Comprendre le règlement eIDAS

Volume 3 - Le règlement eIDAS 2.0

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

Le 20 mai 2024, le règlement modificatif du règlement eIDAS est entré en vigueur.

L'adoption de ce règlement représente une évolution majeure dans le domaine de l'identité numérique, avec une obligation pour les États membres de délivrer des portefeuilles européens d'identité numérique en novembre 2026 au plus tard permettant notamment aux citoyens de s'identifier et s'authentifier électroniquement en ligne et hors-ligne avec un niveau de garantie élevé. Ce nouveau règlement poursuit également un objectif d'harmonisation croissante des services de confiance avec, notamment, l'introduction de nouveaux services de confiance. Enfin, le texte prévoit la mise en place d'une nouvelle instance de coopération transverse au niveau européen, l'European Digital Identity Cooperation Group (EDICG), ayant vocation à accroître la coopération entre les Etats membres et la Commission européenne autant dans le domaine de l'identité numérique que dans celui des services de confiance.

L'implémentation de ce nouveau règlement européen qui vient compléter le précédent règlement eIDAS, et non l'abroger, va présenter de nombreux nouveaux défis pour les entités publiques et privées qui devront travailler de concert pour en garantir le succès.

1

Pourquoi une mise à jour du règlement eIDAS ?

La révision du règlement eIDAS s'inscrit dans un contexte règlementaire qui a évolué depuis 2014 notamment sur les sujets de cybersécurité et de protection des données personnelles. Cette nouvelle version est donc une évolution logique du règlement afin de garantir son adéquation à ces nouvelles problématiques et à l'encadrement européen qui en découle. Cette richesse règlementaire peut s'illustrer par le tableau suivant qui reprend les textes cités par le règlement eIDAS dans sa nouvelle version.

Domaine	Texte règlementaire
Protection des données personnelles	Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques
Protection des données personnelles	Règlement européen 2016/679 sur la protection des données personnelles (RGPD)
Protection des données personnelles	Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données
Cybersécurité (Cybersecurity Act)	Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications
Sécurité de la carte d'identité	Règlement (UE) 2019/1157 du Parlement européen et du Conseil du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation
Accessibilité (personnes handicapées, ...)	Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services
Cybersécurité (NIS 2)	Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union
Plateformes numériques (Digital Market Act)	Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique
Plateformes numériques (Digital Market Act)	Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques
Portefeuille européen d'identité numérique (Groupe d'experts eIDAS en charge d'établir l'architecture de référence du portefeuille)	Recommandation (UE) 2021/946 de la Commission du 3 juin 2021 concernant une boîte à outils commune de l'Union pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique

Dans ce nouveau contexte réglementaire, le règlement eIDAS peut être décrit comme composé de deux parties (directement héritées de sa première version) : les services de confiance et le portefeuille européen d'identité numérique.

2

Les services de confiance

Les services de confiance de la première version du règlement sont maintenus et actualisés pour certains. Naissent également de nouveaux services de confiance dans le but d'harmoniser le cadre règlementaire et les effets juridiques des nouvelles pratiques du marché.

Les tableaux ci-contre représentent ces changements et nouveautés.

Les services de confiance déjà existants dans le règlement V1 et leur évolution dans le règlement V2*

Services de confiance	Evolution dans le règlement eIDAS V2
Délivrance de certificat d'authentification des sites web (QWAC)	Reconnaissance et affichage convivial du certificat par les navigateurs webs
Envoi recommandé électronique (ERE)	Possibilité d'échanges de recommandés entre les prestataires offrant ce service qualifié.
Horodatage qualifié	Nouvel acte d'exécution en attente qui définira, entre autres, la fiabilité des sources de temps
Conservation qualifiée des signatures et cachets électroniques qualifiés	Nouvel acte d'exécution en attente
Validation qualifiée pour les signatures et cachets qualifiés	Nouvel acte d'exécution en attente
Emission de certificat qualifié de cachet électronique qualifié	Nouvel acte d'exécution en attente
Emission de certificat qualifié de signature électronique qualifiée	Nouvel acte d'exécution en attente
Signature avancée	Un acte d'exécution va éventuellement définir les standards applicables à la signature avancée

Nouveaux services de confiance introduits par eIDAS V2*.

