



**European Committee
of the Regions**

ECON-VII/019

146th plenary session, 12-14 October 2021

OPINION

European Digital Identity

THE EUROPEAN COMMITTEE OF THE REGIONS

- backs the idea of a European Digital Identity Wallet. It should enable citizens to prove their identity, including while on the move, so they can access online public administration services, swap digital documents or just attest a personal identity attribute, such as age;
- emphasises the need to ensure that all users are autonomous and not subject to discrimination, and therefore recommends that the Communication state clearly that there must be no indirect coercion to use the European Digital Identity Wallet when services are offered to natural persons. It is a matter of principle that use is a voluntary act;
- urges that provision be made in the proposal for the use of digital identities by minors or in cases where responsibility lies with a guardian or carer, as well as for dealing with digital identities when somebody dies;
- advises that, when it comes to the ID used for access by economic operators, the authorisation check should be designed with a secured certificate whose validity is of limited duration or cyclical;
- suggests that implementation, particularly in the start-up phase, should be configured incrementally. This is important because the hitherto partly unregulated economy is sometimes being involved for the very first time in the use of electronic identities at the assurance levels "substantial" to "high" as the current eIDAS environment evolves;
- warns against hasty implementation of a European Digital Identity Wallet solution because of the technical risks inherent in the centralised storage of identity data in a mostly mobile application. Such a solution will undoubtedly be seen as a prime target for a wide range of cyberattacks and must therefore be able to fend off the threats at any particular moment.

Rapporteur:

Mark Weinmeister (DE/EPP), Secretary of State for European Affairs, Land of Hesse

Reference documents

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
COM(2021) 281 final

Draft opinion of the European Committee of the Regions – European Digital Identity

I. RECOMMENDATIONS FOR AMENDMENTS

Amendment 1

COM(2021) 281

Article 1(4)

Regulation (EU) No 910/2014

Article 5

<i>Text proposed by the European Commission</i>	<i>CoR amendment</i>
Pseudonyms in electronic transaction Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.	Pseudonyms in electronic transaction Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions <i>and in the use of social networks</i> shall not be prohibited.

Reason

Social networks must not prohibit the use of pseudonyms for registration in relation to the European Digital Identity Wallet.

Amendment 2

COM(2021) 281

Article 1(7)

Regulation (EU) No 910/2014

Article 6a (1)

<i>Text proposed by the European Commission</i>	<i>CoR amendment</i>
For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless access to cross-border public and private services, each Member State shall issue a European Digital Identity Wallet within 12 months after the entry into force of this Regulation.	For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless access to cross-border public and private services, each Member State shall issue a European Digital Identity Wallet within 24 months after the entry into force of this Regulation.

Reason

Experience has shown that European Digital Identity Wallets will be a prime target for IT attacks. In such a sensitive environment for personal ID data, quality trumps speed. The deadlines set for transposition at national level are too short (and partly dependent on the provisions of the NIS 2 Directive) and an extended transitional period is therefore necessary.

Amendment 3

COM(2021) 281 final – Part 1

Article 1(7)

Regulation (EU) No 910/2014

Article 6a (12) (new)

<i>Text proposed by the European Commission</i>	<i>CoR amendment</i>
	<i>The European Digital Identity Wallet shall only be made available to people under the age of 18 on condition that their identity can be confirmed from an electronic ID card of their legal representative, who is responsible for them.</i>

Reason

A European Digital Identity Wallet will serve as proof of identity online and offline. Minors cannot be made fully responsible and held accountable for any legal implications or consequences.

Amendment 4

COM(2021) 281 final – Part 1

Article 1(7)

Regulation (EU) No 910/2014

Article 6c (5)

<i>Text proposed by the European Commission</i>	<i>CoR amendment</i>
Member States shall communicate to the Commission the names and addresses of the public or private bodies referred to in paragraph 3. The Commission shall make that information available to Member States.	Member States shall communicate to the Commission the names and addresses of the public or private bodies referred to in paragraph 3. The Commission shall make that information available to the Member States <i>no later than six months after the entry into force of the Regulation.</i>

Reason

To amend Article 6c(5) of Regulation (EU) No 910/2014 as it is appropriate to set a deadline for communicating the information.

Amendment 5
COM(2021) 281
Article 1(9)
Regulation (EU) No 910/2014
Article 7

<i>Text proposed by the European Commission</i>	<i>CoR amendment</i>
[...] within 12 months after entry into force [...]	[...] within 24 months after entry into force [...]

