



Conseil de l'Union européenne
Secrétariat général

Bruxelles, 16 mai 2022

WK 6884/2022 INIT

LIMITE

TELECOM

Ceci est un document destiné à une communauté spécifique de destinataires. La manipulation et la distribution ultérieure sont sous la seule responsabilité des membres de la communauté.

DOCUMENT DE SÉANCE

De: Secrétariat Général du Conseil
A: Groupe "Télécommunications et société de l'information"

Sujet: Règlement sur eIDAS : Projet de rapport sur l'état des travaux (versions FR,EN)

Les délégations trouveront en annexe les versions FR et EN du projet de rapport sur l'état des travaux sur le règlement sur le cadre européen relatif à une identité numérique - eIDAS, en vue de sa présentation au Coreper le 20 mai 2022.



Bruxelles, le 12 mai 2022
(OR. fr)

xxxx/22

**Dossier interinstitutionnel:
2021/0136(COD)**

LIMITE

**TELECOM 187
COMPET 283
MI 338
DATAPROTECT 128
JAI 577
CODEC 597**

NOTE

Origine:	la présidence
Destinataire:	Comité des représentants permanents/Conseil
N° doc. Cion:	9471/21
Objet:	Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique - Rapport sur l'état des travaux

I. INTRODUCTION

1. La Commission a adopté la proposition de règlement sur une identité numérique européenne (eID) le 3 juin 2021¹. L'initiative modifie le règlement eIDAS de 2014², qui avait jeté les bases nécessaires pour accéder en toute sécurité aux services et effectuer des transactions en ligne transfrontalières dans l'UE .

¹ doc. 9471/21.

² [REGULATION \(EU\) No 910/2014](#).

2. La proposition, basée sur l'article 114 du TFUE, impose aux États membres de délivrer un portefeuille européen d'identité numérique dans le cadre d'un schéma d'identification électronique notifié, fondé sur des normes techniques communes et après une évaluation de conformité obligatoire par des organismes d'accréditation nationaux et sur la base d'une certification dans le cadre de la certification européenne de cybersécurité et du RGPD. Afin de mettre en place l'architecture technique nécessaire, d'accélérer la mise en œuvre du règlement révisé, de fournir des lignes directrices aux États membres et d'éviter la fragmentation, la proposition était accompagnée d'une recommandation pour le développement d'une boîte à outils de l'Union.

Plus précisément, la proposition de règlement vise à assurer l'accès universel des personnes et des entreprises à une identification et une authentification électroniques sécurisées et fiables au moyen d'un portefeuille numérique personnel sur le téléphone mobile. Ce portefeuille sera largement utilisable pour l'identification et l'authentification. Il devrait être reconnu dans le secteur public de l'UE ainsi que par les prestataires de services privés qui exigent une authentification forte des utilisateurs et par les très grandes plateformes en ligne. D'autres prestataires de services privés sont encouragés à reconnaître le portefeuille par le biais de mesures réglementaires volontaires. La proposition oblige également les États membres à notifier un schéma d'identification électronique, garantissant ainsi que l'écosystème européen de l'identité numérique peut compter sur la disponibilité de moyens très fiables et sécurisés. La proposition autorise l'utilisation de solutions d'identité numérique et crée un cadre juridique et une plate-forme technique pour l'échange d'attributs et d'informations liés à l'identité. La proposition prévoit le contrôle des utilisateurs et la protection des données ainsi que le partage ciblé des données d'identité limité aux besoins du service spécifique demandé. La proposition garantit également des conditions égales pour la fourniture et la supervision de services de confiance qualifiés dans l'UE.

3. Au Parlement européen, la proposition a été confiée à la commission de l'industrie, de la recherche et de l'énergie (ITRE) avec trois commissions associées pour avis, à savoir le marché intérieur et la protection des consommateurs (IMCO), les affaires juridiques (JURI) et les libertés civiles, la justice et les affaires intérieures (LIBE). Le rapporteur du dossier est Romana Jerković (S&D, Croatie). La commission ITRE n'a pas encore adopté son rapport.

4. Le 15 juillet 2021, le Comité économique et social européen a été invité à rendre son avis sur la proposition, qui a ainsi été rendu le 20 octobre 2021. Le Comité européen des régions a spontanément rendu un avis sur la proposition le 12 octobre 2021.
5. Le Contrôleur Européen de la Protection des Données (CEPD) a publié des commentaires formels sur la proposition le 28 juillet 2021.