Les nouveaux services de confiance introduits par eIDAS v2

Services de confiance	Description	Quel est l'objectif de ce service ?
La gestion de dispositifs de création de signature électronique à distance ou de dispositifs de création de cachet électronique à distance	Ce service de confiance introduit l'activation à distance des signatures et cachets qualifiés comme un service à part entière. Il pourra être fourni par un PSCO qualifié.	Disposer d'une signature électronique qualifié activée à distance. Recourir à des prestataires différents pour la signature et l'émission du certificat.
Service qualifié d'archivage électronique	Ce service introduit la notion d'archivage sécurisé de documents et de données tout au long de leur période de conservation légale ou contractuelle.	Garantir l'intégrité, l'exactitude de l'origine et la pérennité des documents et données. Mais aussi avoir la capacité d'apporter les preuves de ces garanties.
Les registres électroniques qualifiés	Les registres électroniques ont pour vocation de garantir l'origine, l'intégrité et le classement chronologique des données qui les composent.	Introduire un effet juridique (présomption légale) vis à vis des technologies de traçabilité comme la Blockchain. Les registres électroniques qualifiés pourront être reçus comme des preuves à part entière.
Attestations d'attributs qualifiés	Une attestation d'attributs est une preuve sous forme électronique de la qualité, caractéristiques, droits ou permissions d'une personne physique ou morale ou d'un objet (licence, diplômes, pouvoirs, mandats, etc.)	L'attestation d'attributs électronique a pour objectif d'avoir la même valeur légale que l'attestation délivrée sous forme papier. Ces attestations pourront être délivrées et conservées dans des PEIN (Portefeuilles Européens d'Identité numérique)

*Les noms complets des services de confiance sont disponibles à l'article 16 du règlement eIDAS.

3

Le Portefeuille Européen d'Identité Numérique

Le Portefeuille Européen d'Identité Numérique (PEIN) fait son entrée dans cette nouvelle version du règlement et modifie le volet identité numérique de la première version du règlement. Le PEIN vise à favoriser l'adoption par le secteur privé des identités électroniques de manière harmonisée.

Définition et reformulation

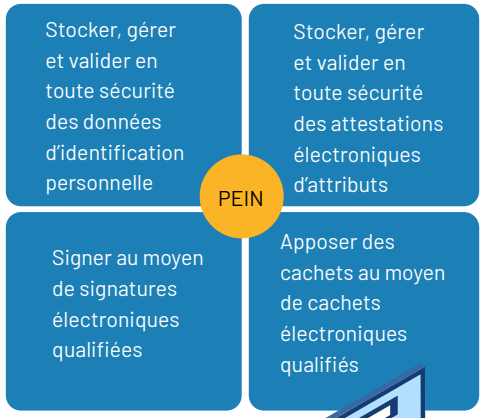
Le Portefeuille Européen d'Identification Numérique (PEIN) est *"un moyen d'identification électronique qui permet à l'utilisateur de stocker, de gérer et de valider en toute sécurité des données d'identification personnelle et des attestations électroniques d'attributs afin de les fournir aux parties utilisatrices et aux autres utilisateurs des portefeuilles européens d'identité numérique, et de signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés."*
(article 3.42 du Règlement eIDAS V2)

Nous vous proposons ici de décomposer cette définition afin d'en faciliter sa compréhension.

Arrêtons nous un instant sur la première partie de la définition afin d'en expliquer certains termes dans le schéma ci-dessous : *"un moyen d'identification électronique qui permet à l'utilisateur de* ***stocker, de gérer et de valider en toute sécurité des données d'identification personnelle et des attestations électroniques d'attributs*** »

Le PEIN garantit de facto la disponibilité, confidentialité et intégrité (sécurité) des données.

Les données d'identification personnelle sont *« un ensemble de données qui sont délivrées conformément au droit de l'Union ou au droit national et qui permettent d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une autre personne physique ou une personne morale »*



Attestations électroniques d'attributs : voir le tableau des nouveaux services de confiance

Expliquons maintenant à quoi servira le PEIN, autrement dit, attelons nous à la deuxième partie de la définition : *"un moyen d'identification électronique qui permet à l'utilisateur de stocker, de gérer et de valider en toute sécurité des données d'identification personnelle et des attestations électroniques d'attributs afin de les* **fournir aux parties utilisatrices et aux autres utilisateurs des portefeuilles européens d'identité numérique**, *et de* ***signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés."***

Authentification et identification

Le Portefeuille Européen en tant que moyen d'identification électronique pourra être utilisé pour s'authentifier sur des services en ligne ou hors-ligne.

