Comprendre le règlement eIDAS

volume 4 – Premier panorama des actes d'exécution du Règlement eIDAS modifié

fntc

Présentation de la FnTC :

La Fédération des Tiers de Confiance du numérique (FnTC) rassemble éditeurs de logiciels, prestataires de services, experts, professionnels réglementés, start up, acteurs internationaux, utilisateurs et structures institutionnelles.

Notre objectif depuis 2001 : **une digitalisation fiable et sécurisée.**

Notre méthode :

- Produire des expertises et des outils pour que les personnes et les organisations puissent au sein du monde numérique préserver leurs droits et limiter leurs risques.
- Elaborer de la doctrine, en produisant des guides, des référentiels et des labels.
- Participer à la normalisation et à la standardisation des bonnes pratiques numériques au niveau national (Afnor) et international (ISO)
- Assurer des formations universitaires, comme les Masters Droit du numérique des Universités de Corse, de La Rochelle et de Lyon, ainsi que de la formation continue.

fntc

Fédération des Tiers de Confiance du Numérique

SOMMAIRE

INTRODUCTION

Le cadre européen relatif à une identité numérique est un élément essentiel pour la mise en place d'un écosystème d'identité numérique sécurisé et interopérable dans l'ensemble de l'Union. Avec pour pierre angulaire les Portefeuilles européens d'identité numérique (PEIN), il vise à faciliter l'accès aux services dans l'ensemble des Etats membres.

Il se définit à l'art. 3.42 du Règlement eIDAS comme *« 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 »*.

Ses fonctionnalités décrites aux articles 5 bis et suivants sont nombreuses ; le PEIN doit prévoir une gestion des données à caractère personnel et des attestations d'attributs (de leur création/ intégration à la gestion de leurs accès, portabilité, et jusqu'à leur suppression). Le PEIN indique également les conditions de prise en compte des relations avec les parties utilisatrices du PEIN et entre PEIN.

Le règlement prévoit d'apporter des précisions au moyen d'actes d'exécution. Le présent document se propose de faire un premier état des lieux des actes d'exécution votés et leur apport du point de vue de la partie utilisatrice.

1

L'Identité numérique

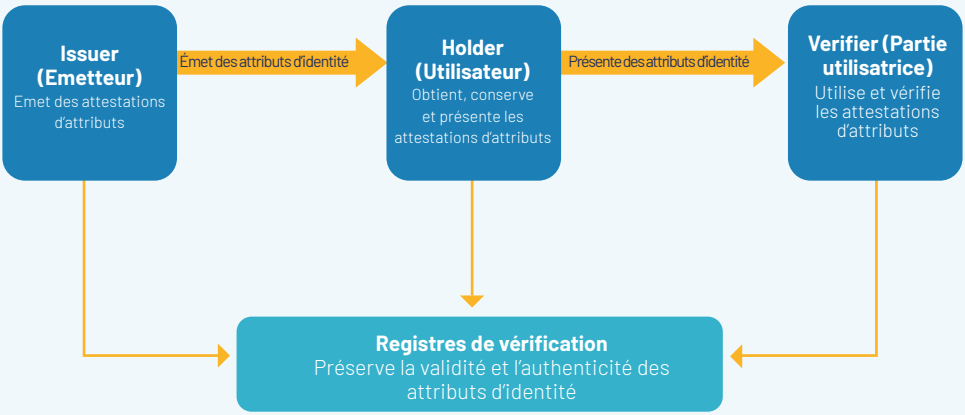
A. Le Triangle de Confiance et les acteurs associés : l'écosystème du PEIN

Le fonctionnement du PEIN repose sur la détention et le seul contrôle par le citoyen des informations le concernant. Ces données peuvent être issues de «fournisseur de données d'identification personnelle» ou des fournisseurs «d'attestation d'attribut». Ces derniers sont régis par le règlement lui même. Le fournisseur de données d'identification personnelle est défini dans l'acte d'exécution CIR 2024/2977 .

Une partie de la sécurité de ce modèle repose sur la séparation des rôles entre l'émetteur d'information (Issuer), l'utilisateur du PEIN (Holder) et la Partie Utilisatrice (Verifier). Cette contrainte imposée par l'acte d'exécution est une garantie de l'intéropérabilité au sein de l'écosystème.

L'"utilisateur" est défini dans le règlement, comme « *une personne physique ou morale, ou une personne physique représentant une autre personne physique ou une personne morale, qui utilise des services de confiance ou des moyens d'identification électronique* ». C'est le porteur du PEIN, la personne physique ou morale qui va prouver son identité ou justifier de qualités, grâce à l'application sécurisée de son smartphone.

