HAL open science

Les acteurs de l'écosystème technique relatifs aux identités numériques - Écosystème élargi à la fourniture d'attributs, de justificatifs, de signatures électroniques et de portefeuilles d'identité numérique, working paper

Claire Levallois-Barth, Maryline Laurent

To cite this version:

Claire Levallois-Barth, Maryline Laurent. Les acteurs de l'écosystème technique relatifs aux identités numériques - Écosystème élargi à la fourniture d'attributs, de justificatifs, de signatures électroniques et de portefeuilles d'identité numérique, working paper. 2024. halshs-04430701

HAL Id: halshs-04430701

https://shs.hal.science/halshs-04430701

Preprint submitted on 1 Feb 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Les acteurs de l'écosystème technique relatifs aux identités numériques

Écosystème élargi à la fourniture d'attributs, de justificatifs, de signatures électroniques et de portefeuilles d'identité numérique

31 janvier2024

Claire Levallois-Barth, enseignante-chercheuse en droit, co-fondatrice et coordinatrice de la Chaire Valeurs et Politiques des Informations Personnelles de l'IMT, IMT Atlantique, France

Maryline Laurent, professeure en informatique, cofondatrice de la Chaire Valeurs et Politiques des Informations Personnelles de l'IMT, Samovar, Télécom SudParis, Institut polytechnique de Paris, France

Pour citer ce document : C. Levallois-Barth, M. Laurent, « Les acteurs de l'écosystème technique relatif aux identités numériques – Écosystème élargi à la fourniture d'attributs, de justificatifs, de signatures électroniques et de portefeuilles d'identité numérique », *working paper*, 39 pages, janvier 2024.

***

Les auteurs remercient les personnes ayant participé aux ateliers organisés par la Chaire Valeurs et Politiques des Informations Personnelles en 2022 et 2023. Leurs remarques ont été d'une aide précieuse dans la compréhension de l'écosystème des identités numériques, en particulier de l'écosystème en cours de définition au niveau de l'Union européenne, et la rédaction de ce document.

« La responsabilité des partenaires de la Chaire Valeurs et Politiques des Informations Personnelles ne peut en aucun cas être mise en cause en raison du contenu de la présente publication, qui n'engage que ses autrices ».

Liste des abréviations

AEA	Attestation électronique d'attributs (*Electronic Attestation of Attributes* ou EAA)
AEQA	Attestation électronique qualifiée d'attributs (*Qualified Electronic Attestation of Attributes* ou QEAA)
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ANTS	Agence Nationale des Titres Sécurisés
ARF	*Architecture and Reference Framework (*Architecture et cadre de référence*)*
Art.	Article
BMID	*Belgian Mobile ID NV/SA*
CNIe	Carte Nationale d'Identité électronique
CNIL	Commission Nationale de l'Informatique et des Libertés
CE	Communauté Européenne
CEE	Communauté Économique Européenne
Cons.	Considérant
eID	*Electronic IDentification* (Identification électronique)
eIDAS	*electronic IDentification, Authentication and trust Services*
eIDAS 1	Règlement (UE) nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur du du 23 juillet 2014
eIDAS 2	Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique
JO	Journal Officiel
JORF	Journal Officiel de la République Française
JOUE	Journal Officiel de l'Union Européenne
PEIN	Portefeuille Européen d'Identité Numérique
PID	*Person Identification Data* (Données d'identification personnelle)
SEQ	Signature électronique qualifiée (*Qualified Electronic Signature* ou QES)
SGIN	Service de Garantie de l'Identité Numérique
SPID	*Sistema Pubblico di Identità*
UE	Union Européenne

Table des matières

Table des matières

Aperçu du règlement eIDAS 1 5

Aperçu de la proposition de règlement eIDAS 2 7

1. Les principaux acteurs de l'ensemble de l'écosystème technique relatif aux identités numériques 10

1.1. Les utilisateurs (« users »)..... 10

1.2. Les fournisseurs d'identités numériques (« digital identity providers ») 11

1.3. Les autorités de délivrance de l'identité primaire 12

1.4. Les fournisseurs de services électroniques (« electronic service providers »)..... 13

1.5. Les fournisseurs de justificatifs ou de données (« credentials and data providers)..... 14

1.6. Les acteurs industriels..... 15

2. Les rôles définis spécifiquement par l'écosystème du règlement eIDAS 1 17

2.1. Les utilisateurs (« users ») au sens de eIDAS 1 17

2.2. Les entités qui délivrent les moyens d'identification électronique (« issuers of electronic identification means ») au sens de eIDAS 1 17

2.3. Les entités qui gèrent l'enregistrement des données d'identification personnelle uniques (« entities which manage the registration of the unique person identification data ») au sens de eIDAS 1 18

2.4. Les parties utilisatrices (« relying parties ») au sens de eIDAS 1 19

2.5. Les prestataires de services « considérés comme » de confiance (« trust services Providers ») au sens de eIDAS 1 20

2.5.1. Les prestataires de services de confiance qualifiés et non qualifiés (« qualified Trust Service Provider » ou QTSP et « trust Service Provider » ou TSP) 20

2.5.2. Les prestataires de services de confiance entrant dans le champ du règlement eIDAS 1 21

3. Les rôles en cours de définition dans le nouvel écosystème eIDAS 2..... 24

3.1. Les utilisateurs (« users ») au sens de eIDAS 2 25

3.2. Les entités qui délivrent les moyens d'identification électronique ou les fournisseurs de moyens d'identification électronique (« issuers or providers of electronic identification means ») au sens de eIDAS 2 26

3.3. Les entités qui gèrent l'enregistrement des données d'identification personnelle uniques (« entities which manage the registration of the unique person identification data ») au sens de eIDAS 2 26

3.4. Les entités qui délivrent les portefeuilles européens d'identité numérique et les fournisseurs de portefeuilles européens d'identité numérique (« issuers and providers of European Digital Identity Wallets ») au sens de eIDAS 2..... 27

3.5. Les parties utilisatrices (« relying parties ») au sens de eIDAS 2 28

3.6. Les prestataires de services « considérés comme » de confiance au sens de eIDAS 2 29

3.5.1. Les prestataires de services de confiance d'attestations électroniques d'attributs (« trust service providers of electronic attestations of attributes ») au sens de eIDAS 2 29
3.5.2. Les prestataires de services de confiance pour l'archivage électronique (« trust service providers for electronic attestation of attributes ») au sens de eIDAS 2 31
3.5.3. Les prestataires de services de confiance pour les registres électroniques (« trust service providers for electronic ledgers ») au sens de eIDAS 2 31
3.7. Les organismes du secteur public responsables des sources authentiques (« public sector body responsible for an authentic source ») et les organismes du secteur public désignés par un Etat membre pour délivrer des attestations électroniques d'attributs au nom d'un organisme du secteur public responsables de sources authentiques (« public sector body designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources ») au sens de eIDAS 2 32
Bibliographie..... 35
Références juridiques..... 35
Références juridiques de l'Union européenne 35
Références juridiques françaises 37
Références juridiques luxembourgeoise..... 38
Ouvrage 38
Webographie..... 38
Union européenne 38
Belgique..... 38
France..... 38
International..... 38

Le 3 juin 2021, la Commission européenne a publié une proposition de règlement relatif à une identité numérique[1] (ci-après « proposition de règlement eIDAS 2), qui actualise le règlement n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur adopté en 2014 (ci-après « règlement eIDAS 1 »[2]). Cette proposition constitue une nouvelle étape dans l'instauration d'interactions électroniques transfrontières à l'échelle européenne. Elle témoigne de la nécessité de disposer d'une identité numérique fiable afin d'accéder à des services de plus en plus dématérialisés.

La pandémie de COVID-19 a accéléré en effet le rythme de la transformation numérique et a démontré l'intérêt, pour les citoyens comme les entreprises, de l'identification à distance sécurisée afin de permettre la continuité d'activité dans une multitude de contextes, notamment avec la e-santé, le pass sanitaire, les paiements en ligne ou le vote électronique. Cette transformation témoigne, selon la Commission européenne, de la nécessité de disposer de services de vérification d'identité à distance, de justificatifs (permis de conduire, diplômes) et d'attributs. Ainsi, cette l'institution européenne constate que « l'écosystème des identités numériques se caractérise par l'émergence d'un nouvel environnement dans lequel l'accent est mis non plus sur la fourniture et l'utilisation d'identités monolithiques, mais sur la fourniture et l'utilisation d'attributs spécifiques en lien avec ces identités »[3].

Dans ce contexte, la proposition de règlement eIDAS 2 participe à la transformation numérique telle que définie au niveau politique européen[4], l'objectif étant de déployer d'ici à 2030 « à grande échelle une identité de confiance contrôlée par l'utilisateur »[5]. Plus précisément, l'ambition est de garantir à au moins 80% des personnes physiques ou morales l'accès à une identité électronique publique « hautement sécurisée et fiable » utilisable partout dans l'UE. Cet objectif passe par une mesure phare, l'instauration du « portefeuille européen d'identité numérique » (ci-après « PEIN »). Ce portefeuille, qui devra être accessible *via* des appareils mobiles de type *smartphone* ou d'autres terminaux, permettra à son utilisateur de gérer ses « données d'identification personnelle » et ses « attestations électroniques d'attributs » pour les communiquer en ligne ou hors ligne. Il lui permettra également de signer au moyen de signatures électroniques et des cachets électroniques.

Aperçu du règlement eIDAS 1

Le but du règlement eIDAS 1, tout comme celui du règlement eIDAS 2, n'est pas d'établir un système européen de gestion de l'identité numérique, par exemple en créant une carte d'identité européenne électronique ou un portefeuille fourni au niveau de l'UE, car la règlementation en matière d'identité relève de la compétence exclusive des États membres, et non de l'Union européenne. L'objectif est ici

---

[1] Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, COM(2021) 281 final du 3 juin 2021, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&qid=1628524321657&from=FR.

[2] Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juill. 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, JOUE L 257 du 28 août 2014, p. 73, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32014R0910.

[3] Exposé des motifs de la proposition de règlement eIDAS 2 – Commission européenne du 21 juin 2021, précitée.

[4] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *Façonner l'avenir numérique de l'Europe*, COM(2020)67 final du 19 fév. 2020, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52020DC0067.

[5] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *Une boussole numérique pour 2030 : l'Europe balise la décennie numérique*, COM(2021)118 final du 9 mars 2021, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52021DC0118.

d'assurer l'interopérabilité transfrontalière. Autrement dit, il s'agit de s'assurer que les citoyens et entreprises peuvent utiliser une **identification électronique fournie par un État A** pour s'authentifier de façon sécurisée dans un État B. À cette fin, le règlement eIDAS 1 comprend deux volets : l'identification électronique et les services dits de confiance pour les transactions électroniques.

Pour le premier volet portant sur l'identification électronique, le texte mobilise un concept classique du droit européen : le principe de reconnaissance mutuelle[6]. Un moyen d'identification électronique délivré par un acteur public ou privé dans un État A conformément aux conditions et procédures fixées par le règlement eIDAS 1 doit être reconnu par l'État B. Il peut alors être utilisé dans cet État B. Le moyen d'identification électronique en question figure sur une liste publiée par la Commission européenne[7] après avoir fait l'objet d'une vérification par les experts nationaux des États membres. En pratique, tous les moyens d'identification électronique, toutes les identités numériques, ne figurent pas sur la liste publiée par la Commission et donc ne relèvent pas du champ du règlement eIDAS 1, loin s'en faut. La France par exemple n'a notifié qu'un seul schéma d'identification électronique, le schéma « FranceConnect/L'identité Numérique La Poste »[8]. Ainsi, un État peut délivrer à la fois un moyen d'identification électronique conforme au règlement eIDAS et un autre moyen basé sur des obligations définies au niveau national. Par exemple, les moyens d'identification impots.gouv.fr ou de l'assurance maladie utilisés dans le cadre de FranceConnect ne figurent pas sur la liste publiée par la Commission européenne. Il en va de même pour les moyens d'identification électronique fournis, par exemple, par Google ou Apple.

Le champ du règlement eIDAS 1 est d'autant plus réduit que, même si un moyen d'identification électronique figure sur la liste publiée, deux conditions doivent être remplies pour que l'État B soit tenu d'accepter ce moyen :

- La personne doit souhaiter accéder à un service en ligne fourni par un organisme du secteur public de l'État B *et*
- Ce service public doit exiger un certain niveau de garantie (garantie substantielle ou élevée).

Ainsi, les acteurs privés fournissant des services électroniques dans un État B n'ont pas l'obligation d'accepter l'utilisation d'un moyen d'identification eIDAS. Concrètement, un loueur de voiture ou une banque n'est pas tenu d'accepter qu'un client prouve son identité en utilisant l'Identité Numérique La Poste. Il peut l'accepter volontairement, mais n'y est pas obligé.

Pour le deuxième volet sur les services dits de confiance pour les transactions électroniques, cinq catégories de services relèvent du règlement eIDAS 1 :

- Les signatures électroniques,
- Les cachets électroniques,
- L'horodatage électronique,
- L'envoi recommandé électronique et

---

[6] Art. 6 « Reconnaissance mutuelle » du règlement eIDAS 1, précité, et non modifié par la proposition de règlement eIDAS 2.

[7] Overview of pre-notified and notified eID schemes under eIDAS, https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS, consulté le 9 janvier 2023.

