EUROPEAN
COMMISSION

Brussels, XXX
[…](2024) XXX draft

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reactions to security breaches of European Digital Identity Wallets

This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reactions to security breaches of European Digital Identity Wallets

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC[1], and in particular Article 5e(5) thereof,

Whereas:

(1) The European Digital Identity Framework established by Regulation (EU) No 910/2014 is a crucial component in the establishment of a secure and interoperable digital identity ecosystem across the Union. With the European Digital Identity Wallets ('wallets') being the cornerstone of the framework, it aims at facilitating access to services across Member States, while ensuring the protection of personal data and privacy.

(2) Regulation (EU) 2016/679 of the European Parliament and of the Council[2] and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council[3] apply to the personal data processing activities under this Regulation.

(3) The Commission regularly assesses new technologies, practices, standards or technical specifications. To ensure the highest level of harmonisation among Member States for the development and certification of the wallets, the technical specifications set out in this Regulation rely on the work carried out on the basis of Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework[4] and in particular the architecture and reference framework which is part of it. In accordance with recital 75 of Regulation 2024/1183[5], the Commission should review and update

---

1 OJ L 257, 28.8.2014, p.73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

3 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj.

4 OJ L 210, 14.6.2021, p. 51–54, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

5 Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj.

this Implementing Regulation, if necessary, to keep it in line with global developments, the architecture and reference framework and to follow the best practices on the internal market.

(4) Without prejudice to Regulation (EU) 2019/881 of the European Parliament and of the Council[6] and Regulation (EU) 2024/2847 of the European Parliament and of the Council[7] and in particular to the handling of vulnerabilities and their consideration as security breaches, in case of a security breach or a compromise of the wallet solutions or of the validation mechanisms referred to in Article 5a(8) of Regulation (EU) No 910/2014, or of the electronic identification scheme under which the wallet solutions are provided, reactions to such security breaches and compromises need to follow in a fast, coordinated and secure manner across Member States to protect users and to maintain trust in the digital identity ecosystem. Therefore, Member States should ensure the timely suspension of the provision and of the use of wallets affected by a security breach or compromise.

(5) With the objective to ensure appropriate reactions to security breaches or compromises, Member States should assess whether a security breach or compromise affects the reliability of a wallet solution. Such an assessment should be based on uniform criteria, such as the number and category of wallet users and wallet-relying parties impacted, the nature of impacted data, the duration of the compromise or breach, the limited availability of a service and financial losses, and the potential compromise of personal data. These criteria should provide Member States with the proportionate flexibility and discretion to establish whether the reliability of a wallet solution is affected and whether the suspension, or where justified by the severity of the breach or compromise, the withdrawal of the wallet solution is appropriate.

(6) To keep wallet users informed about the status of their wallets, wallet users are to be provided with adequate information about the security breaches or compromises affecting their wallets. As relying parties can also be affected by security breaches and compromises, relevant information on the breaches and compromises also are to be shared with them.

(7) With the objective of improving transparency and building trust into the digital identity ecosystem, the information to be provided about the security breach or compromise and about their consequences should at least disclose the details required under this Implementing Regulation.

(8) Due to the impact and inconvenience caused by a suspension of the use of a wallet solution, Member States shall evaluate whether the revocation of wallets or any other additional measure are necessary to adequately react to the security breach or compromise.

(9) In order to enable users to access their wallet units again after a security breach or compromise has been remedied, the Member State that provided the wallet solution, is

---

6 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

7 Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

to re-establish the provision and the use of that wallet solution without undue delay by re-establishing the wallet units, by issuing a wallet unit provided under a new version of the wallet solution or by re-issuing new valid wallet unit attestations. Users, relying parties, single points of contacts and the Commission are to be informed accordingly.

(10) For the purpose of ensuring the withdrawal of European Digital Identity Wallets where the security breach or compromise was not remedied within three months of the suspension or where this is justified by the severity of the breach or compromise, the notifying Member State should ensure that the relevant wallet unit attestations are revoked and that they cannot be reverted to a valid state nor be issued or provided to existing wallet units. Further, no new wallet units should be provided under the affected wallet solution. For transparency purposes, users, relying parties, single points of contacts and the Commission are to be informed of the withdrawal, including description of the potential impacts on the wallet users and notably the management of issued attestations, or on wallet-relying parties.

(11) To reduce the administrative burden for Member States regarding the relevant notifications to be sent in accordance with this Regulation, Member States should use existing notifications tools such as the Cyber Incident Reporting and Analysis System ('CIRAS') operated by the European Union Agency for Cybersecurity ('ENISA').

(12) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[8] and delivered its opinion on [XX.XX.2024].

(13) The measures provided for in this Regulation are in accordance with the opinion of the committee referred to in Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter and scope

This Regulation lays down rules for reactions to security breaches of the wallets, to be updated on a regular basis to keep in line with technology and standards developments and with the work carried out on the basis of Commission Recommendation (EU) 2021/946, and in particular the Architecture and Reference Framework.