II. TRAVAUX AU SEIN DU CONSEIL

6. Au Conseil, l'examen de la proposition a été effectué au sein du groupe "Télécommunications et société de l'information" (ci-après: GT TELECOM). Le GT TELECOM a commencé à discuter de la proposition sous la Présidence PT en juin 2021.
7. L'analyse de la proposition s'est poursuivie au sein du GT TELECOM sous la Présidence SI, la première lecture s'étant conclue avec succès le 15 novembre 2021.
8. La Présidence FR a consacré la réunion du GT TELECOM du 27 janvier 2022 à une présentation par la Commission des progrès réalisés, au niveau technique, sur la boîte à outils. Les délégations ont été invitées à faire part de leurs suggestions et commentaires sur l'ensemble du règlement avant le 31 janvier.
9. Une première proposition de compromis a été présentée lors de la réunion du GT TELECOM du 15 mars 2022. La proposition a suscité des demandes de clarification sur les principales parties du règlement - en particulier le portefeuille européen d'identité numérique et ses fonctionnalités - ainsi que sur la compatibilité avec les solutions nationales existantes. Les discussions ont porté sur la protection des données ainsi que l'interaction avec les législations existantes, en se concentrant sur les définitions, les questions de sécurité et la nécessité d'un niveau de garantie "élevé" ou "substantiel".
10. L'examen de la première proposition de compromis s'est poursuivi lors de la réunion du GT TELECOM du 5 avril 2022. Les discussions ont porté sur les services de confiance, le régime de responsabilité des prestataires de services de confiance et leur supervision. La discussion s'est ensuite déplacée vers la définition et la portée des nouveaux services de confiance

introduits dans la proposition de la Commission (archivage électronique et registres électroniques). Des discussions ont également eu lieu sur l'identifiant unique et persistant.

11. Le 5 mai, la présidence FR a invité les États membres à une discussion approfondie sur quatre questions particulièrement complexes et stratégiquement importantes :
 - Le concept de portefeuille européen d'identité numérique (PEIN) et son articulation avec les moyens d'identification électronique (nationaux) ;
 - Le niveau de garantie du PIEN
 - Le concept de fournisseurs d'attestations électroniques d'attributs ;
 - L'identifiant unique et persistant.

12. Au cours des discussions au sein du GT TELECOM, différentes questions ont été abordées.
 - a. Certains États membres ont souligné la nécessité d'une bonne coordination entre les travaux législatifs au sein du GT TELECOM et les travaux techniques menés pour le développement de la boîte à outils. Certains États membres ont également exprimé leur souhait d'une approche globale plus claire de l'articulation entre le règlement sur le portail unique numérique, qui comprend la mise en place d'un système technique d'échange automatisé de preuves entre les autorités compétentes des États membres, connu sous le nom de "Once Only Technical System" (OOTS) et la révision du règlement eIDAS, car ils étaient préoccupés par les réflexions en silos sur de nouvelles solutions transfrontalières pour la prestation de services et par le caractère soutenable de la création de systèmes potentiellement redondants.

Le portefeuille européen d'identité numérique (PEIN) et l'identification électronique

- b. Certains États membres ayant demandé plus de clarté sur la nature du PEIN, notamment en ce qui concerne sa fonction de moyen d'identification électronique et sa fonction de partage de différents types de données personnelles, d'attributs et de certificats sous le contrôle de l'utilisateur, la présidence FR a tenté de clarifier le concept de PEIN et son articulation avec celui de moyen d'identification électronique en introduisant une approche fonctionnelle du portefeuille. Certains États membres ont exprimé leur soutien au fait que le PEIN soit un moyen d'identification électronique en soi, tandis que d'autres États membres ont rappelé que le PEIN devrait pouvoir fonctionner en synergie avec les moyens d'identification électronique (nationaux) existants et/ou devrait être considéré

comme un "conteneur" permettant d'assurer différentes fonctions. Cette question est toujours ouverte à la discussion.