"L'identité numérique de l'UE peut être utilisée dans un grand nombre de cas, par exemple pour:

- utiliser des services publics, comme pour demander un acte de naissance ou un certificat médical ou signaler un changement d'adresse ;
- ouvrir un compte bancaire ;
- remplir une déclaration fiscale ;
- s'inscrire dans une université, dans son pays d'origine ou dans un autre État membre ;
- conserver une prescription médicale utilisable partout en Europe ;
- prouver son âge ;
- louer une voiture au moyen d'un permis de conduire numérique ;
- s'enregistrer au début d'un séjour à l'hôtel."

Cf : Identité numérique européenne - Commission européenne (europa.eu)

Il est intéressant de comprendre dans ces cas d'usage que l'identité européenne, via le Portefeuille, devrait permettre **d'apporter la preuve de certaines données d'identification sans pour autant dévoiler les autres.** Par exemple dans le cas de la preuve de son âge, la date de naissance ne serait pas dévoilée, et seul le PEIN la conserverait.

Identification et certificat de signature électronique

Le PEIN étant un moyen d'identification élevé, il pourra servir d'identification pour l'émission d'un certificat qualifié de signature ou cachet par une autorité de certification.

Le PEIN permettra à son utilisateur d'utiliser et de fournir ses données d'identification personnelle et ses attestations d'attributs à d'autres utilisateurs de PEIN ou à des parties utilisatrices (dument enregistrées dans l'Etat membre dans lequel elle sont établies), conformément à l'article 5 ter.

Autrement dit les données d'identification et attestations d'attribut permettront non seulement de s'authentifier sur des services publics ou privés, mais aussi d'être reconnues comme données fiables par des tiers (parties utilisatrices) à différentes fins : inscription officielle, contractualisation, etc. Aujourd'hui, les usages concrets sont en cours de définition.

Un PEIN pour tous ?

Notons que le PEIN n'est pas un service de confiance car il est une obligation s'adressant directement aux Etats membres de l'UE.
Par ailleurs il est construit autour d'une identité électronique (volet du règlement de 2014, distinct des services de confiance).
Un PEIN devra obligatoirement être mis à disposition soit :

- Directement par un Etat membre
- Sur mandat de l'Etat membre
- Indépendamment d'un Etat membre tout en étant reconnu par cet Etat membre.

Les PEIN pourront être, selon les Etats, proposés par un acteur public ou par des acteurs privés.

En outre, des incertitudes sur les travaux et textes encadrant le PEIN demeurent encore à ce jour.

A titre d'exemple, selon le règlement, l'utilisation de la signature électronique qualifiée via un PEIN devrait être gratuite lors d'un usage non-professionnel pour les personnes physiques.

Reste à éclaircir à ce sujet différents éléments :

- Comment le PEIN permettra-t-il de signer d'un point de vue technique ?
- Ce que l'on entend par usage non-professionnel ?
- Quelles seront les limites de la gratuité ?

Afin de clarifier certaines zones d'ombre, deux initiatives ont été proposées par la Commission européenne :

- Une boite à outils et des spécifications techniques pour la mise en œuvre d'un PEIN : Architecture and Reference Framework (ARF)(- https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.3.0/arf/)
- Quatre consortiums visant la mise en place de pilotes à large échelle:
  - Potential vise à favoriser l'innovation, la collaboration et la croissance dans six secteurs de l'identité numérique — les services gouvernementaux, les banques, les télécommunications, les permis de conduire mobiles, les signatures électroniques et la santé.

- Le consortium de portefeuilles d'identité numérique de l'UE (EWC) est un effort conjoint visant à tirer parti des avantages de l'identité numérique proposée dans l'UE sous la forme de certificats de voyage numériques dans l'ensemble des États membres. Le CEE a l'intention de s'appuyer sur l'application de portefeuille de référence pour permettre des utilisations liées à Digital Travel Credentials

- NOBID est un ensemble de pays nordiques et baltes qui, avec l'Italie et l'Allemagne, piloteront l'utilisation du portefeuille d'identité numérique de l'UE pour autoriser les paiements de produits et de services.

- DC4EU apporte un soutien tangible aux secteurs public et privé dans les secteurs de l'éducation et de la sécurité sociale en déployant et en accédant à des infrastructures de services numériques transeuropéens interopérables de pointe et à leur intégration dans un cadre de confiance transfrontière.

