EUROPEAN
COMMISSION

Brussels, 19.11.2025
COM(2025) 838 final

ANNEX

ANNEX

to the

Proposal for a Regulation of the European Parliament and of the Council

on the establishment of European Business Wallets

{SWD(2025) 837 final}

ANNEX

Requirements for minimum functionalities and technical requirements of European Business Wallets

1. EUROPEAN BUSINESS WALLETS UNIT AUTHENTICATION

Access to the European Business Wallets Unit shall be granted only after the European Business Wallets user has been successfully authenticated by means of either:

(1) a notified electronic identification (eID) means in accordance with Article 6 of Regulation (EU) No 910/2014, fulfilling at least the requirements for a substantial level of assurance as defined in Article 8 of that Regulation and further specified in Commission Implementing Regulation (EU) 2015/1502; or

(2) an alternative authentication mechanism recognised as equivalent and fulfilling at least the requirements for a substantial level of assurance as defined in Article 8 of Regulation (EU) No 910/2014 and further specified in Commission Implementing Regulation (EU) 2015/1502.

Until such authentication has been completed, no functionality of the European Business Wallets Unit or of any other functionalities shall be made accessible to the Wallets user.

2. EUROPEAN BUSINESS WALLETS UNIT INTEGRITY

Providers of European Business Wallets shall, for each European Business Wallet unit, generate and sign a European Business Wallet unit attestation in accordance with the requirements laid down in point 5. The certificate used to sign or seal the Business Wallet unit attestation shall be issued under a certificate listed in the trusted list referred to in Commission Implementing Regulation (EU) 2024/2980.

3. EUROPEAN BUSINESS WALLETS SECURE COMMUNICATION AND CRITICAL ASSET MANAGEMENT

(1) European Business Wallet back-end shall use at least one Wallet secure cryptographic application and Wallets secure cryptographic device to manage critical assets.

(2) Providers of the European Business Wallets shall ensure integrity, authenticity and confidentiality of the communication between the Business Wallet's back-end, front-end and secure cryptographic applications and device.

(3) Where critical assets relate to performing electronic identification at assurance level substantial, the European Business Wallets cryptographic operations or other operations processing critical assets shall be performed in accordance with the requirements for the characteristics and design of electronic identification means at assurance level substantial, as set out in Commission Implementing Regulation (EU) 2015/1502.

4. WALLETS SECURE CRYPTOGRAPHIC APPLICATIONS

(1) Providers of European Business Wallets shall ensure that European Business Wallets secure cryptographic applications and devices:

(a) perform the wallet's cryptographic operations involving critical assets other than those needed for the Wallets unit to authenticate the Wallets owner only in cases where those applications have successfully authenticated Wallets users;

(b) where they authenticate the European Business Wallet owner in the context of performing electronic identification at assurance level substantial as set out in Implementing Regulation (EU) 2015/1502;

(c) are able to securely generate new cryptographic keys;

(d) are able to perform secure erasure of critical assets;

(e) are able to generate a proof of possession of private keys;

(f) protect the private keys generated by these Wallets secure cryptographic applications and devices during the existence of the keys;

(g) comply with the requirements for the characteristics and design of electronic identification means at assurance level substantial, as set out in Implementing Regulation (EU) 2015/1502.

5. WALLETS UNIT AUTHENTICITY AND VALIDITY

(1) Providers of European Business Wallets shall ensure that the European Business Wallets unit attestations referred to in point 1 contain public keys and that the corresponding private keys are protected by a Wallets secure cryptographic device.

(2) Providers of European Business Wallets shall provide mechanisms, independent of Wallets units, for the secure identification and authentication of Wallets users.

6. REVOCATION OF WALLETS UNIT ATTESTATIONS

(1) Providers of European Business Wallets shall establish a publicly available policy specifying the conditions and the timeframe for the revocation of Wallets unit attestations.

(2) In line with Article 6, where the providers of European Business Wallets revoke European Business Wallets unit attestations, they shall inform the affected European Business Wallets users without undue delay and no later than 24 hours from the revocation of their European Business Wallets units, including the reason for the revocation and the consequences for the European Business Wallets user. This information shall be provided in a manner that is concise, easily accessible and using clear and plain language.

(3) Where European Business Wallets providers have revoked a European Business Wallet's unit attestation, they shall make publicly available the validity status of the European Business Wallet unit attestation and describe the location of that information in the Business Wallet's unit attestation.

7. TRANSACTION LOGS

(1) The providers of European Business Wallets shall provide an appropriate logging policy that shall include, at a minimum, electronic signing, electronic

sealing, and notifications of all transactions with Business-Wallet-relying parties, other European Business Wallets units, and European Digital Identity Wallets units, irrespective of whether the transaction is successfully completed.

(2) The logged information shall at least contain:

(a) the time and date of the transaction;

(b) the name, contact details, and unique identifier of the corresponding Business-Wallet-relying party and the Member State in which that Business-Wallet-relying party is established, or in case of other Wallets units, relevant information from the Wallets unit attestation;

(c) the type or types of data requested and presented in the transaction;

(d) in the case of non-completed transactions, the reason for such non-completion.