[8] Notification of the electronique identification scheme of France, Notices from Member States pursuant to Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, OJUE C 237/6 of 05.07.2023, https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/France?preview=/346784722/443220296/French%20Notification%20Form%20(2).pdf, consulté le 9 janvier 2023.

- L'authentification de site web.

Pour fournir des services « de confiance » eIDAS, les prestataires doivent respecter les obligations en matière de sécurité fixées par le règlement. On distingue ici deux types de prestataires : les prestataires « simples » et les prestataires « qualifiés » soumis à des exigences renforcées. Les informations concernant les prestataires de services de confiance dits qualifiés sont notifiées par les États membres auprès de la Commission européenne ; ils figurent sur une liste de « confiance »[9].

Dans le même temps, les États peuvent instaurer des dispositions nationales relatives aux cinq services de confiance eIDAS 1 ou à d'autres services. Ces services seront reconnus uniquement au niveau national. Par exemple, en France, l'Agence nationale de la sécurité des systèmes d'information (ci-après ANSSI) a publié un référentiel d'exigences pour les prestataires de vérification d'identité à distance afin qu'ils offrent un niveau de garantie donné (garantie substantielle ou élevée) en fonction des risques et des profils des attaquants. L'agence a également adopté le référentiel SecNumCloud afin d'améliorer l'offre de fournisseurs d'informatique en nuage à destination des entités publiques et privées souhaitant externaliser l'hébergement de leurs données auprès de partenaires « de confiance ». La version SecNumCloud 3.2 adoptée le 8 mars 2022[10] « sert de référence dans les travaux sur le niveau élevé » du futur schéma de certification européen relatif aux prestataires de *cloud*. En application du règlement (UE) 2019/881 sur la cybersécurité, les mécanismes d'évaluation au niveau européen sont en effet en cours d'harmonisation[11].

Aperçu de la proposition de règlement eIDAS 2

La proposition de règlement eIDAS 2 publiée en juin 2021 par la Commission européenne modifie ou complète certaines dispositions des deux volets du règlement eIDAS 1. Pour l'essentiel, elle introduit dans **le volet 1** de nouvelles obligations relatives au portefeuille européen d'identité numérique et à sa certification au titre du règlement (UE) 2019/881 sur la cybersécurité. La certification au titre du règlement (UE) 2016/679 sur les données personnelles (RGPD)[12] est possible, sans pour autant devenir obligatoire[13].

En ce qui concerne le **volet 2**, la liste des services de confiance est étendue à trois nouveaux services :

- Les attestations électroniques d'attributs,
- L'archivage électronique et
- Les registres électroniques.

---

[9] Discover the Dashboard and eIDAS trust services, http://esignature.ec.europa.eu/efda/home/#/screen/discover, consulté le 9 janvier 2023.

[10] L'ANSSI actualise le référentiel SecNumCloud, https://www.ssi.gouv.fr/actualite/lanssi-actualise-le-referentiel-secnumcloud/, consulté le 9 janvier 2024.

[11] 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, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité), JOUE L 151 du 7 juin 2019, p. 15, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R0881.

[12] Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE L 119 du 4 mai 2016, p. 1, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

[13] Art. 6c-3 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023 selon lequel « Compliance with the requirements set out in Article 6a related to the personal data processing operations may be certified pursuant to Regulation (EU) 2016/679 ».

La proposition de règlement eIDAS 2 de la Commission européenne publiée le 21 juin 2021 a depuis fait l'objet de discussions législatives. Ainsi, le **Conseil de l'Union européenne** a rendu publique le 25 novembre 2022 son orientation générale[14]. Au **Parlement européen**, le dossier a été confié à la commission de l'industrie, de la recherche et de l'énergie (commission ITRE) qui a publié son rapport le 2 mars 2023[15]. Le 16 mars 2023, la majorité des députés européens a soutenu en session plénière le mandat de négociation basé sur ce rapport. Puis le 8 novembre 2023, les colégislateurs (le Parlement européen et le Conseil de l'UE) sont parvenus à un accord provisoire[16] , dont le contenu a été publié par le Conseil le 10 novembre 2023[17] et approuvé par la commission ITRE du Parlement européen le 7 décembre 2023. **La prochaine étape annoncée pour février 2024 portera sur l'adoption du règlement,** lequel doit être approuvé par le Conseil de l'Union européenne et le Parlement européen en session plénière.

En parallèle du processus législatif, la Commission européenne a publié le même jour que sa proposition de règlement eIDAS 2, le 3 juin 2021, une **recommandation visant à mettre en place une coopération avec les États membres et le secteur privé** afin de définir une « boîte à outils » devant aboutir à une architecture technique commune, un ensemble de normes et de spécifications techniques communes et des bonnes pratiques[18]. Cette coopération vise à définir les objectifs, les acteurs, les nécessités fonctionnelles et les composantes du portefeuille européen d'identité numérique. Ainsi, une version de l'**architecture et du cadre de référence** (ci-après « ARF » pour *Architecture and Reference Framework)* a été publiée en janvier 2023[19], une version intermédiaire ayant été rendue publique en février 2022 par le groupe d'experts eIDAS[20].

Toujours en parallèle du processus législatif, la Commission européenne a chargé fin 2022 un consortium de développer un prototype de base du portefeuille européen d'identité numérique. Les Etats membres qui le souhaitent pourront s'appuyer sur les briques de base ainsi proposées. La

---

[14] Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique – orientation générale, Bruxelles, le 25 novembre 2022, 14959/22, LIMITE, TELECOM 473, COMPET 919, MI 844, DATAPROTECT 321, JAI 1497, CODEC 1774, https://data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/fr/pdf.

[15] Rapport du Parlement européen du 2 mars 2023 sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)), Commission de l'industrie, de la recherche et de l'énergie, Rapporteure: Romana Jerković, A9-0038/2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_FR.html.

[16] EU-wide digital wallet: MEPs reach deal with Council, Press Releases ITRE 08-11-2023 - https://www.europarl.europa.eu/news/en/press-room/20231106IPR09006/eu-wide-digital-wallet-meps-reach-deal-with-council.

[17] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity – Analysis of the final compromise text with a view to agreement, Brussels, 10 November 2023, https://data.consilium.europa.eu/doc/document/ST-15149-2023-INIT/en/pdf.

[18] 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, JOUE L 210 du 14 juin 2021, p. 51, https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32021H0946.

[19] The Common Union Toolbox for a coordinated approach toward a European Digital Identity Framework, The European Digital Identity Wallet Architecture and Reference Framework, January 2023, Version 1.0.0, https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework, consulté le 9 janvier 2024.

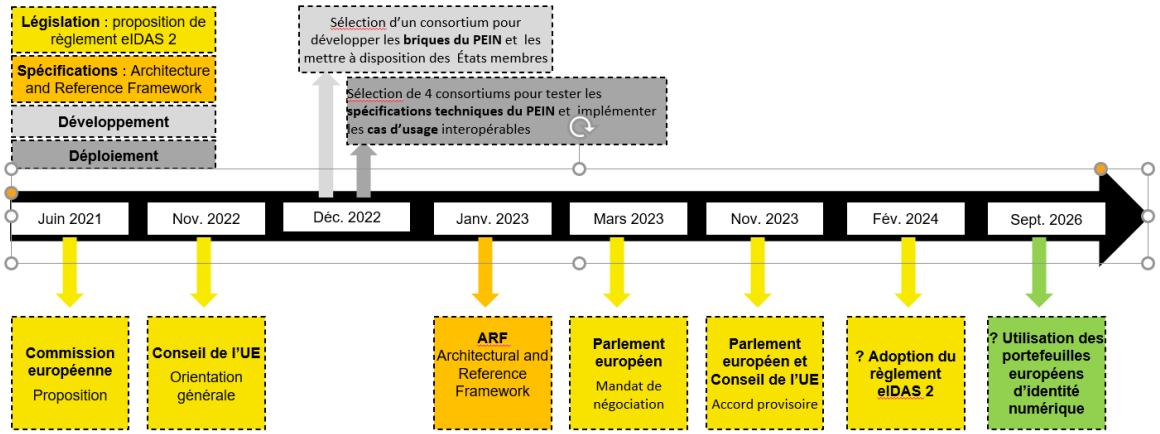
[20] European Digital Identity, Architecture and Reference Framework – Outline, 22 February 2022, https://pixl8-cloud-techuk.s3.eu-west-2.amazonaws.com/prod/public/27a2bdfe-996c-4e48-8cadff04e648c06b/eIDas-Outline-final.pdf, consulté le 9 janvier 2024.

Commission a également sélectionné **quatre projets pilotes à grande échelle** afin de tester les spécifications techniques[21]. Ces projets, lancés le 1e avril 2023, permettront de traiter des cas d'utilisation estimés « hautement prioritaires » pour le PEIN, en particulier le permis de conduire mobile, la santé en ligne, les paiements ainsi que les qualifications scolaires et professionnelles. Trois autres consortia implémenteront des cas d'usage interopérables d'identité numérique. L'objectif est de démonter la faisabilité technique et les apports du PEIN.

Ces tests à large échelle, cette définition des bases d'une architecture et d'un cadre de référence avant même la fin du débat parlementaire européen, ne sont pas sans poser un problème démocratique. Ils interrogent sur une procédure mettant sur les rails, à marche forcée[22], un projet complexe qui, en réalité, est bien plus qu'un projet technique[23].

Or, cette marche forcée ne fait que commencer. Si le règlement eIDAS 2 est adopté en février 2024 dans sa version du 10 novembre 2023, et qu'il est publié au journal officiel en mars 2024, les premiers portefeuilles européens d'identité numérique devraient au plus tard être proposés en septembre 2026. En effet, chaque Etat membre doit veiller à ce qu'un PEIN soit fourni dans un délai de 24 mois à compter de l'entrée en vigueur des actes d'exécution relatif à la mise en œuvre du portefeuille[24]. La Commission européenne doit de son côté adopter ces actes d'exécution définissant les spécifications du PEIN et les modalités de certification dans un délai de 6 mois à compter de l'entrée en vigueur du règlement[25].

Figure 1. Le cadre de révision du règlement eIDAS 2



[21] European Commission, EU Digital Identity Wallet Pilot implementation, https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation, consulté le 9 janvier 2024.

[22] Voir M. Hunyadi, en collaboration avec C. Levallois-Barth, I. Meseguer, M. Laurent, P. Waelboeck, membres de la chaire VP-IP de l'Institut Mines-Télécom, "Union européenne : pourquoi un portefeuille numérique à marche forcée ?", Le club de mediapart, 6 mai 2022, https://blogs.mediapart.fr/carta-academica/blog/060522/union-europeenne-pourquoi-un-portefeuille-numerique-marche-forcee.

[23] Voir M. Hunyadi, en collaboration avec C. Levallois-Barth, I. Meseguer, M. Laurent, P. Waelboeck, membres de la chaire VP-IP de l'Institut Mines-Télécom, « Le portefeuille européen d'identité numérique : objet technique ou projet de société ? », Acteurs publics, 24 novembre 2023, https://acteurspublics.fr/articles/le-portefeuille-europeen-didentite-numerique-objet-technique-ou-projet-de-societe.

[24] Art. 6a-1 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

[25] Art. 6a-11 et art. 6c(4) de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

Dans ce contexte en pleine effervescence, il est nécessaire de mettre à jour la typologie des acteurs et des rôles établis dans l'ouvrage *Identités numériques* publié par la Chaire Valeurs et Politiques des Informations Personnelles en mars 2016[26]. Cette actualisation est loin d'être aisée car elle se situe dans un contexte au périmètre eIDAS 2 en cours de définition et recourant à un vocabulaire essentiellement juridique (partie 3). Ce périmètre en extension modifie et élargit le champ d'application du règlement « eIDAS 1 (partie 2). Il s'insère dans un écosystème général plus vaste dans lequel les acteurs et les rôles sont principalement définis par le marché (partie 1).

1. Les principaux acteurs de l'ensemble de l'écosystème technique relatif aux identités numériques

L'écosystème technique des identités numériques à la fois français, européen et mondial comprend à la base le trinôme « utilisateurs (1.1), fournisseurs de services électroniques (1.4), tiers de confiance » tel que décrit en 2016 dans notre ouvrage *Identités numériques*[27]. Cet écosystème s'est depuis largement complexifié, notamment au niveau des tiers de confiance, qu'il s'agisse des fournisseurs d'identité numérique (1.2), des autorités de délivrance de l'identité primaire (1.3), ou des fournisseurs d'attributs (1.5.). Les acteurs industriels ont, de leur côté, développer leur offre (1.6.).

Notre objectif est ici d'exposer l'agencement de base de cet écosystème et de comprendre le rôle joué par ces six catégories d'acteurs, sans prétendre à l'exhaustivité.

1.1. Les utilisateurs (« users »)

Nous définissons l'utilisateur comme la personne physique ou morale, ou la personne physique représentant une personne physique ou morale, détenteur de l'identité numérique. L'utilisateur est représenté par un ensemble de données permettant de l'identifier ou de l'authentifier en ligne ou hors ligne, de gérer des attributs et des justificatifs rattachés à son identité numérique.

Un utilisateur s'identifie lorsqu'il décline son identité (par exemple nom, prénom, pseudonyme, adresse de courrier électronique).