Article 2

Definitions

For the purpose of this Regulation, the following definitions apply:

(1) 'wallet solution' means a combination of software, hardware, services, settings, and configurations, including wallet instances, one or more wallet secure cryptographic applications and one or more wallet secure cryptographic devices;

(2) 'wallet user' means a user who is in control of the wallet unit;

[8] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj.

(3) ‘wallet-relying party’ means a relying party that intends to rely upon wallet units for the provision of public or private services by means of digital interaction;

(4) ‘wallet instance’ means the application installed and configured on a wallet user’s device or environment, which is part of a wallet unit, and that the wallet user uses to interact with the wallet unit;

(5) ‘wallet secure cryptographic application’ means an application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device;

(6) 'wallet secure cryptographic device' means a tamper-resistant device that provides an environment that is linked to and used by the wallet secure cryptographic application to protect critical assets and provide cryptographic functions for the secure execution of critical operations;

(7) ‘wallet provider’ means a natural or legal person who provides wallet solutions;

(8) ‘wallet unit’ means a unique configuration of a wallet solution that includes wallet instances, wallet secure cryptographic applications and wallet secure cryptographic devices provided by a wallet provider to an individual wallet user;

(9) 'critical assets' means assets within or in relation to a wallet unit of such extraordinary importance that where their availability, confidentiality or integrity are compromised, this would have a very serious, debilitating effect on the ability to rely on the wallet unit;

(10) ‘wallet unit attestation’ means a data object that describes the components of the wallet unit or allows authentication and validation of those components.

Article 3

Establishing a security breach or compromise

1. To assess whether a security breach or compromise of their wallet solution, of the validation mechanisms referred to in Article 5a(8) of Regulation (EU) No 910/2014, or of the electronic identification scheme under which their wallet solution is provided, is affecting their reliability or the reliability of other wallet solutions, Member States shall duly consider the criteria set out in the Annex I.

2. Where Member States on the basis of the assessment pursuant to paragraph 1 establish that a security breach or compromise is affecting the reliability of the wallet solution, they shall take the measures set out in Articles 4 and 5.

3. When a Member State becomes aware of a security breach or compromise affecting the reliability of one or more wallet solutions by another Member State, that Member State shall, without undue delay, notify the Commission and the single points of contact designated pursuant to Article 46c(1) of Regulation (EU) No 910/2014. This notification shall include the information set out in Article 5(3), where applicable.

4. The Member State receiving this notification shall take the measures set out in paragraph 1 and 2 without undue delay.

Article 4

Suspension of the provision and the use of European Digital Identity Wallets and other remedies

1. Where a Member State suspends the provision and the use of a wallet solution pursuant to Article 5e(1) of Regulation (EU) No 910/2014, that Member State shall ensure that no wallet units are provided, used or activated under that wallet solution.

2. For the purpose of the suspension of the use of the wallet solutions, Member States shall evaluate whether the revocation of a wallet unit attestation of the affected wallet units or any other additional remedy is necessary to adequately react to the security breach or compromise.

3. The measures referred to in paragraph 1 and 2 shall be taken without undue delay, and in any event within 24 hours after having become aware of the security breach or compromise.

Article 5

Notifications about suspensions and remedies

1. Where a Member State suspends the provision and the use of a wallet solution, it shall inform the affected wallet users and the wallet-relying parties registered in accordance with Article 5b of Regulation (EU) No 910/2014;

2. Suspension notifications shall be sent without undue delay and no later than 24 hours after the suspension of the provision and of the use of the wallet solution, to:

   (a) the single points of contact designated pursuant to Article 46c(1) Regulation (EU) No 910/2014;

   (b) the Commission.

3. The suspension notifications shall include at least the following:

   (a) the name of the provider of the affected wallet solution;

   (b) the reference number of that wallet solution indicated on the list of certified wallets established pursuant to Article 5d of Regulation (EU) 910/2014, and where applicable the concerned versions;

   (c) the date and time when the security breach or compromise was detected;

   (d) the date and time when the security breach or compromise started, if known, based on network or system logs or other data sources;

   (e) the date and time of the suspension of the affected wallet solution;

   (f) contact details, including at a minimum an e-mail address and a telephone number of the notifying Member State;

   (g) a description of the data compromised, including, where applicable, the categories of personal data as defined in Articles 9(1) and 10 of Regulation (EU) 2016/679[9];

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of

(h) a description of the security breach or compromise;

(i) an estimate of the approximated number of wallet users impacted, where possible;

(j) a description of the measures that are taken or planned to remedy the security breach or compromise;

(k) a description of the potential impacts on the wallet users or on wallet-relying parties.

Article 6

Re-establishment of the provision and the use of European Digital Identity Wallets

1. Where a security breach or compromise regarding a wallet solution is remedied, the Member State providing that wallet solution shall ensure the re-establishment of the provision, the activation and the use of that wallet solution without undue delay.