Ces consortiums travaillent sur les cas d'usages suivants :

1. Accès aux services publics: Accès sécurisé aux services publics numériques, tels que la demande de passeport ou de permis de conduire, le dépôt de taxes ou l'accès aux informations de sécurité sociale.

2. Ouverture d'un compte bancaire: Vérification de l'identité d'un utilisateur lors de l'ouverture d'un compte bancaire en ligne, éliminant la nécessité pour l'utilisateur de fournir à plusieurs reprises ses informations personnelles

3. Enregistrement SIM: Preuve d'identité aux fins des contrats de carte SIM prépayée et post-payée (enregistrement et activation), réduisant la fraude et les coûts pour les opérateurs de réseaux mobiles.

4. Permis de conduire mobile: Stockage et présentation du permis de conduire mobile dans les interactions en ligne et physiques d'un conducteur fournissant son permis de conduire.

5. Signature des contrats: Créer des signatures numériques sécurisées pour la signature de contrats en ligne, éliminant ainsi le besoin de documents papier et de signatures physiques.

6. Demande d'ordonnances: Fournir les détails de la prescription aux pharmacies et initier la dispense des produits médicaux.

(cf Mise en œuvre pilote du portefeuille d'identité numérique de l'UE | Bâtir l'avenir numérique de l'Europe (europa.eu)

Source documentaire : Identité numérique européenne (eID): le Conseil adopte un cadre juridique relatif à un portefeuille numérique sécurisé et fiable pour tous les Européens - Consilium (europa.eu)

3

7. Voyage: Présenter des informations provenant de documents de voyage (p. ex. passeport, visa), permettant un accès rapide et facile lorsque vous passez par la sécurité de l'aéroport et les douanes.

8. Identités numériques organisationnelles: Pour prouver qu'une personne est la représentante légitime d'une organisation» par «Gérer les délégations au sein d'une structure.

9. Paiements: Vérification de l'identité d'un utilisateur lors de l'initiation d'un paiement en ligne.

10. Certification de l'éducation: Preuve de possession de titres d'études, tels que des diplômes, des diplômes et des certificats, ce qui facilite la demande d'emploi ou de formation continue.

11. Accès aux prestations de sécurité sociale: Un portefeuille d'identité numérique de l'UE peut être utilisé pour accéder en toute sécurité aux informations et aux prestations de sécurité sociale d'un utilisateur (par exemple, retraite, prestations d'invalidité). Il peut également être utilisé pour faciliter la libre circulation en stockant des documents tels que la carte européenne d'assurance maladie.

En conclusion, le portefeuille européen d'identité se présente comme un formidable accélérateur de la transformation digitale. Il apporte aux citoyens européens un moyen unique, interopérable et sécurisé pour se connecter, signer et échanger avec des fournisseurs de services. Il est aussi une opportunité pour les fournisseurs de services de réduire les risques, en particulier d'usurpation d'identité et les coûts de conformité, mais aussi d'augmenter les capacités de simplification de la conquête client.

Le challenge principal auquel il va faire face sera son déploiement et son adoption. Certains secteurs seront obligés de l'accepter comme les grandes plateformes en ligne. D'autres secteurs y verront une simplification et un apport comme les banques et assurances. L'homogénéisation des niveaux de sécurité sera également un challenge important avec une forte disparité à ce jour des niveaux d'identification substantiel et élevé selon les pays ainsi que le cadre de certification qui s'annonce national pour un portefeuille européen.

(NB : les actes d'exécution ne sont pas publiés au moment de la rédaction de ce guide).

4

Le régime de sanction du règlement eIDAS

Les sanctions administratives (article 16) visant des prestataires de service de confiance qualifiés et non qualifiés (Voir le guide «Comprendre le règlement eIDAS - Volume 1») ont été définies dans le nouveau règlement. Elles peuvent aller jusqu'à 5M€ ou 1% du CA du groupe dont fait partie le prestataire de service de confiance (PSCO).

Certains Etats, à l'instar de la France, avaient déjà prévu des sanctions dans certaines situations. Le règlement vient compléter pour tous les États membres ce régime de sanction. Cet apport du texte est fondamental car elle renforce la confiance que les utilisateurs peuvent avoir dans les PSCO.

La responsabilité des PSCO est rappelée à l'article 13 du règlement eIDAS. Celle-ci s'appuie sur le droit national applicable en la matière pour les PSCO. La charge de la preuve incombe à la partie qui entend engager la responsabilité du PSCO pour les PSCO non qualifiés.