Un utilisateur s'authentifie lorsqu'il fournit des données prouvant son identité (par exemple mot de passe envoyé par SMS)[28].

Il s'agit donc ici d'un **individu** qui dispose d'un support numérique (*smartphone*, ordinateur, tablette …) afin de gérer ses données d'identification (nom de famille, prénom, date de naissance, lieu de naissance, adresse actuelle, sexe, adresse de courrier électronique ...), ses attributs (couleur des yeux, statut vaccinal, photographies de l'utilisateur, données biométriques …), ses justificatifs (permis de conduire, diplôme, attestation de vaccination …) rattachés à son identité numérique.

---

[26] CHAIRE VALEURS ET POLITIQUES DES INFORMATION PERSONNELLES, *Identités numériques*, coordonné par Claire LEVALLOIS-BARTH, mars 2016, https://cvpip.wp.imt.fr/2016/03/19/2016-03-identites-numeriques/.

[27] Chaire Valeurs et Politiques des Information Personnelles, *Identités numériques*, p. 46, précité.

[28] CNIL, Sécurité : authentifier les utilisateurs, https://www.cnil.fr/fr/securite-authentifier-les-utilisateurs, consulté le 9 janvier 2024.

Il peut également s'agir d'une **personne morale**, c'est-à-dire d'un groupement doté de la personnalité juridique[29], qui par l'intermédiaire d'une personne physique, s'identifie ou s'authentifie en ligne ou hors ligne, fournit des attributs (immatriculation au Registre du Commerce et des Sociétés) ou des justificatifs (déclaration d'imposition) rattachés à son identité numérique.

1.2. Les fournisseurs d'identités numériques (« digital identity providers »)

Le fournisseur d'identité numérique est un organisme public ou privé qui fournit à l'utilisateur une identité numérique. Cette identité numérique est soit dérivée d'une identité émise par l'autorité de délivrance de l'identité primaire, soit créée *ex nihilo*. Dans sa fonction minimale, le fournisseur d'identité numérique procède à l'enrôlement de l'utilisateur ; il gère les données d'identification (par exemple nom ou pseudonyme de l'utilisateur associé à une adresse de courrier électronique) et les données d'authentification (par exemple un mot de passe renforcé par un code envoyé par SMS) pour une authentification en ligne.

Dans certains cas, le fournisseur d'identité numérique dérive l'identité numérique d'une identité émise par l'autorité de délivrance de l'identité primaire. Par exemple, le fournisseur d'identité numérique

- Du futur **Service de Garantie de l'Identité Numérique** (SGIN) est le ministère de l'intérieur, lequel se base sur la carte nationale d'identité française[30] ;
- De **L'identité Numérique La Poste** est La poste, société anonyme appartenant à l'État français, laquelle se base sur la carte nationale d'identité française, le passeport français ou le titre de séjour d'une durée supérieure ou égale à 5 ans.

Le consortium Belge Belgian Mobile ID NV/SA (BMID), constitué de quatre institutions financières et de trois opérateurs de réseaux mobiles belges, fournit l'identité numérique **itsme**. Un compte itsme peut être créé soit à partir de la carte d'identité électronique (eID) belge[31] et d'un lecteur de carte eID spécifique[32], soit, si l'utilisateur est client de l'une des banques participant au programme, d'une carte bancaire à puce et d'un lecteur de cette carte[33].

Le fournisseur d'identité numérique peut également créer une identité numérique *ex nihilo*. Afin que l'utilisateur puisse s'authentifier auprès de différents services, **Facebook** ou **Google**, par exemple,

---

[29] Généralement une personne morale se compose d'un groupe de personnes physiques réunies pour accomplir quelque chose en commun. Ce groupe peut aussi réunir des personnes physiques et des personnes morales. Il peut aussi n'être constitué que d'un seul élément.

[30] Décret n° 2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », JORF du 27 avril 2022, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045667825. Voir également CNIL, délibération n° 2021-151 du 9 décembre 2021 portant avis sur un projet de décret en Conseil d'État autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique.

[31] Précisément, la carte d'identité électronique pour ressortissants belges et la carte d'identité électronique pour étrangers.

[32] Activez un compte itsme® avec votre eID, https://www.itsme-id.com/fr-BE/get-started/eid, consulté le 9 janvier 2024.

[33] Comment créer votre compte itsme® avec votre carte de banque et son lecteur de carte, https://www.itsme-id.com/fr-BE/get-started/bank#video, consulté le 9 janvier 2024.

fournissent un compte auquel est associé un nom d'utilisateur créé à partir de données déclaratives[34]. Le niveau de garantie est donc des plus faibles au moment de la création de l'identité numérique, même si **Facebook** exige que l'utilisateur donne à son compte le même nom que celui qu'il utilise au quotidien[35]. De son côté, **Google** se réserve la possibilité de demander à l'utilisateur une photocopie de sa pièce d'identité ou de sa carte bancaire afin de vérifier qu'il a bien l'âge minimal requis pour utiliser certains services et fonctionnalités (notamment les vidéos YouTube non accessibles aux enfants). Le niveau de garantie obtenu reste cependant faible même si Google propose à l'utilisateur de « protéger son compte », ce qui revient à mieux l'identifier, en fournissant un numéro de téléphone ou une adresse e-mail de récupération[36]. Une fois le compte Facebook ou Google créé, l'individu va pouvoir s'identifier sur les sites web affichant le bouton « Facebook Connect » ou « *Sign-in with* Google ».

Apple permet à l'utilisateur de générer un **identifiant Apple**. Cet identifiant sert ensuite à créer un compte et à se connecter sur les applications ou sites web affichant le bouton « Se connecter avec Apple » (« *Sign in with Apple* »)[37]. Aux États-Unis, une expérimentation porte sur l'intégration d'une carte d'identité ou d'un permis de conduite dans l'*Apple wallet*. Ce « portefeuille », qui offre ainsi un niveau de garantie de l'identification supérieur, peut être utilisé lors des contrôles de sécurité effectués par la *Transportation Security Administration* (TSA) dans certains aéroports américains[38]. Ici, Apple se base sur une identité non pas déclarative mais émise et garantie par l'autorité de délivrance d'une identité primaire. La multinationale travaille également sur des solutions permettant aux utilisateurs de déverrouiller leur maison, leur bureau ou leur chambre d'hôtel grâce aux clés stockées dans le portefeuille.

1.3. Les autorités de délivrance de l'identité primaire

L'autorité de délivrance de l'identité primaire est un organisme public qui garantit la fiabilité du lien initial entre la personne physique ou morale et l'identité électronique ou numérique qui lui est attribuée sur un support physique et/ou logiciel. Cette autorité émet une identité primaire ou un titre d'identité (carte nationale d'identité, passeport, titre de séjour). Ces identités primaires peuvent comprendre différentes données d'identification (données d'état civil, données dites « pivot »).

---

[34] Nom, prénom, numéro de mobile ou e-mail, date de naissance, genre renseignés par l'utilisateur.

[35] Conditions de service de Facebook, https://www.facebook.com/legal/terms/update, consulté le 9 janvier 2024. Le réseau social précise : « Nous pouvons être amenés à changer le nom d'utilisateur associé à votre compte dans certaines circonstances (par exemple, lorsqu'une autre personne revendique le nom d'utilisateur et que le nom d'utilisateur semble sans rapport avec le nom que vous utilisez au quotidien ».

[36] Créer un compte Google, https://support.google.com/accounts/answer/27441?hl=fr, consulté le 9 janvier 2024.

[37] Qu'est-ce que le service « Se connecter avec Apple » ?, https://support.apple.com/fr-fr/HT210318, consulté le 9 janvier 2024. L'option « Masquer mon adresse e-mail » permet de générer une adresse électronique aléatoire unique dont les messages sont transférés à l'adresse e-mail personnelle de l'utilisateur. Apple se positionne en tiers de confiance en permettant à l'utilisateur de recevoir des messages sans avoir à dévoiler son adresse e-mail personnelle. Anthony Nelzin-Santos, Sign in with Apple : Apple devient fournisseur d'identité privée, 11 juin 2019, https://www.macg.co/macos/2019/06/sign-apple-apple-devient-fournisseur-didentite-privee-106479, consulté le 9 janvier 2024.

[38] Apple teams up with TSA to enable digital identification at security checkpoints, June 2021, https://www.futuretravelexperience.com/2021/06/apple-teams-up-with-tsa-to-enable-digital-identification-at-security-checkpoints/, consulté le 9 janvier 2024.

À titre d'exemple, l'autorité de délivrance de la carte nationale d'identité électronique (CNIe) est l'État français, plus spécifiquement l'Agence nationale des titres sécurisés (ANTS), placée sous la tutelle du ministère de l'intérieur. La délivrance en mairie, qui intervient après la validation du dossier au niveau de la préfecture par le centre d'expertise et de ressources des titres, établit ainsi le lien initial entre l'identité physique de la personne et son identité numérique[39].

Au Luxembourg, l'État délivre la CNIe par l'intermédiaire des administrations communales[40]. Un lecteur spécifique de carte sans contact connecté à un ordinateur permet à l'utilisateur de s'authentifier pour notamment effectuer des démarches administratives *via* l'application MyGuichet.lu ou des opérations de *eBanking*[41]. Le dispositif permet également de signer électroniquement.

Le choix de l'autorité de délivrance de l'identité primaire est conditionné par le niveau de garantie et de sécurité du service requis par le service électronique requérant l'authentification de l'utilisateur. C'est parce que l'utilisateur a besoin d'un service électronique pour payer ses impôts qu'il utilise une identité numérique fournie par une autorité de délivrance de référence correspondant au niveau de garantie attendu.

1.4. Les fournisseurs de services électroniques (« electronic service providers »)

Le fournisseur de services électroniques fournit un service électronique public ou privé qui permet à l'utilisateur d'accéder à des ressources ou d'accomplir des actions en ligne ou hors ligne. Pour cela, le fournisseur de services peut identifier et/ou authentifier l'utilisateur, c'est-à-dire s'assurer qu'il s'agit de la bonne personne en recourant, en général, à un tiers de confiance.

Les fournisseurs de services électroniques proposent un nombre croissant de services électroniques.

Les **services électroniques publics** peuvent, par exemple, être fournis par l'assurance maladie, Pôle emploi, la CNIL afin de suivre l'avancement du traitement d'une demande. Ils offrent une possibilité d'actions variées, notamment accéder aux documents administratifs (certificat de naissance notamment), déclarer et payer ses impôts, procéder à une démarche relative au permis de conduire, accéder à son dossier médical partagé, bénéficier d'offres de soins. Impots.gouv.fr est à la fois un fournisseur de service électronique et un fournisseur d'identité numérique. Il peut s'appuyer sur l'identification/authentification électronique de l'usager qu'il réalise lui-même ou qui est réalisée par un autre service de l'État *via* FranceConnect[42].

Les **services électroniques privés** peuvent notamment être fournis par des opérateurs de télécommunications, des plateformes d'achat en ligne, des banques, des plateformes de jeux, des

---

[39] Assemblée nationale, rapport d'information n° 3190, *Pour une identité numérique régalienne citoyenne*, mission d'information commune M. KARAMANLI, C. HENNION et J-M. MIS, juillet 2020, p. 18, https://www.assemblee-nationale.fr/dyn/15/rapports/micnum/l15b3190_rapport-information#.

[40] Loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques, JO du Grand-Duché du Luxembourg, https://legilux.public.lu/eli/etat/leg/loi/2013/06/19/n3/jo.

[41] Utiliser la carte d'identité électronique avec un lecteur de carte, https://gouvernement.lu/fr/dossiers.gouv_ctie%2Bfr%2Bdossiers%2BeID%2Blecteur-carte.html, consulté le 9 janvier 2024.

[42] FranceConnect repose sur une fédération d'identités, qui permet de mettre en œuvre un mécanisme de liaison entre les identités d'un utilisateur dans différents systèmes d'information.

plateformes collaboratives (Blablacar), des sites pornographiques, des assureurs. L'utilisateur peut ainsi consulter ses comptes bancaires et virements, souscrire à une assurance ou un abonnement mobile, effectuer des paiements en ligne, accéder à une place de marché (*marketplace)* ou à des plateformes de jeux en ligne.

Certains services sont accessibles à la fois en ligne et hors ligne. « On observe en effet une utilisation croissante de l'identité numérique hors ligne, notamment dans le secteur de la santé où les services peuvent être fournis *via* une interaction directe (par exemple, la présentation de son statut vaccinal à l'entrée d'un hôpital) »[43].

Dans ce contexte, le fournisseur de services électroniques identifie ou authentifie l'utilisateur en se basant notamment sur :

- Une identité numérique accessible à partir d'un support physique (carte nationale d'identité électronique, passeport électronique, titre de séjour électronique) délivré par une autorité de délivrance de l'identité primaire,
- Une identité numérique délivrée par un fournisseur d'identité numérique (améli.fr, impots.gouv.fr fournis par des organismes publics, Mobile Connect et moi ou YRIS fournis par des organismes privés),
- Un moyen d'identification électronique notifié auprès de la Commission européenne conformément aux dispositions du règlement eIDAS 1 (par exemple, L'Identité Numérique La Poste).