(3) Providers of European Business Wallets shall ensure integrity, authenticity and confidentiality of the logged information.

(4) European Business Wallets back-end shall log reports sent by the Wallets user to the competent authorities via the Wallets unit, including interactions related to notifications, regulatory compliance, data sharing, or audit requests.

(5) The logs referred to in subpoints 1 and 2 shall be accessible to the European Business Wallets provider, where it is necessary for the provision of Wallets services.

(6) The logs referred to in subpoints 1 and 2 shall remain accessible for as long as required to be accessible by Union law or national law.

8. QUALIFIED ELECTRONIC SIGNATURES AND SEALS

(1) In line with Article 6, providers of European Business Wallets shall ensure that Wallets users are able to receive qualified certificates for qualified electronic signatures or seals which are linked to qualified signature or seal creation devices that are either local, external, or remote in relation to the Wallet's unit.

(2) Providers of European Business Wallets shall ensure that European Business Wallets solutions can securely interface with one of the following types of qualified signature or seal creation devices: local, external, or remotely managed qualified signature or seal creation devices for the purposes of using the qualified certificates referred to in subpoint 1.

9. SIGNATURE CREATION APPLICATIONS

(1) The signature creation applications used by European Business Wallets units may be provided either by European Business Wallets providers, by providers of trust services or by Business-Wallet-relying parties.

(2) Signature creation applications shall have the following functions:

(a) signing or sealing data provided by European Business Wallets users;

(b) signing or sealing data provided by relying parties;

(c) creating signatures or seals in accordance with at least the mandatory format;

– creating signatures or seals in accordance with the optional format;

– informing Wallets users about the result of the signature or seal creation process.

To ensure uniform conditions for the implementation of this Regulation, the Commission is empowered to adopt implementing acts in accordance with Article 6 that specify the technical standards referred to in subpoint 2, letters (c) and (c)(ii).

(3) The signature creation applications may either be integrated into or be external to European Business Wallets back-end. Where signature creation applications rely on remote qualified signature creation devices and where they are integrated into European Business Wallets back-end, they shall support the application programming interface set out in the implementing acts, which the Commission is empowered to adopt in accordance with Article 5 in order to ensure uniform conditions for the implementation of this Regulation.

10. DATA EXPORT AND PORTABILITY

Business Wallets shall support the secure export and portability of an owner's European Business Wallet data in at least an open format. This shall enable the owner to migrate their data to another Business Wallets solution while ensuring a level of assurance of at least "substantial", as defined in Implementing Regulation (EU) 2015/1502.

11. SECURE LEGAL COMMUNICATION CHANNEL FOR THE BUSINESS WALLET

(1) In line with Article 5 of this Regulation, Business Wallets shall integrate and support the use of a specific qualified electronic registered delivery service in accordance with Articles 43 and 44 of Regulation (EU) No 910/2014.

(2) The Commission shall, by means of implementing acts:

(a) designate one qualified electronic registered delivery service that shall serve as the mandatory secure legal communication channel for European Business Wallets;

(b) define the minimum technical and interoperability requirements that such qualified electronic registered delivery service must fulfil, including alignment with the reference standards, specifications and procedures established under Articles 43 and 44 of Regulation (EU) No 910/2014;

(c) ensure that the chosen qualified electronic registered delivery service is based on open, publicly available and royalty-free standards to guarantee interoperability and prevent vendor lock-in;

(d) ensure that the chosen qualified electronic registered delivery service provides end-to-end encryption to guarantee confidentiality;

(e) establish procedures for ensuring continuous availability, redundancy and fallback mechanisms in case of service failure.

(3) Interoperability between Business Wallets and the designated qualified electronic registered delivery service shall be mandatory. Providers of Business Wallets shall ensure technical integration in accordance with the implementing acts referred to in subpoint 2.

12. EUROPEAN BUSINESS WALLETS ACCESS CONTROL MECHANISM

(1) Providers of European Business Wallets shall ensure that authorisation decisions under the access control mechanism are based on one or more of the following criteria, as appropriate to the specific access request:

(a) the electronic attestation of attributes of the acting subject;

(b) the formal role of the acting subjects within a recognised organisational structure or economic operator;

(c) the scope, validity and constraints of any mandate, delegation, or power of attorney;

(d) contextual information or policies and rules adopted at Union or national level for sector-specific compliance.

(2) Providers of European Business Wallets shall ensure the access control mechanism nables fine-grained and auditable authorisation outcomes, ensuring that:

(a) visibility of credentials and attestations is selective and conditioned on access rights;

(b) access to business processes, digital procedures or submission interfaces is controlled by real-time validation of roles and mandates;

(c) all access and execution events are logged, timestamped, and bound to cryptographically verifiable proofs of authorisation, suitable for audit and legal proceedings.

