Notaires d'Europe

Garants de la sécurité juridique

Proposition de la Commission européenne 2021/0136 (COD) 3 juin 2021

«Révision du règlement eIDAS — Identité numérique européenne (EUid)».

Retour d'information du CNUE

Le Conseil des notaires de l'Union européenne (CNUE) est l'organisation faîtière européenne représentant 22 chambres notariales nationales et plus de 45,000 notaires.

Le CNUE suit avec un grand intérêt l' **initiative** prise par la Commission européenne dans le cadre de la **feuille de route «*Révision du règlement eIDAS — Identité numérique européenne (EUid)*»**, qui vise à améliorer l'efficacité du règlement eIDAS, à étendre son application au secteur privé et à promouvoir des identités numériques fiables pour tous les citoyens européens. Le CNUE apprécie la **proposition** de règlement du Parlement européen et du Conseil modifiant le règlement (UE) no 910/2014 en ce qui concerne l'établissement d'un cadre pour une identité numérique européenne, adoptée par la Commission **européenne**.

Dans le contexte d'une numérisation sans cesse croissante dans de nombreux domaines de la vie et de l'économie, la proposition de la Commission prévoit heureusement que **tous les États membres doivent proposer à leurs citoyens des identités électroniques pouvant être utilisées par-delà les frontières**. Cela permettra de mieux exploiter le potentiel de l'identification et de l'authentification électroniques au titre du règlement eIDAS, qui n'a pas été exploité jusqu'à présent. Étant donné que l'introduction d'une identification électronique transfrontière dans le cadre du règlement eIDAS n'a jusqu'à présent été possible que sur une base volontaire, seuls 14 des 27 États membres proposent une telle identification électronique. Cela signifie qu'à l'heure actuelle, seuls 59 % de l'ensemble des citoyens de l'Union ont accès à une carte d'identité électronique transfrontière. Par conséquent, les services en ligne qui sont disponibles dans leur pays ne peuvent être accessibles que dans une mesure très limitée dans un contexte transfrontière par l'intermédiaire du réseau eIDAS. L'obligation faite aux États membres d'introduire des identités électroniques transfrontières apportera une contribution importante à la mise en place **du marché unique numérique**.

De l'avis du CNUE, ces progrès doivent être abordés avec détermination, mais pas à la hâte. Il importe avant tout qu'un **système fiable, sûr et facilement accessible** de gestion des identités dans l'espace numérique soit disponible dans l' **ensemble de l'UE,** permettant l'identification, l'authentification et la fourniture d'attributs, de diplômes et de certificats.

Le CNUE considère également que certains aspects de la proposition de la Commission sont très critiques. Ces éléments seront soulignés comme suit:

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

1. **Réserve concernant les exigences formelles nationales formulées de manière non claire**

Premièrement, le **nouveau libellé peu clair de l'article 2 (3) de la proposition de la Commission** est très préoccupant.

L'article 2 (3) et le considérant 19 prévoient que le règlement n'affecte aucune législation nationale ou de l'Union qui exige une certaine forme juridique pour la conclusion ou la validité d'un contrat ou d'autres obligations. En d'autres termes: Le règlement laisse aux États membres le soin de décider de la manière dont certains actes juridiques doivent être conclus. C'est pour une bonne raison: Les exigences relatives à la forme juridique ont pour but de protéger les parties à un acte juridique et de les sensibiliser aux risques économiques et juridiques sous-jacents. Ces exigences ont également des fonctions de preuve et de conseil. C'est la raison pour laquelle, dans de nombreux États membres, par exemple, les contrats d'achat immobilier doivent être notariés. Cette réserve concernant la forme juridique de l'article 2 (3) n'est pas controversée et n'a pas été remise en cause par la Commission.

La version actuelle de l'article 2 (3) est donc libellée comme suit:

> *«Le présent règlement n'affecte pas le droit national ou le droit de l'Union relatif à la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales en matière de forme.»*

La nouvelle proposition eIDAS inclut désormais l'attestation électronique qualifiée d'attributs au **considérant 27 et aux articles 45 bis et suivants.** Ces attributs peuvent inclure un permis de conduire, un diplôme ou un permis médical. L'attestation électronique de ces attributs peut être stockée dans le portefeuille. Le règlement fixe des exigences pour que les attestations électroniques puissent être reconnues dans d'autres États membres comme équivalentes aux attestations sur support papier. Il s'agira d'une amélioration essentielle pour la liberté de circulation au sein de l'UE et pour la vie quotidienne de nombreux citoyens.