En fonction du service électronique, le fournisseur de service électronique peut exiger que l'utilisateur s'authentifie avec un certain niveau de garantie ou lui transmette une attestation électronique d'attributs dont le niveau d'assurance spécifique dépend également du service fourni. Dans certaines situations, le fournisseur de services électroniques n'a pas besoin d'identifier et/ou d'authentifier l'utilisateur en passant par un fournisseur d'identité numérique mais simplement d'accéder à certains attributs (« plus de 18 ans », « détenteur du permis de conduire »). Dans cette hypothèse, il fait appel à un fournisseur de justificatifs ou de données.

1.5. Les fournisseurs de justificatifs ou de données (« credentials and data providers)

Le fournisseur de justificatifs ou de données collecte, crée et délivre des attributs caractérisant une personne et/ou des attestations d'attributs. Il interagit avec le fournisseur de service électronique et le fournisseur d'identité numérique à la demande de l'utilisateur.

Le fournisseur de justificatifs ou de données peut soit collecter directement des attributs, soit les créer à partir de justificatifs tels qu'un diplôme, un permis de conduire, un certificat d'état civil, une facture d'électricité. En 2016, nous avons précisé qu'il s'agissait d'un acteur facultatif[44]. La proposition de règlement eIDAS 2 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique en fait un acteur incontournable.

[43] Exposé des motifs de la proposition de règlement eIDAS 2 – Commission européenne du 3 juin 2021, précitée.
[44] Chaire Valeurs et Politiques des Information Personnelles, *Identités numériques*, p. 46, précité.

L'expérimentation **MonFranceConnect** met à disposition des usagers un ensemble de données personnelles les concernant détenues par les administrations françaises[45]. Après une authentification avec FranceConnect, le téléservice propose à chaque usager d'afficher une sélection de données personnelles et de générer à partir de ces informations des justificatifs susceptibles de lui être demandés lors de l'accomplissement de ses démarches (par exemple un justificatif d'adresse postale, de droits à l'assurance maladie, de revenus). Il peut ensuite télécharger ses justificatifs et les transmettre aux personnes et organismes de son choix. Un QR code apposé sur le justificatif permet de vérifier la véracité des informations.

Le service en ligne « **diplome.gouv.fr** » délivre des attestations numériques certifiées de diplômes[46]. Il permet à des tiers de vérifier l'authenticité d'un diplôme grâce à une clé de contrôle à huit caractères fournie par le diplômé. Pour se connecter au service, le diplômé peut créer un compte ou s'identifier *via* FranceConnect. Il accède alors à son tableau de bord d'attestations de diplômes, qu'il peut conserver dans son coffre-fort numérique Digiposte.

1.6. Les acteurs industriels

Nous distinguons ici deux types d'acteurs industriels.

Les **acteurs industriels du marché des identités** offrent des solutions matérielles et/ou logicielles qui peuvent prendre la forme de briques technologiques, comme une carte à puce, un élément sécurisé[47] au sein d'un *smartphone*, une puce NFC[48] intégrée au *smartphone* permettant de lire les données enregistrées dans la carte à puce intégrée à une carte d'identité, ou bien de communiquer hors ligne des éléments d'identités virtuelles avec des systèmes de vérification d'identités. Ces acteurs répondent au besoin direct des autorités de délivrance de l'identité primaire, des fournisseurs d'identités numériques, des fournisseurs de services et des fournisseurs de justificatifs ou de données.

Les **acteurs industriels fournissant l'infrastructure technique des identités sous-jacente** mettent en œuvre, opèrent et assurent la maintenance de l'ensemble des moyens informatiques déployés. Leur objectif est de garantir la disponibilité et la fiabilité de l'infrastructure sous-jacente à l'ensemble des acteurs de l'écosystème. Figurent dans cette catégorie les prestataires de services de *cloud* ou les prestataires mettant en œuvre une *blockchain*, ainsi que les concepteurs et administrateurs des interfaces de programmation ou *Application Programming Interface* (API)

N'oublions pas bien sur les fabricants de *smartphones* qui distribuent à leurs utilisateurs, *via* leur banque d'applications mobiles, des applications gestionnaires de portefeuilles d'identités numériques.

---

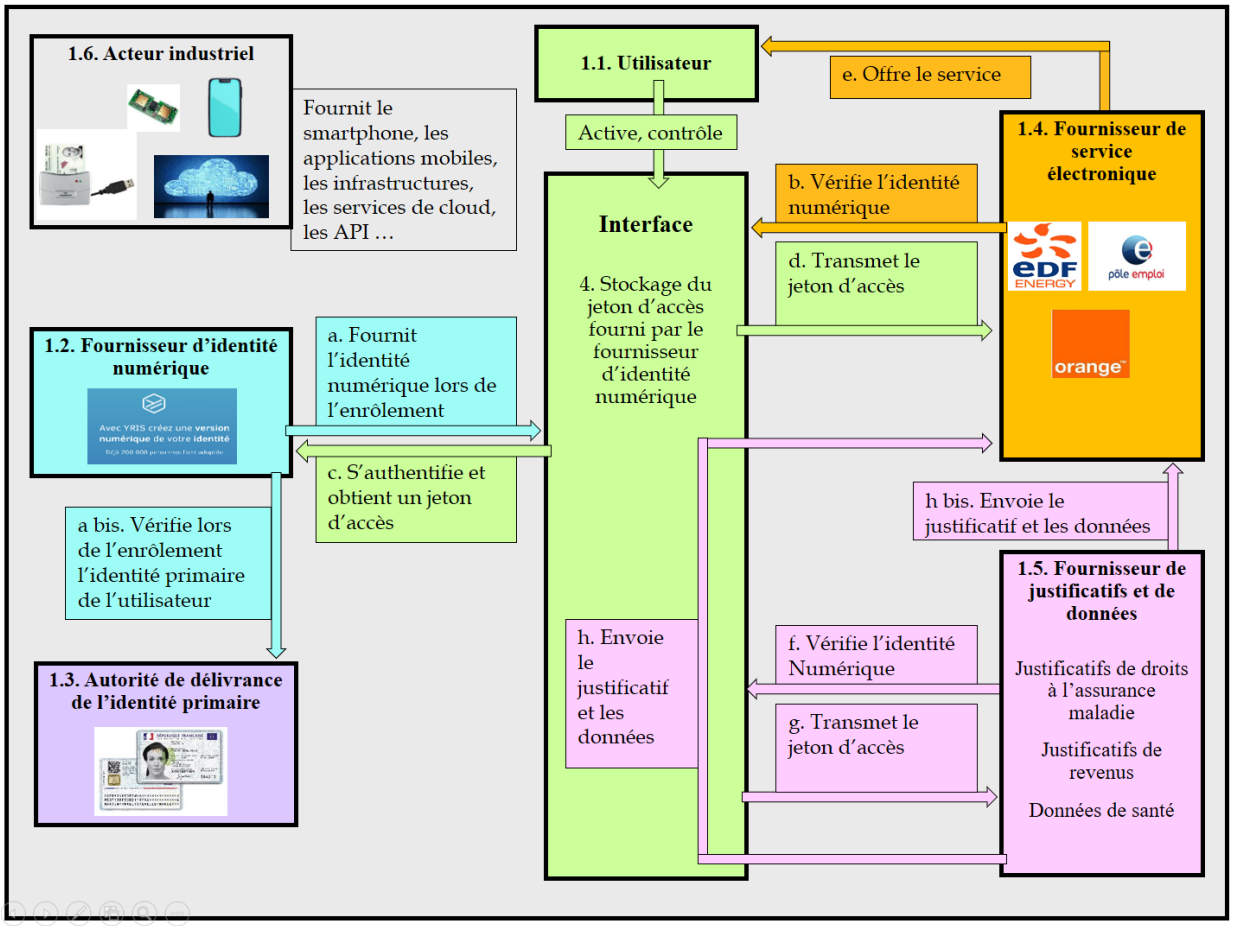
[45] Décret n° 2021-1538 du 29 novembre 2021 relatif à l'expérimentation du téléservice dénommé « Mon FranceConnect » (MFC), JORF du 30 nov. 2021, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044385101.

[46] Diplome.gouv.fr : attestations de diplômes en ligne, https://www.education.gouv.fr/diplomegouvfr-attestations-de-diplomes-en-ligne-1745, consulté le 9 janvier 2024.

[47] Un *secure element* est un composant isolé dans l'appareil de l'utilisateur qui fait office de coffre-fort afin de stocker de façon sécurisée des données sensibles, telles que les informations d'identification de l'utilisateur.

[48] NFC pour *Near Field Communication* ou Communication en champ proche d'une dizaine de centimètres.

Figure 2. Les principaux acteurs de l'ensemble de l'écosystème technique relatif aux identités numériques : un exemple d'interactions



2. Les rôles définis spécifiquement par l'écosystème du règlement eIDAS 1

Afin d'assurer l'identification transfrontalières des personnes physiques et morales *via* un mécanisme de reconnaissance mutuelle, le règlement n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur adopté en 2014 (règlement eIDAS 1) et ses actes d'exécution établissent un socle commun pour les interactions électroniques de « confiance ». Ce socle comprend les utilisateurs (2.1.), les entités qui délivrent les moyens d'identification électronique (2.2.), les entités qui gèrent l'enregistrement des données d'identification personnelle uniques (2.3.), les parties utilisatrices (2.4.) et les prestataires de services « considérés comme » de confiance (2.5.).

2.1. Les utilisateurs (« users ») au sens de eIDAS 1

Le règlement eIDAS 1 ne définit pas l'utilisateur. L'utilisateur au sens du règlement eIDAS 1 recourt à des moyens d'identification électronique notifiés par un État membre de l'UE et/ou à des services dits de confiance tels que réglementés par le règlement eIDAS 1.

L'utilisateur au sens de eIDAS 1 est un sous-ensemble des utilisateurs tels que nous les avons décrits au point 1.1.

2.2. Les entités qui délivrent les moyens d'identification électronique (« issuers of electronic identification means ») au sens de eIDAS 1

Le terme « entités qui délivrent les moyens d'identification électronique » est utilisé une fois par le règlement eIDAS 1[49], sans être défini. Ce terme est traduit par « issuers of electronic identication means » dans la version anglaise du règlement[50].

Le règlement eIDAS 1 définit l'« **identification électronique** » 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 »[51] et le « **moyen d'identification électronique** » comme « un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne »[52].

L'entité qui délivre un moyen d'identification électronique au titre de eIDAS 1 est donc un fournisseur d'identité numérique tel que défini au point 1.4. de ce document. Elle peut fournir un logiciel ou une application mobile aux utilisateurs qui souhaitent s'authentifier auprès des « parties utilisatrices ».

Le moyen d'identification électronique peut être un élément matériel (carte d'identité électronique ou passeport électronique muni d'une puce) ou un élément immatériel (application sur mobile). Il peut répondre à trois niveaux de garantie, le cadre eIDAS 1 distinguant :

---

[49] Art. 9-1, point a) du règlement eIDAS 1, précité.
[50] La proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023 utilise elle aussi dans son article 12b. le terme de « issuers of notified electronic identication means », expression qui peut aussi être traduite par « émetteurs de moyens d'identification électronique notifiés ».
[51] Art. 3-1 du règlement eIDAS 1, précité.
[52] Art. 3-2 du règlement eIDAS 1, précité.

- Le niveau de **garantie « faible »** : l'objectif est de réduire le risque d'utilisation abusive de l'identité revendiquée, par exemple en se basant sur un seul facteur d'authentification comme un mot de passe ;
- Le niveau de **garantie « substantiel »** : l'objectif est de réduire substantiellement le risque d'utilisation abusive d'identité, en ajoutant un second facteur d'authentification au mot de passe préalablement saisi, par exemple un code temporaire envoyé par SMS ;
- Le niveau de **garantie « élevé »** : l'objectif est d'empêcher l'utilisation abusive de l'identité, en complétant les exigences du niveau substantiel, notamment par des moyens de protection « contre les attaquants à potentiel d'attaque élevé ».[53]. La France utilise le titre d'identité électronique pour valider une authentification de garantie élevée.

Le règlement eIDAS 1 précise également que « les moyens d'identification électronique relevant du schéma d'identification électronique » sont délivrés :

i) Par l'État membre qui notifie ce schéma d'identification électronique auprès de la Commission européen (ci-après « État membre notifiant »),
ii) Dans le cadre d'un mandat de l'État membre notifiant, ou
iii) Indépendamment de l'État membre notifiant et sont reconnus par cet État membre »[54].

Les modalités du mandat ou de la reconnaissance du moyen d'identification sont déterminés par chaque État membre. Ainsi, **l'Italie** a notifié un élément matériel de garantie élevée, la carte d'identité électronique délivrée par les municipalités au titre du point i). Elle a également notifié un élément immatériel, le *Sistema Pubblico di Identità Digitale* (SPID) de garantie faible, substantielle ou élevée en fonction des vérifications effectuées, au titre du point ii). Au titre du point iii), en **France**, l'émetteur du moyen d'identification électronique notifié L'Identité Numérique La Poste, de garantie substantielle, est La Poste et, en **Belgique**, l'émetteur de l'application mobile Itsme de garantie élevée est la BMID.

2.3. Les entités qui gèrent l'enregistrement des données d'identification personnelle uniques (« entities which manage the registration of the unique person identification data ») au sens de eIDAS 1

Selon le règlement eIDAS 1, l'État membre qui délivre le moyen d'identification électronique doit notifier « des informations sur **l'entité ou les entités qui gèrent l'enregistrement des données d'identification personnelle uniques** »[55]. Le texte ne définit pas cet acteur.

