Conseil de
l'Union européenne

Bruxelles, le 3 juin 2021
(OR. en)

9471/21

Dossier interinstitutionnel:
2021/0136(COD)

TELECOM 242
COMPET 457
MI 432
DATAPROTECT 156
JAI 670
IA 108
CODEC 826

PROPOSITION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	3 juin 2021
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2021) 281 final
Objet:	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

Les délégations trouveront ci-joint le document COM(2021) 281 final.

p.j.: COM(2021) 281 final

COMMISSION
EUROPÉENNE

Bruxelles, le 3.6.2021
COM(2021) 281 final

2021/0136 (COD)

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

{SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Le présent exposé des motifs accompagne la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (ci-après le «règlement eIDAS»)[1]. Par cet instrument juridique, il s'agit de garantir, à des fins d'utilisation transfrontalière, les aspects suivants:

– donner accès à des solutions d'identité électronique hautement sécurisées et fiables,

– faire en sorte que les services publics et privés puissent s'appuyer sur des solutions d'identité numérique fiables et sécurisées,

– donner aux personnes physiques et morales les moyens d'utiliser des solutions d'identité numérique,

– faire en sorte que ces solutions soient rattachées à divers attributs et permettent le partage ciblé de données d'identité dans la limite des besoins du service particulier demandé,

– faire accepter les services de confiance qualifiés dans l'UE et en garantir la fourniture dans des conditions égales.

Le marché 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 numériques monolithiques, mais sur la fourniture et l'utilisation d'attributs spécifiques en lien avec ces identités. On observe une demande croissante de solutions d'identité électronique qui puissent offrir ces capacités, des gains d'efficacité et un niveau élevé de confiance dans toute l'UE, dans les secteurs tant privé que public, pour lesquels il est indispensable de pouvoir identifier et authentifier les utilisateurs avec un degré élevé de garantie.

Il ressort de l'évaluation du règlement eIDAS[2] que, dans sa version actuelle, cet instrument n'est pas en mesure de répondre à ces nouvelles demandes du marché, principalement pour les raisons suivantes: les limitations au secteur public qui lui sont inhérentes, les possibilités limitées et la difficulté pour les prestataires privés de services en ligne de se connecter au système, la disponibilité insuffisante de solutions d'identification électronique notifiées dans tous les États membres, et un manque de souplesse pour répondre à des cas d'utilisation variés. En outre, les solutions d'identité qui ne relèvent pas du champ d'application du règlement eIDAS, telles que celles proposées par les fournisseurs de médias sociaux et les établissements financiers, suscitent des inquiétudes quant au respect de la vie privée et à la protection des données. Elles ne peuvent pas satisfaire efficacement aux nouvelles demandes du marché et n'ont pas la portée transfrontalière nécessaire pour répondre à des besoins sectoriels pour lesquels l'identification est un aspect sensible et requiert un niveau élevé de certitude.

---

1 JO L 257 du 28.8.2014, p. 73.

2 [ajouter référence après adoption].

Depuis l'entrée en vigueur du volet relatif à l'identification électronique du règlement en septembre 2018, seuls 14 États membres ont notifié au moins un schéma d'identification électronique. En conséquence, seuls 59 % des résidents de l'UE ont accès à des schémas d'identification électronique fiables et sécurisés par-delà les frontières. Seuls sept schémas sont entièrement mobiles et répondent ainsi aux attentes actuelles des utilisateurs. Étant donné que les nœuds techniques nécessaires pour assurer la connexion au cadre d'interopérabilité eIDAS ne sont pas tous entièrement opérationnels, l'accès transfrontalier est limité: très peu de services publics en ligne accessibles au niveau national peuvent être obtenus par-delà les frontières par l'intermédiaire du réseau eIDAS.

La mise en place d'un cadre européen relatif à une identité numérique fondé sur la révision du cadre actuel devrait permettre à au moins 80 % des citoyens d'utiliser une solution d'identification numérique pour accéder à des services publics essentiels d'ici à 2030. En outre, la sécurité et le contrôle assurés par le cadre européen relatif à une identité numérique devraient donner aux citoyens et aux résidents pleinement confiance dans le fait que le cadre européen relatif à une identité numérique donnera à chacun les moyens de contrôler qui a accès à son jumeau numérique et à quelles données exactement. Cela nécessitera également un niveau élevé de sécurité en ce qui concerne tous les aspects de la fourniture d'identités numériques, y compris la délivrance d'un portefeuille européen d'identité numérique, et l'infrastructure pour la collecte, le stockage et la divulgation de données d'identité numérique.

En outre, le cadre eIDAS actuel n'englobe pas la fourniture d'attributs électroniques, tels que les certificats médicaux ou les qualifications professionnelles, ce qui rend difficile de garantir la reconnaissance juridique paneuropéenne de tels justificatifs sous forme électronique. De plus, le règlement eIDAS ne permet pas aux utilisateurs de limiter le partage des données d'identité à ce qui est strictement nécessaire à la fourniture d'un service.

Si l'évaluation du règlement eIDAS montre que le cadre relatif à la fourniture de services de confiance a été plutôt efficace, offrant un niveau élevé de confiance et garantissant l'adoption et l'utilisation de la plupart des services de confiance, il reste encore beaucoup à faire pour parvenir à une harmonisation et à une acceptation complètes. En ce qui concerne les certificats qualifiés d'authentification de site internet, les citoyens doivent pouvoir se fier à ceux-ci et bénéficier d'informations sûres et fiables sur les administrateurs de site internet, réduisant ainsi les cas de fraude.

En outre, afin de réagir à la dynamique des marchés et aux évolutions technologiques, la présente proposition élargit la liste actuelle des services de confiance eIDAS à trois nouveaux services de confiance qualifiés, à savoir la fourniture de services d'archivage électronique, les registres électroniques et la gestion des dispositifs de création de signatures et de cachets électroniques à distance.

La présente proposition offre également une approche harmonisée de la sécurité, pour les citoyens qui ont recours à une identité numérique européenne qui les représente en ligne et pour les fournisseurs de services en ligne qui pourront pleinement s'appuyer sur des solutions d'identité numérique et les accepter, indépendamment du lieu où elles auront été délivrées. La présente proposition suppose un changement pour les entités qui délivrent des solutions d'identité numérique européennes, en prévoyant une architecture technique et un cadre de référence communs ainsi que des normes communes devant être élaborés en collaboration avec les États membres. Il est nécessaire d'adopter une approche harmonisée pour éviter que le développement de nouvelles solutions d'identité numérique dans les États membres n'accentue la fragmentation due à l'utilisation de solutions nationales divergentes. Une

approche harmonisée renforcera également le marché unique car elle permettrait aux citoyens, aux autres résidents et aux entreprises de s'identifier en ligne de manière sécurisée, pratique et uniforme dans toute l'UE pour accéder à des services aussi bien publics que privés. Les utilisateurs pourraient avoir recours à un écosystème amélioré d'identité électronique et de services de confiance reconnus et acceptés partout dans l'Union.

Afin d'éviter la fragmentation et les obstacles dus à des normes divergentes, la Commission adoptera une recommandation en même temps que la présente proposition. Cette recommandation définira un processus visant à soutenir une approche commune qui permette aux États membres et aux autres parties prenantes concernées du secteur public et du secteur privé, en étroite coordination avec la Commission, d'œuvrer à l'élaboration d'une boîte à outils destinée à éviter que des approches divergentes ne soient adoptées, d'une part, et que la future mise en œuvre du cadre européen relatif à une identité numérique ne soit compromise, d'autre part.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

La présente proposition repose sur l'actuel règlement eIDAS, sur le rôle des États membres en tant que fournisseurs d'identités juridiques et sur le cadre relatif à la prestation de services électroniques de confiance dans l'Union européenne. Elle complète les autres instruments d'action au niveau de l'UE visant à traduire les avantages du marché intérieur dans le monde numérique et cadre parfaitement avec ces instruments, notamment en élargissant les possibilités offertes aux citoyens d'accéder à des services transfrontaliers. À cet égard, la proposition met en œuvre le mandat politique conféré par le Conseil européen[3] et la présidente de la Commission européenne[4] de fournir un cadre à l'échelle de l'UE concernant les identités électroniques publiques, qui garantisse à tout citoyen ou résident l'accès à une identité électronique européenne sécurisée, utilisable partout dans l'UE pour s'identifier et s'authentifier en vue d'accéder à des services du secteur public et du secteur privé, de sorte que les citoyens peuvent exercer un contrôle sur les données communiquées et sur la manière dont elles sont utilisées.

- **Cohérence avec les autres politiques de l'Union**

La proposition est cohérente avec les priorités de la transformation numérique telles qu'elles sont définies dans la stratégie «Façonner l'avenir numérique de l'Europe»[5] et soutiendra la réalisation des objectifs fixés dans la communication sur la décennie numérique[6]. Toute opération de traitement de données à caractère personnel au titre du présent règlement devrait être effectuée dans le strict respect du règlement général sur la protection des données (ci-après le «RGPD»)[7]. En outre, le présent règlement introduit des garanties spécifiques en matière de protection des données.

---

3 https://www.consilium.europa.eu/media/45918/021020-euco-final-conclusions-fr.pdf

4 Discours sur l'état de l'Union du 16 septembre 2020, voir https://ec.europa.eu/commission/presscorner/detail/fr/SPEECH_20_1655

5 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.

6 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.

7 Règlement (UE) 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 (JO L 119 du 4.5.2016, p. 1).

Afin de garantir un niveau élevé de sécurité, la proposition est également conforme aux politiques de l'Union en matière de cybersécurité[8]. Elle a été conçue pour réduire la fragmentation par l'application des exigences générales en matière de cybersécurité aux prestataires de services de confiance régis par le règlement eIDAS.

La présente proposition est en outre cohérente avec d'autres politiques sectorielles reposant sur l'utilisation d'identités électroniques, d'attestations électroniques d'attributs et d'autres services de confiance. On peut citer, à cet égard, le règlement établissant un portail numérique unique[9], les exigences à remplir dans le secteur financier en matière de lutte contre le blanchiment de capitaux et contre le financement du terrorisme, les initiatives de partage de justificatifs de sécurité sociale, celles concernant l'obtention d'un permis de conduire numérique ou pour les futurs documents de voyage numériques, ainsi que d'autres initiatives visant à réduire la charge administrative pesant sur les citoyens et les entreprises qui s'appuient pleinement sur les possibilités offertes par la transformation numérique des procédures, tant dans le secteur public que dans le secteur privé. Le portefeuille permettra en outre de disposer de signatures électroniques qualifiées susceptibles de faciliter la participation à la vie politique[10].

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La présente initiative vise à soutenir la transformation de l'Union permettant la mise en place d'un marché unique numérique. Compte tenu de la dématérialisation croissante des services publics et privés transfrontaliers, qui reposent sur l'utilisation de solutions d'identité numérique, il existe un risque que, dans le cadre juridique actuel, les citoyens demeurent confrontés à des obstacles et ne soient pas en mesure d'utiliser pleinement les services en ligne de manière fluide dans l'ensemble de l'UE tout en préservant leur vie privée. Par ailleurs, les lacunes du cadre juridique actuel relatif aux services de confiance risquent d'accroître la fragmentation et de réduire la confiance s'il est laissé aux seuls États membres le soin de prendre des mesures à cet égard. L'article 114 TFUE est donc considéré comme la base juridique pertinente de la présente initiative.

• Subsidiarité (en cas de compétence non exclusive)

Les citoyens et les entreprises devraient pouvoir bénéficier de la disponibilité de solutions d'identité numérique hautement sécurisées et fiables, qui puissent être utilisées dans toute l'UE, et de la portabilité des attestations électroniques d'attributs liés à l'identité. Les évolutions technologiques récentes ainsi que la demande du marché et des utilisateurs exigent la disponibilité de solutions transfrontalières plus conviviales, qui permettent d'avoir accès à des services en ligne à l'échelle de l'UE, ce que le règlement eIDAS, sous sa forme actuelle, ne peut offrir.

En outre, les utilisateurs se sont de plus en plus habitués aux solutions disponibles dans le monde entier, par exemple lorsqu'ils acceptent l'utilisation de solutions d'authentification unique fournies par les grandes plateformes de médias sociaux pour accéder à des services en ligne. Les États membres ne peuvent à eux seuls relever les défis qui découlent de cette situation du point de

---

8 https://ec.europa.eu/commission/presscorner/detail/fr/IP_20_2391

9 Règlement (UE) 2018/1724 du Parlement européen et du Conseil du 2 octobre 2018 établissant un portail numérique unique pour donner accès à des informations, à des procédures et à des services d'assistance et de résolution de problèmes (JO L 295 du 21.11.2018, p. 1).

10 Plan d'action pour la démocratie européenne, COM(2020) 790 final.

vue du pouvoir de marché des grands fournisseurs, qui nécessite de garantir l'interopérabilité et la fiabilité des identifications électroniques à l'échelle de l'UE. En outre, les attestations électroniques d'attributs délivrées et acceptées dans un État membre donné, telles que les certificats sanitaires électroniques, ne sont souvent pas juridiquement reconnues et acceptées dans les autres États membres. Il en découle le risque que les États membres ne continuent à développer des solutions nationales fragmentées qui ne soient pas opérationnelles par-delà les frontières.

En ce qui concerne la fourniture de services de confiance, bien que ceux-ci soient réglementés dans une large mesure et fonctionnent conformément au cadre juridique actuel, les pratiques nationales créent également un risque de fragmentation accrue.

En définitive, l'intervention au niveau de l'UE est la mieux adaptée pour doter les citoyens et les entreprises, dans le respect des règles de l'UE relatives à la protection des données, des moyens de s'identifier par-delà les frontières et d'échanger des attributs d'identité personnels et des justificatifs grâce à des solutions d'identité numérique hautement sécurisées et fiables. Cela nécessite une identification électronique sécurisée et fiable ainsi qu'un cadre réglementaire permettant de faire le lien avec les attributs et les justificatifs à l'échelle de l'UE. Seule une intervention au niveau de l'UE peut créer les conditions harmonisées garantissant le contrôle par les utilisateurs et l'accès de ceux-ci à des services numériques en ligne transfrontaliers, ainsi qu'un cadre d'interopérabilité permettant aux services en ligne de s'appuyer aisément sur l'utilisation de solutions d'identité numérique sécurisées, quel que soit le lieu de délivrance dans l'UE ou le lieu de résidence du citoyen. Comme le réexamen du règlement eIDAS le montre dans une grande mesure, il est peu probable qu'une intervention nationale soit aussi efficace et efficiente.

- **Proportionnalité**

La présente initiative est proportionnée aux objectifs poursuivis et fournit un instrument approprié pour la mise en place de la structure d'interopérabilité nécessaire à la création d'un écosystème d'identité numérique de l'UE, fondé sur les identités juridiques délivrées par les États membres et sur la fourniture d'attributs d'identité numérique qualifiés et non qualifiés. Elle apporte une contribution claire à l'objectif consistant à améliorer le marché unique numérique grâce à un cadre juridique plus harmonisé. Les portefeuilles européens d'identité numérique harmonisés qui doivent être délivrés par les États membres sur la base de normes techniques communes prévoient également une approche commune de l'UE qui profite aux utilisateurs et aux parties s'appuient sur la disponibilité de solutions d'identité électronique transfrontalières sécurisées. La présente initiative vise à remédier aux limites de l'infrastructure actuelle d'interopérabilité en matière d'identification électronique fondée sur la reconnaissance mutuelle de divers schémas nationaux d'identification électronique. Compte tenu des objectifs fixés, la présente initiative est considérée comme étant suffisamment proportionnée et les coûts comme étant probablement proportionnés aux avantages potentiels. Le règlement proposé entraînera des coûts financiers et administratifs, qui devront être supportés par les États membres en leur qualité d'entités délivrant les portefeuilles européens d'identité numérique, par les prestataires de services de confiance et par les fournisseurs de services en ligne. Toutefois, ces coûts seraient probablement compensés par les avantages potentiels considérables pour les citoyens et les utilisateurs découlant directement de la reconnaissance et de l'acceptation transfrontalières accrues des services électroniques d'identité et d'attributs.

L'objectif de facilité d'utilisation et d'accessibilité ne pourra pas être atteint sans que les prestataires de services de confiance et les fournisseurs de services en ligne n'assument les coûts induits par la création de nouvelles normes et par la mise en conformité avec celles-ci. L'initiative vise à mettre à profit et à exploiter les investissements déjà réalisés par les États

membres dans leurs schémas d'identité nationaux respectifs. En outre, les coûts supplémentaires engendrés par la proposition, qui visent à soutenir l'harmonisation, sont justifiés par les perspectives à long terme de réduction de la charge administrative et des coûts de mise en conformité. Les coûts liés à l'acceptation, dans les secteurs réglementés, des attributs d'authentification de l'identité numérique peuvent également être considérés comme nécessaires et proportionnés, dans la mesure où ils soutiennent la réalisation de l'objectif général et fournissent les moyens par lesquels les secteurs réglementés peuvent remplir les obligations juridiques d'identifier légalement les utilisateurs.

- **Choix de l'instrument**

Le choix d'un règlement comme instrument juridique se justifie par la nécessité d'assurer des conditions uniformes dans le marché intérieur pour la mise en application de l'identité numérique européenne au moyen d'un cadre harmonisé qui vise à créer une interopérabilité homogène//fluide et à fournir aux citoyens européens et aux entreprises européennes, dans l'ensemble de l'Union, des services publics et privés grâce à des identifications électroniques hautement sécurisées et fiables.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Évaluations ex post/bilans de qualité de la législation existante**

Une évaluation du fonctionnement du règlement eIDAS a été réalisée dans le cadre du processus de réexamen imposé par l'article 49 dudit règlement. Les principales conclusions de l'évaluation en ce qui concerne l'identité électronique sont que le règlement eIDAS n'a pas atteint son potentiel. Seul un nombre limité de schémas d'identification électronique a été notifié, ce qui restreint la part de la population de l'UE couverte par un tel schéma notifié à environ 59 %. En outre, l'acceptation des schémas d'identification électronique notifiés est limitée, aussi bien au niveau des États membres que des prestataires de services. Il apparaît également que seuls quelques-uns des services accessibles par l'identification électronique nationale sont connectés à l'infrastructure nationale eIDAS. L'étude d'évaluation a également montré que le champ d'application actuel du règlement eIDAS et l'accent mis par ce texte sur les schémas d'identification électronique notifiés par les États membres de l'UE et sur l'accès aux services publics en ligne semblent trop limités et inadéquats. La grande majorité des besoins en matière d'identité électronique et d'authentification à distance s'observent dans le secteur privé, en particulier chez les acteurs de domaines comme la banque, les télécommunications et l'exploitation de plateformes, qui sont tenus par la loi de vérifier l'identité de leurs clients. La valeur ajoutée du règlement eIDAS en ce qui concerne l'identité électronique est limitée en raison de sa faible couverture et de son faible degré d'adoption et d'utilisation.

Les problèmes recensés dans la présente proposition sont liés aux lacunes du cadre eIDAS actuel et aux changements contextuels fondamentaux en ce qui concerne les marchés ainsi que les évolutions sociétales et technologiques, source de nouveaux besoins chez les utilisateurs et sur le marché.

- **Consultation des parties intéressées**

Une consultation publique ouverte a été lancée le 24 juillet 2020 et a pris fin le 2 octobre 2020. Au total, la Commission a reçu 318 contributions. La Commission a également reçu 106 réponses à une enquête ciblée auprès des parties prenantes. Des avis ont également été recueillis auprès des États membres lors de diverses réunions et enquêtes

bilatérales et multilatérales organisées depuis le début de l'année 2020. Citons notamment une enquête réalisée auprès des représentants des États membres du réseau de coopération eIDAS en juillet-août 2020, ainsi que divers ateliers spécialisés. La Commission a également mené des entretiens approfondis avec des représentants du secteur et rencontré des parties prenantes dans divers secteurs (commerce électronique, santé, services financiers, opérateurs de télécommunications, fabricants d'équipements, etc.) lors de réunions bilatérales.

Dans leur grande majorité, les participants à la consultation publique ouverte ont salué la création d'une identité numérique unique et universellement acceptée, s'appuyant sur les identités juridiques délivrées par les États membres. Les États membres soutiennent dans une large mesure la nécessité de renforcer le règlement eIDAS actuel, en donnant aux citoyens la possibilité d'accéder à des services tant publics que privés, et reconnaissent la nécessité d'établir un service de confiance permettant la délivrance et l'utilisation transfrontalière d'attestations électroniques d'attributs. Dans l'ensemble, les États membres ont souligné la nécessité d'instaurer en place un cadre européen relatif à une identité numérique reposant sur l'expérience acquise et les points forts des solutions nationales, en cherchant à trouver des synergies et en tirant parti des investissements réalisés. De nombreuses parties prenantes ont évoqué la manière dont la pandémie de COVID-19 avait démontré l'utilité de l'identification à distance sécurisée pour permettre à tous d'accéder à des services publics et privés. En ce qui concerne les services de confiance, la plupart des acteurs conviennent que le cadre actuel a été un succès, mais que certaines mesures supplémentaires s'imposent pour harmoniser davantage certaines pratiques liées à l'identification à distance et au contrôle dans les États membres. Les parties prenantes disposant d'une clientèle principalement nationale ont exprimé davantage de doutes quant à la valeur ajoutée d'un cadre européen relatif à une identité numérique.