La définition d'une "partie utilisatrice" dans le règlement : « *une personne physique ou morale qui se fie à une identification électronique, aux portefeuilles européens d'identité numérique ou à d'autres moyens d'identification électronique, ou à un service de confiance* ». Les utilisateurs s'identifient et s'authentifient vis à vis des services en ligne de la partie utilisatrice grâce au PEIN.



Les rôles et les flux d'informations constituant les bases de cette spécification.

Source : Recommendation W3C : Verifiable Credentials Data Model v2.0.

Acronymes :

ISSUER (Emetteur) :

Entité qui crée une attestation, composée d'une série d'attributs relatives au porteur.
Par exemple, une université qui délivre des diplômes universitaires ou des certificats à ses anciens étudiants.

HOLDER (Utilisateur) :

Entité qui possède une ou plusieurs attestations et qui peut les transmettre à des tiers.
Par exemple, une personne qui « détient » ses propres diplômes universitaires.

VERIFIER (Partie Utilisatrice) :

Entité qui effectue la vérification d'une attestation afin de contrôler la validité, la cohérence, etc.
Par exemple, un service numérique qui vérifie la validité d'une diplôme avant l'embauche d'une personne.

Verifiable Data Registry (Registres de vérification)

Ensemble des mécanismes permettant une vérification de la validité des attestations.
Par exemple, une liste de révocation.

Enrôlement et constitution de sa base d'attributs par l'utilisateur:

Concrètement, le citoyen télécharge sur son téléphone mobile, une application proposée par un fournisseur de PEIN. Ce fournisseur authentifie le portefeuille en lui attribuant une attestation d'authenticité. Sur la base de cette attestation, prouvant la détention du PEIN par le citoyen, le citoyen demande aux fournisseurs de données d'identité (PID provider) une attestation de son identité de personne physique ou morale et l'associe à son PEIN. Il peut ensuite demander des attestations d'attributs à d'autres fournisseurs pour enrichir son identité.

Utilisation du PEIN auprès des parties utilisatrices :

Lors des échanges avec une partie utilisatrice, celle-ci demande au citoyen les attributs nécessaires à la délivrance de son service. Le citoyen consent à fournir ses attributs et uniquement ceux-là. La partie utilisatrice peut alors vérifier que les attributs sont bien authentiques et les utiliser à des fins de preuve.

Le recours au PEIN pour des parties utilisatrices doit toujours appréhender les exigences nationales applicables à un service cible ainsi que le principe de minimisation des données concernant la délivrance du service cible (art. 5 ter 4 du RGPD).

La transparence est de rigueur quant aux parties utilisatrices. Comme les fournisseurs de PEIN, d'attributs et de PID, elles devraient apparaître sur des listes de confiance d'ici le 21 mai 2026.

Un règlement d'exécution n°2025/848 du 6 mai 2025 vient traiter les modalités d'enregistrement en question, à savoir la mise en place de registres nationaux des parties utilisatrices des PEIN (art.3), la publication d'une ou plusieurs politiques d'enregistrement nationales ainsi que des procédures d'enregistrement établies par les bureaux d'enregistrement, à savoir un organisme désigné par un Etat membre et chargé de dresser et de tenir à jour la liste des parties utilisatrices.
Il précise également les conditions de suspension et d'annulation d'un tel enregistrement.
Ces informations devront être conservées pendant 10 ans.

En outre, un intermédiaire pourra être mandaté par une partie utilisatrice (ex. : une entreprise voulant mettre à disposition de ses propres clients un PEIN). Cet intermédiaire fera l'interface entre la partie utilisatrice et les porteurs de PEIN mais ne pourra en aucun cas conserver le contenu des transactions.

B. Cadre juridique : Panorama des Règlements d'exécution

Différents Règlements d'application ont été publiés sur ce sujet en novembre 2024.

Le Règlement d'exécution n°2024/2982 précise les protocoles et interfaces utilisés par les solutions de PEIN en prévoyant un mécanisme fiable permettant d'authentifier les parties utilisatrices, à d'autres moyens d'identification électronique (MIE), ou à un service de confiance ;

Le Règlement d'exécution n°2024/2981 prévoit les conditions de certification des solutions par des propriétaires de schémas nationaux en se référant aux schémas européens de certification de cybersécurité établis en vertu du CyberSecurity Act. L'intégralité des solutions de PEIN doit être certifiée au niveau de garantie élevé conformément au Règlement eIDAS et au Règlement d'exécution n°2015/1502.