(3) Providers of the European Business Wallets shall ensure that:

(a) mappings between roles and attributes are verifiable, auditable, revocable and traceable to their legitimate issuers;

(b) conflicts of roles, over-delegation, or expired authorisations are automatically detected and prevented in real time;

(c) all authorisation logic is interoperable across Member States.

(4) The list of reference standards, technical specifications and procedures to be applied for the implementation of the access control mechanism shall be defined in the implementing acts, which the Commission is empowered to adopt in accordance with Article 5 in order to ensure uniform conditions for the implementation of this Regulation. These shall cover in particular:

(a) the formats for the representation of roles and attributes;

(b) interoperability mechanisms for mandates and delegations across wallets;

(c) protocols, policy language and constraint enforcement;

(d) requirements for secure logging, timestamping and auditability of authorisation events.

(5) Compliance with the requirements laid down in this Article shall be presumed where the standards, specifications and procedures referred to in subpoint 1 are met.

13. GENERAL PROVISIONS FOR PROTOCOLS AND INTERFACES

In line with Article 6 of this Regulation, providers of European Business Wallets shall ensure that European Business Wallets units:

(1) authorise requests and, where applicable, authenticate those made through relying-party access certificates or Wallet unit attestations. Authentication of the relying party shall be required where attestations are intended for a restricted audience; in all other cases, attestations may be presented by any requesting party;

(2) display to Wallet users' information contained in the Business-Wallet-relying party access certificates or in the Wallets unit attestations where applicable;

(3) display to Wallets users, where applicable, the attributes that Wallets users are requested to present;

(4) present Wallet unit attestations of the Wallet unit to Business-Wallet-relying parties or Wallets units that request it.

14. ISSUANCE OF ELECTRONIC ATTESTATIONS OF ATTRIBUTES TO WALLETS UNITS

(1) In line with Article 5 of this Regulation, providers of European Business Wallets shall ensure that Business Wallet units requesting issuance of, electronic attestations of attributes are able to authenticate relying parties.

(2) In relation to the issuance of electronic attestations of attributes to a Wallet unit, Wallet providers shall ensure that the following requirements are complied with:

(a) where European Business Wallets owners, through their Business Wallet unit, request from the provider of the European Business Wallet the issuance of Business Wallets owner identification data or of electronic attestations of attributes from providers of Business Wallets owner identification data or providers of electronic attestations of attributes that enable issuance of Business Wallets owner identification data or electronic attestations in more than one format, the Wallets unit shall request it in all formats referred to in Article 8 to this Regulation laying down rules for the application of the Business Wallets Regulation as regards the integrity and core functionalities of Business Wallets;

(b) where Business Wallet owners use their Business Wallets unit to interact with competent national authorities and providers of electronic attestations of attributes, Wallet units shall enable authentication and validation of the Wallet unit components by presenting the Wallet unit attestations to those competent national authorities and providers upon their request;

(c) Wallet solutions shall support mechanisms that enable providers of Business Wallets Owner Identification Data to verify issuance, delivery and activation in compliance with assurance level substantial requirements set out in Commission Implementing Regulation (EU) 2015/1502 (11);

(d) Wallet units shall verify the authenticity and validity of Business Wallets owner identification data and electronic attestations of attributes.

15. PRESENTATION OF ATTRIBUTES TO EUROPEAN BUSINESS WALLET RELYING PARTIES

In line with point (d) and (k) of paragraph 1 of Article 5, European Business Wallet providers shall ensure that:

(1) European Business Wallet solutions support protocols and interfaces for the presentation of attributes to Business-Wallet-relying parties in accordance with the standards defined in the implementing acts;

(2) At the request of users, European Business Wallet units respond to successfully authenticated and validated requests from Business-Wallet-relying parties in accordance with the standards defined in the implementing acts;

(3) European Business Wallet units support proving the possession of private keys corresponding to public keys used in cryptographic bindings.

16. ISSUANCE OF EUROPEAN BUSINESS WALLET OWNER IDENTIFICATION DATA TO WALLETS UNITS

(1) Competent authorities shall ensure that Business Wallets owner identification data issued to Business Wallets units comply with the technical specifications set out in the implementing acts, in line with Article 8 of this Regulation.

(2) Competent national authorities shall ensure that Business Wallets owner identification data that they issue is cryptographically bound to the Wallets unit to which it is issued.

17. ISSUANCE OF ELECTRONIC ATTESTATIONS OF ATTRIBUTES TO WALLETS UNITS

(1) Electronic attestations of attributes issued to European Business Wallets units shall comply with at least one of the standards in the list set out in the implementing acts, in line with Article 5 of this Regulation.

(2) Providers of electronic attestations of attributes shall identify themselves to European Business Wallets units using their wallet-relying party access certificate.

(3) Providers of electronic attestations of attributes shall ensure that electronic attestations of attributes issued to European Business Wallets units contain the information necessary for authentication and validation of those electronic attestations of attributes.