Reason
Experience has shown that European Digital Identity Wallets will be a prime target for IT attacks. In such a sensitive environment for personal ID data, quality trumps speed. The deadlines set for transposition at national level are too short (and partly dependent on the provisions of the NIS 2 Directive) and an extended transitional period is therefore necessary.

Amendment 6
COM(2021) 281
Article 1(11)
Regulation (EU) No 910/2014
Article 10a(4)

<i>Text proposed by the European Commission</i>	<i>CoR amendment</i>
The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 6d without undue delay.	The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 6d without undue delay <i>and shall make these amendments available in a separate list.</i>

Reason
A clear (blocking) list should make use easier.

Amendment 7
COM(2021) 281- Part 1
Article 1(12)
Regulation (EU) No 910/2014
Article 11a (4) (new)

<i>Text proposed by the European Commission</i>	<i>CoR amendment</i>
	<i>The Member States shall use unique identification systems to ensure that no citizen is issued with two or more European Digital Identity Wallets as a result of multiple nationalities or residence in different Member States.</i>

Reason

It should be ensured that citizens with more than one nationality and/or residence in more than one Member State are only issued one European Digital Identity Wallet.

Amendment 8

COM(2021) 281- Part 1

Article 1(14)

Regulation (EU) No 910/2014

Article 12a (3)

<i>Text proposed by the European Commission</i>	<i>CoR amendment</i>
Member States shall notify to the Commission with the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.	Member States shall notify to the Commission with the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to the Member States <i>no later than six months after the entry into force of the Regulation.</i>

Reason

To amend Article 12a(3) of Regulation (EU) No 910/2014 as it is appropriate to set a deadline for communicating the information.

Amendment 9

COM(2021) 281

Article 1(29)

Regulation (EU) No 910/2014

Article 30(3a)

<i>Text proposed by the European Commission</i>	<i>CoR amendment</i>
The certification referred to in paragraph 1 shall be valid for 5 years, conditional upon a regular 2 year vulnerabilities assessment. Where vulnerabilities are identified and not remedied, the certification shall be withdrawn.	The certification referred to in paragraph 1 shall be valid for 5 years, conditional upon a regular 2 year vulnerabilities assessment. Where vulnerabilities are identified and not remedied, the certification shall be withdrawn. <i>Recertification may take place at the earliest after a waiting period of 2 years and a new vulnerability assessment.</i>

Reason

The ban on recertification should be time-limited, since it should remain possible to remedy vulnerabilities, perhaps after a thorough technical revamping.

II. POLICY RECOMMENDATIONS

THE EUROPEAN COMMITTEE OF THE REGIONS

Introduction

1. backs the idea of a European Digital Identity Wallet. It should enable citizens to prove their identity, including while on the move, so they can access online public administration services, swap digital documents or just attest a personal identity attribute, such as age. And they can do this without disclosing their identity or other personal data;
2. welcomes the European Commission's proposals to create a European digital identity as an interim step towards a more comprehensive digital identity wallet and the amendment of the eIDAS Regulation this would necessitate. The European Digital Identity Wallet is not confined to personal identity data (EUID) as narrowly construed but is intended to hold other documents (including official ones) in electronic form, such as driving licences or educational qualifications;
3. supports the European Commission's aim of further developing the eIDAS Regulation for use in the economic sphere in response to evolving market demands, while continuing to make use of the current notified national means of identification. Secure means of electronic identification are of particular importance for the digitalisation of administrative procedures;
4. calls for clear data protection provisions in the European Commission's proposal for a European Digital Identity, which should adhere to the principles set out in the General Data Protection Regulation (GDPR), notably data economy, data privacy and adequate justification, and also ensure that users will be able to control which data they want to share and with whom;
5. sees the European Digital Identity Wallet – because it can be used anywhere, and especially on the go – as a tool that is intended to facilitate social participation and that once deployed throughout the EU, could become an element of European identity that every EU citizen is aware of and can grasp;

Use for citizens

6. sees the creation of a European Digital Identity Wallet as a great opportunity to firmly establish among citizens an EU identity that is tangible and of practical use, including in the single market. The European Digital Identity Wallet creates an unequivocally binding form of identification for all parties concerned whose symbolism far exceeds its purely technical utility;
7. notes that the European Digital Identity Wallet is essentially a mobile technology capable of remaining functionally viable even as today's devices (smartphones or watches) evolve. Further advances such as digital glasses (e.g. augmented reality glasses or digital avatars) or similar digital devices should be able to use the European Digital Identity Wallet via an appropriate (possibly optical) interface;