Afin d'assurer l'interopérabilité à l'échelle européenne, le règlement eIDAS 1 précise que des données d'identification personnelle (*Person Identification Data* – PID) doivent être attribuées à la personne au moment de la délivrance d'un moyen d'identification électronique par l'État membre[56], c'est-à-dire lors de l'enrôlement. Ces **PID** sont définies comme « un ensemble de données permettant d'établir

[53] Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, JOUE L 235 du 9 sept. 2015, p. 7, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32015R1502.
[54] Art. 7-a du règlement eIDAS 1, précité.
[55] Art. 9-1, point d) du règlement eIDAS 1, précité.
[56] Art. 7-d du règlement eIDAS 1, précité.

l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale »[57].

Le règlement eIDAS 1 définit un cadre d'interopérabilité pour assurer la fourniture des systèmes d'identification électronique et des services de confiance à l'échelle transfrontalière. Ce cadre se compose notamment d'une référence à un ensemble minimal de données d'identification personnelle représentant « de manière univoque une personne physique ou morale, qui est disponible dans les schémas d'identification électronique »[58]. Cet ensemble minimal de données comprend pour une personne physique :

- **Quatre attributs obligatoires** : 1. nom(s) de famille actuel(s) ; 2. prénom(s) actuel(s) ; 3. date de naissance ; 4. un identifiant unique créé par l'État membre expéditeur … qui soit aussi persistant que possible dans le temps, et
- **Un ou plusieurs attributs supplémentaires** : 1. prénom(s) et nom(s) de famille à la naissance ; 2. lieu de naissance ; 3. adresse actuelle ; 4. sexe[59].

Pour Istme, la BMID est l'entité qui gère l'enregistrement des données d'identification personnelle *via* des registres d'identité et deux processus d'enrôlement possibles :

- Le premier processus concerne les clients d'une des institutions financières participant à itsme : chaque institution gère un Registres d'identité itsme selon son processus de « *Know Your Customer* » (KYC), lui-même basé sur la carte d'identité électronique pour les ressortissants belges (eCard Citoyen Belge) ou pour les étrangers (eCard Étranger).
- Le second processus concerne les personnes qui ne sont pas clientes d'une des institutions financières et qui donc ne figurent pas dans un registre KYC. Leur inscription à Itsme se base directement sur l'eCard Citoyen Belge ou l'eCard Étranger[60].

2.4. Les parties utilisatrices (« relying parties ») au sens de eIDAS 1

Le règlement eIDAS 1 définit la partie utilisatrice comme « une personne physique ou morale qui se fie à une identification électronique ou à un service de confiance »[61]. Les États membres peuvent agir en qualité de parties utilisatrices. Il peut s'agir également d'une personne physique, par exemple le salarié d'une agence de location de voitures ou un pharmacien.

Une partie utilisatrice peut être un fournisseur de service électronique public ou privé tel que défini au point 1.2. de ce document.

---

[57] Art. 3-3 du règlement eIDAS 1, précité.
[58] Art. 12, §4, point d) du règlement eIDAS 1, précité.
[59] Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, JOUE L 235 du 9.9.2015, p. 1, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32015R1501
[60] Itsme Notification form for electronic identity scheme under article 9(5) of regulation (EU) n° 910/2014, https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/87064906/1.1.1%20NOTIFICATION%20FORM_Belgian%20FAS%20itsme-Signed.pdf?version=1&modificationDate=1571043055346&api=v2, consulté le 9 janvier 2024.
[61] Art. 3-6 du règlement eIDAS 1, précité.

2.5. Les prestataires de services « considérés comme » de confiance (« trust services Providers ») au sens de eIDAS 1

Le règlement eIDAS 1 distingue le prestataire de services de confiance sans statut spécifique que nous appelons statut « non qualifié » et le prestataire de services de confiance « qualifié » (2.5.1.). Ces prestataires peuvent fournir cinq catégories de services règlementés par le règlement eIDAS 1 (2.5.2.).

2.5.1. Les prestataires de services de confiance qualifiés et non qualifiés (« qualified Trust Service Provider » ou QTSP et « trust Service Provider » ou TSP)

Le règlement eIDAS 1 définit le « **prestataire de services de confiance** » comme « 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 »[62]. Ainsi, certains acteurs sont considérés « de confiance » dans la mesure où ils sont tenus de respecter les obligations fixées par le règlement, en particulier des exigences de sécurité, qu'ils soient qualifiés ou non[63].

Le règlement eIDAS 1 définit le « **prestataire de services de confiance qualifié** » comme « 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 »[64].

La **notion de statut « qualifié »** indique ici qu'un acteur (le prestataire) ou un objet (par exemple, une signature électronique, un certificat électronique) respecte des exigences et obligations de sécurité renforcée. Ces prestataires sont soumis à des obligations supplémentaires. Inscrits sur une « liste de confiance », ils doivent notamment être audités au moins tous les vingt-quatre mois[65] par un organisme d'évaluation de la conformité dont le statut et les conditions d'accréditation sont définis par le règlement (CE) 765/2008[66].

Les prestataires de services de confiance « qualifiés » sont supervisés par l'organe de contrôle de l'État membre dont ils dépendent, en France l'ANSSI[67], qui leur octroie leur statut « qualifié »[68]. Ils offrent des services de confiance qualifiés.

---

[62] Art. 3-19 du règlement eIDAS 1, précité.
[63] Art. 19 du règlement eIDAS 1, précité, définissant les exigences de sécurité applicables aux prestataires de services de confiance.
[64] Art. 3-20 du règlement eIDAS 1, précité.
[65] Art. 20-1 du règlement eIDAS 1, précité.
[66] Art. 3-18 du règlement eIDAS 1, précité. Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, JOUE L 218 du 13.8.2008, p. 30, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:fr:PDF.
[67] Pour un aperçu des organes de contrôle des différents États membres de l'UE, voir https://eidas.ec.europa.eu/efda/notification-tool/#/screen/browse/list/SUPERVISORY_BODIES, consulté le 9 janvier 2024.
[68] Art. 3-20 du règlement eIDAS 1, précité.

2.5.2. Les prestataires de services de confiance entrant dans le champ du règlement eIDAS 1

En 2014, cinq services électroniques de confiance « normalement fournis contre rémunération » sont inclus dans le champ du règlement eIDAS 1[69].

2.5.2.1. Les prestataires de services de signatures électroniques et de certificats relatifs à ce service au sens de eIDAS 1

En ce qui concerne les prestataires de services de signatures électroniques et des certificats relatifs à ce service, le règlement eIDAS 1 vise la création, la vérification, la validation et la conservation de ces signatures et certificats[70].

Il définit la « **signature électronique** » comme « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer »[71]. Celle-ci permet un processus de signature sans papier.

Un certificat qualifié de signature électronique est délivré par un prestataire de services de confiance qualifié[72]. Une signature électronique qualifiée bénéficie d'un effet juridique équivalent à celui d'une signature manuscrite et présente un niveau élevé de sécurité[73].

2.5.2.2. Les prestataires de services de cachets électroniques et de certificats relatifs à ce service au sens de eIDAS 1

Le règlement eIDAS 1 vise la création, la vérification, la validation et la conservation des cachets électroniques et des certificats relatifs à ce service[74].

Le « **cachet électronique** » est défini comme « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières »[75]. Il permet de prouver qu'un document électronique a été délivré par une personne morale en garantissant l'origine et l'intégrité du document. Dans le cadre du règlement eIDAS 1, les signatures électroniques sont donc émises par un individu, les cachets électroniques par les entreprises ou des organismes publics.

Un certificat qualifié de cachet électronique est délivré par un prestataire de services de confiance qualifié[76]. Il bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié[77].

2.5.2.3. Les prestataires de services d'horodatage électronique au sens de eIDAS 1

En ce qui concerne les services d'horodatage électronique, le règlement eIDAS 1 vise la création, la vérification et la validation de ce service et des certificats relatifs à ce service[78].

---

[69] Art. 3-16 du règlement eIDAS 1, précité.
[70] Art. 3-16 du règlement eIDAS 1, précité.
[71] Art. 3-10 du règlement eIDAS 1, précité.
[72] Art. 32-1, point b) du règlement eIDAS 1, précité.
[73] Art. 25-2 du règlement eIDAS 1, précité.
[74] Art. 3-16 du règlement eIDAS 1, précité.
[75] Art. 3-25 du règlement eIDAS 1, précité.
[76] Art. 40 du règlement eIDAS 1, précité.
[77] Art. 35-2 du règlement eIDAS 1, précité.
[78] Art. 3-16 du règlement eIDAS 1, précité.

L'« **horodatage électronique** » est défini comme « des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant »[79]. Il établit la preuve que des données sous format électronique existaient à un instant particulier.

Un horodatage électronique qualifié est signé au moyen d'une signature électronique avancée ou cachetée au moyen d'un cachet électronique avancé du prestataire de confiance qualifiée[80]. Il bénéficie d'une 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[81].

2.5.2.4. Les prestataires de services d'envois recommandés électroniques au sens de eIDAS 1

Le règlement eIDAS 1 vise la création, la vérification et la validation des envois recommandés électroniques et des certificats relatifs à ce service[82].

Le « **service d'envoi recommandé** électronique » est défini comme « un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée »[83].

Les services d'envoi recommandé électronique qualifiés sont fournis par un prestataire de services de confiance qualifié[84]. Les données envoyées et reçues bénéficient « d'une présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié et 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 par le service d'envoi recommandé électronique qualifié »[85].

2.5.2.5. Les prestataires de services délivrant des certificats d'authentification de site web au sens de eIDAS 1

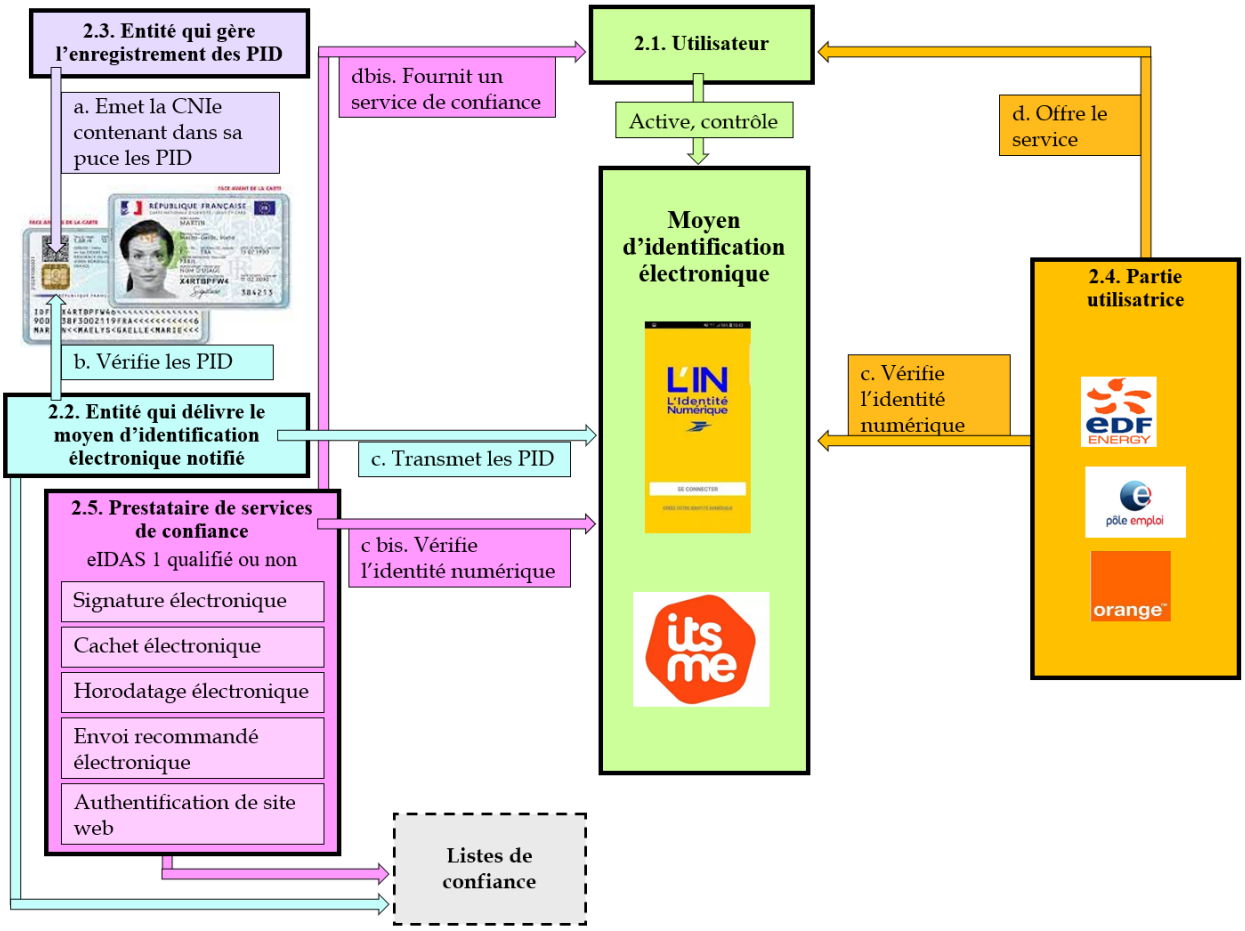
Le règlement eIDAS 1 vise la création, la vérification et la validation des certificats d'authentification de site web[86].