Toutefois, selon la **dernière phrase du considérant 27**, les États membres peuvent encore définir des exigences formelles sectorielles supplémentaires pour la reconnaissance transfrontière des attestations électroniques qualifiées d'attributs. Par exemple, lorsqu'un médecin d'un État membre demande un permis médical pour exercer la profession de médecin dans un autre État membre, cet État membre peut toujours exiger une demande sur papier et/ou une preuve sur papier de certains faits tels que l'accréditation médicale.

Selon la Commission, ce droit des États membres de prévoir des exigences formelles supplémentaires pour la reconnaissance transfrontière des attributs attestés par voie électronique dans la dernière phrase du considérant 27 est censé se refléter dans les deux amendements à l'article 2 (3) eIDAS ***mis en évidence*** comme suit:

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

«Le présent règlement n'affecte pas le droit national ou le droit de l'Union relatif à la conclusion et à la validité de contrats ou d'autres obligations juridiques ou procédurales liées à des ***exigences sectorielles spécifiques en ce qui concerne*** *la forme et* ***les effets juridiques sous-jacents.»***

Toutefois, il est non seulement systématiquement erroné et confus, mais aussi inutile de «mélanger» les deux types de réserves dans une seule et même nouvelle disposition. **L'article 2 (3) et le considérant 19**, d'une part, et le **considérant 27**, d'autre part, traitent de notions fondamentalement différentes: Le *droit civil relatif à la forme juridique des contrats et autres obligations* n'a rien à voir avec les exigences formelles qu'un État membre peut prévoir dans le cadre *d'une procédure administrative dans un secteur* donné pour la reconnaissance de certains attributs. Il est essentiel de ne pas mélanger les deux concepts, et il n'y a aucune raison de:

- Les amendements conduisent à une formulation peu claire et peu compréhensible de l'article 2 (3), d'autant plus que le considérant 19 (ancien considérant 21) reste inchangé.

- Le processus législatif n'a pas eu l'intention de modifier en premier lieu l'article 2 (3). Toutefois, du seul fait de ces modifications, l'article 2 (3) pourrait être interprété de manière plus étroite par la suite par les tribunaux.

- Il est facile et ne devrait pas faire l'objet de controverses pour éviter cette insécurité juridique inutile (i) en conservant la forme originale de l'article 2 (3) et (i) en déplaçant les amendements à l'endroit où ils appartiennent: Article 45 quater relatif aux exigences applicables à l'attestation électronique qualifiée d'attributs.

Une nouvelle formulation proposée est jointe en annexe I.

2. Mise en place d'outils d'identification plus sûrs

Lorsqu'un citoyen doit avoir accès à un service fourni en ligne par un organisme du secteur public, sans intervention directe et personnelle d'aucune autorité publique, il doit simplement s'identifier, conformément au règlement eIDAS, au moyen de deux procédures interconnectées: **identification électronique** (art. 3 (1)) et **authentification** (art. 3 (5)).

Ces procédures électroniques sont deux concepts différents, mais interconnectés, qui tentent tous deux de s'assurer que le citoyen qui accède à un service en ligne est celui qu'il prétend être: premièrement, l'intéressé s'identifie par voie électronique, ce qui signifie qu'il utilise son identification électronique pour exprimer, dans un format électronique, ce qu'il est. Il envoie les données au système. Deuxièmement, le système authentifie que l'identification électronique est correcte, de sorte que l'utilisateur peut accéder au service en ligne.

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

Pour ce faire, le citoyen a besoin de la **délivrance** d'un moyen d'identification électronique qu'il pourra ultérieurement utiliser pour s'identifier par voie électronique. L'article 8 du règlement eIDAS fixe les critères des trois niveaux de garantie existants (faibles, substantiels et élevés), la différence fondamentale entre ces deux critères étant la manière dont l'identité du demandeur est vérifiée par l'émetteur de l'identification électronique. Ces trois niveaux sont précisés dans le règlement d'exécution (UE) 2015/1502 du 8 septembre 2015 pour la délivrance des moyens d'identification électronique («inscription») et le mécanisme d'authentification utilisé pour confirmer l'identité à un tiers.

Ce dispositif d'identification et d'authentification dans le cadre de la présente proposition envisage exclusivement l'accès des citoyens aux services offerts entièrement en ligne et de manière automatisée. Par conséquent, eIDAS envisage des interactions strictement techniques et électroniques.