8. recommends that the development and deployment of the European eID and the European Digital Identity Wallet should be carried out with a view to providing services with real cross-border added value for citizens;
9. emphasises the need to ensure that all users are autonomous and not subject to discrimination, and therefore recommends that the Communication state clearly that there must be no indirect coercion to use the European Digital Identity Wallet when services are offered to natural persons. It is a matter of principle that use is a voluntary act;
10. emphasises that the European Digital Identity Wallet should be perceived as an offer to citizens so that it is positively received by civil society;
11. calls for a simple recommendation for the design that, in the nature of a toolbox, goes beyond mere data protection and accessibility and also enables people with minor impediments or lack of language knowledge to use the European Digital Identity Wallet (e.g. by more use of pictograms);
12. urges that provision be made in the proposal for the use of digital identities by minors or in cases where responsibility lies with a guardian or carer, as well as for dealing with digital identities when somebody dies;

Involving the economic sphere

13. sees the close involvement of technology leaders through a relaxation of the rules on industry as a particularly essential ingredient for success. Only a market-based approach will guarantee a use on the right scale in the EU;
14. draws attention to one essential aspect regarding use for economic purposes, namely the use of e-payment interfaces (Paypal, Google/Apple-Pay, SWIFT, etc.), which, in the economic sphere, are currently based on proprietary user accounts. A European Digital Identity Wallet should comply with the relevant rules on money laundering and digital currencies (Bitcoin, Ethereum, Digital EUR, etc.);
15. calls for account to be taken of two existing and substantively competing business models where use of the European Digital Identity Wallet in the economic sphere is concerned. These are, on the one hand, the major global social networks, which have a valid interest in getting their pseudonym accounts verified, possibly by a public institution. This would, however, undermine the freedom to use the internet and further drive users from its protected area into the dark web. The Committee of the Regions can see no interest in this. On the other hand, there are identity providers who make offers competing with the European Digital Identity Wallet and in order to do so also want to use an identity validated by a public institution;
16. advises that, when it comes to the ID used for access by economic operators, the authorisation check should be designed with a secured certificate whose validity is of limited duration or cyclical. The Committee of the Regions welcomes similar considerations regarding trust service

providers, but points out that the justification for the demand for data from the European Digital Identity Wallet by institutions or organisations must also be protected from abuse;

17. notes that digital solutions for the public and private sectors have already been developed and implemented in some Member States. These country-specific specificities should be integrated as far as possible into the European eID, firstly as changing the existing systems would involve a considerable administrative and financial burden and, secondly, as over the years citizens of these Member States have developed a high level of trust in the existing systems, which should not be jeopardised by the introduction of the European eID;

Implementation and involvement of the Member States

18. therefore strongly recommends that the recommendation to Member States referred to in the Commission's legislative proposal to develop a common toolbox for a coordinated approach to creating the necessary technical framework for the EUid draws heavily on national expertise. This should include current examples of best practice, such as the outcomes and experience of Germany's "Digital Identities" and "Secure Digital Identities Showcase" projects;
19. believes that, when considering the costs and expenses incurred in the planning, the national parameters also need to be logged and merged into an overall EU plan that fairly reflects costs. The national implementation timetables in particular should be gathered and included for this purpose, in addition to timeframes in the EU;
20. calls for the staffing and monetary costs of implementation in the Member States and in local and regional authorities to be taken into account in the overall planning. The European Digital Identity Wallet will be successful if it can be used often enough. National administrations at all levels play a key role here, alongside business. They are increasingly involved by virtue of their own actions, but also through Commission initiatives. The EU Services Directive and the EU Single Digital Gateway make valuable contributions to the digitalisation of the EU single market;
21. suggests that implementation, particularly in the start-up phase, should be configured incrementally. This is important because the hitherto partly unregulated economy is sometimes being involved for the very first time in the use of electronic identities at the assurance levels "substantial" to "high" as the current eIDAS environment evolves;

Data protection and cybersecurity

22. warns against hasty implementation of a European Digital Identity Wallet solution because of the technical risks inherent in the centralised storage of identity data in a mostly mobile application. Such a solution will undoubtedly be seen as a prime target for a wide range of cyberattacks and must therefore be able to fend off the threats at any particular moment;
23. draws attention to the importance of an adequate definition of certification schemes for digital identity wallets and electronic identification schemes, which should not be developed by a

commercial entity, but by the European Union Agency for Cybersecurity (ENISA), in close cooperation with groups of experts, including representatives of local and regional authorities;