Les portefeuilles d'identité numérique sont de plus en plus perçus par le secteur public et le secteur privé comme l'instrument le plus approprié pour permettre aux utilisateurs de choisir quand et avec quel prestataire de services privé ils souhaitent partager différents attributs, en fonction du cas d'utilisation et du degré de sécurité nécessaires à la transaction concernée. Les identités numériques fondées sur des portefeuilles numériques stockés de manière sécurisée sur des appareils mobiles ont été considérées comme un atout majeur pour une solution à l'épreuve du temps. Tant le marché privé (par exemple Apple, Google, Thales) que les pouvoirs publics s'engagent déjà dans cette voie.

- **Obtention et utilisation d'expertise**

La proposition se fonde sur les informations recueillies dans le cadre de la consultation des parties prenantes aux fins de l'analyse d'impact et de l'établissement des rapports d'évaluation du règlement eIDAS conformément aux obligations en matière de réexamen énoncées à l'article 49 dudit règlement. De nombreuses réunions ont été organisées avec des représentants des États membres et des experts.

- **Analyse d'impact**

Une analyse d'impact a été réalisée pour les besoins de la présente proposition. Le 19 mars 2021, le comité d'examen de la réglementation a émis un avis défavorable assorti d'observations. À la suite de la présentation d'une version révisée, il a rendu un avis favorable le 5 mai 2021.

La Commission étudie différentes options pour atteindre l'objectif général de la présente initiative, qui est d'assurer le bon fonctionnement du marché intérieur, en particulier en ce qui

concerne la fourniture et l'utilisation de solutions d'identité électronique hautement sécurisées et fiables.

Dans l'analyse d'impact sont examinés le scénario de référence, les options et les incidences pour les trois options envisagées. Chaque option correspond à un choix devant être examiné sur le plan politique et fondé sur le niveau d'ambition. La première option, qui présente un faible niveau d'ambition, prévoit un ensemble de mesures visant principalement à renforcer l'efficacité et l'efficience de l'actuel règlement eIDAS. En imposant la notification obligatoire des identifications électroniques nationales et en rationalisant les instruments existants mis à disposition pour parvenir à la reconnaissance mutuelle, la première option consiste à répondre aux besoins des citoyens en s'appuyant sur la disponibilité de divers schémas nationaux d'identification électronique, avec l'objectif de les rendre interopérables à terme.

La deuxième option présente un niveau d'ambition moyen et vise principalement à élargir les possibilités d'échange sécurisé de données liées à l'identité, en complétant les schémas d'identification électronique des pouvoirs publics et en soutenant la transition actuelle vers des services d'identité fondés sur des attributs. L'objectif de cette option aurait consisté à répondre à la demande des utilisateurs et à créer un nouveau service de confiance qualifié pour la fourniture d'attestations électroniques d'attributs qui soient liés à des sources fiables et opposables par-delà les frontières. Cette option aurait élargi le champ d'application du règlement eIDAS actuel et favorisé autant de cas d'utilisation que possible qui s'appuient sur la nécessité de vérifier les attributs d'identité liés à une personne avec un niveau élevé de garantie.

La troisième option a été privilégiée: elle présente le niveau d'ambition le plus élevé et vise à réglementer la fourniture d'un portefeuille d'identité numérique personnel hautement sécurisé délivré par les États membres. L'option privilégiée a été jugée appropriée pour atteindre le plus efficacement possible les objectifs de la présente initiative. Pour atteindre pleinement les objectifs d'action, l'option privilégiée s'appuie sur la plupart des mesures évaluées dans le cadre de la première option (recours à des identités juridiques attestées par les États membres et disponibilité de moyens d'identification électronique mutuellement reconnus) et de la deuxième option (attestations électroniques d'attributs juridiquement reconnus par-delà les frontières).

En ce qui concerne le cadre général de services de confiance, le niveau d'ambition exige un ensemble de mesures ne nécessitant pas d'approche par étapes pour atteindre les objectifs d'action.

Le nouveau service de confiance qualifié pour la gestion des dispositifs de création de signatures et de cachets électroniques à distance apporterait des avantages considérables du point de vue de la sécurité, de l'uniformité, de la sécurité juridique et des possibilités de choix pour les consommateurs, en ce qui concerne tant la certification des dispositifs de création de signatures qualifiés que les exigences auxquelles doivent satisfaire les prestataires de services de confiance qualifiés qui gèrent ces dispositifs. Les nouvelles dispositions renforceraient le cadre global de réglementation et de contrôle relatif à la fourniture de services de confiance.

Les incidences des options sur différentes catégories de parties prenantes sont expliquées en détail à l'annexe 3 de l'analyse d'impact produite à l'appui de la présente initiative. L'évaluation est à la fois quantitative et qualitative. L'analyse d'impact indique que les coûts minimaux quantifiables peuvent être estimés à au moins 3,2 milliards d'EUR, certains postes de coûts ne pouvant être quantifiés. Les bénéfices totaux quantifiables ont été estimés entre

3,9 milliards d'EUR et 9,6 milliards d'EUR. En ce qui concerne les incidences économiques plus larges, l'option privilégiée devrait avoir une incidence positive sur l'innovation, le commerce international et la compétitivité, contribuer à la croissance économique et générer des investissements supplémentaires dans des solutions d'identité numérique. Par exemple, un investissement supplémentaire de 500 millions d'EUR suscité par les modifications législatives prévues dans la troisième option devrait générer des bénéfices de 1 268 millions d'EUR au bout de dix ans (si on table sur un taux d'adoption de 67 %).

L'option privilégiée devrait également avoir une incidence positive sur l'emploi, par la création de 5 000 à 27 000 emplois supplémentaires au cours des cinq années qui suivront sa mise en œuvre. Cela s'explique par les investissements supplémentaires et la réduction des coûts pour les entreprises qui recourent à des solutions d'identification électronique.

La troisième option devrait avoir l'incidence la plus positive sur le plan environnemental, et elle devrait améliorer dans la plus large mesure possible l'adoption et la facilité d'utilisation de l'identification électronique, ce qui aura des incidences positives sur la réduction des émissions liées à la fourniture de services publics.

Les registres électroniques fournissent aux utilisateurs des preuves et une piste d'audit immuable pour le séquençage des transactions et des enregistrements de données, préservant ainsi l'intégrité des données. Bien que ce service de confiance n'ait pas fait partie de l'analyse d'impact, il capitalise sur les services de confiance existants car il combine l'horodatage et le séquençage des données à des garanties concernant l'initiateur des données, ce qui est semblable au processus de signature électronique. Ce service de confiance est nécessaire pour éviter la fragmentation du marché intérieur, en définissant un cadre paneuropéen unique permettant la reconnaissance transfrontalière des services de confiance qui soutiennent le fonctionnement des registres électroniques qualifiés. L'intégrité des données, quant à elle, est très importante pour la mise en commun de données provenant de sources décentralisées, pour les solutions d'identité autonomes, pour l'attribution de la propriété des actifs numériques, pour l'enregistrement des processus d'entreprise à des fins de vérification du respect des critères de durabilité et pour différents cas d'utilisation sur les marchés des capitaux.

- **Réglementation affûtée et simplification**

La présente proposition prévoit des mesures qui s'appliqueront aux pouvoirs publics, aux citoyens et aux prestataires de services en ligne. Elle réduira les coûts administratifs et les coûts de mise en conformité pour les administrations publiques ainsi que les coûts opérationnels et les dépenses liées à la sécurité pour les prestataires de services en ligne. Les citoyens réaliseront des économies grâce à l'allègement de la charge administrative, en tirant pleinement parti des moyens numériques d'identification et de la possibilité d'échanger facilement et en toute sécurité des attributs d'identité numérique ayant la même valeur juridique par-delà les frontières. Les fournisseurs de solutions d'identité électronique réaliseront également des économies sur les coûts de mise en conformité.

- **Droits fondamentaux**

Étant donné que les données à caractère personnel relèvent du champ d'application de certains éléments du règlement, les mesures sont conçues pour être pleinement conformes à la législation en matière de protection des données. Par exemple, la proposition améliore les possibilités de partage de données et de divulgation discrétionnaire. En utilisant le portefeuille européen d'identité numérique, l'utilisateur pourra exercer un contrôle sur la quantité de données fournies aux parties utilisatrices et être informé des attributs qui seront exigés pour la

fourniture d'un service particulier. Les prestataires de services devront informer les États membres de leur intention d'avoir recours à un portefeuille européen d'identité numérique, ce qui permettra aux États membres de contrôler que les demandes des prestataires de services portant sur des ensembles de données confidentielles, par exemple en rapport avec la santé, sont faites dans le respect du droit national.

4. INCIDENCE BUDGÉTAIRE

Dans le but d'atteindre de manière optimale les objectifs de la présente initiative, il est nécessaire de financer un certain nombre d'actions, tant au niveau de la Commission, à laquelle il est envisagé d'allouer environ 60 ETP (équivalents temps plein) au cours de la période 2022-2027, qu'au niveau des États membres par leur participation active aux groupes d'experts et aux comités chargés de travaux en rapport avec l'initiative, et qui sont constitués des représentants des États membres. Les ressources financières totales nécessaires à la mise en œuvre de la proposition au cours de la période 2022-2027 s'élèveront à 30,825 millions d'EUR, dont 8,825 millions d'EUR de frais administratifs et jusqu'à 22 millions d'EUR de dépenses opérationnelles couvertes par le programme pour une Europe numérique (qui doit encore faire l'objet d'un accord). Le financement soutiendra les coûts liés à la maintenance, à la mise au point, à l'hébergement, à l'exploitation et au soutien des éléments constitutifs de l'identification électronique et des services de confiance. Il pourra aussi soutenir des subventions pour la connexion des services à l'écosystème du portefeuille européen d'identité numérique, ainsi que l'élaboration de normes et de spécifications techniques. Enfin, le financement soutiendra également la réalisation d'enquêtes et d'études annuelles visant à évaluer l'efficacité et l'efficience du règlement dans la réalisation de ses objectifs. La «fiche financière» liée à la présente initiative donne un aperçu détaillé des coûts engagés.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

Les incidences feront l'objet d'un suivi et d'une évaluation conformément aux lignes directrices pour une meilleure réglementation qui couvrent la mise en œuvre et l'application du règlement proposé. Le dispositif de suivi constitue un volet important de la proposition, compte tenu notamment des lacunes du cadre actuel en matière d'établissement de rapports, constatées dans l'étude d'évaluation. Outre les exigences en matière de rapports introduites dans la proposition de règlement, qui visent à garantir une meilleure base de données et d'analyse, le cadre de suivi permettra de contrôler: 1) la mesure dans laquelle les modifications nécessaires ont été mises en œuvre conformément aux mesures adoptées; 2) si les modifications devant être apportées aux systèmes nationaux concernés ont été mises en œuvre; 3) si les modifications devant être apportées par les entités réglementées aux obligations de mise en conformité ont été respectées. La Commission européenne (points 1, 2 et 3) et les autorités nationales compétentes (points 2 et 3) seront chargées de la collecte des données sur la base d'indicateurs prédéfinis.

En ce qui concerne l'application de l'instrument proposé, la Commission européenne et les autorités nationales compétentes évalueront, au moyen d'enquêtes annuelles: 1) si tous les citoyens de l'UE ont accès à des moyens d'identification électronique; 2) l'amélioration de la reconnaissance et de l'acceptation transfrontalières des schémas d'identification électronique; 3) les mesures visant à stimuler l'adoption par le secteur privé de nouveaux services d'identité numérique et le développement de ceux-ci.

Des informations contextuelles seront recueillies par la Commission européenne au moyen d'enquêtes annuelles concernant: 1) la taille du marché des identités numériques; 2) les dépenses relatives aux marchés publics liées à l'identité numérique; 3) la part des entreprises fournissant leurs services en ligne; 4) la part des transactions en ligne nécessitant une identification forte du client; 5) la part des citoyens de l'UE utilisant des services publics et privés en ligne.

- **Explication détaillée de certaines dispositions de la proposition**

À son article 6 *bis*, le projet de règlement impose aux États membres de délivrer un portefeuille européen d'identité numérique, au titre d'un schéma d'identification électronique notifié, conçu selon des normes techniques communes, et à la suite d'une évaluation obligatoire de la conformité et d'une certification volontaire au sein du cadre européen de certification de cybersécurité, tel qu'établi par le règlement sur la cybersécurité. Il comprend des dispositions visant à faire en sorte que les personnes physiques et morales aient la possibilité de demander et d'obtenir, de stocker, de combiner et d'utiliser en toute sécurité des données d'identification personnelle et des attestations électroniques d'attributs pour s'authentifier en ligne et hors ligne, ainsi qu'à permettre l'accès aux biens et aux services en ligne publics et privés sous le contrôle de l'utilisateur. Cette certification est sans préjudice du RGPD en ce sens que les opérations de traitement de données à caractère personnel liées au portefeuille européen d'identité numérique ne peuvent être certifiées que selon les modalités prévues par les articles 42 et 43 du RGPD.

À son article 6 *ter*, la proposition énonce des dispositions spécifiques concernant les exigences applicables aux parties utilisatrices visant à prévenir la fraude et à garantir l'authentification des données d'identification personnelle et des attestations électroniques d'attributs provenant du portefeuille européen d'identité numérique.

Afin de mettre davantage de moyens d'identification électronique à disposition en vue d'une utilisation transfrontalière et d'améliorer l'efficacité du processus de reconnaissance mutuelle des schémas d'identification électronique notifiés, l'article 7 rend obligatoire la notification d'au moins un schéma d'identification électronique par les États membres. En outre, des dispositions visant à faciliter l'identification univoque sont ajoutées à l'article 11 *bis* afin de garantir l'identification univoque et constante des personnes physiques. Ces dispositions s'appliquent aux cas dans lesquels l'identification est requise par la loi, par exemple dans le domaine de la santé, dans le domaine financier, notamment aux fins des obligations en matière de lutte contre le blanchiment de capitaux, ou en vue d'une utilisation judiciaire. À cette fin, les États membres seront tenus d'inclure un identifiant univoque et constant dans l'ensemble minimal de données d'identification personnelle. La possibilité pour les États membres d'avoir recours à la certification pour assurer la conformité avec le règlement en lieu et place du processus d'évaluation par les pairs améliore l'efficacité de la reconnaissance mutuelle.

La section 3 présente de nouvelles dispositions relatives au recours transfrontalier au portefeuille européen d'identité numérique, afin que les utilisateurs puissent s'appuyer sur les portefeuilles européens d'identité numérique pour accéder à des services en ligne fournis par des organismes du secteur public et par des prestataires de services privés et nécessitant le recours à une authentification forte des utilisateurs.

Au chapitre III relatif aux services de confiance, l'article 14 sur les aspects internationaux est modifié afin de permettre à la Commission d'adopter des décisions d'exécution attestant l'équivalence des exigences appliquées aux prestataires de services de confiance établis dans

des pays tiers et aux services qu'ils fournissent, en plus d'avoir recours à des accords de reconnaissance mutuelle conclus conformément à l'article 218 du TFUE.

En ce qui concerne la disposition générale applicable aux services de confiance, y compris aux prestataires de services de confiance qualifiés, les articles 17, 18, 20, 21 et 24 sont modifiés afin d'être mis en adéquation avec les règles applicables à la sécurité des réseaux et de l'information dans l'UE. Pour ce qui est des méthodes devant être utilisées par les prestataires de services de confiance qualifiés pour vérifier l'identité des personnes physiques ou morales auxquelles les certificats qualifiés sont délivrés, les dispositions relatives à l'utilisation de moyens d'identification à distance ont été harmonisées et précisées afin de garantir l'application de règles identiques dans l'ensemble de l'UE.

Le chapitre III comporte un nouvel article 29 *bis* visant à définir les exigences applicables à un service qualifié de gestion des dispositifs de création de signatures électroniques à distance. Le nouveau service de confiance qualifié serait directement lié à des mesures répertoriées et évaluées dans l'analyse d'impact et s'appuierait sur celles-ci, notamment des mesures relatives à l'«harmonisation du processus de certification pour la signature électronique à distance» et d'autres mesures appelant à l'harmonisation des pratiques de contrôle des États membres.

Afin que les utilisateurs puissent identifier les administrateurs des sites internet, l'article 45 est modifié afin d'exiger des fournisseurs de navigateurs internet qu'ils facilitent l'utilisation de certificats qualifiés pour l'authentification de sites internet.

Le chapitre III comporte trois nouvelles sections.

La nouvelle section 9 insère des dispositions sur les effets juridiques des attestations électroniques d'attributs, sur l'utilisation de celles-ci dans des secteurs définis et sur les exigences applicables aux attestations qualifiées d'attributs. Afin de garantir un niveau élevé de confiance, une disposition relative à la vérification des attributs par rapport à des sources authentiques est insérée à l'article 45 *quinquies*. Afin de veiller à ce que les utilisateurs du portefeuille européen d'identité numérique puissent bénéficier de la disponibilité d'attestations électroniques d'attributs, et à ce que ces attestations soient délivrées dans le portefeuille européen d'identité numérique, une exigence est insérée à l'article 45 *sexies*. L'article 45 *septies* contient plutôt des règles supplémentaires régissant la fourniture de services d'attestation électronique d'attributs, y compris en matière de protection des données à caractère personnel.

La nouvelle section 10 autorise la fourniture de services qualifiés d'archivage électronique au niveau de l'UE. L'article 45 *octies* relatif aux services qualifiés d'archivage électronique complète les articles 34 et 40 concernant les services de conservation qualifiés pour les signatures électroniques qualifiées et les cachets électroniques qualifiés.

La nouvelle section 11 établit un cadre pour les services de confiance en ce qui concerne la création et la tenue de registres électroniques et de registres électroniques qualifiés. Les registres électroniques combinent l'horodatage et le séquençage des données à des garanties concernant l'initiateur, de manière analogue au processus de signature électronique, ce qui a pour avantage supplémentaire de permettre une gouvernance plus décentralisée adaptée à la coopération multipartite. Cet élément est important pour différents cas d'utilisation qui peuvent reposer sur des registres électroniques.

Les registres électroniques aident les entreprises à réduire leurs coûts en rendant la coordination multipartite plus efficace et plus sûre, et ils facilitent le contrôle réglementaire. En l'absence de réglementation européenne, les législateurs nationaux risquent de définir des normes nationales divergentes. Afin d'éviter la fragmentation, il est nécessaire de définir un

cadre paneuropéen unique qui permettra la reconnaissance transfrontalière des services de confiance qui contribuent au bon fonctionnement des registres électroniques. Cette norme paneuropéenne pour les opérateurs de nœuds s'appliquera par dérogation aux autres dispositions du droit dérivé de l'UE. Si des registres électroniques sont utilisés pour faciliter l'émission et/ou la négociation d'obligations, ou pour des crypto-actifs, ces cas d'utilisation devraient être compatibles avec toutes les règles financières applicables, par exemple avec la directive concernant les marchés d'instruments financiers[11], avec la directive concernant les services de paiement[12] et avec le futur règlement sur les marchés de crypto-actifs[13]. Lorsque les cas d'utilisation feront intervenir des données à caractère personnel, les prestataires de services devront respecter le RGPD.

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[14].

Enfin, le chapitre VI contient un nouvel article 48 *ter* qui vise à ce que des données statistiques sur l'utilisation du portefeuille européen d'identité numérique soient collectées en vue de contrôler l'efficacité du règlement modifié.

---

11 Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE, texte présentant de l'intérêt pour l'EEE (JO L 173 du 12.6.2014, p. 349).

12 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

13 Proposition de règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937, COM(2020) 593 final.

14 Gartner, «Blockchain Evolution», 2020.

2021/0136 (COD)

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[15],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) La communication de la Commission du 19 février 2020 intitulée «Façonner l'avenir numérique de l'Europe»[16] annonce une révision du règlement (UE) nº 910/2014 du Parlement européen et du Conseil en vue d'en améliorer l'efficacité, d'étendre ses avantages au secteur privé et de promouvoir une identité numérique fiable pour tous les Européens.

(2) Dans ses conclusions des 1er et 2 octobre 2020[17], le Conseil européen a invité la Commission à proposer la mise en place, à l'échelle de l'UE, d'un cadre pour une identification électronique publique sécurisée, y compris des signatures numériques interopérables, qui permette aux personnes d'exercer un contrôle sur leur identité et leurs données en ligne et donne accès à des services numériques publics, privés et transfrontaliers.

(3) La communication de la Commission du 9 mars 2021 intitulée «Une boussole numérique pour 2030: l'Europe balise la décennie numérique»[18] fixe l'objectif de mettre en place un cadre de l'UE qui, d'ici à 2030, devrait avoir conduit au déploiement à grande échelle d'une identité de confiance contrôlée par l'utilisateur, permettant à chaque citoyen d'avoir la maîtrise de ses propres interactions et de sa présence en ligne.