Ce type de certificat est défini comme « une attestation qui permet d'authentifier un site internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré »[87]. Délivré par un prestataire de service de confiance qualifié[88], il permet d'authentifier une entité véritable et de l'associer à un individu ou une entreprise notamment.

---

[79] Art. 3-33 du règlement eIDAS 1, précité.
[80] Art. 42-1, point c) du règlement eIDAS 1, précité.
[81] Art. 41-2 du règlement eIDAS 1, précité.
[82] Art. 3-16 du règlement eIDAS 1, précité.
[83] Art. 3-36 du règlement eIDAS 1, précité.
[84] Art. 44-1, point a) du règlement eIDAS 1, précité.
[85] Art. 43-2 du règlement eIDAS 1, précité.
[86] Art. 3-16 du règlement eIDAS 1, précité.
[87] Art. 3-38 du règlement eIDAS 1, précité.
[88] Annexe IV du règlement eIDAS 1, précité.

Figure 3. Les rôles définis spécifiquement par l'écosystème eIDAS 1 : un exemple d'interactions



3. Les rôles en cours de définition dans le nouvel écosystème eIDAS 2

Comme souligné précédemment, le règlement eIDAS 1 sur l'identification électronique et les services de confiance pour les transactions électroniques adopté en 2014 est en cours de révision. De façon générale, la proposition de règlement eIDAS 2 « Identité numérique » conserve, tout en les modifiant, les rôles déjà définis, qu'il s'agisse des « utilisateurs » (3.1.), des « entités qui délivrent les moyens d'identification électronique » (3.2.), des « entités qui gèrent l'enregistrement des données d'identification personnelle uniques » (3.4.), des « parties utilisatrices » (3.5.) ou des « prestataires de services « considérés comme » de confiance » (3.6.). Deux nouveaux rôles apparaissent : celui des « entités qui délivrent les portefeuilles européens d'identité numérique et des fournisseurs de portefeuilles européens d'identité numérique » (3.3.) et celui des « organismes du secteur public responsables des sources authentiques et les organismes délivrant des attestations électroniques d'attributs au nom d'un organisme du secteur public responsables de sources authentiques » (3.7).

En ce qui concerne les « entités qui gèrent l'enregistrement des données d'identification personnelle uniques », si la proposition de règlement ne modifie pas l'article 9-1, point d) du règlement eIDAS 1, elle introduit le terme d' « organismes chargés de veiller à ce que les données d'identification personnelle soient associées au portefeuille »[89], sans fournir plus de précision.

Un même acteur peut cumuler plusieurs rôles. Par exemple, des organismes du secteur de l'énergie ou du transport de voyageurs (EDF, SNCF) pourraient être « parties utilisatrices » et « prestataires de services délivrant des attestations d'attributs ». Une multinationale américaine pourrait être « partie utilisatrice » et « émetteur d'un portefeuille européen d'identité numérique ».

Certains de ces rôles sont spécifiés dans l'*Architecture and Reference Framework* (ARF), la difficulté étant que ce document technique, disponible uniquement en version anglaise, ne reprend pas systématiquement le vocabulaire employé dans les textes juridiques. De plus, la dernière version rendue publique date du 22 février 2022[90]. Elle ne prend donc pas en compte le résultat du compromis final en vue d'un accord publié le 10 novembre 2023.

Afin d'expliciter les rôles joués par les différents acteurs dans le cadre de eIDAS 2, nous nous référons à ce compromis disponible uniquement en anglais et proposons certaines traductions. Ces traductions sont soit issues de textes publiés à la fois en français et en anglais (cas de la proposition de règlement eIDAS 2 de la Commission européenne du 21 juin 2021, du texte issu de l'orientation générale du Conseil du 25 novembre 2022 ou du rapport du Parlement européen adopté le 2 mars 2023), soit effectuées par nos soins.

---

[89] Art. 6a-7d, point c) de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée

[90] Les experts ont depuis travaillé sur plusieurs autres versions, non publiées, qui prennent en compte les différentes propositions avancées par le Conseil de l'UE et le Parlement européen.

3.1. Les utilisateurs (« users ») au sens de eIDAS 2

La proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023 définit **l'utilisateur** comme « une personne physique ou morale, ou une personne physique représentant une personne morale, utilisant des services de confiance ou des moyens d'identification électronique ou des portefeuilles d'identité numérique européens »[91].

L'utilisateur au sens du règlement eIDAS 2 est donc la personne qui utilise des moyens d'identification électronique, y compris un portefeuille européen d'identité numérique. Ce portefeuille lui permet de recevoir, de gérer et de valider des données d'identification personnelle et des attestations électroniques d'attributs le concernant, notamment pour prouver son identité. L'utilisateur peut également créer des signatures et des cachets électroniques qualifiés.

L'utilisateur au sens du règlement eIDAS 2 est un sous-ensemble des utilisateurs tels que nous les avons décrits au point 1.1. En effet, si chaque État membre de l'UE est tenu d'offrir au moins une solution de portefeuille, une personne physique ou morale n'est pas obligée d'utiliser ce portefeuille. La proposition de règlement eIDAS 2 précise à cet égard que les États membres ne doivent pas, directement ou indirectement, limiter l'accès aux services publics ou privés aux personnes physiques ou morales qui n'ont pas choisi d'utiliser les PEIN et doivent mettre à disposition des solutions alternatives appropriées[92].

Un utilisateur tel que défini au point 1.1. de ce document doit donc pouvoir choisir :

- De recourir à un ou des portefeuilles d'identités numériques conformes au règlement eIDAS 2[93] ;
- D'utiliser un ou des portefeuilles conformes à d'autres spécifications techniques, par exemple des spécifications définies au niveau national ou par des acteurs privés (*Apple wallet*),
- De ne pas recourir à un dispositif numérique.

Le parallèle peut être fait ici avec les moyens de paiement. Un achat de vêtement peut s'effectuer dans une boutique ou en ligne en choisissant un mode de paiement électronique : une carte bancaire, une solution en ligne de type *paypal*, un *wallet* de type Apple, ou dans quelques années un PEIN.

---

[91] "'User' means a natural or legal person, or a natural person representing a legal person, using trust services, electronic identification means, provided according to this Regulation". Art. 3, point 5a de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

[92] "Member States should not, directly or indirectly, limit access to public or private services to natural or legal persons not opting to use EDIWs and should make available appropriate alternative solutions". Cons. 7 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

[93] En effet, selon l'article 6a-1 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, chaque État membre fournit au moins un portefeuille européen d'identité numérique.

3.2. Les entités qui délivrent les moyens d'identification électronique ou les fournisseurs de moyens d'identification électronique (« issuers or providers of electronic identification means ») au sens de eIDAS 2

La proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023 ne modifie pas l'article 9-1, point a) du règlement eIDAS 1 qui se réfère aux « entités qui délivrent les moyens d'identification électronique ». Ce terme est repris par l'article 12b de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023 ; en revanche, le considérant 6 de cette version se réfère aux fournisseurs de moyens d'identification (« providers of electronic means »[94]).

La proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023 modifie légèrement la définition de l'« **identification électronique** » en prenant en compte le cas d'une personne physique représentant une personne physique. Ainsi, l'identification électronique désigne « 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 physique* ou morale »[95].

La définition du « **moyen d'identification électronique** » est aussi modifiée pour tenir d'une possible utilisation hors ligne. Il s'agit d'« un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne *ou, le cas échéant, pour un service hors ligne* »[96].

L'entité qui délivre un moyen d'identification électronique et le fournisseur de moyens d'identification électronique au titre de eIDAS 2 sont donc des fournisseurs d'identité numérique tels que nous l'avons défini au point 1.4. de ce document. Ils peuvent fournir un logiciel, une application mobile, des portefeuilles européens d'identité numérique ou des cartes nationales d'identité électronique[97] aux utilisateurs qui souhaitent s'authentifier auprès des parties utilisatrices en ligne ou hors ligne.

3.3. Les entités qui gèrent l'enregistrement des données d'identification personnelle uniques (« entities which manage the registration of the unique person identification data ») au sens de eIDAS 2

La proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023 ne modifie pas l'article 9-1, point d) du règlement eIDAS 1 qui se réfère aux entités qui gèrent l'enregistrement des données d'identification personnelle uniques.

En revanche, elle modifie légèrement la définition des données d'identification personnelle (*Person Identification Data* – PID) pour préciser que les PID sont fournies conformément au droit de l'Union ou au droit national et pour prendre en compte la possibilité qu'une personne physique puisse

---

[94] Ainsi il est précisé : « … this amending Regulation should lay down specific safeguards to prevent providers of electronic identification means and electronic attestation of attributes from combining personal data from other services with the personal data processed to provide the services falling within the scope of this amending Regulation ».

[95] Art. 3-1 du règlement eIDAS 1, précité.

[96] Art. 3-2 par la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

[97] Dans ce sens, cons. 13 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée, selon lequel « Regulation (EU) No 2019/11575 strengthens the security of identity cards with enhanced security features by August 2021. Member States should consider the feasibility of notifying them under electronic identification schemes to extend the cross-border availability of electronic identification means ».

représenter une autre personne physique. Les données d'identification personnelles sont ainsi définies comme « un ensemble de données, *fournies conformément au droit de l'Union ou au droit national*, permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne *physique* ou morale »[98].

De plus, la proposition de règlement eIDAS 2 du 10 novembre 2023 prend en compte l'introduction du portefeuille européen d'identité numérique et la nécessaire gestion des données d'identification personnelle par ce dernier. Ainsi, les PEIN doivent notamment permettre à l'utilisateur de demander, sélectionner et supprimer des données d'identification personnelle[99] et offrir une série d'interfaces pour permettre aux parties utilisatrices de demander et de recevoir des PID.

3.4. Les entités qui délivrent les portefeuilles européens d'identité numérique et les fournisseurs de portefeuilles européens d'identité numérique (« issuers and providers of European Digital Identity Wallets ») au sens de eIDAS 2

La proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023 se réfère aux entités qui délivrent les portefeuilles européens d'identité numérique et aux fournisseurs de portefeuilles européens d'identité numérique. Elle définit le **portefeuille européen d'identité numérique** 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 et des attestations électroniques d'attributs, de les communiquer à des parties utilisatrices et à d'autres utilisateurs de portefeuilles européens d'identité numérique, et de les signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés »[100].

La proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023 distingue l'entité qui délivre le portefeuille européen d'identité numérique (« *issuer of the European Digital Identity Wallet* »)[101] et le « fournisseur portefeuille européen d'identité numérique » (« *provider of European Digital Identity Wallets»).*

---

[98] Art. 3-3 du règlement eIDAS 2, précité.

[99] « European Digital Identity Wallets are electronic identification means that shall enable the user in a manner that is user-friendly, transparent, and traceable by the user to: securely request, obtain, select, combine, store, delete, share and present, under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, offline in order to use public and private services, while ensuring that selective disclosure of data is possible ». Art. 6a-3, point a) de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

[100] Art. 3-42 par la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

[101] Voir la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée, en particulier au considérant 8a le terme de « wallet issuers », au considérant 9a le terme de « issuers of European Digital Identity Wallets », l'article 46a-3, point a) selon lequel : « The role of the supervisory bodies shall be: (a) to supervise providers of European Digital Identity Wallets established in the designating Member State and to ensure, through ex ante and ex post supervisory activities, that those issuers and the European Digital Identity Wallets they provide meet the requirements laid down in this Regulation » et l'article 46a-3, point b) « to take action, if necessary, in relation to providers of European Digital Identity Wallets established in the territory of the designating Member State, through ex post supervisory activities, when informed that those issuers and the European Digital Identity Wallets they provide allegedly do not meet the requirements laid down in this Regulation ».

La proposition de règlement de la Commission européenne de juin 2021 emploie uniquement le première terme, celui d'« entité qui délivre le PEIN ». Au cours des discussions, le terme de fournisseur de PEIN est en effet apparu ; il permet de distinguer les entités publiques qui délivrent des portefeuilles européens d'identité numérique (par exemple, en France, le ministère de l'intérieur qui devrait fournir France Identité) des fournisseurs privés de PEIN (par exemple, en Belgique, si itsme décide également de proposer un PEIN).

En effet, les portefeuilles sont fournis :

a. Directement par un État membre,
b. Sur mandat d'un Etat membre,
c. Indépendamment d'un État membre, mais sont reconnus par cet État membre[102].

Ainsi, un PEIN peut être délivré par une partie privée conformément aux points b) et c)[103]. Dans tous les cas, il est délivré dans le cadre d'un schéma d'identification électronique notifié de niveau de garantie élevé[104]. L'utilisateur doit exercer un contrôle total sur son utilisation et les données qui y figurent[105], notamment en sélectionnant, combinant, stockant, supprimant, partageant et présentant des données relatives à son identité. Le portefeuille européen d'identité numérique doit également permettre d'émettre des attestations électroniques attributs et de sélectionner des attributs, y compris lorsqu'ils font initialement partie de plusieurs attestations électroniques distinctes.