- c. Les fonctionnalités et exigences devant être respectées par le PEIN ont été considérablement retravaillées par la Présidence FR, laissant la question du niveau de garantie [élevé/substantiel] ouverte à la discussion. Certains États membres ont apporté leur plein soutien à la proposition de la Commission appelant à un niveau de garantie « élevé » du PEIN, car ils estiment qu'il est essentiel pour garantir la sécurité et la confiance des utilisateurs. D'autres, au contraire, ont exprimé leur préférence pour le niveau « substantiel » estimant qu'un niveau « élevé » risquerait de limiter l'adoption de l'utilisation du PEIN. Certains États membres ont également demandé davantage de précisions sur le modèle commercial du PEIN.
- d. Les dispositions relatives aux parties utilisatrices ont également été profondément modifiées afin de définir plus précisément leurs obligations (par exemple l'enregistrement et l'information sur l'utilisation prévue du portefeuille européen d'identité numérique) et de tenir compte des pratiques nationales en vigueur. Les dispositions relatives à la certification de l'EDIW ont été entièrement remaniées afin de les aligner sur le RGPD et les exigences de cybersécurité.
- e. Certains États membres se sont interrogés sur l'opportunité d'introduire un nouveau service de confiance pour la fourniture d'attestations électroniques d'attributs considérant que la valeur ajoutée de ce service de confiance semble limitée et ont demandé des éclaircissements sur le rôle du secteur public dans ce nouveau service de confiance. D'autres États membres ont soutenu la création de ce nouveau service de confiance et l'ont considéré comme un complément utile à l'écosystème du portefeuille . Les modifications les plus importantes introduites par la Présidence FR concernent la séparation fonctionnelle et/ou juridique à mettre en place par les fournisseurs d'attestations électroniques qualifiée d'attributs dans la prestation de leurs services. La vérification des attributs par rapport aux sources authentiques et le rôle/obligations des fournisseurs d'attestations électroniques des attributs à l'EDIW n'ont été que légèrement modifiés et sont toujours ouverts à la discussion.
- f. Certains États membres ont pleinement soutenu la proposition de la Commission de mettre en place un identifiant unique et persistant, estimant que l'identifiant ne devrait pas seulement être unique, mais également persistant afin de permettre l'appariement des identités et de faciliter la fourniture de services publics en ligne. Certains États membres,

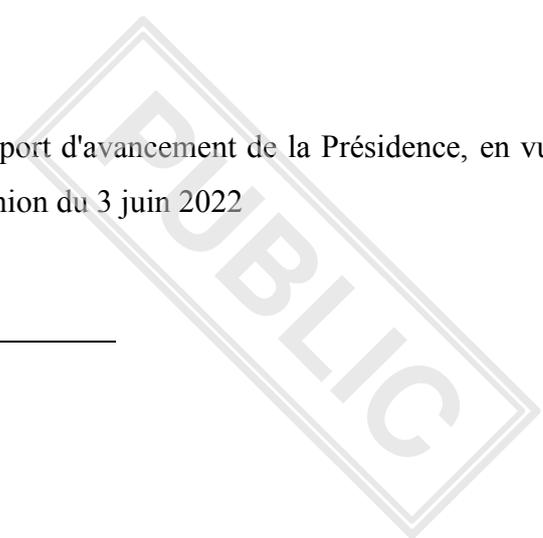
au contraire, ont estimé qu'un tel identifiant unique et persistant pourrait éventuellement faciliter le profilage et le suivi des citoyens dans le monde numérique, ont remis en question la nécessité d'introduire un tel identifiant et ont suggéré d'envisager d'autres options. Cette question est toujours ouverte à la discussion.

Services de confiance

- g. La Présidence FR a rétabli les dispositions relatives à la responsabilité et à la charge de la preuve des fournisseurs de services de confiance, car elles étaient considérées par les États membres comme un point essentiel pour la crédibilité de l'ensemble du règlement.
- h. La Présidence FR a tenté de clarifier et de renforcer les dispositions sur les aspects internationaux afin de garantir la sécurité juridique et que les exigences appliquées aux fournisseurs de services de confiance établis dans des pays tiers soient identiques ou équivalentes à celles imposées aux fournisseurs de services de confiance qualifiés dans l'Union et que ces exigences puissent être correctement appliquées et supervisées.
- i. Dans la perspective de la révision de la directive NIS et de l'adoption de la directive NIS2 et de l'inclusion du régime de sécurité des fournisseurs de services de confiance dans NIS2, la Présidence FR a clarifié les rôles, la coopération et les processus respectifs des organes de contrôle au titre de la directive NIS2 et du règlement eIDAS. La Présidence FR a également proposé de rétablir les exigences spécifiques eIDAS pour les prestataires de services de confiance non qualifiés qui ont été supprimées en tant qu'effet secondaire de la révision de la directive NIS et ne releveront pas du champ d'application de la nouvelle directive. La Présidence FR a également détaillé les délais et processus applicables aux fournisseurs de services de confiance pour notifier une violation de données ou une interruption de la fourniture de leurs services.
- j. En ce qui concerne l'archivage électronique et les registres électroniques, la Présidence FR a proposé des changements substantiels à la définition et aux exigences de ces deux nouveaux services de confiance qui ont été introduits dans la révision eIDAS. Certains États membres ont remis en question la nécessité d'introduire de tels services de confiance tandis que d'autres l'ont pleinement soutenu.