(4) Une approche plus harmonisée de l'identification numérique devrait réduire les risques et les coûts engendrés par la fragmentation actuelle due à l'utilisation de solutions nationales divergentes, et elle renforcera le marché unique en permettant aux citoyens, aux autres résidents au sens du droit national et aux entreprises de s'identifier en ligne de manière pratique et uniforme dans toute l'Union. Chacun devrait être en mesure d'accéder en toute sécurité aux services publics et privés en ayant recours à un

15 JO C […] du […], p. […].
16 COM(2020) 67 final.
17 https://www.consilium.europa.eu/media/45918/021020-euco-final-conclusions-fr.pdf
18 COM(2021) 118 final/2.

écosystème amélioré de services de confiance et à des preuves d'identité et des attestations d'attributs vérifiées, comme un diplôme universitaire légalement reconnu et accepté partout dans l'Union. Le cadre européen relatif à une identité numérique va permettre de passer d'un recours aux seules solutions nationales d'identité numérique à la fourniture d'attestations électroniques d'attributs valides à l'échelle européenne. Les fournisseurs d'attestations électroniques d'attributs devraient bénéficier d'un ensemble de règles clair et uniforme et les administrations publiques devraient pouvoir se fier à des documents électroniques dans un format donné.

(5) Pour soutenir la compétitivité des entreprises européennes, les prestataires de services en ligne devraient pouvoir utiliser des solutions d'identité numérique reconnues dans toute l'Union, indépendamment de l'État membre dans lequel elles ont été délivrées, et bénéficier ainsi d'une approche européenne harmonisée en matière de confiance, de sécurité et d'interopérabilité. Tant les utilisateurs que les prestataires de services devraient pouvoir bénéficier de la fourniture d'attestations électroniques d'attributs ayant la même valeur juridique dans l'ensemble de l'Union.

(6) Le règlement (UE) 2016/679[19] s'applique aux traitements de données à caractère personnel effectués en application du présent règlement. Par conséquent, le présent règlement devrait prévoir des garanties spécifiques pour empêcher les fournisseurs de moyens d'identification électronique et d'attestations électroniques d'attributs de combiner des données à caractère personnel provenant d'autres services avec des données à caractère personnel liées aux services relevant du champ d'application du présent règlement.

(7) Il est nécessaire de définir des conditions harmonisées pour l'établissement d'un cadre régissant les portefeuilles européens d'identité numérique devant être délivrés par les États membres, lesquels devraient permettre à tous les citoyens et aux autres résidents de l'Union, au sens du droit national, de partager de manière sécurisée les données relatives à leur identité d'une manière conviviale et pratique, sous le contrôle exclusif de l'utilisateur. Il convient de développer les technologies utilisées pour parvenir à ces objectifs de manière à atteindre le niveau le plus élevé de sécurité, de facilité d'utilisation et d'adoption. Les États membres devraient garantir à tous leurs ressortissants et résidents l'égalité d'accès à l'identification numérique.

(8) Afin de garantir le respect du droit de l'Union ou du droit national conforme au droit de l'Union, les prestataires de services devraient informer les États membres de leur intention d'avoir recours aux portefeuilles européens d'identité numérique. Cela permettra aux États membres de protéger les utilisateurs contre la fraude et d'empêcher l'utilisation illicite de données d'identité et d'attestations électroniques d'attributs, ainsi que de faire en sorte que le traitement de données confidentielles, telles que les données relatives à la santé, puisse être vérifié par les parties utilisatrices conformément au droit de l'Union ou au droit national.

(9) Tous les portefeuilles européens d'identité numérique devraient permettre aux utilisateurs de s'identifier et de s'authentifier par voie électronique en ligne et hors ligne, par-delà les frontières, en vue d'accéder à un large éventail de services publics et privés. Sans préjudice des prérogatives des États membres en ce qui concerne

[19] Règlement (UE) 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) (JO L 119 du 4.5.2016, p. 1).

l'identification de leurs ressortissants et résidents, les portefeuilles peuvent aussi répondre aux besoins institutionnels des administrations publiques, des organisations internationales et des institutions, organes et organismes de l'Union. L'utilisation hors ligne serait importante dans de nombreux secteurs, y compris dans le secteur de la santé, où les services sont souvent fournis par interaction directe et où la vérification de l'authenticité des prescriptions électroniques devrait pouvoir être effectuée à l'aide de codes QR ou de technologies similaires. En s'appuyant sur le niveau de garantie «élevé», les portefeuilles européens d'identité numérique devraient bénéficier du potentiel offert par des solutions infalsifiables, telles que des éléments sécurisés, pour se conformer aux exigences de sécurité prévues par le présent règlement. Les portefeuilles européens d'identité numérique devraient aussi permettre aux utilisateurs de créer et d'utiliser des signatures et cachets électroniques qualifiés qui sont acceptés dans toute l'UE. Afin de permettre à la population et aux entreprises de toute l'UE de bénéficier des avantages liés à la simplification et à la réduction des coûts, notamment en accordant des pouvoirs de représentation et des mandats électroniques, les États membres devraient délivrer des portefeuilles européens d'identité numérique reposant sur des normes communes afin de garantir leur pleine interopérabilité et un niveau élevé de sécurité. Seules les autorités compétentes des États membres peuvent établir l'identité d'une personne avec un niveau élevé de fiabilité et, partant, garantir que la personne revendiquant ou affirmant une identité particulière est effectivement la personne qu'elle prétend être. Il est donc nécessaire que les portefeuilles européens d'identité numérique reposent sur l'identité juridique des citoyens, autres résidents ou personnes morales. La confiance dans les portefeuilles européens d'identité numérique serait renforcée par le fait que les entités qui les délivrent sont tenues de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité proportionné aux risques présentés pour les droits et libertés des personnes physiques, conformément au règlement (UE) 2016/679.

(10) Afin d'atteindre un niveau élevé de sécurité et de fiabilité, le présent règlement établit les exigences applicables aux portefeuilles européens d'identité numérique. La conformité des portefeuilles européens d'identité numérique avec ces exigences devrait être certifiée par des organismes accrédités, du secteur public ou du secteur privé, désignés par les États membres. Le recours à un schéma de certification fondé sur la disponibilité de normes convenues d'un commun accord avec les États membres devrait garantir un niveau élevé de confiance et d'interopérabilité. La certification devrait notamment se fonder sur les schémas européens de certification de cybersécurité pertinents établis en application du règlement (UE) 2019/881[20]. Cette certification devrait être sans préjudice de la certification concernant le traitement des données à caractère personnel en application du règlement (UE) 2016/679.

(11) Les portefeuilles européens d'identité numérique devraient garantir le niveau de sécurité le plus élevé possible pour les données à caractère personnel utilisées pour l'authentification, que ces données soient stockées localement ou à l'aide de solutions en nuage, en tenant compte des différents niveaux de risque. Le recours à l'authentification biométrique est l'une des méthodes d'identification offrant un niveau de confiance élevé, en particulier lorsqu'elle est utilisée en combinaison avec

[20] 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) (JO L 151 du 7.6.2019, p. 15).

d'autres éléments d'authentification. Étant donné que les données biométriques représentent une caractéristique univoque d'une personne, leur utilisation exige des mesures organisationnelles et de sécurité proportionnées au risque que le traitement de ces données peut entraîner pour les droits et libertés des personnes physiques et conformément au règlement (UE) 2016/679.

(12) Afin de veiller à ce que le cadre européen relatif à une identité numérique soit ouvert à l'innovation, compatible avec les évolutions technologiques et capable de résister à l'épreuve du temps, les États membres devraient être encouragés à mettre en place conjointement des espaces d'expérimentation pour mettre à l'essai des solutions innovantes dans un environnement contrôlé et sécurisé, en particulier dans le but d'améliorer la fonctionnalité, la protection des données à caractère personnel, la sécurité et l'interopérabilité des solutions, et de servir de base aux futures mises à jour des références techniques et des exigences légales. Cet environnement devrait favoriser la participation des petites et moyennes entreprises européennes, des start-up et des innovateurs et chercheurs.

(13) Le règlement (UE) 2019/1157[21] renforce la sécurité des cartes d'identité par la mise en place d'éléments de sécurité renforcés d'ici au mois d'août 2021. Les États membres devraient envisager la possibilité de notifier ces cartes dans le cadre des schémas d'identification électronique afin d'étendre la disponibilité transfrontalière des moyens d'identification électronique.

(14) Le processus de notification des schémas d'identification électronique devrait être simplifié et accéléré afin de promouvoir l'accès à des solutions d'authentification et d'identification pratiques, fiables, sécurisées et innovantes et, le cas échéant, d'encourager les fournisseurs d'identité privés à proposer des schémas d'identification électronique aux autorités des États membres pour notification en tant que schémas nationaux de cartes d'identité électroniques au titre du règlement (UE) nº 910/2014.

(15) La rationalisation des procédures actuelles de notification et d'examen par les pairs empêchera les approches hétérogènes de l'évaluation des différents schémas d'identification électronique notifiés et facilitera l'instauration de la confiance entre les États membres. De nouveaux mécanismes simplifiés devraient favoriser la coopération entre les États membres en ce qui concerne la sécurité et l'interopérabilité de leurs schémas d'identification électronique notifiés.

(16) Les États membres devraient bénéficier de nouveaux outils souples pour ce qui est de garantir le respect des exigences du présent règlement et des actes d'exécution correspondants. Le présent règlement devrait permettre aux États membres d'utiliser les rapports et évaluations réalisés par des organismes d'évaluation de la conformité accrédités ou des schémas de certification volontaire de sécurité des TIC, tels que les schémas de certification à établir au niveau de l'Union en application du règlement (UE) 2019/881, afin d'étayer leurs demandes concernant l'alignement des schémas ou de certaines parties de ceux-ci sur les exigences du règlement concernant l'interopérabilité et la sécurité des schémas d'identification électronique notifiés.

(17) Les prestataires de services utilisent les données d'identité fournies par l'ensemble de données d'identification personnelle disponible dans le cadre des schémas

[21] 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 (JO L 188 du 12.7.2019, p. 67).

d'identification électronique prévus par le règlement (UE) nº 910/2014 afin d'établir une correspondance entre un utilisateur d'un autre État membre et son identité juridique. Toutefois, malgré l'utilisation de l'ensemble de données eIDAS, dans de nombreux cas, la garantie d'une réconciliation d'identités exacte requiert des informations supplémentaires concernant l'utilisateur et des procédures d'identification univoques spécifiques au niveau national. Afin de rendre encore plus facile l'utilisation des moyens d'identification électronique, le présent règlement devrait exiger des États membres qu'ils prennent des mesures spécifiques pour garantir une réconciliation d'identités correctes dans le processus d'identification électronique. Dans le même but, le présent règlement devrait aussi étendre l'ensemble de données minimal obligatoire et exiger l'utilisation d'un identifiant électronique univoque et persistant en conformité avec le droit de l'Union dans les cas où il est nécessaire d'identifier juridiquement l'utilisateur à sa demande d'une manière univoque et persistante.

(18) Conformément à la directive (UE) 2019/882[22], les personnes handicapées devraient pouvoir utiliser, dans les mêmes conditions que les autres utilisateurs, les portefeuilles européens d'identité numérique, les services de confiance et les produits destinés à un utilisateur final qui servent à fournir ces services.

(19) Le présent règlement ne devrait pas couvrir les aspects relatifs à la conclusion et à la validité des contrats ou autres obligations juridiques lorsque des exigences d'ordre formel sont établies par le droit national ou de l'Union. En outre, il ne devrait pas porter atteinte à des exigences d'ordre formel imposées au niveau national aux registres publics, notamment les registres du commerce et les registres fonciers.

(20) La fourniture et l'utilisation de services de confiance revêtent une importance croissante pour le commerce et la coopération sur le plan international. Les partenaires internationaux de l'UE mettent en place des cadres de confiance inspirés du règlement (UE) nº 910/2014. Par conséquent, afin de faciliter la reconnaissance de ces services et de leurs prestataires, les dispositions d'exécution peuvent fixer les conditions dans lesquelles les cadres de confiance de pays tiers pourraient être considérés comme équivalents au cadre de confiance pour les services de confiance qualifiés et leurs prestataires prévu par le présent règlement, en complément de la possibilité de reconnaissance mutuelle des services de confiance et des prestataires établis dans l'Union et dans les pays tiers conformément à l'article 218 du traité.

(21) Le présent règlement devrait s'appuyer sur la législation de l'Union relative aux marchés contestables et équitables dans le secteur numérique. En particulier, il repose sur le règlement XXX/XXXX [législation sur les marchés numériques], qui introduit des règles pour les fournisseurs de services de plateforme essentiels, désignés comme contrôleurs d'accès, interdisant notamment à ces derniers d'exiger des entreprises utilisatrices qu'elles utilisent, proposent ou interagissent avec un service d'identification du contrôleur d'accès dans le cadre des services qu'elles proposent en ayant recours aux services de plateforme essentiels de ce contrôleur d'accès. L'article 6, paragraphe 1, point f), du règlement XXX/XXXX [législation sur les marchés numériques] exige des contrôleurs d'accès qu'ils permettent aux entreprises utilisatrices et aux fournisseurs de services accessoires d'accéder aux mêmes fonctionnalités du système d'exploitation, du matériel informatique ou du logiciel que

[22] Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).

celles qui sont disponibles ou utilisées dans le cadre de la fourniture de tout service accessoire par le contrôleur d'accès, et d'interopérer avec ces fonctionnalités. Selon l'article 2, point 15, de la [législation sur les marchés numériques], les services d'identification constituent un type de services accessoires. Les entreprises utilisatrices et les fournisseurs de services accessoires devraient donc être en mesure d'accéder à certaines fonctionnalités du matériel informatique ou des logiciels, telles que les éléments sécurisés des téléphones intelligents, et d'interagir avec celles-ci par l'intermédiaire des portefeuilles européens d'identité numérique ou des moyens d'identification électronique notifiés par les États membres.

(22) Afin de rationaliser les obligations en matière de cybersécurité imposées aux prestataires de services de confiance et de permettre à ces prestataires et à leurs autorités compétentes respectives de bénéficier du cadre juridique établi par la directive XXXX/XXXX (directive SRI 2), les services de confiance sont tenus de prendre les mesures techniques et organisationnelles appropriées en vertu de la directive XXXX/XXXX (directive SRI 2), notamment des mesures visant à faire face aux défaillances du système, aux erreurs humaines, aux actions malveillantes ou aux phénomènes naturels, afin de gérer les risques pesant sur la sécurité des réseaux et des systèmes d'information utilisés par ces prestataires pour fournir leurs services, ainsi que de notifier les incidents importants et les cybermenaces conformément à la directive XXXX/XXXX (directive SRI 2). En ce qui concerne le signalement des incidents, les prestataires de services de confiance devraient notifier tout incident ayant un effet significatif sur la fourniture de leurs services, y compris les incidents causés par le vol ou la perte d'appareils, l'endommagement du câble réseau ou les incidents survenus dans le contexte de l'identification des personnes. Les exigences en matière de gestion des risques liés à la cybersécurité et les obligations en matière de communication d'informations prévues par la directive XXXX/XXXX [SRI 2] devraient être considérées comme étant complémentaires des exigences imposées aux prestataires de services de confiance en application du présent règlement. Le cas échéant, les autorités compétentes désignées en vertu de la directive XXXX/XXXX (directive SRI 2) devraient continuer à appliquer les pratiques ou orientations nationales établies en ce qui concerne la mise en œuvre des exigences en matière de sécurité et de communication d'informations et le contrôle du respect de ces exigences en vertu du règlement (UE) nº 910/2014. Les exigences prévues par le présent règlement ne portent pas atteinte à l'obligation de notification des violations de données à caractère personnel prévue par le règlement (UE) 2016/679.

(23) Une attention particulière devrait être accordée à l'efficacité de la coopération entre les autorités SRI et eIDAS. Lorsque l'organe de contrôle au titre du présent règlement est différent des autorités compétentes désignées au titre de la directive XXXX/XXXX [SRI 2], ces autorités devraient coopérer étroitement, en temps utile, en échangeant les informations pertinentes afin de garantir un contrôle efficace et le respect, par les prestataires de services de confiance, des exigences énoncées dans le présent règlement et dans la directive XXXX/XXXX [SRI 2]. En particulier, les organes de contrôle prévus par le présent règlement devraient être habilités à demander à l'autorité compétente au titre de la directive XXXXX/XXXX [SRI 2] de fournir les informations pertinentes nécessaires pour accorder le statut qualifié et de mener des actions de surveillance pour vérifier le respect, par les prestataires de services de confiance, des exigences pertinentes prévues par la directive SRI 2 ou pour leur demander de remédier aux manquements.

(24) Il est essentiel de prévoir un cadre juridique en vue de faciliter la reconnaissance transfrontalière entre les systèmes juridiques nationaux existants en matière de services d'envoi recommandé électronique. Ce cadre pourrait également ouvrir aux prestataires de services de confiance de l'Union de nouveaux débouchés commerciaux leur permettant de proposer de nouveaux services paneuropéens d'envoi recommandé électronique et de veiller à ce que l'identification des destinataires soit assurée avec un niveau de confiance plus élevé que l'identification de l'expéditeur.

(25) Dans la plupart des cas, les citoyens et les autres résidents ne peuvent pas échanger, par voie numérique et par-delà les frontières, des informations relatives à leur identité, telles que leur adresse, leur âge et leurs qualifications professionnelles, permis de conduire et autres licences et données de paiement, en toute sécurité et avec un niveau élevé de protection des données.

(26) Il devrait être possible de délivrer et de traiter des attributs numériques fiables et de contribuer à réduire la charge administrative, en donnant aux citoyens et aux autres résidents les moyens de les utiliser dans le cadre de leurs transactions privées et publiques. Les citoyens et les autres résidents devraient, par exemple, être en mesure de prouver qu'ils détiennent un permis de conduire en cours de validité délivré par une autorité d'un État membre et les autorités compétentes d'autres États membres devraient pouvoir le vérifier et s'y fier. Ils devraient aussi pouvoir avoir recours à leurs justificatifs de sécurité sociale ou à de futurs documents de voyage numériques dans un contexte transfrontalier.

(27) Toute entité qui collecte, crée et délivre des attributs attestés tels que des diplômes, permis et certificats de naissance devrait pouvoir devenir fournisseur d'attestations électroniques d'attributs. Les parties utilisatrices devraient utiliser les attestations électroniques d'attributs comme des équivalents aux attestations sur papier. Par conséquent, une attestation électronique d'attributs ne devrait pas se voir refuser un effet juridique au motif qu'elle se présente sous une forme électronique ou qu'elle ne satisfait pas à toutes les exigences de l'attestation électronique qualifiée d'attributs. À cet effet, il convient d'établir des exigences générales visant à garantir qu'une attestation électronique qualifiée d'attributs a un effet juridique équivalent à celui des attestations délivrées légalement sur papier. Toutefois, ces exigences devraient s'appliquer sans préjudice du droit de l'Union ou du droit national définissant des exigences sectorielles particulières supplémentaires en ce qui concerne la forme ayant des effets juridiques sous-jacents et, en particulier, la reconnaissance transfrontalière des attestations électroniques qualifiées d'attributs, le cas échéant.

(28) La large disponibilité et la facilité d'utilisation des portefeuilles européens d'identité numérique dépendent de l'acceptation de ceux-ci par les prestataires de services privés. Les parties utilisatrices privées qui fournissent des services dans les domaines des transports, de l'énergie, des services bancaires et financiers, de la sécurité sociale, de la santé, de l'eau potable, des services postaux, des infrastructures numériques, de l'éducation ou des télécommunications devraient accepter l'utilisation de portefeuilles européens d'identité numérique pour la fourniture de services lorsque le droit national ou de l'Union ou une obligation contractuelle exigent une authentification forte des utilisateurs à des fins d'identification en ligne. Lorsque de très grandes plateformes en ligne au sens de l'article 25, paragraphe 1, du règlement [référence du règlement sur les services numériques] exigent des utilisateurs qu'ils s'authentifient pour accéder à des services en ligne, ces plateformes devraient être tenues d'accepter l'utilisation de portefeuilles européens d'identité numérique à la demande volontaire de l'utilisateur. Les utilisateurs ne devraient pas être tenus d'utiliser le portefeuille pour accéder à des

services privés, mais, lorsque l'utilisateur le souhaite, les très grandes plateformes en ligne devraient accepter que le portefeuille européen d'identité numérique soit utilisé à cette fin, dans le respect du principe de minimisation des données. Cela est nécessaire, eu égard à l'importance des très grandes plateformes en ligne et de leur audience, exprimée notamment en nombre de destinataires du service et de transactions économiques, pour renforcer la protection des utilisateurs contre la fraude et garantir un niveau élevé de protection des données. Il convient d'élaborer des codes de conduite d'autorégulation au niveau de l'Union (ci-après dénommés «codes de conduite») afin de contribuer à la grande disponibilité et à la facilité d'utilisation des moyens d'identification électronique, notamment des portefeuilles européens d'identité numérique relevant du champ d'application du présent règlement. Les codes de conduite devraient faciliter une large acceptation des moyens d'identification électronique, y compris des portefeuilles européens d'identité numérique, par les prestataires de services qui ne sont pas considérés comme de très grandes plateformes et qui ont recours à des services d'identification électronique tiers pour l'authentification des utilisateurs. Ils devraient être élaborés dans un délai de douze mois à compter de l'adoption du présent règlement. La Commission devrait évaluer l'efficacité de ces dispositions en ce qui concerne la disponibilité et la facilité d'utilisation des portefeuilles européens d'identité numérique au bout de dix-huit mois de déploiement, et réviser ensuite les dispositions afin de garantir leur acceptation par voie d'actes délégués à la lumière de cette évaluation.