3.5. Les parties utilisatrices (« relying parties ») au sens de eIDAS 2

La version du 10 novembre 2023 du règlement eIDAS 2 prend en compte le recours au PEIN et à d'autres moyens d'identification électronique en modifiant la définition d'une **partie utilisatrice** désignée comme « 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 »[106]. Une partie utilisatrice peut être un Etat membre[107].

Les parties utilisatrices sont soumises à des obligations spécifiques dans le cadre du règlement eIDAS 2. Ainsi, lorsqu'elles ont l'intention de recourir à des PEIN, qu'il s'agisse de la fourniture de services publics ou privées, elles doivent s'enregistrer dans l'Etat membre sur le territoire duquel elles sont établies, en précisant notamment l'utilisation prévue du portefeuille européen d'identité numérique, y compris les données à demander[108]. Elles doivent ensuite s'identifier auprès de l'utilisateur du PEIN, puis exécuter la procédure d'authentification et de validation des données d'identification personnelle et des attestations électroniques d'attributs demandées aux PEIN[109]. En outre, elles ne peuvent pas

[102] Art. 6a-2 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[103] Dans ce sens, dernière phrase de l'article 6a-7 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée : « If the European Digital Identity Wallet is provided by private parties in accordance to paragraph 2 (b) and (c), the provisions of article 45f paragraph 4 shall apply mutatis mutandis ».
[104] Art. 6a-6 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[105] Art. 6a-7 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[106] « Relying party' means a natural or legal person that relies upon an electronic identification, European Digital Identity Wallets or other electronic identification means, or a trust service ». Art. 3-6 de la proposition de règlement dans sa version du 10 novembre 2023, précitée.
[107] Art. 11a-1 de la proposition de règlement eIDAS dans sa version du 10 novembre 2023, précitée, qui se réfère aux Etats lorsqu'ils agissent en tant que parties utilisatrices.
[108] Art. 6b-1 et art. 6b-1a de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[109] Art. 6b-2a et 6b-3 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

refuser l'utilisation de pseudonymes, lorsque l'identification de l'utilisateur n'est pas requise par le droit de l'Union ou le droit national.

3.6. Les prestataires de services « considérés comme » de confiance au sens de eIDAS 2

La proposition de règlement eIDAS 2, dans sa version du 10 novembre 2023 modifie la définition des services de confiance. Pour les cinq domaines déjà inclus dans le champ d'application du règlement eIDAS 1 (signatures, cachets, horodatage et envoi recommandé électroniques ainsi que l'authentification de site web), il s'agit d'un service électronique normalement fourni contre rémunération qui consiste :

- En la délivrance et la validation[110] des certificats de signatures électroniques pour la fourniture des signatures et cachets électroniques et des autres services de confiance,
- En la création et la validation de signatures électroniques ou de cachets électroniques,
- En la conservation de signatures électroniques, de cachets électroniques, de certificats de signature électronique ou de certificats de cachet électronique,
- En la création et validation d'horodatages électroniques,
- En la fourniture de services d'envoi recommandé électronique et en la validation de données transmises au moyen de services d'envoi recommandé électronique, ainsi que de preuves connexes,
- En la gestion de dispositifs de création de signatures électroniques qualifiées à distance ou de dispositifs de création de cachets électroniques qualifiés à distance[111].

Ainsi, le champ d'application de la proposition de règlement eIDAS 2 couvre les signatures et cachets électroniques créés soit par le portefeuille européen d'identité numérique, soit à distance dans le cloud.

Outre les cinq catégories de prestataires régulés par le règlement eIDAS 1, la proposition de règlement eIDAS 2, dans sa version du 10 novembre 2023, ajoute :

- Les prestataires de services d'attestations électroniques d'attributs (3.5.1.),
- Les prestataires de services d'archivage électronique (3.5.2.),
- Les prestataires de services d'enregistrement de données électroniques dans un registre électronique (3.5.3.).

3.5.1. Les prestataires de services de confiance d'attestations électroniques d'attributs (« trust service providers of electronic attestations of attributes ») au sens de eIDAS 2

La proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023 vise la délivrance et la validation des attestations électroniques d'attributs[112] qui sont définies comme « des attestations sous forme électronique qui permet l'authentification d'attributs »[113]. Les **attributs** correspondent pour leur part à « une caractéristique, une qualité, un droit ou l'autorisation d'une personne physique ou morale

---

[110] L'article 3-41 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée, définit la validation comme « le processus consistant à vérifier et à confirmer que les données sous forme électronique sont valides conformément aux exigences du présent règlement ».
[111] Art. 3-16 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[112] Art. 3-16f et art. 3-16fa de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[113] « Electronic attestation of attributes' means an attestation in electronic form that allows the authentication of attributes ». Art. 3-44 du de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

ou d'un objet »[114]. Notre consommation électrique, notre revenu, le nombre de personnes rattachés à notre foyer fiscal, la date et l'horaire d'arrivée de notre train, notre régime alimentaire, le type de voiture que nous préférons, notre photographie sont autant d'attributs. Ces derniers peuvent faire l'objet de plusieurs attestations électroniques distinctes (diplômes, permis, certificats …), puis être ensuite combinés.

Les prestataires de service de confiance d'attestation électronique d'attributs au sens du règlement eIDAS 2 font partie de la catégorie des fournisseurs de justificatifs ou de données telle que décrite au point 1.5.

À cet égard, toute entité qui délivre des attributs attestés tels que des diplômes, permis et certificats de naissance ou des pouvoirs et mandats pour représenter ou agir au nom de personnes physiques ou morales doit pouvoir devenir prestataires d'attestations électroniques d'attributs au titre du règlement eIDAS 2[115]. Si tel est le cas, quel que soit l'État membre dans lequel le PEIN est fourni, cette entité doit donner à l'utilisateur du portefeuille la possibilité d'obtenir, stocker et gérer ses attestations électroniques[116].

Par ailleurs, les prestataires qualifiés et non qualifiés d'attestations électroniques d'attributs ne doivent pas combiner les données personnelles relatives à la fourniture de services d'attestations électroniques avec des données personnelles provenant de tout autre service qu'ils offrent ou que leurs partenaires commerciaux offrent[117].

L'attestation électronique qualifiée d'attributs (AEQA) est délivrée par un prestataire de services de confiance qualifiés conformément aux exigences fixées à l'annexe V du règlement eIDAS 2[118]. Elle a le même effet juridique qu'une attestation délivrée légalement sur papier[119]. Si elle est révoquée, elle perd sa validité à compter du moment de sa révocation ; elle ne peut en aucun cas recouvrer son statut antérieur[120].

Un prestataire qualifié doit obligatoirement vérifier l'identité et, s'il y a lieu, tous les attributs spécifiques de la personne à laquelle il délivre l'attestation qualifiée[121]. Cette vérification est effectuée soit directement par la présence de la personne, soit indirectement en ayant recours à un tiers. En particulier, il doit pouvoir vérifier, à la demande de l'utilisateur, au moins les types d'attributs énumérés à l'annexe VI du règlement eIDAS 2 auprès d'une source authentique du secteur public, lorsqu'ils reposent sur une telle source[122]. Ces attributs sont :

1. L'adresse,
2. L'âge,
3. Le sexe,
4. L'état civil,
5. La composition de la famille,
6. La nationalité ou la citoyenneté,

---

[114] « 'Attribute' means a characteristic, quality, right or permission of a natural or legal person or of an object ». Art. 3-43 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[115] Cons. 27 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[116] Art. 45e-1 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[117] Art. 45f-1 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[118] Art. 3-45 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[119] Art. 45a-2 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[120] Art. 45c-3 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[121] Art. 24-1 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[122] Art. 45d-1 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

7. Les diplômes, titres et certificats du système éducatif,
8. Les diplômes, titres et certificats professionnels,
8a. Les pouvoirs et mandats pour représenter des personnes physiques ou morales,
9. Les permis publics et licences,
10. Pour les personnes morales, les informations financières et les données des entreprises.

Une attestation électronique d'attributs peut également être délivrée par un organisme du secteur public, responsable d'une source authentique ou en son nom (cf. 3.6).

3.5.2. Les prestataires de services de confiance pour l'archivage électronique (« trust service providers for electronic attestation of attributes ») au sens de eIDAS 2

La proposition de règlement eIDAS 2 vise l'archivage électronique de données[123], l'« **archivage électronique** » étant défini comme « un service assurant la réception, le stockage, la récupération et la suppression de données et documents électroniques afin d'en garantir la durabilité et la lisibilité, ainsi que d'en préserver l'intégrité, la confidentialité et la preuve de l'origine pendant toute la période de conservation »[124]. Ce service permet d'étendre la fiabilité des données ou des documents électroniques au-delà de la période de validité technologique grâce à l'utilisation de procédures et technologies adéquates.

Un service qualifié d'archivage électronique de documents électroniques est fourni par un prestataire de services de confiance qualifié[125]. Les données et documents électroniques qu'il conserve bénéficient de la présomption de leur intégrité et de leur origine pendant leur durée de conservation[126]. A cette fin, le prestataire qualifié utilise des procédures et des technologies pouvant étendre la durabilité et la lisibilité des données électroniques au-delà de la période de validité technologique et au moins tout au long de la période de conservation légale ou contractuelle, tout en préservant leur intégrité et leur origine[127].

3.5.3. Les prestataires de services de confiance pour les registres électroniques (« trust service providers for electronic ledgers ») au sens de eIDAS 2

La proposition de règlement eIDAS 2 vise l'enregistrement de données électroniques dans un registre électronique[128], le « **registre électronique** » étant défini comme « « une séquence d'enregistrement de données électroniques afin de garantir leur intégrité et l'exactitude de leur classement chronologique »[129].

Ce type d'enregistrements permet de détecter toute modification ultérieure des données. Il offre une gouvernance plus décentralisée des actifs numériques adaptée à la coopération multipartite et évite notamment que ces actifs ne soient copiés ou vendus à plusieurs destinataires. Utilisé dans de

---

[123] Art. 3-16ff de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[124] « 'Electronic archiving' means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to guarantee their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period ». Art. 3-47 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[125] Art. 45 ga de la proposition de règlement eIDAS 2, version du 10 novembre 2023, précitée.
[126] Art. 45 g-2 de la proposition de règlement eIDAS 2, version du 10 novembre 2023, précitée.
[127] Art. 45 ga-1b de la proposition de règlement eIDAS 2, version du 10 novembre 2023, précitée.
[128] Art. 3-16fg de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.
[129] « 'Electronic ledger' means a sequence of electronic data records, ensuring their integrity and the accuracy of their chronological ordering ». Art. 3-53 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

nombreux domaines, notamment les enregistrements numériques de propriété, de financement de la chaîne d'approvisionnement, de vote électronique, de produits de base tels que l'électricité[130], il peut être mis en œuvre de façon centralisée ou distribuée. Un registre centralisé peut par exemple se baser sur une infrastructure à clés publiques ou *Public Key Infrastructure* (PKI) tandis qu'un registre distribué peut recourir à une *blockchain*.

Un registre électronique qualifié est créé et géré par un ou plusieurs prestataires de services de confiance qualifiés[131]. Ce registre établit l'origine des enregistrements de données, garantit le classement chronologique séquentiel unique des enregistrements et enregistre les données de telle sorte que toute modification ultérieure de ces dernières soit immédiatement détectable, assurant ainsi leur intégrité dans le temps. Les enregistrements de données qu'il contient bénéficient d'une présomption quant à leur classement chronologique séquentiel unique et précis et à leur intégrité[132].

3.7. Les organismes du secteur public responsables des sources authentiques (« public sector body responsible for an authentic source ») et les organismes du secteur public désignés par un Etat membre pour délivrer des attestations électroniques d'attributs au nom d'un organisme du secteur public responsables de sources authentiques (« public sector body designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources ») au sens de eIDAS 2

L'attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou en son nom (ci-après organisme du secteur public) est définie par le règlement eIDAS 2 dans sa version du 10 novembre 2023 comme « une attestation électronique d'attributs délivrée par un organisme du secteur public responsable d'une source authentique ou par un organisme du secteur public désigné par l'État membre pour délivrer de telles attestations d'attributs au nom des organismes du secteur public responsables de sources authentiques conformément à l'article 45 quinquies bis et répondant aux exigences fixées à l'annexe VIa »[133].

La notion de « **source authentique** » est définie comme « un répertoire ou un système, administré sous la responsabilité d'un organisme du secteur public ou d'une entité privée, qui contient les attributs concernant une personne physique ou morale et qui est considéré comme étant la source

---

[130] « En 2017, 75 % de tous les cas d'utilisation de registres électroniques concernaient le domaine bancaire et financier. Aujourd'hui, les cas d'utilisation de registres électroniques ne cessent de se diversifier, 17 % d'entre eux relevant du domaine de la communication et des médias, 15 % de l'industrie manufacturière et de l'exploitation des ressources naturelles, 10 % du secteur public, 8 % du secteur des assurances, 5 % du commerce de détail, 6 % du secteur des transports et 5 % des services collectifs ». Exposé des motifs de la proposition de règlement eIDAS 2 de la Commission européenne du 3 juin 2021, p. 13, précitée, citant le rapport Gartner, Blockchain Evolution, 2020.