III. CONCLUSION

13. Le COREPER est invité à prendre note de ce rapport d'avancement de la Présidence, en vue de le soumettre au Conseil Télécom lors de sa réunion du 3 juin 2022





Brussels, 12 May 2022
(OR. en)

xxxx/22

**Interinstitutional File:
2021/0136(COD)**

LIMITE

**TELECOM 187
COMPET 283
MI 338
DATAPROTECT 128
JAI 577
CODEC 597**

NOTE

From: Presidency
To: Permanent Representatives Committee/Council
No. Cion doc.: 9471/21
Subject: Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity
- Progress report

I. INTRODUCTION

1. The Commission adopted the proposal for a Regulation on a European Digital Identity (European eID) on 3 June 2021¹. The initiative amends the eIDAS Regulation from 2014², which had laid the necessary foundations to safely access services and carry out transactions online and across borders in the EU.

¹ doc. 9471/21.

² [REGULATION \(EU\) No 910/2014](#).

2. The proposal, based on Article 114 TFEU, requires Member States to issue a European Digital Identity Wallet under a notified eID scheme, built on common technical standards and following compulsory compliance assessment by national accreditation bodies and based on certification under the European cybersecurity certification and GDPR frameworks. In order to set up the necessary technical architecture, to speed –up the implementation of the revised Regulation, provide guidelines to Member states and to avoid fragmentation, the proposal was accompanied by a Recommendation for the development of a Union Toolbox.

More specifically, the proposed Regulation aims to provide for universal access for people and businesses to secure and trustworthy electronic identification and authentication by means of a personal digital wallet on the mobile phone. This wallet will be widely usable for identification and authentication. It should be recognized in the public sector across the EU as well as by private service providers that require strong user authentication and by very large online platforms. Other private service providers are encouraged to recognize the wallet through voluntary regulatory measures. The proposal also makes it mandatory for Member States to notify an electronic identification scheme, ensuring the European Digital Identity Ecosystem can rely on the availability of highly trustworthy and secure means for onboarding. The proposal empowers the use of digital identity solutions and creates a legal framework and a technical platform for the exchange of attributes and credentials linked to identity. The proposal provides for user control and data protection and the targeted sharing of identity data limited to the needs of the specific service requested. The proposal also ensures equal conditions for the provision and supervision of qualified trust services in the EU.

3. In the European Parliament, the proposal was assigned to the Committee on Industry, Research and Energy (ITRE) with three associated committees for opinion, namely Internal Market and Consumer Protection (IMCO), Legal Affairs (JURI) and Civil Liberties, Justice and Home Affairs (LIBE). The rapporteur for the file is Romana Jerković (S&D, Croatia). The ITRE committee has not yet adopted its report.

4. On 15 July 2021 the European Economic and Social Committee was requested to provide its opinion on the proposal, which was subsequently delivered on 20 October 2021. The European Committee of the Regions spontaneously issued an opinion on the proposal on 12 October 2021.
5. The European Data Protection Supervisor (EDPS) issued formal comments on the proposal on 28 July 2021.

II. WORK WITHIN THE COUNCIL

6. In the Council, the examination of the proposal has been carried out in the Working Party on Telecommunications and Information Society (hereinafter: WP TELECOM). The WP TELECOM started discussing the proposal under the PT Presidency in June 2021.
7. The analysis of the proposal continued in the WP TELECOM under the SI Presidency, with the first reading being successfully concluded on 15 November 2021.
8. The FR Presidency dedicated the WP TELECOM meeting of 27 January 2022 to a presentation by the Commission on the progress made on the Toolbox, at technical level. Delegations were invited to share their suggestions and comments on the whole Regulation by 31 January.
9. A first compromise proposal was presented at the WP TELECOM meeting of 15 March 2022. The proposal triggered requests for further clarity on the main components of the Regulation — in particular the European Digital Identity Wallet and its functionality — as well as for compatibility with existing national solutions. The discussions spanned from data protection to the interplay with existing legislation, focusing on definitions, security aspects, and the need for an assurance level "high" or "substantial".
10. The examination of the first compromise proposal continued at the WP TELECOM meeting of 5 April 2022. The discussions focused on trust services, the liability regime of trust service providers and their supervision. The discussion then shifted towards the definition and scope of new trust services introduced in the proposal of the Commission (electronic archiving and electronic ledgers). There were also discussions on the unique and persistent identifier.