(29) Les portefeuilles européens d'identité numérique devraient permettre, sur le plan technique, la divulgation sélective des attributs aux parties utilisatrices. Cette fonctionnalité devrait devenir un élément de conception de base, renforçant ainsi la commodité du service et la protection des données à caractère personnel, notamment s'agissant de la minimisation du traitement des données à caractère personnel.

(30) Les attributs fournis par les prestataires de services de confiance qualifiés dans le cadre d'une attestation d'attributs qualifiée devraient faire l'objet d'une vérification par rapport aux sources authentiques, effectuée soit directement par le prestataire de services de confiance qualifié, soit par des intermédiaires désignés reconnus au niveau national conformément au droit national ou au droit de l'Union, aux fins de l'échange sécurisé d'attributs attestés entre les prestataires de services de confiance et les parties utilisatrices.

(31) L'identification électronique sécurisée et la fourniture d'attestations d'attributs devraient offrir davantage de souplesse et de solutions au secteur des services financiers en ce qui concerne l'identification des clients et l'échange des attributs spécifiques nécessaires pour respecter, par exemple, les exigences de vigilance à l'égard de la clientèle prévues par la réglementation relative à la lutte contre le blanchiment de capitaux [référence à ajouter après l'adoption de la proposition] et les exigences en matière d'adéquation découlant de la législation sur la protection des investisseurs, ou pour permettre le respect d'exigences en matière d'authentification forte du client à des fins d'ouverture de session et d'exécution de transactions dans le domaine des services de paiement.

(32) Les services d'authentification de site internet permettent aux utilisateurs d'un site internet de s'assurer que celui-ci est présenté par une entité véritable et légitime. Ces services contribuent à instaurer un climat de confiance pour la réalisation de transactions commerciales en ligne, les utilisateurs tendant à se fier à un site internet qui a été authentifié. L'utilisation de services d'authentification de sites internet par les sites internet est facultative. Cependant, pour que l'authentification de site internet

s'affirme comme un moyen de renforcer la confiance, d'améliorer l'expérience de l'utilisateur et de favoriser la croissance dans le marché intérieur, le présent règlement impose aux prestataires de services d'authentification de sites internet et à leurs services des obligations minimales de sécurité et de responsabilité. À cette fin, les navigateurs internet devraient veiller à assurer la compatibilité et l'interopérabilité avec les certificats qualifiés d'authentification de site internet, conformément au règlement (UE) nº 910/2014. Ils devraient reconnaître et afficher les certificats qualifiés d'authentification de site internet afin d'offrir un niveau élevé de garantie, permettant aux propriétaires de sites internet de déclarer leur identité de propriétaire d'un site internet et aux utilisateurs d'identifier les propriétaires de sites internet avec un degré élevé de certitude. Afin de promouvoir davantage l'utilisation des certificats qualifiés d'authentification de site internet, les autorités publiques des États membres devraient envisager d'intégrer ces certificats à leurs sites internet.

(33) De nombreux États membres ont introduit des exigences nationales pour les services fournissant un archivage numérique sécurisé et fiable visant à permettre la conservation à long terme des documents électroniques et des services de confiance associés. Pour garantir la sécurité juridique et la confiance, il est essentiel de fournir un cadre juridique pour faciliter la reconnaissance transfrontalière des services qualifiés d'archivage électronique. Ce cadre pourrait également ouvrir de nouveaux débouchés aux prestataires de services de confiance de l'Union.

(34) Les registres électroniques qualifiés enregistrent les données de manière à garantir l'unicité, l'authenticité et le séquençage correct des données fournies et à les rendre infalsifiables. Les registres électroniques combinent les effets de l'horodatage des données à une garantie concernant le créateur des données, à l'instar des processus de signature électronique, et présentent l'avantage supplémentaire de permettre des modèles de gouvernance plus décentralisés adaptés aux coopérations multipartites. Par exemple, ils créent une piste d'audit fiable pour la provenance des matières premières dans les échanges transfrontaliers, soutiennent la protection des droits de propriété intellectuelle, permettent une plus grande adaptabilité des marchés de l'électricité, sont à la base de solutions d'identité autonomes avancées, et soutiennent des services publics plus efficaces et plus transformateurs. Afin d'éviter la fragmentation du marché intérieur, il importe de définir un cadre juridique paneuropéen qui permette la reconnaissance transfrontalière de services de confiance pour l'enregistrement des données dans les registres électroniques.

(35) La certification en tant que prestataires de services de confiance qualifiés devrait apporter une sécurité juridique aux cas d'utilisation fondés sur des registres électroniques. Ce service de confiance pour les registres électroniques et les registres électroniques qualifiés, ainsi que la certification de prestataire de services de confiance qualifiés pour les registres électroniques, devraient être sans préjudice de l'obligation, pour les cas d'utilisation, de respecter le droit de l'Union ou le droit national conforme au droit de l'Union. Les cas d'utilisation nécessitant le traitement de données à caractère personnel doivent être conformes au règlement (UE) 2016/679. Les cas d'utilisation concernant des crypto-actifs devraient être compatibles avec toutes les règles financières applicables, par exemple avec la directive concernant les marchés

d'instruments financiers[23], la directive concernant les services de paiement[24] et le futur règlement sur les marchés de crypto-actifs[25].

(36) Afin d'éviter la fragmentation et les obstacles dus à des normes et restrictions techniques divergentes, et d'assurer un processus coordonné pour éviter de compromettre la mise en œuvre du futur cadre européen relatif à une identité numérique, il y a lieu d'instaurer un processus de coopération étroite et structurée entre la Commission, les États membres et le secteur privé. Pour atteindre cet objectif, les États membres devraient coopérer dans le cadre défini dans la recommandation XXX/XXXX de la Commission [Boîte à outils pour une approche coordonnée en vue d'un cadre européen relatif à une identité numérique][26] afin de définir une boîte à outils pour un cadre européen relatif à une identité numérique. La boîte à outils devrait comprendre une architecture technique et un cadre de référence complets, un ensemble de normes communes et de références techniques et un ensemble de lignes directrices et de descriptions des meilleures pratiques couvrant au moins tous les aspects des fonctionnalités et de l'interopérabilité des portefeuilles européens d'identité numérique, y compris les signatures électroniques, ainsi que du service de confiance qualifié pour l'attestation d'attributs prévu par le présent règlement. Dans ce contexte, les États membres devraient également parvenir à un accord sur les éléments communs d'un modèle économique et d'une structure tarifaire pour les portefeuilles européens d'identité numérique, afin de faciliter leur adoption, en particulier par les petites et moyennes entreprises dans un contexte transfrontalier. Le contenu de la boîte à outils devrait continuer à évoluer parallèlement au débat et au processus d'adoption du cadre européen relatif à une identité numérique et tenir compte de leurs résultats.

(37) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1525 du Parlement européen et du Conseil[27].

(38) Il convient dès lors de modifier le règlement (UE) nº 910/2014 en conséquence,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Le règlement (UE) 910/2014 est modifié comme suit:

(1) L'article 1er est remplacé par le texte suivant:

---

23 Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE, texte présentant de l'intérêt pour l'EEE (JO L 173 du 12.6.2014, p. 349–496).

24 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35–127).

25 Proposition de règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937, COM(2020) 593 final.

26 [insérer référence après adoption].

27 Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

«Le présent règlement vise à assurer le bon fonctionnement du marché intérieur et à offrir un niveau adéquat de sécurité des moyens d'identification électronique et des services de confiance. Pour ce faire, le présent règlement:

(a) fixe les conditions dans lesquelles un État membre fournit et reconnaît les moyens d'identification électronique des personnes physiques et morales qui relèvent d'un schéma d'identification électronique notifié d'un autre État membre;

(b) établit des règles applicables aux services de confiance, en particulier pour les transactions électroniques;

(c) instaure un cadre juridique régissant les signatures électroniques, les cachets électroniques, les horodatages électroniques, les documents électroniques, les services d'envoi recommandé électronique, les services de certificats pour l'authentification de site internet, l'archivage électronique et l'attestation électronique d'attributs, la gestion des dispositifs de création de signature électronique et de cachet électronique à distance, et les registres électroniques;

(d) fixe les conditions de délivrance, par les États membres, des portefeuilles européens d'identité numérique.»;

(2) l'article 2 est modifié comme suit:

(a) le paragraphe 1 est remplacé par le texte suivant:

«1. Le présent règlement s'applique aux schémas d'identification électronique qui ont été notifiés par un État membre, aux portefeuilles européens d'identité numérique délivrés par les États membres et aux prestataires de services de confiance établis dans l'Union.»;

(b) le paragraphe 3 est remplacé par le texte suivant:

«3. Le présent règlement ne porte pas atteinte au droit national ou de l'Union relatif à la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales concernant des exigences sectorielles d'ordre formel et les effets juridiques qui y sont attachés.»;

(3) l'article 3 est modifié comme suit:

(a) le point 2. est remplacé par le texte suivant:

«2. "moyen d'identification électronique", un élément matériel et/ou immatériel, y compris les portefeuilles européens d'identité numérique ou les cartes d'identité suivant le règlement 2019/1157, qui contient des données d'identification personnelle et est utilisé pour s'authentifier sur un service en ligne ou hors ligne;»;

(b) le point 4. est remplacé par le texte suivant:

«4. "schéma d'identification électronique", un système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales ou à des personnes physiques représentant des personnes morales;»;

(c) le point 14. est remplacé par le texte suivant:

«14. "certificat de signature électronique", une attestation électronique ou un ensemble d'attestations qui associe les données de validation d'une

signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne;»;

(d) le point 16. est remplacé par le texte suivant:

«16. "service de confiance", un service électronique normalement fourni contre paiement qui consiste:

(a) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique, de l'attestation électronique d'attributs et des certificats relatifs à ces services;

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

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

(d) en l'archivage électronique de documents électroniques;

(e) en la gestion des dispositifs de création de signature électronique et de cachet électronique à distance;

(f) en l'enregistrement de données électroniques dans un registre électronique.»;

(e) le point 21. est remplacé par le texte suivant:

«21. "produit", un dispositif matériel ou logiciel, ou les composants correspondants du dispositif matériel et / ou logiciel, qui sont destinés à être utilisés pour la fourniture de services d'identification électronique et de services de confiance;»;

(f) les points 23. *bis* et 23. *ter* suivants sont insérés:

«23. *bis*. "dispositif de création de signature électronique qualifié à distance", un dispositif de création de signature électronique qualifié par lequel un prestataire de services de confiance qualifié génère, gère ou reproduit les données de création de signature électronique pour le compte d'un signataire;

23. *ter*. "dispositif de création de cachet électronique qualifié à distance", un dispositif de création de cachet électronique qualifié par lequel un prestataire de services de confiance qualifié génère, gère ou reproduit les données de création de cachet électronique pour le compte d'un créateur de cachet;»;

(g) le point 29. est remplacé par le texte suivant:

«29. "certificat de cachet électronique", une attestation électronique ou un ensemble d'attestations qui associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne;»;

(h) le point 41. est remplacé par le texte suivant:

«41. "validation", le processus de vérification et de confirmation de la validité d'une signature ou d'un cachet électronique, des données

d'identification personnelle ou encore d'une attestation électronique d'attributs;»

(i) les points 42. à 55. suivants sont ajoutés:

«42. "portefeuille européen d'identité numérique", un produit et un service qui permettent à l'utilisateur de stocker des données d'identification, des justificatifs et des attributs liés à son identité, de les communiquer aux parties utilisatrices sur demande et de les utiliser pour s'authentifier, en ligne et hors ligne, sur un service conformément à l'article 6 *bis*; et de créer des signatures et cachets électroniques qualifiés;

43. "attribut", une particularité, une caractéristique ou une qualité d'une personne physique ou morale ou d'une entité, sous forme électronique;

44. "attestation électronique d'attributs", une attestation sous forme électronique qui permet l'authentification d'attributs;

45. "attestation électronique qualifiée d'attributs", une attestation électronique d'attributs, qui est délivrée par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe V;

46. "source authentique", 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 première de ces informations ou est reconnu comme authentique en droit national;

47. "archivage électronique", un service assurant la réception, le stockage, la suppression et la transmission de données ou documents électroniques afin de garantir leur intégrité, l'exactitude de leur origine et leurs particularités juridiques pendant toute la durée de leur conservation;

48. "service qualifié d'archivage électronique", un service qui satisfait aux exigences prévues à l'article 45 *octies*;

49. "label de confiance de l'UE pour le portefeuille d'identité numérique", une indication formulée d'une manière simple, claire et reconnaissable selon laquelle un portefeuille d'identité numérique a été délivré conformément au présent règlement;

50. "authentification forte de l'utilisateur", une authentification reposant sur l'utilisation d'au moins deux éléments qui appartiennent aux catégories 'connaissance de l'utilisateur', 'possession' et 'inhérence' et qui sont indépendants, de manière à ce que la compromission de l'un ne remette pas en question la fiabilité des autres, et qui est conçue de façon à protéger la confidentialité des données d'authentification;

51. "compte d'utilisateur", un mécanisme qui permet à un utilisateur d'avoir accès à des services publics ou privés selon les modalités et conditions définies par le prestataire de services;

52. "justificatif", la preuve des aptitudes d'une personne, de son expérience, de son droit ou de son autorisation;

53. “registre électronique”, un enregistrement électronique inviolable de données, assurant l’authenticité et l’intégrité des données qu’il contient, l’exactitude de la date et de l’heure de ces données ainsi que de leur classement chronologique»;

54. “données à caractère personnel”, toute information telle qu’elle est définie à l’article 4, point 1), du règlement (UE) 2016/679.»;

55. “identification univoque”, un processus selon lequel les données d’identification personnelle ou les moyens d’identification personnelle sont mis en correspondance avec un compte existant appartenant à la même personne ou sont reliés à celui-ci.»;

(4) L’article 5 est remplacé par le texte suivant:

«*Article 5*

Pseudonymes utilisés dans les transactions électroniques

Sans préjudice de l’effet juridique donné aux pseudonymes en droit national, l’utilisation de pseudonymes dans les transactions électroniques n’est pas interdite.»;

(5) au chapitre II, l’intitulé est remplacé par le texte suivant:

«SECTION I

IDENTIFICATION ÉLECTRONIQUE»;

(6) l’article 6 est supprimé;

(7) les articles suivants (6 *bis*, 6 *ter*, 6 *quater* et 6 *quinquies*) sont insérés:

«*Article 6 bis*

Portefeuilles européens d’identité numérique

1. Afin de garantir à toutes les personnes physiques et morales dans l’Union un accès sécurisé, fiable et continu à des services publics et privés transfrontaliers, chaque État membre délivre un portefeuille européen d’identité numérique dans un délai de 12 mois à compter de l’entrée en vigueur du présent règlement.

2. Les portefeuilles européens d’identité numérique sont délivrés:

   (a) par un État membre;

   (b) sur mandat d’un État membre;

   (c) indépendamment d’un État membre mais sont reconnus par ce dernier.

3. Les portefeuilles européens d’identité numérique permettent à l’utilisateur:

   (a) de demander et d’obtenir, de stocker, de sélectionner, de combiner et de partager en toute sécurité, d’une manière qui soit transparente pour l’utilisateur et traçable par ce dernier, les données légales nécessaires d’identification personnelle et l’attestation électronique d’attributs pour s’authentifier en ligne et hors ligne en vue d’utiliser des services publics et privés en ligne;

   (b) de signer au moyen de signatures électroniques qualifiées.

4. En particulier, les portefeuilles européens d’identité numérique:

   (a) offrent une interface commune:

(1) aux prestataires de services de confiance qualifiés et non qualifiés qui délivrent des attestations électroniques qualifiées et non qualifiées d'attributs ou d'autres certificats qualifiés et non qualifiés aux fins de la délivrance de ces attestations et certificats au portefeuille européen d'identité numérique;

(2) pour permettre aux parties utilisatrices de demander et de valider des données d'identification personnelle et des attestations électroniques d'attributs;

(3) pour la présentation aux parties utilisatrices de données d'identification personnelle, de l'attestation électronique d'attributs ou d'autres données telles que des justificatifs, en mode local ne nécessitant pas d'accès à l'internet pour le portefeuille;

(4) pour que l'utilisateur autorise une interaction avec le portefeuille européen d'identité numérique et affiche un "label de confiance de l'UE pour le portefeuille européen d'identité numérique";

(b) font en sorte que les prestataires de services de confiance d'attestations qualifiées d'attributs ne puissent pas recevoir d'informations concernant l'utilisation de ces attributs;

(c) satisfont aux exigences énoncées à l'article 8 quant au niveau de garantie "élevé", tel qu'il est appliqué en particulier aux exigences concernant la preuve et la vérification d'identité, et à la gestion des moyens d'identification électronique et à l'authentification;

(d) fournissent un mécanisme permettant de faire en sorte que la partie utilisatrice puisse authentifier l'utilisateur et recevoir des attestations électroniques d'attributs;

(e) font en sorte que les données d'identification personnelle visées à l'article 12, paragraphe 4, point d), représentent de manière univoque et constante la personne physique ou morale qui y est associée.

5. Les États membres fournissent des mécanismes de validation pour les portefeuilles européens d'identité numérique:

(a) pour veiller à ce que leur authenticité et leur validité puissent être vérifiées;

(b) pour permettre aux parties utilisatrices de vérifier la validité des attestations d'attributs;

(c) pour permettre aux parties utilisatrices et aux prestataires de services de confiance qualifiés de vérifier l'authenticité et la validité des données d'identification personnelle attribuées.

6. Les portefeuilles européens d'identité numérique sont délivrés dans le cadre d'un schéma d'identification électronique notifié de niveau de garantie "élevé". L'utilisation des portefeuilles européens d'identité numérique est gratuite pour les personnes physiques.

7. L'utilisateur exerce un contrôle total sur le portefeuille européen d'identité numérique. L'entité qui délivre le portefeuille européen d'identité numérique ne collecte pas les informations sur l'utilisation du portefeuille qui ne sont pas nécessaires à la fourniture des services qui y sont attachés; elle ne combine pas

non plus des données d'identification personnelle et d'autres données à caractère personnel stockées ou relatives à l'utilisation du portefeuille européen d'identité numérique avec des données à caractère personnel provenant de tout autre service offert par cette entité ou de services tiers qui ne sont pas nécessaires à la fourniture des services attachés au portefeuille, à moins que l'utilisateur n'en ait fait expressément la demande. Les données à caractère personnel relatives à la fourniture des portefeuilles européens d'identité numérique sont maintenues séparées, de manière physique et logique, de toute autre donnée détenue. Si le portefeuille européen d'identité numérique est fourni par des parties privées conformément au paragraphe 1, points b) et c), les dispositions de l'article 45 *septies*, paragraphe 4, s'appliquent mutatis mutandis.

8. L'article 11 s'applique mutatis mutandis au portefeuille européen d'identité numérique.

9. L'article 24, paragraphe 2, points b), e), g) et h), s'applique mutatis mutandis aux États membres qui délivrent les portefeuilles européens d'identité numérique.

10. Le portefeuille européen d'identité numérique est accessible aux personnes handicapées, conformément aux exigences en matière d'accessibilité énoncées à l'annexe I de la directive 2019/882.

11. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission définit les spécifications techniques et opérationnelles ainsi que les normes de référence applicables aux exigences visées aux paragraphes 3, 4 et 5 au moyen d'un acte d'exécution relatif à la mise en œuvre du portefeuille européen d'identité numérique. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 6 ter

Parties utilisatrices de portefeuilles européens d'identité numérique

1. Lorsque les parties utilisatrices ont l'intention d'avoir recours à des portefeuilles européens d'identité numérique délivrés en conformité avec le présent règlement, elles en informent l'État membre sur le territoire duquel elles sont établies afin d'assurer le respect des exigences prévues en droit de l'Union ou en droit national pour la fourniture de services particuliers. Lorsqu'elles font part de leur intention de recourir à des portefeuilles européens d'identité numérique, elles précisent également l'utilisation qu'elles prévoient d'en faire.

2. Les États membres mettent en œuvre un mécanisme commun d'authentification des parties utilisatrices.

3. Les parties utilisatrices sont chargées d'effectuer la procédure d'authentification des données d'identification personnelle et de l'attestation électronique d'attributs provenant des portefeuilles européens d'identité numérique.

4. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission établit des spécifications techniques et opérationnelles applicables aux exigences visées aux paragraphes 1 et 2 au

moyen d'un acte d'exécution relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi qu'il est prévu à l'article 6 *bis*, paragraphe 10.

Article 6 ter

Certification des portefeuilles européens d'identité numérique

1. Les portefeuilles européens d'identité numérique qui ont été certifiés ou pour lesquels une déclaration de conformité a été délivrée dans le cadre d'un schéma de cybersécurité en application du règlement (UE) 2019/881 et dont les références ont été publiées au *Journal officiel de l'Union européenne* sont présumés conformes aux exigences pertinentes en matière de cybersécurité énoncées à l'article 6 *bis*, paragraphes 3, 4 et 5, pour autant que le certificat de cybersécurité ou la déclaration de conformité ou des éléments de l'un ou de l'autre couvrent ces exigences.