Il existe toutefois d'autres procédures publiques, telles que la procédure d'authentification notariale, qui nécessitent une interaction en face à face entre les demandeurs et l'organisme du secteur public qui doit respecter les **normes d'identification les plus élevées**, par exemple pour les contrats de vente de biens immobiliers ou les formations en ligne d'entreprises. Ces normes sont notamment nécessaires pour **prévenir la fraude à l'identité** (par exemple, en transmettant des moyens d'identification électronique plus le code PIN), pour **garantir l'exactitude et la fiabilité des registres publics** (par exemple, les registres nationaux du commerce et les registres fonciers) qui sont dotés de la confiance du public dans de nombreux États membres et pour **prévenir le blanchiment de capitaux**.

Lorsque cette procédure entre l'organisme public et le citoyen est effectuée par voie électronique, il ne suffit pas de se fonder sur l'identification faite par un tiers lors de la délivrance du certificat. Au contraire, l' **identité et la capacité doivent également être vérifiées par l'organisme public au moment exact de l' utilisation de l'identification électronique, afin de s'assurer que la bonne personne l'utilise.** Cela ne peut être garanti par les processus d'authentification électronique précédemment expliqués.

Afin que le règlement puisse également être utilisé à l'avenir pour les procédures publiques présentant les **exigences les plus élevées en matière de sécurité de l'identification,** le règlement doit combiner l'identification électronique selon le niveau de garantie «élevé» avec **une procédure complémentaire d'identification par vidéoconférence.** Le résultat de cette combinaison serait une procédure d'identification en deux étapes hautement sécurisée consistant en (i) l'authentification au moyen de l'identification électronique garantissant l'utilisation d'une identification électronique en cours de validité; et ii) une procédure complémentaire d'identification par vidéoconférence garantissant que la personne à laquelle l'identification électronique a été délivrée figure effectivement dans la vidéoconférence.

Cette procédure d'identification en deux étapes est explicitement reconnue dans le considérant 22 de la directive 2019/1151 sur les outils numériques, qui prévoit des contrôles d'identité complémentaires

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

au moment même de la constitution en ligne d'une entreprise au moyen de vidéoconférences ou d'autres moyens en ligne qui fournissent une connexion audiovisuelle en temps réel. Les deux procédures, à savoir l'identification électronique et la vidéoconférence, devraient être combinées afin de garantir l'identification la plus fiable des parties concernées. Pour accéder ~~à~~ la plateforme électronique, la partie doit d'abord s'identifier en fournissant un moyen d'identification électronique présentant le niveau de garantie «élevé». Dans un deuxième temps, le notaire, via la plateforme, identifiera la partie concernée en comparant la photo de la visioconférence à la photographie officielle de la partie.

Afin de réaliser la deuxième étape de cette procédure d'identification, le notaire faisant fonction doit être en mesure de recevoir l'élément d'identification photographique et toute donnée biométrique de la partie via l'identification électronique et, optionnellement, à partir du système d'identification électronique national. L'élément d'identification photographique et les données biométriques devraient être conservées dans l'ensemble minimal de données d'identification des personnes conformément à l'article 12, paragraphe 4, point a), et dans la liste des attributs figurant à l'annexe VI. **Cela est nettement plus sûr que la procédure vidéo classique**, car la carte d'identité n'y est conservée qu'à huis clos et l'authenticité de la carte d'identité ne peut être vérifiée. Cette combinaison de l'identification électronique actuelle (niveau de garantie «élevé») et de la procédure susmentionnée d'identification par vidéoconférence réduit considérablement les risques de manipulation et d'utilisation de la carte d'identité par des tiers.

L'objectif du règlement eIDAS est de servir de **boîte à outils, qui réglemente de manière concluante le domaine des procédures d'identification électronique**. Une telle boîte à outils **ne sera complète que si elle contient cette procédure d'identification en deux étapes**. Cette procédure est nécessaire pour garantir une sécurité suffisante pour les transactions importantes, par exemple dans le domaine du droit immobilier et du droit des sociétés. En outre, il est essentiel pour la prévention du **blanchiment de capitaux**. La vérification de l'élément d'identification photographique et de toute donnée biométrique s'inscrit bien dans le système eIDAS actuel: L'annexe no 2.1.2 du règlement d'exécution (UE) 2015/1502 prévoit déjà un contrôle de la photo pour la délivrance d'un moyen d'identification électronique. Ce qui fait défaut jusqu'à présent, c'est la vérification d'une photo lors de l' utilisation de l'identification électronique afin de réaliser une identification.

Nous notons que cette procédure d'identification en deux étapes ne nécessite aucune modification du cadre des trois niveaux de garantie existants. La manière dont les États membres mettront en œuvre la procédure de visioconférence et la fonction de comparaison de la photo ou d'autres données biométriques relèveraient de leur compétence et ne devraient pas être abordées dans le règlement eIDAS.