11. On 5 May the FR Presidency invited Member States to an in-depth discussion on four particularly complex and strategically important issues:
- The concept of the European Digital Identity Wallet (EDIW) and its articulation with the (national) electronic identification means;
 - The level of assurance of the EDIW;
 - The concept of providers of electronic attestations of attributes ;
 - The unique and persistent identifier.
12. During discussions in WP TELECOM, different issues were addressed.
- a. Some Member States stressed the need for good coordination between the legislative work within the WP TELECOM and the technical work carried out for the development of the Toolbox. Some Member States also expressed their wish of a clearer overall approach of the articulation between the Single Digital Gateway Regulation (SDGR), which includes establishing a technical system for the automated exchange of evidence between competent authorities in Member States, known as the Once Only Technical System (OOTS) and the revision of eIDAS Regulation, as they were concerned about thinking in silos on new cross-border solutions for delivery of services and regarding the sustainability of making potentially redundant systems.

The European Digital Identity Wallet (EDIW) and the electronic identification

- b. As some Member States asked for more clarity on the nature of the EDIW, notably regarding its function as an electronic identification means and its function of sharing different types of personal data, attributes and certificates under control of the user, the FR Presidency tried to clarify the concept of the EDIW and its articulation with that of electronic identification means by introducing a functional approach to the EDIW. Some Member States expressed support for the EDIW being an electronic identification means in itself, whereas other Member States reminded that the EDIW should be able to operate in synergy with existing (national) electronic identification means and/or should be considered as a “container” allowing different functions. This issue is still open for discussion.
- c. The functionality and requirements of the EDIW were reworked substantially by the FR Presidency, with leaving the issue of assurance level [high/substantial] open for discussion. Some Member States gave their full support for the proposal of the

Commission calling for a “high” level of assurance of the EDIW, as they believe it to be essential to guarantee the security and confidence of users. Others, on the contrary, expressed their preference for level "substantial" considering that level “high” would risk limiting the take up of the use of the EDIW. Some Member States also requested more clarity on the business model of the EDIW.

- d. Provisions regarding relying parties were also profoundly changed with a view to defining more precisely their obligations (i.e. registration and information on the intended use of the European Digital Identity Wallet) and to taking established national practices into account. Provisions on the certification of the EDIW were completely redrafted in order to align the provision with GDPR and cybersecurity requirements.
- e. Some Member States have asked about the advisability of introducing a new trust service for the provision of electronic attestation of attributes considering that the added value of this trust service appears to be limited and asked clarification about the role of the public sector in this new trust service. Other Member States supported the creation of this new trust service and considered it a useful complement of the wallet ecosystem . The most important modifications introduced by FR Presidency concern the functional and/or legal separation to be enacted by providers of qualified electronic attestation of attributes in providing their services. The verification of attributes against authentic sources and the role/rules for providers of electronic attestation of attributes to the EDIW have been changed only slightly and are still open for discussion.
- f. Some Member States fully supported the proposal of the Commission to set up a unique and persistent identifier, considering that the identifier should not only be unique, but also persistent in order to enable identity matching and facilitate the provision of public services online. Some Member States, on the contrary, considered that such a unique and persistent identifier could possibly facilitate the profiling and monitoring of citizens in the digital world, questioned the need to introduce such an identifier and suggested the consideration of other options. This issue is still open for discussion.

Trust services

- g. The FR Presidency reinstated provisions on liability and burden of proof of trust service providers as it was considered by Member States as a crucial point for the credibility of the whole regulation.

- h. The FR Presidency tried to clarify and to strengthen the provisions on international aspects in order to ensure legal certainty and that the requirements applied for trust services providers established in third countries are the same or equivalent as to those imposed on qualified trust service providers in the Union and that these requirements can be properly enforced and supervised.
- i. In view of the revision of the NIS directive and the adoption of directive NIS2 and of the inclusion of security regime of trust service providers under NIS2, the FR Presidency intended to clarify the respective roles, cooperation and processes of supervisory bodies under NIS2 directive and eIDAS regulation. The FR Presidency also proposed to reinstate specific eIDAS requirements for non-qualified trust service providers which were deleted as a side effect of the revision of the NIS directive and did not fall within the scope of the new directive. The FR Presidency also detailed the time-delays and processes for trust service providers to notify a data breach or disruption in the provision of their services.
- j. Concerning electronic archiving and electronic ledgers, the FR Presidency proposed substantial changes to the definition and the requirements for these two new trust services which have been introduced in the eIDAS revision. Some Member States have questioned the need to introduce such trust services whereas others fully supported it.

III. CONCLUSION

- 13. The COREPER is invited to take note of this progress report from the Presidency, with a view to submitting it to the TTE Telecom Council at its meeting on 3 June 2022.