2. La conformité aux exigences énoncées à l'article 6 *bis*, paragraphes 3, 4 et 5, relatives aux opérations de traitement de données à caractère personnel effectuées par l'entité qui délivre les portefeuilles européens d'identité numérique est certifiée selon les modalités prévues par le règlement (UE) 2016/679.

3. La conformité des portefeuilles européens d'identité numérique aux exigences énoncées à l'article 6 *bis*, paragraphes 3, 4 et 5, est certifiée par les organismes accrédités, publics ou privés, désignés par les États membres.

4. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission dresse, par voie d'actes d'exécution, une liste des normes de certification des portefeuilles européens d'identité numérique visée au paragraphe 3.

5. Les États membres communiquent à la Commission le nom et l'adresse des organismes publics ou privés visés au paragraphe 3. La Commission met ces informations à la disposition des États membres.

6. La Commission est habilitée à adopter des actes délégués, conformément à l'article 47, en ce qui concerne la définition de critères spécifiques que doivent respecter les organismes désignés visés au paragraphe 3.

Article 6 quinquies

Publication d'une liste des portefeuilles européens d'identité numérique certifiés

1. Les États membres informent la Commission dans les meilleurs délais des portefeuilles européens d'identité numérique qui ont été délivrés en application de l'article 6 *bis* et certifiés par les organismes visés à l'article 6 *quater*, paragraphe 3. Ils informent également la Commission, dans les meilleurs délais, de l'annulation de la certification.

2. Sur la base des informations reçues, la Commission établit, publie et met à jour une liste des portefeuilles européens d'identité numérique certifiés.

3. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission définit les formats et procédures applicables aux fins du paragraphe 1 au moyen d'un acte d'exécution relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi qu'il est indiqué à l'article 6 *bis*, paragraphe 10.»

(8) l'intitulé suivant est inséré avant l'article 7:

«SECTION II

SCHÉMAS D'IDENTIFICATION ÉLECTRONIQUE»;

(9) À l'article 7, la phrase introductive est remplacée par le texte suivant:

«En application de l'article 9, paragraphe 1, les États membres notifient, dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, au moins un schéma d'identification électronique comprenant au moins un moyen d'identification:»;

(10) à l'article 9, les paragraphes 2 et 3 sont remplacés par le texte suivant:

«2. La Commission publie au *Journal officiel de l'Union européenne* la liste des schémas d'identification électronique qui ont été notifiés par application du paragraphe 1 du présent article, et les informations essentielles à leur sujet.

3. La Commission publie au *Journal officiel de l'Union européenne* les modifications apportées à la liste prévue au paragraphe 2 dans un délai d'un mois à compter de la date de réception de cette notification.»;

(11) L'article 10 *bis* suivant est inséré:

«*Article 10 bis*

Atteinte à la sécurité des portefeuilles européens d'identité numérique

1. En cas d'atteinte aux portefeuilles européens d'identité numérique délivrés par application de l'article 6 *bis* et aux mécanismes de validation prévus à l'article 6 *bis*, paragraphe 5, points a), b) et c), ou de compromission partielle des uns ou des autres, d'une manière qui affecte leur fiabilité ou la fiabilité des autres portefeuilles européens d'identité numérique, l'État membre de délivrance suspend immédiatement la délivrance du portefeuille européen d'identité numérique et en révoque sans retard la validité puis informe les autres États membres et la Commission en conséquence.

2. Lorsqu'il a été remédié à l'atteinte ou à la compromission visée au paragraphe 1, l'État membre de délivrance rétablit la délivrance et l'utilisation du portefeuille européen d'identité numérique et en informe les autres États membres et la Commission dans les meilleurs délais.

3. S'il n'est pas remédié à l'atteinte ou à la compromission visée au paragraphe 1 dans un délai de trois mois à compter de la suspension ou de la révocation, l'État membre concerné retire le portefeuille européen d'identité numérique concerné et en informe les autres États membres et la Commission en conséquence. Lorsque la gravité de l'atteinte le justifie, le portefeuille européen d'identité numérique concerné est retiré immédiatement.

4. La Commission publie, dans les meilleurs délais, au *Journal officiel de l'Union européenne*, les modifications correspondantes apportées à la liste prévue à l'article 6 *quinquies*.

5. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission précise davantage les mesures visées aux paragraphes 1 et 3, au moyen d'un acte d'exécution relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi qu'il est indiqué à l'article 6 *bis*, paragraphe 10.»

(12) L'article 11 *bis* suivant est inséré:

«*Article 11 bis*

Identification univoque

1. Lorsque des moyens d'identification électronique notifiés et les portefeuilles européens d'identité numérique sont utilisés en vue de l'authentification, les États membres garantissent une identification univoque.

2. Aux fins du présent règlement, les États membres incluent, dans l'ensemble minimal de données d'identification personnelle mentionné à l'article 12, paragraphe 4, point d), un identifiant univoque et constant en conformité avec le droit de l'Union, afin d'identifier l'utilisateur à leur demande dans les cas où l'identification de l'utilisateur est exigée par la loi.

3. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission précise davantage les mesures visées aux paragraphes 1 et 2 au moyen d'un acte d'exécution relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi que cela est indiqué à l'article 6 *bis*, paragraphe 10.»

(13) L'article 12 est modifié comme suit:

(a) au paragraphe 3, les points c) et d) sont supprimés;

(b) au paragraphe 4, le point d) est remplacé par le texte suivant:

«d) d'une référence à un ensemble minimal de données d'identification personnelle nécessaires pour représenter de manière univoque et constante une personne physique ou morale;»;

(c) au paragraphe 6, le point a) est remplacé par le texte suivant:

«a) en un échange d'informations, d'expériences et de bonnes pratiques en ce qui concerne les schémas d'identification électronique, notamment les exigences techniques liées à l'interopérabilité, à l'identification univoque et aux niveaux de garantie;»;

(14) L'article 12 *bis* suivant est inséré:

«*Article 12 bis*

Certification des schémas d'identification électronique

1. La conformité des schémas d'identification électronique notifiés aux exigences énoncées à l'article 6 *bis*, à l'article 8 et à l'article 10 peut être certifiée par les organismes publics ou privés désignés par les États membres.

2. L'évaluation par les pairs des schémas d'identification électronique prévue à l'article 12, paragraphe 6, point c), ne s'applique pas aux schémas d'identification électronique ni à une partie de tels schémas qui ont été certifiés conformément au paragraphe 1. Les États membres peuvent utiliser un certificat ou une déclaration de conformité de l'Union délivré(e) conformément à un schéma européen de certification de cybersécurité pertinent établi en application du règlement (UE) 2019/881 afin de démontrer la conformité de ces schémas avec les exigences énoncées à l'article 8, paragraphe 2, relatives aux niveaux de garantie des schémas d'identification électronique.

3. Les États membres notifient à la Commission le nom et l'adresse de l'organisme public ou privé visé au paragraphe 1. La Commission met ces informations à la disposition des États membres.»;

(15) l'intitulé suivant est inséré après l'article 12 *bis*:

«SECTION III

RECOURS TRANSFRONTALIER À DES MOYENS D'IDENTIFICATION ÉLECTRONIQUE»;

(16) Les articles 12 *ter* et 12 *quater* suivants sont insérés:

«Article 12 *ter*

Recours transfrontalier aux portefeuilles européens d'identité numérique

1. Lorsque les États membres exigent, en vertu du droit national ou de pratiques administratives nationales, une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification pour accéder à un service en ligne fourni par un organisme du secteur public, ils acceptent également les portefeuilles européens d'identité numérique délivrés en conformité avec le présent règlement.

2. Lorsque le droit national ou de l'Union exige des parties utilisatrices privées fournissant des services qu'elles utilisent une authentification forte de l'utilisateur pour l'identification en ligne, ou lorsqu'une identification forte de l'utilisateur est imposée par une obligation contractuelle, y compris dans les domaines des transports, de l'énergie, des services bancaires et financiers, de la sécurité sociale, de la santé, de l'eau potable, des services postaux, des infrastructures numériques, de l'éducation ou des télécommunications, les parties utilisatrices privées acceptent également l'utilisation des portefeuilles européens d'identité numérique délivrés conformément à l'article 6 *bis*.

3. Lorsque les très grandes plateformes en ligne, telles qu'elles sont définies à l'article 25, paragraphe 1, du règlement [relatif à un marché intérieur des services numériques], exigent des utilisateurs qu'ils s'authentifient pour avoir accès à des services en ligne, elles acceptent également l'utilisation des portefeuilles européens d'identité numérique délivrés conformément à l'article 6 *bis* uniquement à la demande volontaire de l'utilisateur et en ce qui concerne les attributs minimaux nécessaires pour le service en ligne particulier pour lequel l'authentification est demandée, tels que la preuve de l'âge.

4. La Commission encourage et facilite l'élaboration de codes de conduite par autorégulation au niveau de l'Union (ci-après dénommés «codes de conduite»), afin de contribuer à une disponibilité et à une facilité d'utilisation étendues des portefeuilles européens d'identité numérique dans le champ d'application du présent règlement. Ces codes de conduite veillent à ce que les moyens d'identification électronique, y compris les portefeuilles européens d'identité numérique, relevant du champ d'application du présent règlement, soient acceptés en particulier par les prestataires de services qui recourent à des services d'identification électronique tiers pour l'authentification de l'utilisateur. La Commission facilite l'élaboration de ces codes de conduite en étroite coopération avec toutes les parties intéressées et encourage les prestataires de services à achever l'élaboration des codes de conduite dans un délai de douze mois à compter de l'adoption du présent règlement et à les

mettre effectivement en œuvre dans un délai de dix-huit mois à compter de l'adoption du présent règlement.

5. Dans un délai de dix-huit mois à compter du déploiement des portefeuilles européens d'identité numérique, la Commission évalue si, sur le fondement d'éléments prouvant la disponibilité et la facilité d'utilisation du portefeuille européen d'identité numérique, il faut obliger des prestataires de services en ligne privés supplémentaires à accepter l'utilisation du portefeuille européen d'identité numérique uniquement à la demande volontaire de l'utilisateur. Les critères d'évaluation peuvent notamment comprendre l'étendue de la base d'utilisateurs, la présence transfrontalière de prestataires de services, les évolutions technologiques et l'évolution des modalités d'utilisation. La Commission est habilitée à adopter des actes délégués sur le fondement de cette évaluation, qui concernent une révision des exigences en matière de reconnaissance du portefeuille européen d'identité numérique énoncées aux paragraphes 1 à 4 du présent article.

6. Aux fins du présent article, les portefeuilles européens d'identité numérique ne sont pas soumis aux exigences énoncées aux articles 7 et 9.

Article 12 quater

Reconnaissance mutuelle d'autres moyens d'identification électronique

1. Lorsqu'une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification est exigée par application du droit national ou de pratiques administratives nationales pour accéder à un service en ligne fourni par un organisme du secteur public dans un État membre, le moyen d'identification électronique délivré dans un autre État membre est reconnu dans le premier État membre aux fins de l'authentification transfrontalière pour ce service en ligne, à condition que les conditions suivantes soient réunies:

   (a) la délivrance de ce moyen d'identification électronique relève d'un schéma d'identification électronique qui figure sur la liste prévue à l'article 9;

   (b) le niveau de garantie de ce moyen d'identification électronique correspond à un niveau de garantie égal ou supérieur à celui requis par l'organisme du secteur public concerné pour accéder à ce service en ligne dans l'État membre concerné et, en tout état de cause, n'est pas inférieur à un niveau de garantie "substantiel";

   (c) l'organisme du secteur public concerné dans l'État membre concerné utilise le niveau de garantie "substantiel" ou "élevé" pour ce qui concerne l'accès à ce service en ligne.

   Cette reconnaissance intervient au plus tard six mois après la publication par la Commission de la liste visée au premier alinéa, point a).

2. Un moyen d'identification électronique dont la délivrance relève d'un schéma d'identification électronique figurant sur la liste prévue par l'article 9 et qui correspond au niveau de garantie "faible" peut être reconnu par des organismes du secteur public aux fins de l'authentification transfrontalière du service en ligne fourni par ces organismes.»;

(17) À l'article 13, le paragraphe 1 est remplacé par le texte suivant:

«1. Nonobstant le paragraphe 2 du présent article, les prestataires de services de confiance sont responsables des dommages causés intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations prévues par le présent règlement et aux obligations en matière de gestion des risques de cybersécurité qui découlent de l'article 18 de la directive (UE) XXXX/XXXX [SRI 2].»;

(18) L'article 14 est remplacé par le texte suivant:

«*Article 14*

Aspects internationaux

1. La Commission peut adopter des actes d'exécution, conformément à l'article 48, paragraphe 2, arrêtant les conditions dans lesquelles les exigences d'un pays tiers applicables aux prestataires de services de confiance établis sur son territoire et aux services de confiance qu'ils fournissent peuvent être considérées comme équivalentes aux exigences applicables aux prestataires de services de confiance qualifiés établis dans l'Union et aux services de confiance qualifiés qu'ils offrent.

2. Si la Commission a adopté un acte d'exécution en vertu du paragraphe 1 ou a conclu un accord international sur la reconnaissance mutuelle de services de confiance conformément à l'article 218 du traité, les services de confiance fournis par les prestataires établis dans le pays tiers concerné sont considérés comme équivalents aux services de confiance qualifiés offerts par les prestataires de services de confiance qualifiés établis dans l'Union.»;

(19) L'article 15 est remplacé par le texte suivant:

«*Article 15*

Accessibilité aux personnes handicapées

La fourniture de services de confiance ainsi que de produits destinés à un utilisateur final qui servent à fournir ces services sont accessibles aux personnes handicapées conformément aux exigences en matière d'accessibilité prévues par l'annexe I de la directive 2019/882 relative aux exigences en matière d'accessibilité applicables aux produits et services.»;

(20) L'article 17 est modifié comme suit:

(a) le paragraphe 4 est modifié comme suit:

(1) au paragraphe 4, le point c) est remplacé par le texte suivant:

«c) à informer les autorités nationales compétentes des États membres concernés, désignées en application de la directive (UE) XXXX/XXXX [SRI 2], des atteintes importantes à la sécurité ou des pertes d'intégrité dont il prend connaissance dans l'exécution de ses tâches. Lorsque l'atteinte importante à la sécurité ou la perte d'intégrité concerne d'autres États membres, l'organe de contrôle en informe le point de contact unique de l'État membre concerné désigné en application de la directive (UE) XXXX/XXXX [SRI 2];»;

(2) le point f) est remplacé par le texte suivant:

«f) à coopérer avec les autorités de contrôle instituées en application du règlement (UE) 2016/679, en particulier en les informant, dans les meilleurs délais, des résultats des audits des prestataires de services de confiance qualifiés, lorsque les règles en matière de protection des données à caractère personnel ont été violées, ainsi que des atteintes à la sécurité qui constituent des violations de données à caractère personnel;»;

(b) le paragraphe 6 est remplacé par le texte suivant:

«6. Au plus tard le 31 mars de chaque année, chaque organe de contrôle soumet à la Commission un rapport sur ses principales activités de l'année civile précédente.»;

(c) le paragraphe 8 est remplacé par le texte suivant:

«8. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission précise davantage, au moyen d'actes d'exécution, les tâches des autorités de contrôle énumérées au paragraphe 4 et définit les formats et procédures applicables aux fins du rapport prévu au paragraphe 6. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(21) l'article 18 est modifié comme suit:

(a) le titre de l'article 18 est remplacé par le texte suivant:

«Assistance mutuelle et coopération»

(b) le paragraphe 1 est remplacé par le texte suivant:

«1. Les organes de contrôle coopèrent en vue d'échanger de bonnes pratiques et des informations concernant la fourniture de services de confiance.

(c) les paragraphes 4 et 5 suivants sont ajoutés:

«4. Les organes de contrôle et les autorités nationales compétentes désignées en vertu de la directive (UE) XXXX/XXXX du Parlement européen et du Conseil [SRI 2] coopèrent et se prêtent mutuellement assistance afin de veiller à ce que les prestataires de services de confiance respectent les exigences établies dans le présent règlement et dans la directive (UE) XXXX/XXXX [SRI 2]. L'organe de contrôle demande à l'autorité nationale compétente désignée en vertu de la directive (UE) XXXX/XXXX [SRI 2] de mener des actions de surveillance pour vérifier que les prestataires de services de confiance respectent les exigences énoncées dans la directive (UE) XXXX/XXXX [SRI 2], d'exiger des prestataires de services de confiance qu'ils remédient à tout non-respect de ces exigences, de fournir en temps voulu les résultats de toute activité de surveillance ayant trait aux prestataires de services de confiance et d'informer les organes de contrôle des incidents pertinents notifiés conformément à la directive (UE) XXXX/XXXX [SRI 2].

5. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission établit, au moyen d'actes

d'exécution, les modalités de procédure nécessaires pour faciliter la coopération entre les organes de contrôle visés au paragraphe 1.»;

(22) l'article 20 est modifié comme suit:

(a) le paragraphe 1 est remplacé par le texte suivant:

«1. Les prestataires de services de confiance qualifiés font l'objet, au moins tous les vingt-quatre mois, d'un audit effectué à leurs frais par un organisme d'évaluation de la conformité. Le but de l'audit est de confirmer que les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent respectent les exigences fixées par le présent règlement et à l'article 18 de la directive (UE) XXXX/XXXX [SRI 2]. Les prestataires de services de confiance qualifiés transmettent le rapport d'évaluation de la conformité qui en résulte à l'organe de contrôle dans un délai de trois jours ouvrables à compter de la réception dudit rapport.»;

(b) au paragraphe 2, la dernière phrase est remplacée par le texte suivant:

«Lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées, l'organe de contrôle informe les autorités de contrôle instituées en vertu du règlement (UE) 2016/679 des résultats de ses audits.»;

(c) les paragraphes 3 et 4 sont remplacés par le texte suivant:

«3. Si le prestataire de services de confiance qualifié ne respecte pas les exigences énoncées par le présent règlement, l'organe de contrôle exige dudit prestataire qu'il remédie à ce manquement, dans un délai fixé par l'organe de contrôle, s'il y a lieu.

Si ce prestataire ne remédie pas au manquement, le cas échéant, dans le délai fixé par l'organe de contrôle, ce dernier, tenant compte, en particulier, de l'ampleur, de la durée et des conséquences de ce manquement, peut retirer à ce prestataire ou au service concerné le statut qualifié et demander à ce prestataire, le cas échéant dans un délai déterminé, de se conformer aux exigences de la directive (UE) XXXX/XXXX [SRI 2]. L'organe de contrôle en informe l'organisme visé à l'article 22, paragraphe 3, aux fins de la mise à jour des listes de confiance visées à l'article 22, paragraphe 1.

L'organe de contrôle informe le prestataire de services de confiance qualifié du retrait de son statut qualifié ou du retrait du statut qualifié du service concerné.

«4. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes suivantes:

(a) l'accréditation des organismes d'évaluation de la conformité et le rapport d'évaluation de la conformité visé au paragraphe 1;

(b) les exigences en matière d'audit en application desquelles les organismes d'évaluation de la conformité procéderont à leur évaluation de la conformité des prestataires de services de confiance qualifiés visés au paragraphe 1;

(c) les systèmes d'évaluation de la conformité utilisés par les organismes d'évaluation de la conformité pour évaluer la conformité des prestataires de services de confiance qualifiés et pour fournir le rapport d'évaluation visé au paragraphe 1.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.».

(23) L'article 21 est modifié comme suit:

(a) le paragraphe 2 est remplacé par le texte suivant:

«2. L'organe de contrôle vérifie si le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences fixées par le présent règlement, en particulier les exigences applicables aux prestataires de services de confiance qualifiés et aux services de confiance qualifiés qu'ils fournissent.

Afin de vérifier que le prestataire de services de confiance respecte les exigences énoncées à l'article 18 de la directive (UE) XXXX/XXXX [SRI 2], l'organe de contrôle demande aux autorités compétentes visées par ladite directive de mener les actions de surveillance nécessaires à cet égard et de fournir des informations sur leur résultat dans un délai de trois jours à compter de leur achèvement.

Si l'organe de contrôle conclut que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences visées au premier alinéa, l'organe de contrôle accorde le statut qualifié au prestataire de services de confiance et aux services de confiance qu'il fournit et en informe l'organisme visé à l'article 22, paragraphe 3, aux fins de la mise à jour des listes de confiance visées à l'article 22, paragraphe 1, au plus tard trois mois suivant la notification conformément au paragraphe 1 du présent article.

Si la vérification n'est pas terminée dans un délai de trois mois à compter de la notification, l'organe de contrôle en informe le prestataire de services de confiance en précisant les raisons du retard et le délai nécessaire pour terminer la vérification.»;

(b) le paragraphe 4 est remplacé par le texte suivant:

«4. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission définit, au moyen d'actes d'exécution, les formats et procédures de notification et de vérification applicables aux fins des paragraphes 1 et 2 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(24) à l'article 23, le paragraphe 2 *bis* suivant est ajouté:

«2 *bis*. Les paragraphes 1 et 2 s'appliquent également aux prestataires de services de confiance établis dans des pays tiers et aux services qu'ils fournissent, dès lors qu'ils ont été reconnus dans l'Union conformément à l'article 14.»;

(25) l'article 24 est modifié comme suit:

(a) le paragraphe 1 est remplacé par le texte suivant:

«1. Lorsqu'un prestataire de services de confiance qualifié délivre un certificat qualifié ou une attestation électronique qualifiée d'attributs pour un service de confiance, il vérifie l'identité et, s'il y a lieu, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat qualifié ou l'attestation électronique qualifiée d'attributs.