[131] Art. 45i-1 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

[132] Art. 45h-2 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

[133] « 'Electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source' means an electronic attestations of attributes issued by a public sector body responsible for an authentic source or by a public sector body designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45da and meeting the requirements laid down in Annex Via. Art. 3-45a de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

première de ces informations ou est reconnu comme authentique conformément au droit de l'Union ou au droit national, y compris les pratiques administratives »[134].

Les organismes du secteur public responsables d'une source authentique ou en son nom sont notifiés par les Etats membres à la Commission européenne. Ils figurent sur une liste mise à la disposition du public. Les exigences concernant les attestations qu'ils délivrent sont calquées sur celles applicables aux attestations électroniques qualifiées d'attributs, qu'il s'agisse du contenu de l'attestation fixé par l'annexe VIa, du niveau de fiabilité présenté par l'organisme public, qui doit être équivalent à celui d'un prestataire de services de confiance qualifié ou des conséquences de la révocation des attestations qu'ils délivrent[135].

Les organismes du secteur public qui délivrent des attestations électroniques d'attributs fournissent une interface avec les portefeuilles européens d'identité numérique[136].

Possibles sources authentiques en France

Type de données	Sources authentiques
Personne physique : Nom de famille, prénoms, lieu et date de naissance, sexe, date et lieu de décès	INSEE – Répertoire national d'identification des personnes physiques (RNIPP)[137]
Brevet et baccalauréat	Service interacadémique des examens et concours[138]
Permis de conduire	Système national des permis de conduire (SNPC)[139]
Données d'entreprise (dénomination, catégorie juridique, état, activité principale …)	INSEE – Répertoire National d'identification des entreprises et des établissements (SIRENE)[140]

[134] « 'Authentic source' is a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person and is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice ». Art. 3-46 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

[135] Art. 45da de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

[136] Article. 45da, point 8 de la proposition de règlement eIDAS 2 dans sa version du 10 novembre 2023, précitée.

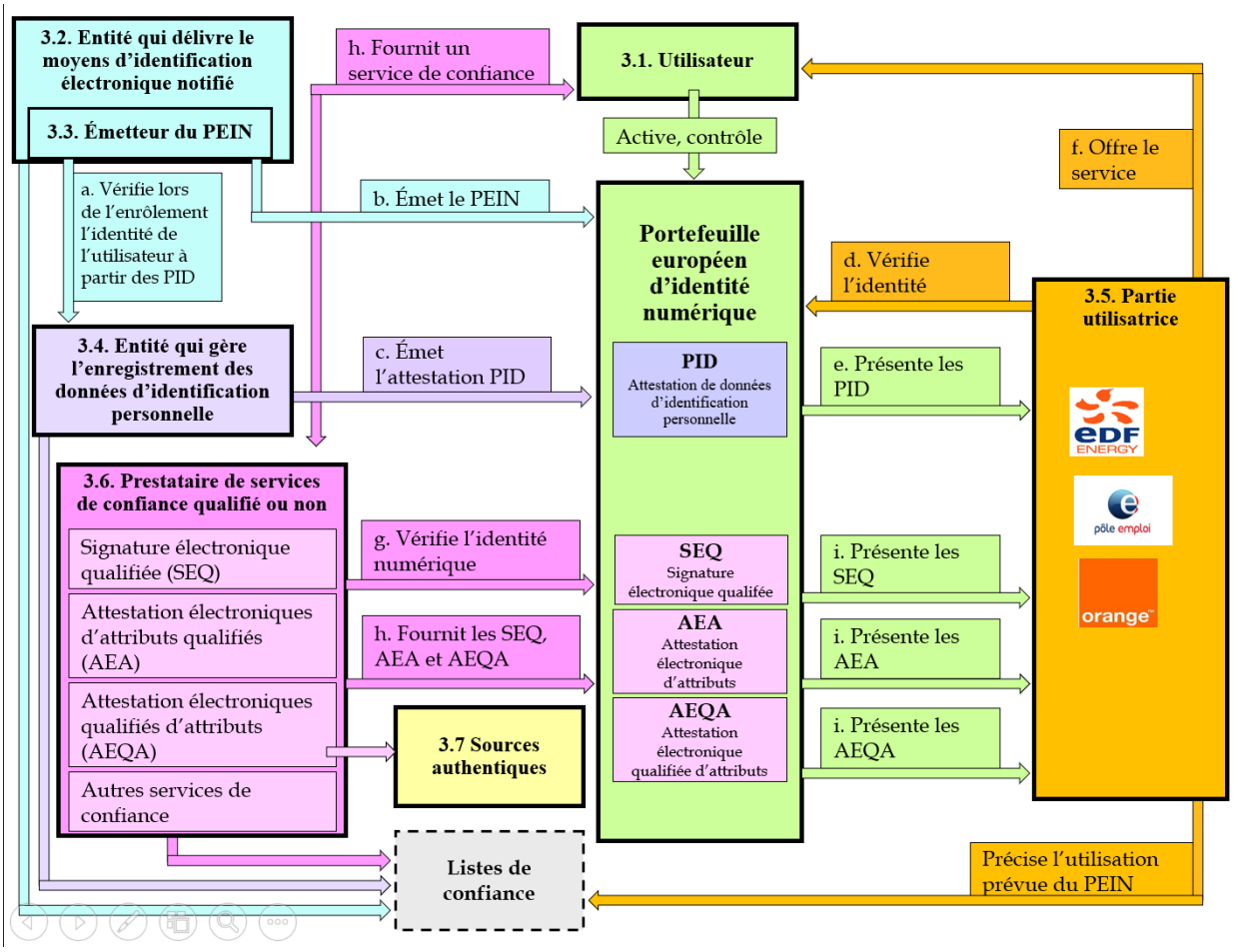
[137] Décret n°82-103 du 22 janvier 1982 relatif au répertoire national d'identification des personnes physiques, JORF du 29 janvier 1982.

[138] Pour l'ensemble des diplômes du secondaire et du supérieur, voir https://www.service-public.fr/particuliers/vosdroits/F10492, consulté le 30 janvier 2024.

[139] Arrêté du 29 juin 1992 portant création du Système national des permis de conduire, JORF du 30 juin 1992.

[140] Décret n°73-314 du 14 mars 1973 portant création d'un système national d'identification et d'un répertoire des entreprises et de leurs établissements, JORF du 21 mars 1973.

Figure 4. Les rôles en cours de définition dans le nouvel écosystème eIDAS 2 : exemple d'interactions



Bibliographie

Références juridiques

Références juridiques de l'Union européenne

Règlements

Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, JOUE L 218 du 13.8.2008, p. 30, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:fr:PDF.

Règlement (CE) n° 444/2009 du Parlement européen et du Conseil du 28 mai 2009 modifiant le règlement (CE) n°2252/2004 du Conseil établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, JOUE L 142 du 6 juin 2009, p. 1, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L:2009:142:TOC.

Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juill. 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, JOUE L 257 du 28 août 2014, p. 73, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32014R0910 (règlement eIDAS 1).

Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE L 119 du 4 mai 2016, p. 1, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

Règlement (UE) n° 2017/1954 du Parlement européen et du Conseil du 25 octobre 2017 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers, JOUE L 286 du 1e nov. 2017, p. 9, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32017R1954.

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, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité), JOUE L 151 du 7 juin 2019, p. 15, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R0881.

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, JOUE L 188 du 12 juil. 2019, p. 67, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32019R1157.

Règlements d'exécution

Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen

et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, JOUE L 235 du 9 sept. 2015, p. 7.

Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, JOUE L 235 du 9.9.2015, p. 1, https://op.europa.eu/en/publication-detail/-/publication/6c875413-4dd5-4ee3-a0e4-25e60ce8aacc/language-fr/format-PDFA1A.

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, JOUE L 210 du 14 juin 2021, p. 51, https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32021H0946.

Propositions de règlement eIDAS 2 « Identité numérique »

Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, COM(2021) 281 final du 3 juin 2021, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&qid=1628524321657&from=FR.

Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique – orientation générale, Bruxelles, le 25 novembre 2022, 14959/22, LIMITE, TELECOM 473, COMPET 919, MI 844, DATAPROTECT 321, JAI 1497, CODEC 1774, https://data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/fr/pdf.

Rapport du Parlement européen du 2 mars 2023 sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)), Commission de l'industrie, de la recherche et de l'énergie, Rapporteure: Romana Jerković, A9-0038/2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_FR.html

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity – Analysis of the final compromise text with a view to agreement, Brussels, 10 November 2023, https://data.consilium.europa.eu/doc/document/ST-15149-2023-INIT/en/pdf.

Communications de la Commission européenne

Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *Une boussole numérique pour 2030 : l'Europe balise la décennie numérique*, COM(2021)118 final du 9 mars 2021, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52021DC0118

Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *Façonner l'avenir numérique de l'Europe*, COM(2020)67 final du 19 fév. 2020, https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52020DC0067.

ARF

European Digital Identity, Architecture and Reference Framework – Outline, 22 February 2022, https://pixl8-cloud-techuk.s3.eu-west-2.amazonaws.com/prod/public/27a2bdfe-996c-4e48-8cadff04e648c06b/eIDas-Outline-final.pdf.

The Common Union Toolbox for a coordinated approach toward a European Digital Identity Framework, The European Digital Identity Wallet Architecture and Reference Framework, January 2023, Version 1.0.0, https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework.

Schémas d'identification électronique notifiés

Overview of pre-notified and notified eID schemes under eIDAS, https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS.

Références juridiques françaises

Décret n°73-314 du 14 mars 1973 portant création d'un système national d'identification et d'un répertoire des entreprises et de leurs établissements, JORF du 21 mars 1973.

Décret n°82-103 du 22 janvier 1982 relatif au répertoire national d'identification des personnes physiques, JORF du 29 janvier 1982.

Arrêté du 29 juin 1992 portant création du Système national des permis de conduire, JORF du 30 juin 1992.

Assemblée nationale, rapport d'information n° 3019, *Pour une identité numérique régalienne citoyenne*, mission d'information commune M. Karamanli, C. Hennion et J-M. Mis, juil. 2020, p. 18, https://www.assemblee-nationale.fr/dyn/15/rapports/micnum/l15b3190_rapport-information#.

Décret n° 2021-1538 du 29 novembre 2021 relatif à l'expérimentation du téléservice dénommé « Mon FranceConnect » (MFC), JORF du 30 nov. 2021. Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, COM(2021) 281 final du 3 juin 2021, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0281&qid=1628524321657&from=FR.

CNIL, délibération n° 2021-151 du 9 décembre 2021 portant avis sur un projet de décret en Conseil d'État autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile » (demande d'avis n° 21015556).

Décret n° 2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », JORF du 27 avril 2022, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045667825.

Références juridiques luxembourgeoise

Loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques, JO du Grand-Duché du Luxembourg, https://legilux.public.lu/eli/etat/leg/loi/2013/06/19/n3/jo.

Ouvrage

Chaire Valeurs et Politiques des Information Personnelles, *Identités numériques*, coordonné par Claire Levallois-Barth, mars 2016, https://cvpip.wp.imt.fr/2016/03/19/2016-03-identites-numeriques/.

Webographie

Union européenne

Discover the Dashboard and eIDAS trust services, http://esignature.ec.europa.eu/efda/home/#/screen/discover.

Portefeuilles européens d'identité numérique : la Commission publie une première boîte à outils technique pour les prototypes, 10 février 2023, https://digital-strategy.ec.europa.eu/fr/news/european-digital-identity-wallets-commission-publishes-first-technical-toolbox-towards-prototypes.

Belgique

Créez un compte itsme® avec votre eID, https://www.itsme-id.com/fr-BE/get-started/eid.

Créez un compte itsme® avec votre carte de banque, https://www.itsme-id.com/fr-BE/get-started/bank#video.

Itsme Notification form for electronic identity scheme under article 9(5) of regulation (EU) n° 910/2014, https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/87064906/1.1.1%20NOTIFICATION%20FORM_Belgian%20FAS%20itsme-Signed.pdf?version=1&modificationDate=1571043055346&api=v2.

France

L'ANSSI actualise le référentiel SecNumCloud, https://www.ssi.gouv.fr/actualite/lanssi-actualise-le-referentiel-secnumcloud/.

Utiliser la carte d'identité électronique avec le lecteur de carte Gemalto, https://gouvernement.lu/fr/dossiers.gouv_ctie%2Bfr%2Bdossiers%2BeID%2Blecteur-carte.html.

International

Conditions de service de Facebook, https://www.facebook.com/legal/terms/update. Le réseau social précise qu'il peut « être amené à changer le nom d'utilisateur associé [au] compte dans certaines circonstances (par exemple, lorsqu'une autre personne revendique le nom d'utilisateur et que le nom d'utilisateur semble sans rapport avec le nom [utilisé] au quotidien », https://www.facebook.com/legal/terms/update.

Créer un compte Google, https://support.google.com/accounts/answer/27441?hl=fr.

Qu'est-ce que le service « Se connecter avec Apple » ?, https://support.apple.com/fr-fr/HT210318.

Anthony Nelzin-SantosSign in with Apple : Apple devient fournisseur d'identité privée, 11 juin 2019, https://www.macg.co/macos/2019/06/sign-apple-apple-devient-fournisseur-didentite-privee-106479.

Apple teams up with TSA to enable digital identification at security checkpoints, June 2021, https://www.futuretravelexperience.com/2021/06/apple-teams-up-with-tsa-to-enable-digital-identification-at-security-checkpoints/.