Le Règlement d'exécution n°2024/2979 prévoit une différenciation technique et une répartition claire des responsabilités en distinguant les différents composants et configurations des PEIN. De plus, tous les PEIN doivent être techniquement capables de recevoir et de présenter des données d'identification personnelle et des attestations électroniques d'attributs dans des scenarii transfrontaliers sans compromettre l'interopérabilité en prenant en charge des types prédéterminés de formats de données et permettre une divulgation sélective.

Le Règlement d'exécution n°2024/2977 précise que certaines fonctionnalités communes devraient être disponibles dans tous les PEIN, y compris la capacité de demander, d'obtenir, de sélectionner, de combiner, de stocker, de supprimer, de partager et de présenter en toute sécurité, sous le contrôle exclusif de l'utilisateur, les données d'identification personnelle et les attestations électroniques d'attributs.

En mai 2025, d'autres Règlements d'exécution ont été publiés :

Le Règlement d'exécution n°2025/846 établit les règles relatives au processus de mise en correspondance d'identité transfrontière des personnes physiques par des organismes du secteur public en précisant les exigences d'ordre général pour garantir une mise en correspondance sans équivoque de l'identité des personnes physiques, en rappelant les obligations des parties utilisatrices lorsque le processus de mise en correspondance d'identité est ou non concluant ainsi qu'à l'issue dudit processus.

Le Règlement d'exécution n°2025/847 traite des règles relatives aux réactions aux atteintes à la sécurité du PEIN, à savoir les modalités de constatation d'une telle atteinte et ses conséquences (suspension et rétablissement de la fourniture et de l'utilisation du PEIN, information, retrait du PEIN).

Le Règlement d'exécution n°2025/848 détermine les conditions d'enregistrement des parties utilisatrices , qu'il s'agisse de la tenue de registres nationaux de ces dernières en fonction de politiques d'enregistrement établies par les Etats membres, de la délivrance de certificats d'accès ou d'enregistrement de partie utilisatrice, des conditions de suspension et d'annulation d'un tel enregistrement ainsi que des modalités de conservation des informations.

Ainsi qu'en juillet 2025 :

Le Règlement d'exécution n°2025/1566 vient préciser l'article 24 du règlement concernant l'identification des personnes. Il traite des normes de référence applicables à la vérification de l'identité et des attributs de la personne à laquelle le certificat qualifié ou l'attestation électronique d'attributs qualifiée doit être délivré, à savoir la norme ETSI TS 119 461 V2.1.1 (2025-02): *Exigences en matière de politique et de sécurité pour les composants de services de confiance fournissant une preuve d'identité.*

Le Règlement d'exécution n°2025/1567 définit les règles applicables au nouveau prestataire de service de confiance qualifié de gestion de Dispositifs qualifiés de création de signature électronique (QSCD) à distance. Ce dernier devra respecter la norme ETSI TS 119 431-1 qui s'appliquera aux fins de l'évaluation de la conformité avec la politique du service d'application de serveur de signature électronique EU Server Signing Application Service v2, moyennant des adaptations concernant notamment les contrôles de sécurité.

Le Règlement d'exécution n°2025/1568 met à jour les procédures de coopération des Etats membres et de revue par les pairs au sein de l'Union Européenne. Ce règlement d'exécution vise à normer la procédure de revue par les pairs, ainsi qu'à assurer la traçabilité des décisions prises sur la base de ces revues, et le suivi des schémas substantiellement modifiés après leur notification. En particulier, le déclenchement de la revue par les pairs devient automatique dès lors

qu'un Etat membre procède à la notification préalable d'un schéma d'identification électronique à la Commission. L'avis final du groupe de coopération, sur la conclusion de l'examen par les pairs, fait l'objet d'une publication en ligne.

Le Règlement d'exécution n°2025/1569 définit les règles applicables au nouveau prestataire de service qualifié de fourniture d'attestations électronique d'attribut. Il précise les normes, procédures de délivrance et de révocation, ainsi que les mécanismes de notification, de catalogue des attributs et de vérification des sources authentiques pour les attestations électroniques d'attributs qualifiées délivrées. Des mécanismes de vérification des attributs doivent être mis en place par les Etats membres.