Le prestataire de services de confiance qualifié vérifie les informations visées au premier alinéa, soit directement, soit en ayant recours à un tiers selon l'une ou l'autre des modalités suivantes:

(a) à l'aide d'un moyen d'identification électronique notifié conforme aux exigences énoncées à l'article 8 en ce qui concerne les niveaux de garantie "substantiel" ou "élevé";

(b) au moyen d'une attestation électronique qualifiée d'attributs, d'un certificat de signature électronique qualifié ou d'un cachet électronique qualifié délivré conformément au point a), c) ou d);

(c) à l'aide d'autres méthodes d'identification qui permettent l'identification d'une personne physique avec un degré de confiance élevé et dont la conformité est confirmée par un organisme d'évaluation de la conformité;

(d) par la présence en personne de la personne physique ou du représentant autorisé de la personne morale, en recourant aux procédures appropriées et conformément au droit national si aucun autre moyen n'est disponible.»;

(b) le paragraphe 1 *bis*. suivant est inséré:

«1 *bis*. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission fixe, au moyen d'actes d'exécution, les spécifications techniques, normes et procédures minimales concernant la vérification de l'identité et des attributs conformément au paragraphe 1, point c). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(c) le paragraphe 2 est modifié comme suit:

(1) le point d) est remplacé par le texte suivant:

«d) avant d'établir une relation contractuelle, informe, de manière claire, exhaustive et aisément accessible, dans un espace accessible au public et de manière individuelle, toute personne désireuse d'utiliser un service de confiance qualifié des conditions précises relatives à l'utilisation de ce service, y compris toute limite quant à son utilisation;»;

(2) les points f *bis*) et f *ter*) suivants sont insérés:

«f *bis*) se dote des procédures appropriées et prend les mesures adaptées pour gérer les risques juridiques, commerciaux et opérationnels ainsi que les autres risques directs ou indirects liés à la fourniture du service de confiance qualifié. Nonobstant

les dispositions de l'article 18 de la directive (UE) XXXX/XXXX [SRI 2], ces mesures incluent au moins:

i) des mesures ayant trait à l'enregistrement et aux procédures d'enrôlement auprès d'un service;

ii) des mesures ayant trait à des vérifications procédurales ou administratives;

iii) des mesures ayant trait à la gestion et à la mise en œuvre des services.

f *ter*) notifie à l'organe de contrôle et, le cas échéant, à d'autres organismes concernés, toute violation ou perturbation liée à la mise en œuvre des mesures énumérées au point f *bis*), i), ii) et iii) ayant une incidence importance sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.»;

(3) les points g) et h) sont remplacés par le texte suivant:

«g) prend des mesures appropriées contre la falsification, le vol ou le détournement de données ou le fait d'effacer, de modifier ou de rendre inaccessibles des données sans en avoir le droit;

h) enregistre et maintient accessibles aussi longtemps que nécessaire après que les activités du prestataire de services de confiance qualifié ont cessé, toutes les informations pertinentes concernant les données délivrées et reçues par le prestataire de services de confiance qualifié, aux fins de pouvoir fournir des preuves en justice et aux fins d'assurer la continuité du service. Ces enregistrements peuvent être effectués par des moyens électroniques;»;

(4) Le point j) est supprimé.

(d) le paragraphe 4 *bis* suivant est inséré:

«4 *bis*. En ce qui concerne la révocation des attestations électroniques d'attributs, les paragraphes 3 et 4 s'appliquent en conséquence.»;

(e) le paragraphe 5 est remplacé par le texte suivant:

«5. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux exigences énoncées au paragraphe 2. Les systèmes et produits fiables sont présumés satisfaire aux exigences fixées au présent article lorsqu'ils respectent ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(f) le paragraphe 6 suivant est inséré:

«6. La Commission est habilitée à adopter des actes délégués en ce qui concerne les mesures supplémentaires prévues au paragraphe 2, point f *bis)*.»;

(26) à l'article 28, le paragraphe 6 est remplacé par le texte suivant:

«6. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux certificats qualifiés de signature électronique. Un certificat qualifié de signature électronique est présumé satisfaire aux exigences fixées à l'annexe I lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(27) à l'article 29, le paragraphe 1 *bis*. suivant est ajouté:

«1 *bis*. La génération, la gestion et la reproduction de données de création de signature électronique pour le compte du signataire ne peuvent être confiées qu'à un prestataire de services de confiance qualifié fournissant un service de confiance qualifié pour la gestion d'un dispositif de création de signature électronique qualifié à distance.»;

(28) l'article 29 *bis* suivant est inséré:

«Article 29 *bis*

Exigences applicables aux services qualifiés de gestion d'un dispositif de création de signature électronique à distance

1. La gestion d'un dispositif de création de signature électronique qualifié à distance en tant que service qualifié ne peut être confiée qu'à un prestataire de services de confiance qualifié qui:

   (a) génère ou gère des données de création de signature électronique pour le compte du signataire;

   (b) sans préjudice de l'annexe II, point 1 d), reproduit les données de création de signature électronique exclusivement à des fins de sauvegarde, sous réserve du respect des exigences suivantes:

   le niveau de sécurité des ensembles de données reproduits doit être équivalent à celui des ensembles de données d'origine;

   le nombre d'ensembles de données reproduits n'excède pas le minimum nécessaire pour assurer la continuité du service.

   (c) respecte les exigences énoncées dans le rapport de certification du dispositif de création de signature électronique qualifié à distance concerné, établi conformément à l'article 30.

2. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les spécifications techniques et les numéros de référence des normes aux fins du paragraphe 1.»;

(29) à l'article 30, le paragraphe 3 *bis*. suivant est inséré:

«3 *bis*. La certification visée au paragraphe 1 est valable cinq ans, sous réserve d'une évaluation des vulnérabilités régulière effectuée tous les deux ans. Si des vulnérabilités sont décelées et non corrigées, la certification est retirée.»;

(30) à l'article 31, le paragraphe 3 est remplacé par le texte suivant:

«3. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission définit, au moyen d'actes d'exécution, les formats et procédures applicables aux fins du paragraphe 1. Ces actes d'exécution sont

adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(31) l'article 32 est modifié comme suit:

(a) au paragraphe 1, l'alinéa suivant est ajouté:

«La validation des signatures électroniques qualifiées est présumée satisfaire aux exigences fixées au premier alinéa lorsqu'elle respecte les normes visées au paragraphe 3.»;

(b) le paragraphe 3 est remplacé par le texte suivant:

«3. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables à la validation des signatures électroniques qualifiées. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(32) l'article 34 est remplacé par le texte suivant:

«*Article 34*

Service qualifié de conservation des signatures électroniques qualifiées

1. Un service qualifié de conservation des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique.

2. Le service qualifié de conservation des signatures électroniques qualifiées est présumé satisfaire aux exigences fixées au paragraphe 1 lorsqu'il respecte les normes visées au paragraphe 3.

3. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables au service qualifié de conservation des signatures électroniques qualifiées. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(33) l'article 37 est modifié comme suit:

(a) le paragraphe 2 *bis*. suivant est inséré:

«2 *bis*. Un cachet électronique avancé est présumé satisfaire aux exigences applicables aux cachets électroniques avancés visées à l'article 36 et au paragraphe 5 du présent article lorsqu'il respecte les normes visées au paragraphe 4.»;

(b) le paragraphe 4 est remplacé par le texte suivant:

«4. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux cachets électroniques avancés. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(34) l'article 38 est modifié comme suit:

(a) le paragraphe 1 est remplacé par le texte suivant:

«1. Les certificats qualifiés de cachet électronique satisfont aux exigences fixées à l'annexe III. Un certificat qualifié de cachet électronique est présumé satisfaire aux exigences fixées à l'annexe III lorsqu'il respecte les normes visées au paragraphe 6.»;

(b) le paragraphe 6 est remplacé par le texte suivant:

«6. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux certificats qualifiés de cachet électronique. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(35) l'article 39 *bis* suivant est inséré:

«*Article 39 bis*

Exigences applicables aux services qualifiés de gestion des dispositifs de création de cachet électronique à distance

L'article 29 *bis* s'applique mutatis mutandis aux services qualifiés de gestion des dispositifs de création de cachet électronique à distance.»;

(36) l'article 42 est modifié comme suit:

(a) le paragraphe 1 *bis* suivant est inséré:

«1 *bis*. L'établissement du lien entre la date et l'heure et les données ainsi que les horloges exactes sont présumés satisfaire aux exigences fixées au paragraphe 1 lorsqu'ils respectent les normes visées au paragraphe 2.»;

(b) le paragraphe 2 est remplacé par le texte suivant:

«2. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables à l'établissement du lien entre la date et l'heure et les données ainsi qu'aux horloges exactes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(37) l'article 44 est modifié comme suit:

(a) le paragraphe 1 *bis*. suivant est inséré:

«1 *bis*. Le processus d'envoi et de réception de données est présumé satisfaire aux exigences fixées au paragraphe 1 lorsqu'il respecte les normes visées au paragraphe 2.»;

(b) le paragraphe 2 est remplacé par le texte suivant:

«2. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux processus d'envoi et de réception de données. Ces actes d'exécution

sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(38) l'article 45 est remplacé par le texte suivant:

«*Article 45*

Exigences applicables aux certificats qualifiés d'authentification de site internet

1. Les certificats qualifiés d'authentification de site internet satisfont aux exigences fixées à l'annexe IV. Les certificats qualifiés d'authentification de site internet sont réputés conformes aux exigences fixées à l'annexe IV lorsqu'ils respectent les normes visées au paragraphe 3.

2. Les certificats qualifiés d'authentification de site internet visés au paragraphe 1 sont reconnus par les navigateurs internet. À cette fin, les navigateurs garantissent que les données d'identité fournies au moyen de l'une des méthodes s'affichent de manière conviviale. À l'exception des entreprises considérées comme des micro et petites entreprises au sens de la recommandation 2003/361/CE de la Commission pendant leurs cinq premières années d'activité en tant que prestataires de services de navigation sur internet, les navigateurs acceptent les certificats qualifiés d'authentification de site internet visés au paragraphe 1 et garantissent l'interopérabilité avec ces derniers.

3. Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission fournit, au moyen d'actes d'exécution, les spécifications et les numéros de référence des normes applicables aux certificats qualifiés d'authentification de site internet visés au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(39) les sections 9, 10 et 11 suivantes sont insérées après l'article 45:

«SECTION 9

ATTESTATION ÉLECTRONIQUE D'ATTRIBUTS

Article 45 bis

Effets juridiques de l'attestation électronique d'attributs

1. L'effet juridique et la recevabilité d'une attestation électronique d'attributs comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique.

2. Une attestation électronique qualifiée d'attributs a le même effet juridique qu'une attestation délivrée légalement sur papier.

3. Une attestation électronique qualifiée d'attributs délivrée dans un État membre est reconnue en tant qu'attestation électronique qualifiée d'attributs dans tous les États membres.

Article 45 ter

Attestation électronique d'attributs dans les services publics

Lorsqu'une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification est exigée par application du droit national pour accéder à un service en ligne fourni par un organisme du secteur public, les

données d'identification personnelle dans l'attestation électronique d'attributs ne se substituent pas à l'identification électronique à l'aide d'un moyen d'identification électronique et à l'authentification pour une identification électronique, à moins que cela ne soit expressément autorisé par l'État membre ou par l'organisme du secteur public. En pareil cas, les attestations électroniques qualifiées d'attributs délivrées dans d'autres États membres sont également acceptées.

Article 45 quater

Exigences applicables aux attestations qualifiées d'attributs

1. Les attestations électroniques qualifiées d'attributs respectent les exigences fixées à l'annexe V. Les attestations électroniques qualifiées d'attributs sont réputées conformes aux exigences fixées à l'annexe V lorsqu'elles respectent les normes visées au paragraphe 4.
2. Les attestations électroniques qualifiées d'attributs ne font l'objet d'aucune exigence obligatoire en sus des exigences fixées à l'annexe V.
3. Si une attestation électronique qualifiée d'attributs a été révoquée après avoir été délivrée, elle perd sa validité à compter du moment de sa révocation et elle ne peut en aucun cas recouvrer son statut antérieur.
4. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine les numéros de référence des normes applicables aux attestations électroniques qualifiées d'attributs au moyen d'un acte d'exécution relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi qu'il est indiqué à l'article 6 *bis*, paragraphe 10.

Article 45 quinquies

Vérification des attributs par rapport aux sources authentiques

1. Les États membres font en sorte que, au moins pour les attributs qui sont énumérés à l'annexe VI et qui sont fondés sur des sources authentiques dans le secteur public, des mesures soient prises pour permettre aux prestataires qualifiés d'attestations électroniques d'attributs de vérifier par des moyens électroniques, à la demande de l'utilisateur, l'authenticité de l'attribut directement par rapport à la source authentique pertinente au niveau national ou via des intermédiaires désignés reconnus au niveau national, en conformité avec le droit national ou le droit de l'Union.
2. Dans un délai de six mois à compter de l'entrée en vigueur du présent règlement, compte tenu des normes internationales pertinentes, la Commission fixe les spécifications techniques, normes et procédures minimales en ce qui concerne le catalogue d'attributs et de schémas pour l'attestation d'attributs et les procédures de vérification pour les attestations électroniques qualifiées d'attributs au moyen d'un acte d'exécution relatif à la mise en œuvre des portefeuilles européens d'identité numérique, ainsi qu'il est indiqué à l'article 6 bis, paragraphe 10.

Article 45 sexies

Délivrance d'attestations électroniques d'attributs aux portefeuilles européens d'identité numérique

Les prestataires délivrant des attestations électroniques qualifiées d'attributs fournissent une interface avec les portefeuilles européens d'identité numérique délivrés conformément à l'article 6 *bis*.

Article 45 septies

Règles supplémentaires applicables à la fourniture de services d'attestation électronique d'attributs

1. Les prestataires fournissant des services qualifiés et non qualifiés d'attestation électronique d'attributs ne combinent pas les données à caractère personnel relatives à la fourniture de ces services avec des données à caractère personnel provenant de tout autre service qu'ils offrent.

2. Les données à caractère personnel relatives à la fourniture de services d'attestation électronique d'attributs sont maintenues séparées, de manière logique, des autres données détenues.

3. Les données à caractère personnel relatives à la fourniture de services qualifiés d'attestation électronique d'attributs sont maintenues séparées, de manière physique et logique, des autres données détenues.

4. Les prestataires de services qualifiés d'attestation électronique d'attributs fournissent ces services dans le cadre d'une entité juridique distincte.

SECTION 10

SERVICES QUALIFIÉS D'ARCHIVAGE ÉLECTRONIQUE

Article 45 octies

Services qualifiés d'archivage électronique

Un service qualifié d'archivage électronique de documents électroniques ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité du document électronique au-delà de la période de validité technologique.

Dans un délai de douze mois à compter de l'entrée en vigueur du présent règlement, la Commission détermine, au moyen d'actes d'exécution, les numéros de référence des normes applicables aux services d'archivage électronique. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

SECTION 11

REGISTRES ÉLECTRONIQUES

Article 45 nonies

Effets juridiques des registres électroniques

1. L'effet juridique et la recevabilité d'un registre électronique comme preuve en justice ne peuvent être refusés au seul motif que ce registre se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences applicables aux registres électroniques qualifiés.

2. Un registre électronique qualifié bénéficie d'une présomption quant au caractère univoque et à l'authenticité des données qu'il contient, à l'exactitude de la date et de l'heure de ces données et à leur classement chronologique séquentiel dans le registre.

Article 45 decies

Exigences applicables aux registres électroniques qualifiés

1. Les registres électroniques qualifiés satisfont aux exigences suivantes:

   (a) ils sont créés par un ou plusieurs prestataires de services de confiance qualifiés;

   (b) ils garantissent le caractère univoque, l'authenticité et le classement correct des données contenues dans le registre;

   (c) ils garantissent le classement chronologique séquentiel correct des données dans le registre ainsi que l'exactitude de la date et de l'heure de l'entrée de ces données;

   (d) ils enregistrent les données de telle sorte que toute modification ultérieure des données soit immédiatement détectable.

2. Un registre électronique est présumé satisfaire aux exigences fixées au paragraphe 1 lorsqu'il respecte les normes visées au paragraphe 3.

3. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux processus d'exécution et d'enregistrement d'un ensemble de données dans un registre électronique qualifié ainsi qu'au processus de création d'un tel registre. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.»;

(40) l'article 48 *bis* suivant est inséré:

«*Article 48 bis*

Exigences en matière de rapports

1. Les États membres veillent à recueillir des statistiques relatives au fonctionnement des portefeuilles européens d'identité numérique et des services de confiance qualifiés.

2. Les statistiques recueillies conformément au paragraphe 1 incluent les éléments suivants:

   (a) le nombre de personnes physiques et morales ayant un portefeuille européen d'identité numérique valide;

   (b) le type et le nombre de services acceptant l'utilisation du portefeuille européen d'identité numérique;

   (c) les incidents et indisponibilités de l'infrastructure au niveau national empêchant l'utilisation des portefeuilles européens d'identité numérique.

3. Les statistiques visées au paragraphe 2 sont mises à la disposition du public dans un format ouvert, couramment utilisé et lisible par machine.

4. Avant le mois de mars de chaque année, les États membres soumettent à la Commission un rapport sur les statistiques recueillies conformément au paragraphe 2.»;

(41) l'article 49 est remplacé par le texte suivant:

«*Article 49*

Réexamen

1. La Commission procède à un réexamen de l'application du présent règlement et rend compte au Parlement européen et au Conseil dans un délai de vingt-quatre mois à compter de son entrée en vigueur. La Commission évalue, en particulier, s'il convient de modifier le champ d'application du présent règlement ou ses dispositions spécifiques, compte tenu de l'expérience acquise dans l'application du présent règlement ainsi que de l'évolution des technologies, du marché et du contexte juridique. Le rapport est accompagné, si nécessaire, d'une proposition de modification du présent règlement.

2. Le rapport d'évaluation examine notamment la disponibilité et la facilité d'utilisation des moyens d'identification, notamment le portefeuille européen d'identité numérique, relevant du champ d'application du présent règlement, et détermine s'il y a lieu d'obliger tous les prestataires de services en ligne privés qui utilisent des services d'identification électronique tiers à des fins d'authentification de l'utilisateur à accepter l'utilisation des moyens d'identification électroniques notifiés et du portefeuille européen d'identité numérique.

3. En outre, la Commission soumet au Parlement européen et au Conseil, tous les quatre ans après la présentation du rapport visé au paragraphe 1, un rapport sur les progrès accomplis dans la réalisation des objectifs du présent règlement.

(42) l'article 51 est remplacé par le texte suivant:

«*Article 51*

Mesures transitoires

1. Les dispositifs sécurisés de création de signature dont la conformité a été déterminée conformément à l'article 3, paragraphe 4, de la directive 1999/93/CE continuent à être considérés comme des dispositifs de création de signature électronique qualifiés au titre du présent règlement jusqu'au [date - JO veuillez insérer une période de quatre ans à compter de l'entrée en vigueur du présent règlement].

2. Les certificats qualifiés délivrés à des personnes physiques en vertu de la directive 1999/93/CE continuent à être considérés comme des certificats qualifiés de signature électronique au titre du présent règlement jusqu'au [date - OP veuillez insérer une période de quatre ans à compter de l'entrée en vigueur du présent règlement].».

(43) L'annexe I est modifiée conformément à l'annexe I du présent règlement;

(44) l'annexe II est remplacée par le texte figurant à l'annexe II du présent règlement;

(45) l'annexe III est modifiée conformément à l'annexe III du présent règlement;

(46) l'annexe IV est modifiée conformément à l'annexe IV du présent règlement;

(47) une annexe V, dont le texte figure à l'annexe V du présent règlement, est ajoutée;

(48) une annexe VI est ajoutée au présent règlement.

Article 2

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le

Par le Parlement européen
Le président

Par le Conseil
Le président

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

Règlement du Parlement européen et du Conseil concernant un cadre européen relatif à une identité numérique, et modifiant le règlement eIDAS

1.2. Domaine(s) politique(s) concerné(s)

Domaine d'action: Marché intérieur

Une Europe adaptée à l'ère du numérique

1.3. La proposition/l'initiative est relative à:

☐ **une action nouvelle**

☐ **une action nouvelle suite à un projet pilote/une action préparatoire**[28]

☑**la prolongation d'une action existante**

☐ **une fusion ou une réorientation d'une ou de plusieurs actions vers une autre action/une action nouvelle**

1.4. Objectif(s)

1.4.1. Objectif général / objectifs généraux

L'objectif général de la présente initiative est d'assurer le bon fonctionnement du marché intérieur, notamment en ce qui concerne la fourniture et l'utilisation de services publics et privés transfrontaliers et transsectoriels reposant sur la disponibilité et l'utilisation de solutions d'identité électronique hautement sécurisées et fiables. Cet objectif s'inscrit dans le cadre des objectifs stratégiques définis dans la communication «Façonner l'avenir numérique de l'Europe».