Une nouvelle formulation proposée est jointe en annexe II.

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

Si la procédure d'identification en deux étapes n'est pas introduite dans le règlement eIDAS, celui-ci doit au moins prévoir une **clause d'ouverture** afin de donner aux États membres la possibilité de prévoir, le cas échéant, des contrôles de photos. Toutefois, cela priverait le règlement eIDAS de son caractère concluant de boîte à outils et est donc moins recommandé. Dans le cas contraire, une procédure de comparaison de photos doit être prévue dans tout acte juridique ultérieur de l'Union prévoyant l'identification électronique, tel que le règlement LBC proposé.

Dans ce cas, une disposition similaire à celle du considérant 22 de la directive 2019/1151 relative aux outils numériques devrait être introduite dans le règlement e-IDAS, en ce qui concerne toute procédure numérique pour laquelle des contrôles d'identité, de capacité et de légalité supplémentaires sont requis par le droit européen ou national. La proposition suivante de reformulation devrait être introduite à l'article 2 (3) ou, au moins, en tant que considérant:

«Le présent règlement respecte pleinement les dispositions juridiques des États membres permettant à leurs autorités publiques compétentes de vérifier, par des contrôles électroniques complémentaires de l'identité, de la capacité juridique et de la légalité, si toutes les conditions requises pour la conclusion et la validité des contrats sont remplies. Ces contrôles pourraient inclure, entre autres, des vidéoconférences ou d'autres moyens en ligne fournissant une connexion audiovisuelle en temps réel».

Enfin, il est souligné qu'une autorité publique (comme un notaire) a toujours et doit conserver le pouvoir de demander à la personne concernée de comparaître en personne afin de vérifier l'identité de la personne ainsi que la volonté et la compétence pour les actes juridiques souhaités. Nous proposons d'inclure dans le règlement que, dans le cas de certains actes juridiques (tels que les actes authentiques notariés), la présence physique peut être jugée nécessaire parce que cela est dans l'intérêt supérieur de la ou des personnes concernées. Dans ce cas, il peut être demandé à cette personne de comparaître physiquement. Par conséquent, nous proposons d'ajouter un nouveau paragraphe 4 à l'article 8:

«En cas de niveau de garantie le plus élevé, une autorité publique peut refuser l'identification et demander une identification en personne en cas de doute quant à l'identité ou à la compétence de la personne à identifier».

3. Portefeuille européen d'identité numérique

Le CNUE se félicite de l'introduction du «**portefeuille européen d'identité numérique»**, comme le souligne la proposition de la Commission. Il conservera des données et des attributs d'identification à caractère personnel aux fins de l'utilisation de procédures en ligne privées et publiques et facilitera considérablement l'identification électronique. Le portefeuille européen d'identité numérique sera principalement utilisé **pour l'identification sécurisée en cas de services en ligne**.

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

Le CNUE se félicite tout particulièrement du fait que le portefeuille européen d'identité numérique ne sera **délivré** que si l' **identification** a eu lieu **conformément au niveau de sécurité «élevé»** (article 8 du règlement eIDAS). Il s'agit là d'une contribution essentielle pour garantir la sécurité et la fiabilité dans le domaine numérique.

Toutefois, l'introduction du portefeuille européen d'identité numérique **ne modifie pas le système général.** Premièrement, la **réserve relative aux exigences formelles nationales en vertu de l'article 2 (3) du règlement eIDAS** s'applique également au portefeuille européen d'identité numérique. Deuxièmement, **l'utilisation exclusive du portefeuille européen d'identité numérique n'est pas suffisante** si un État membre impose des exigences **plus strictes en matière d'identification dans le cas de services en ligne.** Par conséquent, l'identification au moyen du portefeuille européen d'identité numérique n'est pas suffisante pour la procédure d'authentification et d'autres procédures de droit public répondant aux exigences les plus élevées en matière d'identification. En fait, le portefeuille européen d'identité numérique n'est qu'un moyen de faciliter et de simplifier l'accès aux services en ligne qui exigent tout au plus le niveau de sécurité «élevé» à des fins d'identification.

Si l'identification au moyen du portefeuille européen d'identité numérique devrait **également** s'appliquer aux **procédures présentant les exigences les plus élevées en matière d'identification**, le CNUE suggère que la délivrance du portefeuille européen d'identité numérique soit liée au niveau de d'identification le plus élevé (voir le point 2 traitant déjà de la combinaison de l'identification électronique selon le niveau de garantie «élevé» et d'une procédure complémentaire d'identification par vidéoconférence).

En tout état de cause, il serait louable d'inclure dans **le règlement eIDAS une définition claire du champ d'application** du portefeuille européen d'identité numérique.