Le Règlement d'exécution n°2025/1570 revoit le processus de notification des dispositif de création de signature et de cachet (QSCD/QSealCD). Il définit les formats et procédures obligatoires de notification aux instances européennes sur les dispositifs qualifiés de création de signatures ou de cachets électroniques certifiés ou retirés afin de garantir la transparence et la traçabilité

Le Règlement d'exécution n°2025/1571 en lien avec les articles 46 bis et 46 ter établit les procédures de rapport des autorités et leur collaboration. Il impose aux autorités de supervision (des portefeuilles d'identité numérique européens et des services de confiance) de structurer leurs rapports annuels selon des formats standardisés, incluant les activités de surveillance, incidents majeurs, et coopération transfrontalière.

Le Règlement d'exécution n°2025/1572 définit les modalités de notification d'intention que doivent envoyer les prestataires de services de confiance qualifiés à l'autorité de supervision, avec les rapports d'évaluation de conformité, les plans de cessation, et structures de vérification (y compris inspections sur site)

C. Applications :

Identification : L'utilisation du PEIN facilite la **vérification d'identité puisqu'il permet d'éviter une nouvelle vérification d'identité d'une personne non-cliente de la partie utilisatrice. En effet cette identification a été réalisée lors de la délivrance du PEIN.** Elle est équivalente à une vérification d'identité réalisée lors d'un face à face physique. Cette faculté présente un intérêt indéniable pour répondre aux obligations en matière de KYC tout au long de la relation d'affaire dans le secteur bancaire.

Authentification : Le PEIN pourra aussi être utilisé pour les besoins d'authentification d'un utilisateur d'une plateforme de services. Cela pourrait en particulier être le cas pour l'accès aux sites de banques en ligne, ou pour les paiements électroniques eux-mêmes.

Signature électronique qualifiée : Le PEIN permettra d'apposer des signatures et des cachets électroniques qualifiés. Les mécanismes d'intégration et le rôle de chaque prestataire dans l'écosystème restent très ouverts. Un point d'attention est à garder à l'esprit sur la responsabilité des différents acteurs concourant à la signature électronique dans le cadre du PEIN. La signature électronique étant apportée au travers des PEIN via des Prestataires de Confiance Qualifiés, l'interopérabilité des dispositifs de signature est essentielle. A cette fin, le protocole CSC est défini comme norme minimale à l'annexe 4 du Règlement d'exécution n°2024/2979).

Fourniture d'informations complémentaires : Le Règlement d'exécution 2024/2977, précise au travers de 2 listes, les attributs que le PEIN devra porter de façon obligatoire, (nom, prénom, date de naissance, lieu de naissance, nationalité) et de façon facultative (adresse, pays de résidence, portrait, prénom, nom de naissance, sexe, l'adresse mail et le numéro de téléphone). L'adresse de courrier électronique et le numéro de téléphone sont des données pivot d'une relation dématérialisée. La certification de ces attributs facultatifs au travers du PEIN pourrait permettre une fiabilisation des échanges.

Les PEIN de personnes morales transporteront aussi des attributs, dont les listes sont fixées par le même acte d'exécution. Enfin, le PEIN contiendra d'autres attributs d'identité fournis par des prestataires d'attribut qualifiés et non qualifiés. Ces attributs pourraient permettre par exemple de répondre aux diligences supplémentaires de connaissance client dans le cadre bancaire ou tout autre besoin de consolidation d'information sur un client par une partie utilisatrice. Le Règlement 2025/1566 vient faire le lien et adapter des normes européennes pour permettre la démonstration de la qualification du service. Ceci apporte à la partie utilisatrice une meilleure garantie d'équivalence entre tous les services qualifiés disponibles sur le marché européen.

Utilisation

Afin de garantir la compatibilité entre les acteurs de l'écosystème, des protocoles sont définis par les actes d'exécution. Ils ne sont pas exhaustifs mais sont un socle minimum commun des PEIN. Ainsi les services proposés par les parties utilisatrices seront compatibles avec tous les PEIN dès que ces protocoles seront implémentés. Des protocoles avancés peuvent également être mis en place sans interopérabilité garantie. Il est en est de même sur les services proposés. Un ensemble minimum commun de services est disponible dans tous les PEIN mais des fonctionnalités additionnelles peuvent être librement ajoutées par certains fournisseurs de PEIN sans que cela n'affecte les concepts de base : minimisation des données, pas d'inférence, pas de profilage et isolation des données PEIN et hors PEIN.