1.4.2. Objectif(s) spécifique(s)

Objectif spécifique n° 1

Donner accès à des solutions d'identité numérique sécurisées et fiables qui puissent être utilisées par-delà les frontières, répondant ainsi aux attentes des utilisateurs et à la demande du marché;

Objectif spécifique n° 2

Faire en sorte que les services publics et privés puissent s'appuyer sur des solutions d'identité numérique sécurisées, fiables par-delà les frontières;

Objectif spécifique n° 3

Donner aux citoyens la maîtrise totale de leurs données à caractère personnel et garantir la sécurité de ces données lors de l'utilisation de solutions d'identité numérique;

Objectif spécifique n° 4

[28] Tel(le) que visé(e) à l'article 58, paragraphe 2, point a) ou b), du règlement financier.

Garantir des conditions égales pour la fourniture de services de confiance qualifiés dans l'UE et l'acceptation de ces derniers.

1.4.3. Résultat(s) et incidence(s) attendus

Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.

De manière générale, les principaux bénéficiaires attendus de l'initiative sont les utilisateurs finaux/citoyens, les fournisseurs de services en ligne, les fournisseurs d'applications de portefeuille et les prestataires publics et privés de services d'identité numérique. L'initiative devrait permettre de donner accès à des solutions d'identité numérique sécurisées et fiables qui puissent être utilisées par-delà les frontières, répondant ainsi aux attentes des utilisateurs et à la demande du marché; faire en sorte que les services publics et privés puissent s'appuyer sur des solutions d'identité numérique fiables et sécurisées par-delà les frontières; donner aux citoyens la maîtrise totale de leurs données à caractère personnel et garantir la sécurité de ces données lors de l'utilisation de solutions d'identité numérique; et garantir des conditions égales pour la fourniture de services de confiance qualifiés dans l'UE et l'acceptation de ces derniers.

Outre la facilité d'accès aux services, tant publics que privés, les citoyens et les entreprises bénéficieraient directement de la commodité et de la convivialité de l'interface d'authentification du portefeuille et seraient en mesure de procéder à des transactions nécessitant des niveaux variés de garantie (par exemple, de la connexion aux médias sociaux aux applications de santé en ligne).

Une approche renforcée de la protection de la vie privée dès la conception pourrait apporter des avantages supplémentaires étant donné que le portefeuille ne nécessiterait pas d'intermédiaires dans le processus d'attestation des attributs, ce qui permettrait au citoyen de communiquer directement avec les fournisseurs de services et de justificatifs. Le renforcement de la sécurité des données du portefeuille permettrait de prévenir l'usurpation d'identité et, par là même, d'éviter aux citoyens européens et aux entreprises européennes de subir des pertes financières.

Sur le plan de la croissance économique, l'introduction d'un système fondé sur des normes devrait réduire l'incertitude pour les acteurs du marché et devrait également avoir une incidence positive sur l'innovation.

Surtout, l'introduction de ce système devrait offrir un accès plus inclusif aux services publics et privés liés aux biens publics comme l'éducation et la santé, pour lequel certains groupes sociaux rencontrent actuellement des obstacles. Par exemple, certains citoyens handicapés, souvent ceux à mobilité réduite ou qui vivent dans des zones rurales sont susceptibles d'avoir un accès restreint aux services qui nécessitent normalement une présence physique si ceux-ci ne sont pas fournis localement.

1.4.4. Indicateurs de performance

Préciser les indicateurs permettant de suivre l'avancement et les réalisations.

Aspects relatifs au suivi et à l'évaluation et objectifs pertinents	Indicateur	Responsabilité en matière de collecte	Source(s)
Application			

Donner accès à des moyens d'identification électronique à tous les citoyens de l'UE	Nombre de citoyens européens et d'entreprises européennes auxquels ont été délivrés des identifications électroniques notifiés/des portefeuilles européens d'identité numérique, et nombre de justificatifs d'identité délivrés (attestations d'attributs)	Commission européenne et autorités nationales compétentes	Enquête annuelle/données de suivi et d'évaluation collectées par les autorités nationales compétentes
Donner accès à des moyens d'identification électronique à tous les citoyens de l'UE	Nombre de citoyens européens et d'entreprises européennes qui font un usage actif d'identifications électroniques notifiées /de portefeuilles européens d'identité numérique et de justificatifs d'identité (attestations d'attributs)	Commission européenne et autorités nationales compétentes	Enquête annuelle/données de suivi et d'évaluation collectées par les autorités nationales compétentes
Accroître la reconnaissance et l'acceptation transfrontalières des schémas d'identification électronique, l'ambition étant de parvenir à une acceptation universelle	Nombre de fournisseurs de services en ligne qui acceptent les identifications électroniques notifiées / les portefeuilles européens d'identité numérique et les justificatifs d'identité (attestations d'attributs)	Commission européenne	Enquête annuelle
Accroître la reconnaissance et l'acceptation transfrontalières des schémas d'identification électronique, l'ambition étant de parvenir à une acceptation universelle	Nombre de transactions en ligne effectuées à l'aide d'identifications électroniques notifiées /de portefeuilles européens d'identité numérique et de justificatifs d'identité (attestations d'attributs) (au total et par-delà les frontières)	Commission européenne	Enquête annuelle
Stimuler l'adoption par le secteur privé de nouveaux services d'identité numérique et le développement de ceux-ci	Nombre de nouveaux services d'attestations d'attributs délivrés à titre privé qui satisfont aux normes d'intégration dans le portefeuille européen d'identité numérique	Commission européenne et autorités nationales compétentes	Enquête annuelle
Informations contextuelles			

Stimuler l'adoption par le secteur privé de nouveaux services d'identité numérique et le développement de ceux-ci	Taille du marché des identités numériques	Commission européenne	Enquête annuelle
Stimuler l'adoption par le secteur privé de nouveaux services d'identité numérique et le développement de ceux-ci	Dépenses relatives aux marchés publics liées à l'identité numérique	Commission européenne et autorités nationales compétentes	Enquête annuelle
Accroître la reconnaissance et l'acceptation transfrontalières des schémas d'identification électronique, l'ambition étant de parvenir à une acceptation universelle	% d'entreprises réalisant des ventes en ligne de biens ou de services	Commission européenne	Eurostat
Accroître la reconnaissance et l'acceptation transfrontalières des schémas d'identification électronique, l'ambition étant de parvenir à une acceptation universelle	Part des transactions en ligne nécessitant une forte identification du client (total)	Commission européenne	Enquête annuelle
Donner accès à des moyens d'identification électronique à tous les citoyens de l'UE	% des particuliers réalisant des achats en ligne % des particuliers ayant accès aux services publics en ligne	Commission européenne	Eurostat

1.5. Justification(s) de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre. Les États membres seront tenus de délivrer un portefeuille européen d'identité numérique dans un délai de 24 à 48 mois (à titre indicatif) à compter de l'adoption du règlement. La Commission sera habilitée à adopter des

actes d'exécution établissant les spécifications techniques et les normes de référence applicables à l'architecture technique du cadre européen relatif à une identité numérique dans un délai de 12 à 24 mois (à titre indicatif) à compter de l'adoption du règlement.

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

Justification de l'action au niveau européen (ex ante)

Compte tenu de la demande croissante, de la part des citoyens, des entreprises et des fournisseurs de services en ligne, de solutions d'identité numérique conviviales, sécurisées et respectueuses de la vie privée pouvant être utilisées par-delà les frontières, des mesures complémentaires prises au niveau de l'UE peuvent apporter une plus grande valeur ajoutée que des mesures prises par les différents États membres, comme le montre l'évaluation du règlement eIDAS.

Valeur ajoutée de l'Union escomptée (ex post)

Une approche plus harmonisée au niveau de l'UE, fondée sur une transition fondamentale qui verrait l'abandon du recours aux seules solutions d'identité numérique au profit de la fourniture d'attestations électroniques d'attributs, permettrait aux citoyens et aux entreprises d'avoir accès à des services publics et privés partout dans l'UE s'appuyant sur des preuves d'identité et d'attributs vérifiés. Les fournisseurs de services en ligne seraient en mesure d'accepter des solutions d'identité numérique indépendamment du lieu où elles auront été délivrées, grâce à une approche européenne commune en ce qui concerne la confiance, la sécurité et l'interopérabilité. En outre, les utilisateurs comme les prestataires de services peuvent bénéficier de la même valeur juridique accordée aux attestations électroniques d'attributs dans l'ensemble de l'UE, ce qui est particulièrement important lorsqu'une action coordonnée est nécessaire, comme dans le cas des certificats de santé numériques. Les services de confiance fournissant des attestations électroniques d'attributs bénéficieraient également de la disponibilité d'un marché européen sur lequel offrir leurs services. Par exemple, la récupération des coûts visant à garantir un environnement hautement fiable et sécurisé pour la fourniture d'un service de confiance qualifié est plus facilement compensée au niveau de l'UE en raison des économies d'échelle. Seul un cadre de l'UE peut garantir la portabilité transfrontalière complète des identités juridiques et de l'attestation électronique des attributs qui y sont liés, et permettre ainsi de faire confiance aux déclarations d'identité faites par d'autres États membres.

1.5.3. Leçons tirées d'expériences similaires

Le règlement eIDAS [règlement (UE) nº 910/2014] est le seul cadre transfrontalier relatif à l'identification électronique (eID) fiable des personnes physiques et morales et aux services de confiance. Bien que le règlement eIDAS joue incontestablement un rôle dans le marché intérieur, de nombreuses choses ont changé depuis son adoption en 2014. Cet instrument repose sur des systèmes nationaux d'identification électronique qui obéissent à des normes diverses et il se concentre sur un segment relativement étroit des besoins des citoyens et des entreprises en matière

d'identification électronique: l'accès transfrontalier sécurisé aux services publics. Les services ciblés concernent principalement les 3 % de la population de l'UE qui résident dans un État membre différent de celui dans lequel ils sont nés.

Depuis, la dématérialisation de toutes les fonctions de la société s'est considérablement accrue. En particulier, la pandémie de COVID-19 a eu un effet formidable sur l'accélération de la dématérialisation. En conséquence, la fourniture de services tant publics que privés devient toujours plus numérique. Les citoyens et les entreprises attendent un niveau élevé de sécurité et de commodité dans l'ensemble de leurs activités en ligne, comme la transmission de déclarations fiscales, l'inscription dans une université étrangère, l'ouverture à distance d'un compte bancaire ou une demande de prêt, la location d'une voiture, la création d'une entreprise dans un autre État membre, l'authentification pour les paiements en ligne, la soumission d'une offre en réponse à un appel d'offres en ligne, etc.

En conséquence, la demande de moyens d'identification et d'authentification en ligne, ainsi que de moyens d'échange numérique d'informations liées à notre identité, à nos attributs ou à nos qualifications (identité, adresses, âge, mais également qualifications professionnelles, permis de conduire et autres permis et systèmes de paiement), en toute sécurité et avec un niveau élevé de protection des données, s'est considérablement accrue.

Ce phénomène a provoqué un changement de paradigme, accélérant la transition vers des solutions avancées et pratiques dans lesquelles peuvent être intégrés différents certificats et données vérifiables de l'utilisateur. Les utilisateurs attendent un environnement autodéterminé dans lequel différents justificatifs et attributs peuvent être transportés et partagés, tels que l'identification électronique nationale, les certificats professionnels, les titres de transports en commun, voire, dans certains cas, les billets de concert numériques. Il s'agit de portefeuilles autonomes fondés sur des applications et gérés par l'appareil mobile de l'utilisateur, qui permettent un accès sécurisé et aisé à différents services, tant publics que privés, entièrement contrôlé par l'utilisateur.

1.5.4. Compatibilité avec le cadre financier pluriannuel (CFP) et synergies éventuelles avec d'autres instruments appropriés

L'initiative soutient l'effort européen de relance en fournissant aux citoyens et aux entreprises les outils nécessaires, notamment l'identification électronique pratique et les services de confiance, pour les aider à mener leurs activités quotidiennes en ligne de manière fiable et sécurisée. Elle est donc pleinement conforme aux objectifs du CFP.

Les dépenses opérationnelles doivent être financées au titre du poste DEP SO5. Selon les estimations, les marchés publics soutenant l'élaboration de normes et de spécifications techniques, ainsi que le coût de la maintenance des éléments constitutifs de l'identification électronique et des services de confiance, devraient atteindre entre 3 et 4 millions d'EUR par an. L'affectation exacte de ce budget doit être décidée lors de la définition des futurs programmes de travail. Les subventions destinées à soutenir la connexion des services publics et privés à l'écosystème d'identification électronique favoriseraient grandement la réalisation des objectifs de la proposition. Le coût à la charge d'un prestataire de services pour intégrer l'API nécessaire pour le portefeuille d'identité numérique est estimé à environ 25 000 EUR, étant entendu qu'il s'agira d'un coût exceptionnel unique par prestataire. Dès que la répartition du budget pour le prochain programme de travail

aura été débattue, la connexion d'une masse critique de services pourrait être financée par des subventions pouvant atteindre 0,5 million d'EUR par État membre, sous réserve de leur disponibilité.

Les réunions du groupe d'experts consacrées à l'élaboration des actes d'exécution seront imputées à la partie administrative du programme pour une Europe numérique, à concurrence d'un montant total maximal de 0,5 million d'EUR.

Synergies avec d'autres instruments

La présente initiative établira un cadre relatif à la fourniture d'identités électroniques et de services d'identité électronique dans l'UE, sur lesquels des secteurs particuliers pourront s'appuyer pour satisfaire aux exigences juridiques qui leur sont propres, par exemple en ce qui concerne les documents de voyage numériques, les permis de conduire numériques, etc. De même, la proposition concorde avec les objectifs du règlement 2019/1157, qui renforce la sécurité des cartes d'identité et des documents de séjour. En application du présent règlement, les États membres sont tenus de mettre en œuvre, d'ici août 2021, de nouvelles cartes d'identité comportant les éléments de sécurité mis à jour. Une fois ces nouvelles cartes d'identité mises au point, les États membres pourraient les mettre à niveau afin qu'elles puissent être notifiées en tant que schémas d'identification électronique au sens du règlement eIDAS.

L'initiative contribuera également à transformer le domaine douanier en un environnement électronique sans recours au papier, dans le cadre de l'initiative visant à mettre en place un guichet unique de l'UE pour les douanes. Il convient également de relever que la future proposition contribuera aux politiques européennes de mobilité en facilitant les obligations juridiques de déclaration incombant aux opérateurs du secteur maritime, établies dans le cadre du système de guichet unique maritime européen, qui entrera en application le 15 août 2025. Il en va de même pour l'articulation avec le règlement concernant les informations électroniques relatives au transport de marchandises, qui oblige les autorités des États membres à accepter les informations électroniques relatives au fret. L'application que constitue le portefeuille européen d'identité numérique pourra également traiter les justificatifs liés aux conducteurs, aux véhicules et aux opérations, requis par le cadre juridique de l'UE dans le domaine du transport routier (par exemple, les permis de conduire numériques/directive 2006/126/CE). Les spécifications seront développées plus avant dans ce cadre. La future initiative pourrait également contribuer à l'élaboration d'autres initiatives à venir dans le domaine de la coordination de la sécurité sociale, telles que l'élaboration éventuelle d'un passeport européen de sécurité sociale qui pourrait tirer parti des ancres de confiance offertes par les identités notifiées dans le cadre d'eIDAS.

La présente initiative soutient la mise en œuvre du RGPD [règlement (UE) 2016/679] en donnant à l'utilisateur la maîtrise sur l'utilisation qui est faite de ses données à caractère personnel. Elle offre un niveau élevé de complémentarité avec le nouveau règlement sur la cybersécurité et ses schémas communs de certification de cybersécurité. En outre, la nécessité d'une identité univoque eIDAS pour l'internet des objets garantit la cohérence avec le règlement sur la cybersécurité et avec la nécessité de couvrir un éventail plus large d'acteurs autres que les personnes et les entreprises, tels que les machines, les objets, les fournisseurs et les appareils de l'internet des objets.

Le règlement relatif au portail numérique unique est également conforme à la présente initiative, qu'il rejoint sur plusieurs points importants: l'objectif de ce règlement est de moderniser intégralement les services des administrations publiques et de faciliter l'accès en ligne aux informations, aux procédures administratives et aux services d'assistance dont les citoyens et les entreprises ont besoin lorsqu'ils vivent ou exercent leur activité dans un autre pays de l'UE. La présente initiative fournit des éléments fondamentaux à l'appui des objectifs visant à permettre l'application du principe de la transmission unique d'informations («une fois pour toutes») dans le cadre du portail numérique unique.

La présente initiative est en outre cohérente avec la stratégie européenne pour les données et la proposition de règlement sur la gouvernance européenne des données, qui offrent à un cadre favorisant les applications fondées sur les données dans les cas où la transmission de données d'identité est requise, de sorte que les utilisateurs ont la maîtrise de leurs données et que ces dernières sont entièrement anonymisées.

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

L'initiative s'appuiera sur les éléments constitutifs de l'identification électronique et des services de confiance, qui ont été élaborés dans le cadre du mécanisme pour l'interconnexion en Europe (MIE) et sont en passe d'être intégrés dans le programme pour une Europe numérique.

Les États membres peuvent en outre demander un financement au titre de la facilité pour la reprise et la résilience (FRR) pour la mise en place/l'amélioration des infrastructures nécessaires.

1.6. Durée et incidence financière de la proposition/de l'initiative

☐ **durée limitée**

☐ En vigueur à partir [du JJ/MM] de AAAA jusqu'[au JJ/MM]en AAAA

☐ Incidence financière de AAAA jusqu'en AAAA pour les crédits d'engagement et de AAAA jusqu'en AAAA pour les crédits de paiement.

☑ **durée illimitée**

Mise en œuvre avec une période de montée en puissance de AAAA jusqu'en AAAA,

puis un fonctionnement en rythme de croisière au-delà.

1.7. Mode(s) de gestion prévu(s)[29]

☑ **Gestion directe** par la Commission

☑ dans ses services, y compris par l'intermédiaire de son personnel dans les délégations de l'Union;

☐ par les agences exécutives

☐ **Gestion partagée** avec les États membres

☐ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

☐ à des pays tiers ou aux organismes qu'ils ont désignés;

☐ à des organisations internationales et à leurs agences (à préciser);

☐ à la BEI et au Fonds européen d'investissement;

☐ aux organismes visés aux articles 70 et 71 du règlement financier;

☐ à des organismes de droit public;

☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques».

Remarques

[…]
[…]

[29] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

Le règlement sera réexaminé pour la première fois deux ans après sa pleine application, puis tous les quatre ans. La Commission est tenue de présenter un rapport contenant ses constatations au Parlement européen et au Conseil.

En outre, dans le contexte de l'application des mesures, les États membres collectent des données statistiques sur l'utilisation et le fonctionnement du portefeuille européen d'identité numérique et des services de confiance qualifiés. Les statistiques sont compilées dans un rapport qui est soumis à la Commission chaque année.

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre des financements, des modalités de paiement et de la stratégie de contrôle proposée

Le règlement établit des règles plus harmonisées pour la fourniture de services d'identification électronique et de services de confiance dans le marché intérieur, tout en faisant en sorte que la confiance soit respectée et que les utilisateurs puissent avoir la maîtrise de leurs données. Ces nouvelles règles nécessitent l'élaboration de spécifications et de normes techniques, et devront faire l'objet d'une surveillance des autorités nationales, dont les activités devront être coordonnées. En outre, les éléments constitutifs de l'identification électronique, notamment la signature électronique, seront gérés et fournis dans le cadre du programme pour une Europe numérique. Il est également nécessaire de prendre en considération les ressources nécessaires pour communiquer et négocier avec les pays tiers un accord sur la reconnaissance mutuelle des services de confiance.

Afin qu'ils soient en mesure d'assumer ces tâches, il est nécessaire de doter les services de la Commission des ressources appropriées. L'application du nouveau règlement nécessiterait, selon les estimations, 11 ETP; 4 à 5 ETP pour les travaux juridiques, 4 à 5 ETP se consacrant principalement aux travaux techniques, et 2 ETP pour la coordination, la coopération internationale et le soutien administratif.

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

L'un des principaux problèmes à l'origine des lacunes du cadre législatif actuel est l'absence d'harmonisation des systèmes nationaux. Pour y remédier dans le cadre de l'initiative actuelle, il conviendra de s'appuyer essentiellement sur des normes de référence et des spécifications techniques à définir dans les actes d'exécution.

La Commission sera assistée par un groupe d'experts dans l'élaboration de ces actes d'exécution. En outre, la Commission collaborera dès à présent avec les États membres pour convenir de la nature technique du futur système, afin d'éviter que la fragmentation actuelle ne s'aggrave au cours de la négociation de la proposition.

2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

En ce qui concerne les frais de réunion du groupe d'experts, compte tenu du faible montant par transaction (par exemple, remboursement des frais de déplacement d'un délégué pour une réunion si la réunion se déroule en présentiel), les procédures standard de contrôle interne semblent suffisantes.