4. Utilisation de pseudonymes

Le CNUE est également réticent à l' **article 5 de la proposition de la Commission**, selon lequel l'utilisation de pseudonymes dans les transactions électroniques ne doit pas être interdite. Il est intéressant de noter que la proposition contient une réserve concernant les effets juridiques que les pseudonymes ont en droit national. L'article 5 de la proposition de la Commission dispose en conséquence:

> *«**Sans préjudice** de l'effet juridique conféré aux pseudonymes en vertu du droit national, [...]».*

Toutefois, il serait pratique de limiter l'utilisation des pseudonymes au niveau européen afin de **réduire le manque de transparence** et le risque **d'abus** liés à l'utilisation de pseudonymes dès le départ.

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

5. Liste de l'UE pour les signatures électroniques avancées certifiées

Le CNUE constate avec regret que le nouveau règlement eIDAS proposé par la Commission ne contient pas de dispositions selon lesquelles, à l'instar des signatures électroniques qualifiées, la **Commission** doit établir, publier et tenir à jour une **liste des dispositifs de création de signature électronique avancés certifiés** après que les États membres ont notifié ces dispositifs de création de signature.

L'introduction d'une «liste de l'UE» pour les signatures électroniques avancées permettrait également de vérifier facilement la fiabilité de ces signatures. Cela est essentiel, notamment parce que les signatures électroniques avancées sont principalement utilisées dans des domaines clés.

6. Conclusion

Compte tenu de ce qui précède, la proposition **devrait être révisée avec précision**.

En outre, il est nécessaire de réexaminer soigneusement le **court délai** de mise en œuvre du règlement eIDAS et ses fonctions dans les États membres respectifs. Ce délai **n'est que de 12 mois** et serait difficilement gérable pour de nombreux États membres. Les grandes entreprises en ligne, telles que Google, Amazon, Facebook ou Apple, sont susceptibles de disposer des ressources techniques et financières nécessaires pour notifier leurs services. Cela comporte le risque que le marché, en l'absence de services publics disponibles à temps, se tourne de plus en plus vers des services privés. En particulier pour les services qui sont intrinsèquement gouvernementaux (par exemple, la juridiction), l'identification effectuée par les seules entités privées serait très alarmante. Une telle tendance irait également à l'encontre des objectifs du train de mesures sur les services numériques.

* * *

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

ANNEXE I – Suggestions d'amendements sur l'attestation électronique qualifiée d'attributs

Nouvelle formulation proposée de l'article 2, paragraphe 3

Article 2
Champ d'application

1. Le présent règlement s'applique aux schémas d'identification électronique qui ont été notifiés par un État membre et aux prestataires de services de confiance qui sont établis dans l'Union.

2. Le présent règlement ne s'applique pas à la fourniture de services de confiance qui sont utilisés exclusivement dans le cadre de systèmes fermés résultant du droit national ou d'accords entre un ensemble défini de participants.

3. Le présent règlement n'affecte pas le droit national ou le droit de l'Union relatif à la conclusion et à la validité de contrats ou d'autres obligations juridiques ou procédurales liées à ~~exigences sectorielles spécifiques en ce qui concerne~~ la forme ~~les effets juridiques sous-jacents~~.

Nouvelle formulation proposée de l'article 45 quater

Article 45 quater
Exigences applicables aux attestations qualifiées d'attributs

1. L'attestation électronique qualifiée d'attributs satisfait aux exigences énoncées à l'annexe V. Une attestation électronique d'attributs qualifiée est réputée conforme aux exigences énoncées à l'annexe V lorsqu'elle satisfait aux 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.

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

3. Ces exigences relatives à l'attestation qualifiée d'attributs devraient s'appliquer sans préjudice du droit de l'Union ou du droit national définissant des exigences sectorielles supplémentaires en ce qui concerne la forme ayant des effets juridiques sous-jacents et, en particulier, la reconnaissance transfrontière de l'attestation électronique qualifiée d'attributs, le cas échéant.

4. 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.

5. Dans un délai de 6 mois à compter de l'entrée en vigueur du présent règlement, la Commission établit les numéros de référence des normes 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 visés à l'article 6 bis, paragraphe 10.

***

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

ANNEXE II – Suggestion d'amendements sur le niveau de sécurité combiné

Considérant que:

(nouveau) L'obligation de reconnaître des moyens d'identification électronique devrait se rapporter uniquement aux moyens dont le niveau de garantie de l'identité correspond à un niveau égal ou supérieur au niveau requis pour le service en ligne en question. En outre, cette obligation ne devrait s'appliquer que lorsque l'organisme du secteur public en question utilise le niveau d'assurance «substantiel», «élevé» ou le niveau de sécurité combiné «très élevé» en ce qui concerne l'accès à ce service en ligne. Les États membres devraient demeurer libres, conformément au droit de l'Union, de reconnaître des moyens d'identification électronique disposant d'un niveau inférieur de garantie de l'identité.