24. draws attention to the risk of centrally bundling forms of identity with varying levels of confidentiality in a single technical component. There are significant risks for the authorised user if these fall prey to unauthorised use by third parties. Damage to reputation and integrity can be envisaged as well as financial harm. Spear phishing could also cause significant consequential damage;
25. calls for a technical implementation of the European Digital Identity Wallet that ensures it is sufficiently reinforced against cyberattacks and that suitable blocking facilities and dedicated secure backup systems permit secure reinstallation by the rights-holder.
The strengthening of the European Digital Identity Wallet must be a permanent process. Security by design is the foundation for successful use over the long term and is also essential for the user economy, so it should already be provided in the toolbox;
26. sees a methodically sound solution tailored to the target group of users, with information and documentation, as a critical factor for success, in addition to the requirements of data protection, accessibility and cybersecurity;
27. proposes binding rules on service providers to ensure, as a matter of principle, simple and transparent means of access to European Digital Identity Wallet data via uniform tools (e.g. dashboard) and to make these visible to users;
28. advocates designing the EUid scheme in a way that encourages progress towards the objective of Europe's digital resilience and digital sovereignty;
29. recommends evaluating whether a general technical platform could be created for essential European Digital Identity Wallet functions by making an EU-certified open source toolbox available; maintenance and further development of the toolbox should then be coordinated by the EU;

Familiarising use

30. recommends a requirement, when translating the European Digital Identity Wallet into specific applications, for detailed user guidance in a process-oriented form understandable to the target group of users.
The European Digital Identity Wallet is to be profiled in usage scenarios as a homogeneous component with clear data transfer interfaces and to be presented visually as an EU product by means of distinctive labelling and design;
31. proposes that access to the European Digital Identity Wallet be standardised so that granting use or access to it can become almost a matter of routine for users, while also taking data minimisation requirements into account. This characteristic of routine both makes it easier to use it and enables even the less IT-savvy to do so without error;

Promotion and uptake

32. thinks a big publicity drive is needed to connect with the EU population about the European Digital Identity Wallet and the opportunities it offers for use in the EU internal market, and about the safeguards for data protection and data security; points out that high-speed connectivity is a basic condition for everyone in the European Union, including those living in rural and remote areas, to be able to use and accept the European Digital Identity Wallet;
33. advocates an extension – beyond the original use of the European Digital Identity Wallet – to an EU identity worldwide, including features such as a passport (digital deposit of visas, for instance) or an official EU vaccination certificate. Agreements to be concluded along these lines should enable the European Digital Identity Wallet and the credentials in it to also be used outside the EU;
34. urges the European Commission to engage in intensive discussions and negotiations with suppliers of equipment for the technical provision of the European Digital Identity Wallet to end-users. The aim is to make the technology base available as soon as possible, including in equipment in the low-cost sector.

At present, the first mid-priced and high-end product families with sufficient certification for the "substantial" assurance level under eIDAS are available. It is also useful, in terms of dissemination of the European Digital Identity Wallet, to make sure industry is involved as much as possible as a service provider;

Subsidiarity

35. notes that the proposal for a Regulation is compatible with the subsidiarity principle. An EU-wide technical design of this kind will only have the right effect if the rules are sufficiently uniform. The specific design is a matter exclusively for national rules. Only the cross-cutting tools from the toolbox will have to be assessed.

Brussels, 12 October 2021

The President
of the European Committee of the Regions

Apostolos Tzitzikostas

The Secretary-General
of the European Committee of the Regions

Petr Blížkovský

III. PROCEDURE

Title	European Digital Identity
Reference documents	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 COM(2021) 281 final
Legal basis	Article 307 TFEU
Procedural basis	RoP Rule 41(b)(i)
Date of Council/EP referral/Date of Commission letter	COM(2020) 281 final <ul style="list-style-type: none"> • European Commission: 3.6.2021 • European Parliament: 13.7.2021
Date of Bureau/President's decision	29 June 2021
Commission responsible	Commission for Economic Policy (ECON)
Rapporteur	Mark Weinmeister (DE/EPP)
Analysis	August 2021
Discussed in commission	29.9.2021 (general exploratory debate)
Date adopted by commission	N/A
Result of the vote in commission (majority, unanimity)	unanimity
Date adopted in plenary	12.10.2021
Previous Committee opinions	<i>A strategy for Europe's digital future and a strategy for data.</i> ECON-VII/004, October 2020, rapporteur: Mark Weinmeister (DE/EPP) <i>Digital single market: Mid-term review</i> SEDEC-VI/031, January 2018, rapporteur: Alin-Adrian Nica (RO/EPP) <i>On the Digital Services Act and the Digital Markets Act</i> ECON-VII/012, June 2021, rapporteur: Rodi Kratsa (EL/EPP)
Date of subsidiarity monitoring consultation	N/A