A contrario, un prestataire de service de confiance qualifié (PSCQ) sera présumé responsable en cas de défaillance de son service de confiance qualifié, sauf s'il arrive à démontrer la négligence de son client.

Ce nouveau régime de sanction inscrit donc le règlement eIDAS V2 en concordance avec le cadre règlementaire européen autour de la cyber sécurité et de la protection des données personnelles: des exigences claires et un régime de sanction précis. D'ailleurs, il faut noter que ces régimes de sanctions peuvent se cumuler.

La confiance numérique se trouve donc consolidée par ce maillage règlementaire. Nous retiendrons la référence suivante aux PSCQ dans NIS 2 : "*les prestataires de services de confiance qualifié sont positionnés au plus haut niveau de responsabilité quelle que soient leurs tailles*".

5 Les étapes à venir

A ce jour, les organes de contrôle attendent les actes d'exécution qui référenceront les normes et spécifications techniques sur lesquels ils pourront s'appuyer pour dresser leurs référentiels. Les actes d'exécution seront adoptés au plus tard le 21 mai 2025 à l'exception des actes en référence aux signatures et cachets électroniques avancés. En effet la Commission évalue la nécessité de créer des actes pour ces deux services.

Les prestataires souhaitant se préparer aux futures qualifications peuvent d'ores et déjà se tourner vers le référentiel général disponible sur le site de l'ANSSI (Référentiels d'exigences ANSSI | ANSSI (cyber.gouv.fr)

La mise en place du PEIN doit être effective pour chaque Etat membre le 21 novembre 2026. Pour cela, les exigences minimales des PEIN en matière de services et de sécurité seront détaillées dans les actes d'exécutions respectifs.
Ceux-ci seront adoptés au plus tard le 21 novembre 2024.

L'ARF devra alors être consolidé afin d'apporter les spécifications techniques nécessaires aux Etats membres pour respecter les exigences des actes d'exécutions. Pour cela, l'ARF se nourrit des retours des travaux des consortiums.

Ressources documentaires :

AM_Ple_LegConsolidated (europa.eu)

Révision du Règlement eIDAS et identité numérique (usine-digitale.fr)

Identité numérique, eIDAS et blockchain... Vers un nouveau paradigme centré sur l'utilisateur (usine-digitale.fr)

Vers une révision du règlement eIDAS ? (usine-digitale.fr)

Le ledger comme service de confiance dans la proposition de règlement eIDAS (usine-digitale.fr)

L'archivage électronique, futur service de confiance ? (usine-digitale.fr)

CONCLUSION

Le premier opus du règlement eIDAS avait permis la mise en œuvre et la standardisation des services de confiance numérique. Il introduisait également une notion peu commune d'identité numérique grâce au moyen d'identification électronique.

La seconde version du règlement vient intelligemment compléter la liste des services sans changer le fonctionnement des services existants. Ainsi, les acteurs ayant pris le train de la confiance numérique en 2014 seront sur les rails de ce second wagon. Le service d'archivage vient étendre le périmètre du règlement aux données et documents, le registre vient reconnaitre sans les nommer les blockchains et les attestations d'attributs font le lien avec le portefeuille européen d'identité numérique - véritable révolution de ce règlement.

En lien direct avec le Règlement Général sur la Protection des Données, le portefeuille européen d'identité numérique est un outil fourni aux citoyens pour reprendre le contrôle sur leurs données. Non content d'être utile aux particuliers, il peut également être délivré aux entreprises pour lesquelles sa valeur est peut-être encore plus importante.

Ce texte s'inscrit plus généralement dans une réglementation européenne qui a su évoluer depuis la première version de eIDAS pour tendre vers un cadre cohérent de cybersécurité et de souveraineté. Ce cadre renforce également les sanctions pour les prestataires de service de confiance numérique ; gage supplémentaire de la confiance que l'on peut leur accorder.

Parions que ce portefeuille d'identité et les nouveaux services soient les clés de voûtes d'un écosystème de services sécurisés - un écosystème de confiance numérique.

NOTES

Comité de rédaction

- Pascal Agosti - Cabinet Caprioli & Associés
- Marie-Christine Baldy - Société Générale
- Noémie Boris - BeYs
- Amélie Frezier - Cecurity.com
- Vincent Jamin - Vjamin Conseil
- Sébastien Passelergue - BeYs

Fédération des Tiers de
Confiance du numérique
5 impasse Gomboust
75001 Paris
infos@fntc-numerique.com
fntc-numerique.com

OCTOBRE 2024