(nouveau) L'utilisation du niveau de sécurité combiné «très élevé» devrait être réservée à l'identification des services publics en ligne présentant les exigences de sécurité les plus élevées, exécutés par les organismes du secteur public des États membres, y compris les notaires. Ainsi, les moyens d'identification relevant du niveau de sécurité combiné «très élevé» doivent, outre les exigences du niveau de garantie «élevé», fournir à l'organisme du secteur public agissant un élément d'identification photographique et toute donnée biométrique afin de lui permettre d'effectuer un processus d'identification pouvant inclure des vidéoconférences ou tout autre moyen en ligne fournissant une connexion audiovisuelle en temps réel.

(nouveau) Afin de garantir une prévention efficace du blanchiment de capitaux et du financement du terrorisme ainsi que la réalisation du processus d'identification conformément au considérant précédent, le secteur public devrait avoir accès à des éléments d'identification photographique et toute donnée biométrique. Par conséquent, les États membres devraient inclure l' élément d'identification photographique et toute donnée biométrique utilisée pour le contrôle complémentaire de l'identité dans l'ensemble minimal de données d'identification des personnes conformément à l'article 12, paragraphe 4, point a), et dans la liste des attributs figurant à l'annexe VI. En outre, les États membres peuvent choisir d'accorder l'accès au support de stockage hautement sécurisé de leurs cartes d'identité nationales, comme le prévoit l'article 3, paragraphe 5, du règlement (UE) 2019/1157.

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

Article 8

(a) Niveaux de garantie des systèmes d'identification électronique

1. Un schéma d'identification électronique notifié conformément à l'article 9, paragraphe 1, précise les niveaux de garantie faibles, substantiels et/ou élevés pour les moyens d'identification électronique délivrés dans le cadre de ce système.

2. Les niveaux d'assurance faibles, substantiels et élevés satisfont respectivement aux critères suivants:

(a) le niveau de garantie faible renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un degré limité de fiabilité à l'identité revendiquée ou prétendue d'une personne, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire le risque d'utilisation abusive ou d'altération de l'identité;

(b) le niveau de garantie substantiel renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un degré substantiel de fiabilité à l'identité revendiquée ou prétendue d'une personne, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité;

(c) le niveau de garantie élevé renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un niveau de fiabilité à l'identité revendiquée ou prétendue d'une personne plus élevé qu'un moyen d'identification électronique ayant le niveau de garantie substantiel, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité.

2 bis. Les États membres peuvent compléter le mécanisme d'authentification, par lequel un moyen d'identification électronique est utilisé pour confirmer l'identité à un organisme du secteur public conformément au niveau de garantie «élevé», par des contrôles électroniques supplémentaires de l'identité afin de créer un niveau de sécurité combiné «très élevé». Les États membres peuvent exiger l'utilisation du niveau de sécurité «très élevé» lorsqu'un organisme du secteur public compétent a le plus haut degré de confiance dans l'identité revendiquée ou alléguée d'une personne afin d'exclure le risque d'utilisation abusive ou de modification de l'identité. Ces contrôles supplémentaires

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

comprennent, entre autres, des vidéoconférences ou tout autre moyen en ligne fournissant une connexion audiovisuelle en temps réel pour confirmer l'identité revendiquée ou alléguée d'une personne au moyen d'un élément d'identification photographique et de toute autre donnée biométrique. Les États membres incluent l' élément d'identification photographique et les données biométriques utilisées pour ce contrôle complémentaire de l'identité dans l'ensemble minimal de données d'identification personnelle conformément à l'article 12, paragraphe 4, point a), et dans la liste d'attributs figurant à l'annexe VI. Les États membres peuvent également choisir d'accorder l'accès au support de stockage hautement sécurisé de leurs cartes d'identité nationales, comme le prévoit l'article 3, paragraphe 5, du règlement (UE) 2019/1157.

3. Au plus tard le [18 septembre 2015], compte tenu des normes internationales pertinentes et sous réserve des paragraphes2 et 2 bis, la Commission, au moyen d'actes d'exécution, réexamine et définit, respectivement, des spécifications techniques, des normes et des procédures minimales par rapport auxquelles des niveaux de garantie faibles, substantiels et élevés sont spécifiés pour les moyens d'identification électronique aux fins du paragraphe 1.