2. For the purpose of paragraph 1, Member States shall ensure to:

(a) re-establish the provision and use of the wallet units provided under that wallet solution by the issuing of a wallet unit provided under a new version of the wallet solution to all affected users, if applicable;

(b) issue new wallet unit attestations as set out in Article 6 of Commission Implementing Regulation (EU) 2024/XXX[10] laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets to new wallet units or to previously issued wallet units provided they fulfill the security requirements after the breach or compromise is remedied;

(c) revoke any measure implemented as per Article 4 of this Regulation and hindering the provision of new wallet units under the affected wallet solution where that measure was linked solely to the now remedied security breach or compromise.

Article 7

Re-establishment notifications

1. Where a Member State re-establishes a wallet solution in accordance with Article 6, that Member State shall ensure that re-establishment notification is sent without undue delay to:

(a) the affected wallet users and the wallet -relying parties registered in in accordance with Article 5b of Regulation (EU) No 910/2014;

(b) the bodies referred to in Article 5(2).

---

such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

[10] Commission Implementing Regulation (EU) 2024/XXX laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets, OJ XXX, ELI XXX.

2. Re-establishment notifications referred to in paragraph 1 shall include at least the elements referred to in Article 5(3), points (a) to (b) and Article 5(3), points (f) to (h) and the following:

(a) the date and time when the security breach or compromise was remedied;

(b) the date and time of the re-establishment of the affected wallet solution, and, where appropriate, of the affected wallet units provided under that wallet solution;

(c) a description of the measures that have been taken to remedy the security breach or compromise;

(d) a description of the potential residual impacts on the wallet users or wallet-relying parties.

Article 8

Withdrawal of European Digital Identity Wallets

1. Where justified by the severity of the security breach or compromise as assessed in accordance with Article 3(1) the Member State providing that wallet solution shall ensure the withdrawal of the affected wallet solution without undue delay and in any event respectively within 24 hours of becoming aware of the severe security breach or compromise.

2. Where a security breach or compromise is not remedied within three months after the date of suspension of a wallet solution, the Member State providing that wallet solution shall ensure the withdrawal of the affected wallet solution without undue delay and in any event within 24 hours after the expiry of that three months suspension period.

3. When withdrawing a wallet solution, Member States shall ensure within the timelines set out in paragraph 1 and 2 that:

(a) the wallet unit attestations as set out in Article 6 of Commission Implementing Regulation (EU) 2024/XXX[11] laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets of the wallet unit of the affected wallet solution are revoked;

(b) the wallet unit attestations cannot be reverted to a valid state;

(c) no new wallet unit attestation can be issued to existing wallet units provided under the affected wallet solution;

(d) no new wallet unit can be provided under the affected wallet solution.

[11] Commission Implementing Regulation (EU) 2024/XXX laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets, OJ XXX, ELI XXX.

Article 9

Withdrawal notifications

1. Where a Member State withdraws a wallet solution, that Member State shall, without undue delay inform the affected wallet user and the wallet-relying parties registered in accordance with Article 5b of Regulation (EU) No 910/2014.

2. No later than 24 hours after the withdrawal, withdrawal notifications shall be sent to:

   (a) the single points of contact designated pursuant to Article 46c(1) of Regulation (EU) No 910/2014;

   (b) the Commission.

3. Withdrawal notifications shall include at least the following information:

   (a) the name of the wallet provider of the withdrawn wallet solution;

   (b) the reference number of that wallet solution indicated in the list of certified wallets established pursuant to Article 5d of Regulation (EU) 910/2014, and where applicable the concerned versions;

   (c) the date and time when the security breach or compromise, having led to the withdrawal of the affected wallet solution because of its severity or non-remediation within 3 months, was detected;

   (d) the date and time when that security breach or compromise started, if known;

   (e) the date and time of the withdrawal of the wallet solution and of the effective revocation of the wallet unit attestations of the wallet units provided under the affected wallet solution;

   (f) whether the withdrawal is the result of the severity of the security breach or compromise or is the consequence of a non-remediation of the security breach or compromise;

   (g) contact details, including at a minimum an e-mail address of the notifying Member State;

   (h) a description of the data affected by that security breach or compromise, where applicable, including the categories of personal data as specified in Articles 9(1) and 10 of Regulation (EU) 2016/679;

   (i) a description of that security breach or compromise;

   (j) a description of the potential impacts on the wallet users or wallet-relying parties.

Article 10

Notification system

Member States shall use the [Cyber Incident Reporting and Analysis System (‘CIRAS’) operated by the European Union Agency for Cybersecurity (‘ENISA')], or an equivalent system agreed by the Member States and the Commission to send:

(1) the notifications set out in Article 3(3);

(2) the suspension notifications set out in Article 5(2);

(3) the re-establishment notifications set out in Article 7(1) point (b);

(4) the withdrawal notifications set out in Article 9(2).

Article 11

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States, except for .Article 10, which shall apply from [date to be inserted by the OP – 12 months after publication].

Done at Brussels,

For the Commission
The President
Ursula VON DER LEYEN