De même, pour les projets pilotes à réaliser dans le cadre du programme pour une Europe numérique, les procédures standard normales de la DG CNECT devraient suffire.

2.3. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées, au titre de la stratégie antifraude par exemple.

Les mesures de prévention des fraudes existantes applicables à la Commission couvriront les crédits supplémentaires nécessaires aux fins du présent règlement.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

Lignes budgétaires existantes

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de la dépense	Participation			
	Numéro	CD/CND[30].	de pays AELE[31]	de pays candidats[32]	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
2	02 04 05 01 Déploiement	CD	OUI	NON	NON	NON
2	02 01 30 01 Dépenses d'appui pour le programme pour une Europe numérique	CND				
7	20 02 06 Dépenses de gestion	CND	NON			

Nouvelles lignes budgétaires, dont la création est demandée

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de la dépense	Participation			
	Numéro	CD/CND	de pays AELE	de pays candidats	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
	[XX.YY.YY.YY]		OUI/NON	OUI/NON	OUI/NON	OUI/NON

30 CD = crédits dissociés / CND = crédits non dissociés.

31 AELE: Association européenne de libre-échange.

32 Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

3.2. Incidence financière estimée de la proposition sur les crédits

3.2.1. Synthèse de l'incidence estimée sur les crédits opérationnels

☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

☑ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel	Numéro	2

DG: CNECT			Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**		**TOTAL**
○ Crédits opérationnels				L'affectation du budget sera décidée lors de la formulation des programmes de travail. Les chiffres indiqués correspondent au minimum nécessaire à la maintenance et à la mise à niveau[33].						
Ligne budgétaire[34] 02 04 05	Engagements	(1a)	2,000	4,000	4,000	4,000	4,000	4,000		**22,000**
	Paiements	(2a)	1,000	3,000	4,000	4,000	4,000	4,000	2,000	**22,000**
Ligne budgétaire	Engagements	(1b)								
	Paiements	(2b)								
Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[35]										
Ligne budgétaire 02 01 03 01		(3)	**0,048**	**0,144**	**0,144**	**0,072**	**0,072**	**0,072**		**0,552**
TOTAL des crédits	Engagements	=1a+1b +3	2,048	4,144	4,144	4,072	4,072	**4,072**		**22,552**

33 Si le coût réel dépasse les montants indiqués, les coûts seront financés au titre de la ligne 02 04 05 01.

34 Selon la nomenclature budgétaire officielle.

35 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

pour la DG CNECT	Paiements	=2a+2b +3	1,048	3,144	4,144	4,072	4,072	**4,072**	**2,000**	**22,552**

○ TOTAL des crédits opérationnels	Engagements	(4)	2,000	4,000	4,000	4,000	4,000	4,000		**22,000**
	Paiements	(5)	1,000	3,000	4,000	4,000	4,000	4,000	2,000	**22,000**
○ TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques		(6)	**0,048**	**0,144**	**0,144**	**0,072**	**0,072**	**0,072**		**0,552**
Total des crédits pour la RUBRIQUE 2 du cadre financier pluriannuel	Engagements	= 4+6	2,048	4,144	4,144	4,072	4,072	**4,072**		**22,552**
	Paiements	= 5+6	0,048	4,144	4,144	4,072	4,072	**4,072**	**2,000**	**22,552**

Rubrique du cadre financier pluriannuel	**7**	«Dépenses administratives»

Cette partie est à compléter en utilisant les «données budgétaires de nature administrative», à introduire d'abord dans l'annexe de la fiche financière législative (annexe 5 des règles internes), à charger dans DECIDE pour les besoins de la consultation interservices.

En Mio EUR (à la 3e décimale)

		Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
DG: CNECT								
○ Ressources humaines		0,776	1,470	1,470	1,470	1,470	1,318	**7,974**
○ Autres dépenses administratives		0,006	0,087	0,087	0,087	0,016	0,016	**0,299**
TOTAL DG CNECT	Crédits	0,782	1,557	1,557	1,557	1,486	1,334	**8,273**

TOTAL des crédits pour la RUBRIQUE 7 du cadre financier pluriannuel	(Total engagements = Total paiements)	0,782	1,557	1,557	1,557	1,486	1,334	**8,273**

En Mio EUR (à la 3e décimale)

		Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**		**TOTAL**
TOTAL des crédits pour les RUBRIQUES 1 à 7 du cadre financier pluriannuel	Engagements	2,830	5,701	5,701	5,629	5,558	5,408		**30,825**
	Paiements	1,830	4,701	5,701	5,629	5,558	5,406	2,000	**30,825**

3.2.2. Estimation des réalisations financées avec des crédits opérationnels

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations ⇩			Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		**TOTAL**	
	Type [36]	Coût moyen	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1[37]...			Donner accès à des solutions d'identité numérique sécurisées et fiables qui puissent être utilisées par-delà les frontières, répondant ainsi aux attentes des utilisateurs et à la demande du marché													
Enquêtes/études annuelles			1	0,050	1	0,050	1	0,050,	1	0,050	1	0,050	1	0,050	6	0,300
Sous-total objectif spécifique nº 1			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
OBJECTIF SPÉCIFIQUE nº 2…			Faire en sorte que les services publics et privés puissent s'appuyer sur des solutions d'identité numérique sécurisées et fiables par-delà les frontières													
Enquêtes/études			1	0,050	1	0,050	1	0,050,	1	0,050	1	0,050	1	0,050	6	0,300
Sous-total objectif spécifique nº 2			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
OBJECTIF SPÉCIFIQUE nº 3…			Donner aux citoyens la maîtrise totale de leurs données à caractère personnel et garantir la sécurité de ces données lors de l'utilisation de solutions d'identité numérique													
Enquêtes/études			1	0,050	1	0,050	1	0,050,	1	0,050	1	0,050	1	0,050	6	0,300
Sous-total objectif spécifique nº 3			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300
OBJECTIF SPÉCIFIQUE nº 4…			Garantir des conditions égales pour la fourniture de services de confiance qualifiés dans l'UE et l' acceptation de ces derniers.													
Enquêtes/études			1	0,050	1	0,050	1	0,050,	1	0,050	1	0,050	1	0,050	6	0,300
Sous-total objectif spécifique nº 4			1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	1	0,050	6	0,300

[36] Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

[37] Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

TOTAL	4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	4	0,200	24	1,200

3.2.3. Synthèse de l'incidence estimée sur les crédits administratifs

☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

☑ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**TOTAL**
RUBRIQUE7 du cadre financier pluriannuel							
Ressources humaines	0,776	1,470	1,470	1,470	1,470	1,318	**7,974**
Autres dépenses administratives	0,006	0,087	0,087	0,087	0,0162	0,0162	**0,299**
Sous-total RUBRIQUE7 du cadre financier pluriannuel	0,782	1,557	1,557	1,557	1,486	1,334	**8,273**

Hors RUBRIQUE 7[38] **du cadre financier pluriannuel**							
Ressources humaines							
Autres dépenses de nature administrative Imputer les coûts administratifs à la ligne du DEP	0,048	0,144	0,144	0,072	0,072	**0,072**	**0 552**
Sous-total hors RUBRIQUE7 du cadre financier pluriannuel	0,048	0,144	0,144	0,072	0,072	**0,072**	**0 552**

TOTAL	**0,830**	**1,701**	**1,701**	**1,629**	**1,558**	**1,406**	**8,825**

Les besoins en crédits pour les ressources humaines et les autres dépenses de nature administrative seront couverts par les crédits de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

38 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

3.2.4. Besoins estimés en ressources humaines

☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

☑ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

Estimation à exprimer en équivalents temps plein

		Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**
20 01 02 01 (au siège et dans les bureaux de représentation de la Commission)		4	8	8	8	8	7
20 01 02 03 (en délégation)							
01 01 01 01 (recherche indirecte)							
01 01 01 11 (recherche directe)							
Autres lignes budgétaires (à préciser)							
20 02 01 (AC, END, INT de l'«enveloppe globale»)		2	3	3	3	3	3
20 02 03 (AC, AL, END, INT et JPD dans les délégations)							
XX 01 xx **yy zz** [39]	- au siège						
	- en délégation						
01 01 01 02 (AC, END, INT sur recherche indirecte)							
01 01 01 12 (AC, END, INT sur recherche directe)							
Autres lignes budgétaires (à préciser)							
TOTAL		**6**	**11**	**11**	**11**	**11**	**10**

XX est le domaine politique ou le titre concerné.

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	Les fonctionnaires mèneront principalement des travaux juridiques, des activités de coordination et des négociations avec les pays et organismes tiers en rapport avec la reconnaissance mutuelle des services de confiance.
Personnel externe	Les experts nationaux devraient apporter leur soutien à la mise en place technique et fonctionnelle du système. Le personnel AC devrait également contribuer à la réalisation des tâches techniques, y compris à la gestion des éléments constitutifs.

[39] Sous-plafond de personnel externe financé sur crédits opérationnels (anciennes lignes «BA»).

3.2.5. Compatibilité avec le cadre financier pluriannuel actuel

La proposition/l'initiative:

☑ peut être intégralement financée par voie de redéploiement au sein de la rubrique concernée du cadre financier pluriannuel (CFP).

Expliquez la reprogrammation requise, en précisant les lignes budgétaires concernées et les montants correspondants. Veuillez fournir un tableau Excel en cas de reprogrammation de grande envergure.

☐ nécessite l'utilisation de la marge non allouée sous la rubrique correspondante du CFP et/ou le recours aux instruments spéciaux comme le prévoit le règlement CFP.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées, les montants correspondants et les instruments dont le recours est proposé.

☐ nécessite une révision du CFP.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées et les montants correspondants.

3.2.6. Participation de tiers au financement

La proposition/l'initiative:

☑ ne prévoit pas de cofinancement par des tierces parties

☐ prévoit le cofinancement par des tiers estimé ci-après:

Crédits en Mio EUR (à la 3e décimale)

	Année **N**[40]	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)			Total
Préciser l'organisme de cofinancement								
TOTAL crédits cofinancés								

[40] L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

3.3. Incidence estimée sur les recettes

☑ La proposition/l'initiative est sans incidence financière sur les recettes.

☐ La proposition/l'initiative a une incidence financière décrite ci-après:

☐ sur les ressources propres

☐ sur les autres recettes

veuillez indiquer si les recettes sont affectées à des lignes de dépenses ☐

En Mio EUR (à la 3e décimale)

Ligne budgétaire de recettes:	Montants inscrits pour l'exercice en cours	Incidence de la proposition/de l'initiative[41]						
		Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)		
Article …….								

Pour les recettes qui seront «affectées», préciser la (les) ligne(s) budgétaire(s) de dépenses concernée(s).

[…]

Autres remarques (relatives, par exemple, à la méthode/formule utilisée pour le calcul de l'incidence sur les recettes ou toute autre information).

[…]

41 En ce qui concerne les ressources propres traditionnelles (droits de douane et cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % de frais de perception.

ANNEXE
de la FICHE FINANCIÈRE LÉGISLATIVE

Dénomination de la proposition/l'initiative:

Proposition de règlement concernant un cadre européen relatif à une identité numérique et modifiant le règlement eIDAS

1. VOLUME ET COÛT DES RESSOURCES HUMAINES ESTIMÉES NÉCESSAIRES

2. COÛT DES AUTRES DÉPENSES DE NATURE ADMINISTRATIVE

3. TOTAL DES FRAIS ADMINISTRATIFS

4. MÉTHODES DE CALCUL UTILISÉES POUR L'ESTIMATION DES COÛTS

4.1. Ressources humaines

4.2. Autres dépenses administratives

La présente annexe accompagne la fiche financière législative lors du lancement de la consultation interservices.

Les tableaux de données servent à alimenter les tableaux contenus dans la fiche financière législative. Ils constituent un document strictement interne à la Commission.

(1) Coût des ressources humaines estimées nécessaires

☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

☑ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

HEADING 7 of the multiannual financial framework		Year 2022		Year 2023		Year 2024		Year 2025		Year 2026		Year 2027		TOTAL	
		FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations	FTE	Appropriations
• Establishment plan posts (officials and temporary staff)															
20 01 02 01 - Headquarters and Representation offices	AD	4	608	7	1.064	7	1.064	7	1.064	7	1.064	6	912	38	5.776
	AST	0	-	1	152	1	152	1	152	1	152	1	152	5	760
20 01 02 03 - Union Delegations	AD														
	AST														
External staff [1]															
20 02 01 and 20 02 02 – External personnel – Headquarters and Representation offices	AC	1	82	1	82	1	82	1	82	1	82	1	82	6	492
	END	1	86	2	172	2	172	2	172	2	172	2	172	11	946
	INT														
20 02 03 – External personnel - Union Delegations	AC														
	AL														
	END														
	INT														
	JPD														
Other HR related budget lines (*specify*)															
Subtotal HR – HEADING 7		6	776	11	1.470	11	1.470	11	1.470	11	1.470	10	1.318	60	7.974

4.3. Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

4.4.

4.5.

Hors RUBRIQUE 7 du cadre financier pluriannuel		**Année 2022**		**Année 2023**		**Année 2024**		**Année 2025**		**Année 2026**		**Année 2027**		**TOTAL**	
		ETP	Crédits	ETP	Crédits	ETP	Crédits	ETP	Crédits	ETP	Crédits	ETP	Crédits	ETP	Crédits
01 01 01 01 Recherche indirecte[42]	AD														
01 01 01 11 Recherche directe	AST														
Autres (veuillez préciser)															
Personnel externe financé sur crédits opérationnels (anciennes lignes «BA») – au siège	AC														
	END														
	INT														
Personnel externe financé sur crédits opérationnels (anciennes lignes «BA») – en délégation	AC														
	AL														
	END														
	INT														
	JPD														
01 01 01 02 Recherche indirecte	AC														
01 01 01 12 Recherche directe	END														
Autres (veuillez préciser)[43]	INT														

[42] Veuillez choisir la ligne budgétaire concernée ou préciser une autre ligne si nécessaire; si davantage de lignes budgétaires sont concernées, le personnel devrait être différencié en fonction de chaque ligne budgétaire concernée.

[43] Veuillez choisir la ligne budgétaire concernée ou préciser une autre ligne si nécessaire; si davantage de lignes budgétaires sont concernées, le personnel devrait être différencié en fonction de chaque ligne budgétaire concernée.

Autres lignes budgétaires (à préciser)															
Sous-total RH - Hors RUBRIQUE 7															
Total RH (toutes les rubriques du CFP)		6	0,776	11	1,470	11	1,470	11	1,470	11	1,470	10	1,318	60	7,974

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

4.6. Coût des autres dépenses de nature administrative

4.7. ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative

4.8. ☑ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

RUBRIQUE 7 du cadre financier pluriannuel	Année 2022	Année 2023	Année 2024	Année 2025	Année 2026	Année 2027	Total
Au siège ou sur le territoire de l'UE:							
20 02 06 01 - Frais de mission et de représentation	0,006	0,015	0,015	0,015	0,015	0,015	**0,081**
20 02 06 02 - Frais de conférences et de réunions							
20 02 06 03 – Comités[44]		0,072	0,072	0,072	0,0012	0,012	**0,218**
20 02 06 04 Études et consultations							
20 04 – Dépenses informatiques (institutionnelles)[45]							
Autres lignes budgétaires hors RH (*à préciser le cas échéant*)							
En délégation							
20 02 07 01 – Frais de mission, de conférence et de représentation							
20 02 07 02 – Perfectionnement professionnel							
20 03 05 – Infrastructure et logistique							
Autres lignes budgétaires hors RH (*à préciser le cas échéant*)							
Sous-total Autres – RUBRIQUE 7 du cadre financier pluriannuel	0,006	0,087	0,087	0,087	0,016	0,016	**0,299**

44 Préciser le type de comité, ainsi que le groupe auquel il appartient.

45 L'avis de l'équipe chargée des investissements informatiques de la DG DIGIT est requis (voir les lignes directrices sur le financement de la technologie de l'information, C(2020) 6126 final du 10.9.2020, page 7).

En Mio EUR (à la 3e décimale)

Hors RUBRIQUE 7 du cadre financier pluriannuel	**Année 2022**	**Année 2023**	**Année 2024**	**Année 2025**	**Année 2026**	**Année 2027**	**Total**
Dépenses d'assistance technique et administrative (hors personnel externe), sur crédits opérationnels (anciennes lignes «BA»):	0,048	0,144	0,144	0,072	0,072	0,072	**0,552**
- au siège							
- en délégation							
Autres dépenses de gestion pour la recherche							
Dépenses liées à la politique informatique pour les programmes opérationnels[46]							
Dépenses informatiques institutionnelles pour les programmes opérationnels[47]							
Autres lignes budgétaires hors RH (*à préciser le cas échéant*)							
Sous-total Autres – Hors RUBRIQUE 7 du cadre financier pluriannuel	0,048	0,144	0,144	0,072	0,072	0,072	**0,552**
Total des autres dépenses administratives (toutes les rubriques du CFP)	0,054	0,231	0,231	0,159	0,088	0,088	0,851

46 L'avis de l'équipe chargée des investissements informatiques de la DG DIGIT est requis (voir les lignes directrices sur le financement de la technologie de l'information, C(2020) 6126 final du 10.9.2020, page 7).

47 Ce poste comprend les systèmes administratifs locaux et les contributions au cofinancement des systèmes informatiques institutionnels (voir les lignes directrices sur le financement de la technologie de l'information, C(2020) 6126 final du 10.9.2020).

5. TOTAL DES DEPENSES ADMINISTRATIVES (TOUTES LES RUBRIQUES DU CFP)

En Mio EUR (à la 3e décimale)

Synthèse	Année 2022	Année 2023	Année 2024	Année 2025	Année 2026	Année 2027	Total
Rubrique 7 – Ressources humaines	0,776	1,470	1,470	1,470	1,470	1,318	**7,974**
Rubrique 7 – Autres dépenses administratives	0,006	0,087	0,087	0,087	0,016	0,016	**0,218**
Sous-total RUBRIQUE 7							
Hors Rubrique 7 – Ressources humaines							
Hors Rubrique 7 – Autres dépenses administratives	0,048	0,144	0,144	0,072	0,072	0,072	**0,552**
Sous-total autres rubriques							
1. TOTAL 2. RUBRIQUE 7 et Hors RUBRIQUE 7	0,830	1,701	1,701	1,629	1,558	1,406	**8,825**

(1) Les besoins en crédits de nature administrative seront couverts par les crédits déjà affectés à la gestion de l'action et/ou réaffectés, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

6. METHODES DE CALCUL UTILISEES POUR L'ESTIMATION DES COUTS

(a) Ressources humaines

Cette partie explicite la méthode de calcul retenue pour l'estimation des ressources humaines jugées nécessaires [hypothèses concernant la charge de travail, y inclus les métiers spécifiques (profils de postes Sysper 2), les catégories de personnel et les coûts moyens correspondants].

1. **RUBRIQUE 7** du cadre financier pluriannuel
2. Note: les coûts moyens par catégorie de personnel au siège sont disponibles sur BudgWeb, à l'adresse suivante: 3. https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
4. O Fonctionnaires et agents temporaires 5. 7 fonctionnaires AD (dont 1 de CNECT/F.3 en 2023-2024) x 152 000 EUR/an en 2023-2027 (moitié moins en 2022 en raison de l'adoption prévue à la mi-2022); 6. 1 fonctionnaire AST x 152 000 EUR/an en 2023-2027 (moitié moins en 2022 en raison de l'adoption prévue à la mi-2022) 7.
8. O Personnel externe 9. AC: 1 x 82 000 EUR/an en 2023-2027 (moitié moins en 2022 en raison de l'adoption prévue à la mi-2022) (le facteur d'indexation est appliqué); 10. END: 2 x 86 000 EUR/an en 2023-2027 (moitié moins en 2022 en raison de l'adoption prévue à la mi-2022) (le facteur d'indexation est appliqué); 11.

12. **Hors RUBRIQUE 7** du cadre financier pluriannuel
13. O Postes financés sur le budget de la recherche uniquement 14.
15. O Personnel externe 16.

7. AUTRES DEPENSES ADMINISTRATIVES

Détailler par ligne budgétaire la méthode de calcul utilisée, en particulier les hypothèses sous-jacentes (par exemple nombre de réunions par an, coûts moyens, etc.)

17. **RUBRIQUE 7** du cadre financier pluriannuel
18. Réunions bimensuelles du comité x 12 000 EUR/réunion 2022-2024 pour l'adoption d'actes d'exécution. Après cela, réunions annuelles du comité pour l'adoption d'actes d'exécution actualisés. 19. La mission consiste principalement à effectuer des voyages Luxembourg-Bruxelles, mais également à assister à des conférences et des réunions avec les États membres et d'autres parties prenantes. 20.

21. **Hors RUBRIQUE 7** du cadre financier pluriannuel
22. Les réunions du groupe d'experts sont imputées à la ligne administrative du DEP.
23. Le groupe devrait tenir des réunions mensuelles (à 12 000 EUR) pendant la préparation de l'acte d'exécution (mi-2022-2024) et, en dehors de cette période, des réunions bimensuelles sont prévues pour assurer la coordination à l'échelle de l'UE en ce qui concerne la mise en œuvre technique.
24.