(...)

Article 12 quater

(b) Reconnaissance mutuelle d'autres moyens d'identification électronique

1. Lorsqu'une identification électronique par le biais d'un moyen d'identification électronique et l'authentification sont requises en vertu du droit national ou de la pratique administrative pour accéder en ligne à un service en ligne fourni par un organisme du secteur public dans un État membre, le moyen d'identification électronique délivré 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 transfrontière pour ce service en ligne, pour autant que les conditions suivantes soient remplies:

(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;

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

(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 d'assurance substantiel ou élevé en ce qui concerne l'accès à ce service en ligne, et le niveau de sécurité combiné très élevé si des contrôles d'identité par voie électronique supplémentaires sont effectués.

Cette reconnaissance intervient au plus tard 6 mois après la publication par la Commission de la liste visée au premier alinéa, point a).

2. Un moyen d'identification électronique qui est délivré dans le cadre d'un schéma d'identification électronique figurant sur la liste visée à l'article 9 et qui correspond au niveau de garantie «faible» peut être reconnu par les organismes du secteur public aux fins de l'authentification transfrontière pour le service en ligne fourni par ces organismes.

Article 24

Exigences applicables aux prestataires de services de confiance qualifiés

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) par le biais d'un moyen d'identification électronique notifié qui satisfait aux exigences énoncées à l'article 8 en ce qui concerne les niveaux de garantie «substantiel» ou «élevé» ou le niveau de sécurité combiné « très élevé » ;

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

(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 *in situ* de la personne physique ou d'un représentant autorisé de la personne morale par des procédures appropriées et conformément à la législation nationale si d'autres moyens ne sont pas disponibles.»

(...)

***

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

ANNEXE III – Suggestion d'amendements sur les attributs du portefeuille digital

Propositions d'amendements relatives aux personnes vulnérables, aux mineurs, au modèle économique du portefeuille numérique européen, à la clôture de ce portefeuille au décès, à la définition et à la révocation des attributs et à la liste des attributs minimaux.

Propositions sur les considérants :

Considérant 18

Commission européenne	Proposition
(18) Conformément à la directive (UE) 2019/88222, 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.	(18) Conformément à la directive (UE) 2019/88222, 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. **Un tiers de confiance de leurs portefeuilles devrait pouvoir être désigné par une autorité judiciaire.** **Les Etats membres organisent l'utilisation des portefeuilles numériques européens par les tiers de confiance.**

Justification :

Pour les adultes placées sous un régime de protection, il devrait être possible de désigner un tiers de confiance qui pourrait utiliser les fonctionnalités du portefeuille à leur place. Car les régimes de protection varient d'un Etat membre à l'autre, il leur revient d'organiser le rôle du tiers de confiance

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

désigné par une autorité judiciaire. Dans le cadre d'une tutelle, il serait possible d'imaginer que le tiers de confiance prenne le contrôle total du portefeuille numérique européen.

Ajout d'un considérant 18 bis

	Proposition
	Les Etats membres organisent l'utilisation des portefeuilles numériques européens pour les personnes mineures d'âge.

Justification :

Le projet de règlement européen ne précise pas les conditions d'utilisation par les mineurs. Il revient aux Etats membres de le préciser au cas par cas.

Considérant 27

Commission européenne	**Proposition**
(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.	(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 **et être chargée de leur révocation**. 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

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

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.	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. **Les Etats membres associent les organisations professionnelles à la définition des attributs qui les concernent.**

Justification :

Cette proposition d'amendement vient préciser qui a la charge de la révocation des attributs et l'implication des organisations professionnelles pour les attributs qui les concernent (qualité professionnelle par exemple).

Propositions sur les articles :

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

(…)

l'article 3 est modifié comme suit:

(…)

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

Commission européenne	Proposition
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;	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 **et est chargé de leur révocation** 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;

Justification :

Il s'agit de préciser la responsabilité de la révocation des attributs.

Ajout d'une nouvelle définition : tiers de confiance

	Proposition
	56 (nouveau) : **« Tiers de confiance » : personne physique désignée par une autorité judiciaire dans le cadre de la mise en place d'un régime de protection. Elle peut utiliser les portefeuilles numériques européens au profit de leur détenteur.**

Justification :

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

Insertion d'une définition pour le nouveau « tiers de confiance ».

Article 6 bis Portefeuilles européens d'identité numérique

Commission européenne :	Proposition :
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.	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. **Un acte délégué détermine le modèle économique des portefeuilles numériques européens.**

Justification :

Le projet de règlement ne précise pas le modèle économique des portefeuilles. Il n'est pas à exclure que les couts pour les entreprises et les administrations qui les utiliseront varient fortement d'un Etat membre à l'autre créant ainsi des discriminations. Il convient que le modèle économique soit fixé au niveau européen.