Chaque unité de portefeuille dispose d'une **attestation d'authenticité** signée qui permet à la Partie Utilisatrice de s'assurer qu'elle échange avec un PEIN valide. A ce stade, la Partie Utilisatrice ne sait pas avec qui elle communique. Elle ne le sait qu'après avoir demandé des attributs qui sont transmis par l'utilisateur du PEIN. En cela, l'acte d'exécution définit des protocoles d'interopérabilité. Selon le contenu de l'attestation, une communication pour une Partie Utilisatrice est possible avec un PEIN sans savoir qui est son utilisateur si cela n'est pas nécessaire au rendu du service (cas des sites nécessitant une preuve de majorité). **Le contenu autorisé de l'attestation a été défini lors de l'enregistrement pour empêcher toute divulgation inutile**.

Effacement

Parmi les cas d'utilisation figurent, l'échange d'attributs mais aussi le suivi des données transmises, leur journalisation, leur portabilité et leur demande d'effacement. Les Parties utilisatrices devront donc implémenter les protocoles non encore définis dans ces actes d'exécution pour répondre aux demandes d'effacement des utilisateurs de PEIN. La journalisation et la portabilité permettent à un utilisateur de changer de fournisseur de PEIN sans perte des attestations déjà reçues et des informations transmises aux Parties utilisatrices.

Ce point anodin est en fait une évolution majeure. Une copie des données est conservée sur un serveur. Le chiffrement de bout en bout, même s'il n'est pas cité, apparait comme la seule solution viable pour assurer la confidentialité.

Quel intérêt d'être Partie utilisatrice ?

Le règlement crée une obligation d'utilisation des PEIN vis-à-vis de 3 catégories d'acteurs, dans certaines conditions :

- Pour l'administration : Lorsque les États membres exigent une identification et une authentification électroniques pour accéder à un service en ligne.
- Pour les acteurs du secteur privé : dès lors qu'une authentification forte est exigée par une réglementation ou contractuellement pour l'identification en ligne.
- Pour les très grandes plateformes : dès lors qu'une authentification est requise par la plateforme en ligne.

2

PARTIE 2 : Les services de confiance numérique

Quelles sont les précisions apportées par les actes d'exécution d'eIDAS v2 ?

L'adoption des actes d'exécution du règlement eIDAS a été mise en œuvre selon un calendrier suivant un lotissement. Une série d'actes d'exécution portant majoritairement sur les services de confiance a été publiée pour appel à commentaire en mai et septembre 2025. Certains sont votés à l'heure de la rédaction de cette note et d'autres sont en attente.

Pour plus de précision sur la liste des services de confiance du règlement eIDAS et les modifications par rapport à la version de 2014, nous vous invitons à consulter le guide « Comprendre le règlement eIDAS volume 3 : le règlement eIDAS 2.0 ».

Ce qu'il faut retenir de ses actes pour la partie utilisatrice est qu'ils apportent une standardisation de la mise en œuvre des services. En effet, avant 2024, les règles permettant de démontrer la fiabilité du service pouvaient différer selon les états membres. Au travers de ces actes d'exécution, la version révisée du règlement permet la définition d'un socle commun. Les normes européennes et internationales sont majoritairement reprises et parfois adaptées. Nous retrouvons donc une liste descriptive de normes ETSI, EUCC, et autres ISO décrivant les services.

Les critères de choix de ces normes et en particulier l'attention portée à la gouvernance de celles-ci représentent un acte fort de souveraineté au service d'un règlement visant lui-même à contribuer à la souveraineté des citoyens européens.

NOTES

NOTES

CONCLUSION

Les parties utilisatrices ne pourront pas imposer le recours à un PEIN.

Elles devront donc se mettre en capacité à gérer les différentes situations :

- des clients personnes physiques avec et sans PEIN.
- des clients personnes morales avec et sans PEIN

Une attention particulière devra être portée par les parties utilisatrices au rapprochement entre leurs clients connus et le PEIN.

La responsabilité des différents acteurs de l'écosystème d'identité numérique dépendra d'une analyse des obligations découlant des actes d'exécution.

Ces actes d'exécution ont pour objectif de parfaire la mise en place d'un écosystème sécurisé et souverain d'identité numérique. De nouveaux actes d'exécution seront encore publiés avant la fin de l'année.

COMITÉ DE RÉDACTION :

- **Pascal Agosti** (Cabinet Caprioli & Associés)
- **Marie-Christine Baldy** (Société Générale)
- **Sébastien Passelergue** (Kipmi Digital Trust Continuity)

5, impasse Gomboust
75001 Paris
infos@fntc-numerique.com
fntc-numerique.com

OCTOBRE 2025