sécurité technique et la fiabilité de ses processus ;
- Utilise des systèmes fiables pour stocker les données qui lui sont confiées ;
- Prend les mesures nécessaires pour se protéger contre la falsification et le vol de données;
- Conserve et maintient accessibles pour une durée appropriée, y compris après que les activités du PSCQ ont cessé, les données permettant d'apporter des preuves en justice ;
- A un plan de continuité d'arrêt d'activité afin d'assurer la continuité de service ;
- Est conforme aux règles de traitement des données à caractère personnel;
- Tient à jour une base de données des certificats qualifiés qu'il délivre et de leur statut (valide ou révoqué) ;

- Doit pouvoir fournir à son utilisateur l'historique du statut d'un certificat qualifié même après sa révocation ;
- Maintient des ressources financières suffisantes et/ou contracte une assurance responsabilité appropriée. »

*Source: La signature électronique: définitions et cas d'usage, FnTC -CR2PA*

Il faut, à ce sujet, rajouter que la qualification est basée sur la technique et la qualité de service des prestataires de services de confiance. Cela ne signifie pas pour autant que ces prestataires n'ont pas un devoir de conseil envers leurs clients. Or, cette notion est primordiale dans l'utilisation des services afin de conserver leurs atouts en termes de confiance numérique.

2

# Comment le règlement eIDAS est-il mis en application ?

**Qu'est ce qu'un organe de contrôle ?**

L'organe de contrôle national est défini par chaque Etat Membre. Il est en charge de définir les exigences nationales pour la qualification des prestataires et de qualifier les prestataires. L'audit incombe au prestataire et doit être mené par un centre d'évaluation agréé par l'organe de contrôle.

Il élabore et tient à jour la liste des prestataires nationaux et de leurs services qui figureront dans la liste européenne de confiance (EUTL). Il assure la certification des dispositifs sécurisés de création de signatures et cachets électroniques qualifiés.

En France, l'organe de contrôle est l'ANSSI.

**L'organe de contrôle a-t-il des marges d'interprétation ?** (référentiels de qualification)

Une certaine marge d'interprétation est possible lorsque le règlement ne définit pas précisément les moyens pour parvenir à un objectif déterminé comme l'identification, le choix des équipements, etc.

Cette marge d'interprétation se retrouve dans les référentiels nationaux : chaque organe de contrôle interprète les modalités d'évaluation et les normes de référence à partir du moment où celles-ci **ne sont pas en contradiction avec le règlement eIDAS.**

De ce fait, nous observons des différences entre les Etats membres de l'Union européenne sur les critères d'évaluation pouvant créer dans certains cas une concurrence. Le règlement eIDAS promeut l'interopérabilité des services de confiance qualifiés entre les Etats membres. Un PSCO qualifié dans un pays selon les critères d'évaluation nationaux peut ensuite opérer avec les mêmes effets juridiques partout en Europe, et de ce fait créer une concurrence avec un prestataire d'un autre Etat soumis à des critères différents.

Le Cyber Security Act publié au Journal Officiel de l'UE le 7 juin 2019 apporte une approche communautaire de la certification des outils de sécurité. Il poursuit un double objectif : l'adoption du mandat permanent de l'ENISA, l'Agence européenne pour la cybersécurité et la définition d'un cadre européen de certification de cybersécurité, essentiel pour renforcer la sécurité du marché unique numérique européen et assurer une homogénéité des procédures de qualification.

### Comment la France a-t-elle mis en application le règlement eIDAS ?

La mise en application du règlement est réalisée à travers le visa dans les textes règlementaires nationaux du règlement eIDAS.

Le droit national fait référence au règlement eIDAS dans certains textes afin d'identifier les champs d'application dans lesquels l'obtention d'une présomption de fiabilité est possible.

Le premier texte faisant référence au règlement eIDAS est le décret du 28 septembre 2017 sur la signature électronique .

D'autres textes ont suivi dans le but de mettre en application le règlement européen dans notre droit national:

- Décret 2016 sur la fiabilité des copies
- Décret 2018 sur les envois recommandés électroniques
- Article 289 du Code général des impôts
- Décret 2022-1299 relatif à la généralisation de la facture électronique et son arrêté d'application du même jour.

Mais aussi un référentiel documentaire mis en œuvre par l'ANSSI, propre à chaque service de confiance qualifié ainsi qu'à la notion de prestataire de services de confiance qualifié.

# CONCLUSION

## Pourquoi un règlement eIDAS ?

Avant 2016 et l'application du règlement eIDAS, seule la directive 1999-93 CE du 13 décembre 1999 relative à un cadre communautaire pour les signatures électroniques existait. Elle était transposée dans les différents droits nationaux de l'Union européenne.

Une harmonisation s'est avérée nécessaire lors de la multiplication des usages autour de la signature électronique pour répondre aux objectifs d'ouverture d'un marché unique numérique entre les Etats membres mais aussi pour encadrer des nouvelles technologies (les «nouveaux» services de confiance).

### Qu'est ce que le marché unique numérique ?

L'Union européenne a mis en place depuis 2015 une stratégie visant à mettre en place un marché unique numérique au sein du marché intérieur. Autrement dit l'ouverture au marché européen pour les acteurs du numérique. Le règlement eIDAS s'inscrit dans cette stratégie, et en est l'un des piliers.

# Remerciements


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



fntc
Fédération des Tiers de Confiance du Numérique

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



Mars 2023