Article 6 bis Portefeuilles européens d'identité numérique

Commission européenne	**Proposition**
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	7. L'utilisateur **ou le tiers de confiance désigné par une autorité judiciaire** exerce un contrôle total sur le portefeuille européen d'identité numérique. L'entité qui délivre le portefeuille européen d'identité numérique ne collecte pas

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

ne sont pas nécessaires à la fourniture des services qui y sont attachés; elle ne combine 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.	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.

Justification :

Cet ajout permet de placer le tiers de confiance et l'utilisateur à égalité dans leur accès aux fonctionnalités.

Ajout d'un 7 bis :

	Proposition
	Au décès de l'utilisateur, l'autorité chargée du règlement de la succession s'assure de la bonne extinction des portefeuilles

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

	numériques européens et de la transmission aux héritiers et ayants droits des éléments à caractère patrimonial.

Justification :

Cet ajout devrait permettre au notaire de s'assurer de la bonne fermeture du portefeuille et de la bonne transmission d'éléments à caractères patrimoniaux comme les cryptomonnaies.

Propositions sur l'annexe VI: liste minimale d'attributs

Commission européenne	Proposition
Conformément à l'article 45 quinquies, les États membres veillent à prendre les mesures nécessaires pour permettre aux prestataires qualifiés d'attestations électroniques d'attributs de vérifier par des moyens électroniques, à la demande de l'utilisateur, l'authenticité des attributs suivants, 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, et lorsque ces attributs sont fondés sur des sources authentiques dans le secteur public: 1. l'adresse; 2. l'âge; 3. le sexe;	Conformément à l'article 45 quinquies, les États membres veillent à prendre les mesures nécessaires pour permettre aux prestataires qualifiés d'attestations électroniques d'attributs de vérifier par des moyens électroniques, à la demande de l'utilisateur, l'authenticité des attributs suivants, 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, et lorsque ces attributs sont fondés sur des sources authentiques dans le secteur public: 1. l'adresse; 2. **la date de naissance** 3. le sexe;

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

4. l'état civil; 5. la composition de famille; 6. la nationalité; 7. les diplômes, titres et certificats du système éducatif; 8. les diplômes, titres et certificats professionnels; 9. les permis et licences; 10. les informations financières et les données des entreprises.	4. l'état civil; 5. **le statut matrimonial** 6. **les nationalités** 7. les diplômes, titres et certificats du système éducatif; 8. les diplômes, titres et certificats professionnels; 9. les permis, licences **et mandats;** 10. les informations financières et les données des entreprises. **11. Activation d'un régime de protection et nom du tiers de confiance** **12. Ascendance et descendance** **13. Un élément d'identification photographique et des données biométriques**

Justification :

La date de naissance est une donnée plus utile que l'âge. L'attribut composition de famille semble compliqué à mettre en œuvre tant qu'il n'existe pas de livret de famille européen.

Le statut matrimonial semble être une donnée plus facilement intégrable. Ce nouvel attribut devrait préciser si la personne est mariée, liée par un partenariat civil, veuve, divorcée et la présence ou non d'un contrat de mariage.

Certains citoyens ont plusieurs nationalités. Comme le nombre de portefeuilles numériques européens disponibles par Etat membre n'est pas arrêté, il est préférable de prévoir l'hypothèse pour laquelle un citoyen européen binational/trinational aurait besoin d'indiquer cette double/triple qualité. Par exemple pour pouvoir voter en ligne.

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu

Il convient de prévoir un champ obligatoire permettant de savoir si la personne est placée sous un régime de protection et les informations relatives au tiers de confiance pour le cas où celui-ci serait désigné.

Il est proposé un attribut relatif à l'ascendance et à la descendance. Il contiendrait des éléments relatifs aux parents et aux enfants du titulaire du portefeuille.

Afin de garantir une lutte efficace contre le blanchiment de capitaux, l'échange sécurisé d'éléments d'identification photographique et de données biométriques doit être garanti. Par conséquent, les photos devraient être incluses dans la liste minimale des attributs.

***

Conseil des Notariats de l'Union européen (CNUE)

Bruxelles, le 18 mars 2022

CNUE asbl - Avenue de Cortenbergh, 120 - B - 1000 Bruxelles - Tél. +32(0)2 513 95 29 - Fax +32(0)2 513 93 82 - E-mail : info@cnue.be - www.cnue.eu