

Financial Law Review

No. 42 (2)/2026

UNIVERSITY OF GDAŃSK • MASARYK UNIVERSITY • PAVEL JOZEF ŠAFÁRIK UNIVERSITY
<http://www.ejournals.eu/FLR>

MICHAŁ GRABOWSKI*

DIGITAL WALLETS AS REGULATORY INTERFACES: PAYMENT WALLETS, IDENTITY WALLETS, AND CRYPTO-ASSET WALLETS

Abstract

In market practice, the term ‘digital wallet’ covers solutions with different legal functions. It may denote a container for tokenised payment credentials, a stored-value wallet holding funds, an identity wallet, or a crypto-asset wallet. In the future, it may also serve as an access point for central bank digital currency, notably the digital euro. PSD2 contains no horizontal definition of the digital wallet. Its legal classification therefore depends on the function performed. This article develops a regime-based typology of digital wallets under EU law. It distinguishes pass-through credential wallets, staged wallets combining funding and payment functions, crypto-asset wallets assessed under MiCA, and identity wallets governed by eIDAS and the European Digital Identity Framework. It also examines the emerging link between identity and payments in the context of the proposed Digital Euro Regulation, including interoperability between digital euro front-end services and EUDI Wallets. The article maps licensing requirements, outsourcing structures, including under DORA, and the boundary between technical services and regulated AIS/PIS. It argues *de lege ferenda* for a more coherent functional taxonomy of digital wallets, clearer criteria for distinguishing technical interfaces from regulated payment services, and greater

* PhD, Assistant Professor at the University of Warsaw, practicing attorney-at-law (qualified in Poland).

Contact email: migrabow@gmail.com, ORCID: 0000-0002-1386-2991.

consistency between EU payment law, crypto-asset regulation, digital identity law, and the future digital euro framework.

Key words: digital wallet, pass-through wallet, staged wallet, PSD2, PSR, PSD3, eIDAS, EUDI Wallet, MiCA, outsourcing

JEL Classification: G18, G28, K23, K24, O33.

1. Introduction

In market practice, the term “digital wallet” is often used as an umbrella label for solutions with fundamentally different, legally relevant functions: from a “container” for tokenised payment-instrument data (e.g., a card in Apple Pay/Google Pay), through value-storing wallets (“stored value”, e.g., funds held on an e-money account), to identity wallets (the European Digital Identity Wallet – EUDI Wallet) and crypto-asset wallets (including custodial and non-custodial). The absence of a uniform concept in the EU’s existing payment law means that the legal classification depends on the wallet’s actual function: whether the wallet provider comes into possession of funds, initiates a transaction on the user’s behalf, stores the “means of access” to crypto-assets, or issues and manages identity credentials.

A meaningful conceptual clarification in the field of payment services appears only in the draft Payment Services Regulation (PSR). In that draft, the EU legislator distinguishes between pass-through wallets and staged wallets. It links these categories to the concept of a “payment instrument”. In the case of staged wallets, it also links the concept to the “issuance” of that payment instrument by the wallet provider.

However, as of 20 January 2026, the PSR still remains in the legislative process [Council of the European Union 2025]. Moreover, the draft PSR does not contain legal definitions of “digital wallets”. It only provides interpretative guidance in the recitals.

At the same time, the market also uses the term “digital wallets” to describe identity wallets and crypto-asset wallets, including custodial and non-custodial wallets. This practice may create conceptual confusion.

The aim of this article is to systematise and classify the existing legal models of so-called digital wallets, and to verify the legal implications arising from a given categorisation.

The article examines differences in licensing requirements applicable to providers of various types of digital wallets. This assessment is made in the context of EU payment services law, as well as the legal framework on electronic identification and crypto-assets. The analysis also addresses how a given digital wallet model affects the contractual relationships of the provider of that solution. This may trigger an obligation to apply an outsourcing regime.

The verification further covers the potential qualification of the relevant services as the operation of a payment system or a payment scheme [European Commission 2021]¹. Such a qualification would entail separate regulatory obligations. The article indicates that legal classification largely follows the type of value made available within the wallet. This includes scriptural money, electronic money, crypto-assets, and, finally, non-monetary elements used for identity verification under the Regulation on electronic identification and trust services for electronic transactions (eIDAS).

The analysis covers EU secondary law, as well as positions taken by legislative bodies and by authorities responsible for enforcement. It also draws on legal scholarship.

2. General concept of a digital wallet – a legal typology

2.1. Existing typologies of digital wallets

In the literature, various typologies of wallets can be found, for example: (i) mobile wallets (smartphone applications) [Payment Systems Regulator 2024:31], (ii) online/cloud wallets (“online” wallets, i.e. hosted and accessible via the internet) [Schwarz et al. 2021: 11], and (iii) super-app wallets (a wallet as a module within a “super app” combining payments with other services) [Júnior, Lopes 2024: 12]. Raúl Carrillo describes the choice between an “online wallet” and a “mobile wallet”, referring, inter alia, to “an online wallet” and “a mobile wallet (where a smartphone app facilitates access and use to virtual currency)” [Tu 2018: 548]. With regard to the early stages of introducing electronic money, the category of an “electronic wallet” appears in the literature. A market shift towards account-based (online) solutions is also identified. In this context, it is noted that “payment systems (such as

¹ Especially the designation of a payment scheme according to the Settlement Finality Directive triggers the increased obligations.

PayPal) and services offered via mobile phones are electronic money's new paradigm" [Kohlbach 2004]. With regard to crypto-assets, the literature distinguishes between a hosted wallet, where a third party holds the user's public and private keys, and an unhosted wallet [Cavagnoli Micali 2024], or custodial wallet [Veerpalu 2019: 277].

The category of the so-called "super app" also appears (for example, in the context of financial services), including references to the "super app" as a development path for payment applications [Tu 2023: 1242; Vezzoso 2024: 331].

Market typologies are descriptively useful, but they do not determine regulatory obligations.

From a legal perspective, the classification of the relevant activities (holding funds; initiating transactions; storing keys; issuing an instrument; authentication) determines legal obligations, such as licensing requirements, liability, outsourcing, and security requirements. This type of distinction is also partly reflected in industry documents, which, for example, emphasise the separation between the wallet as an interface and the payment instrument, as well as the "set of rules" of a payment scheme [European Payments Council 2014: 32]. Regulatory obligations arise from the choice of a specific model and a specific wallet structure.

2.2. A functional approach and legal criteria

In the absence of a single horizontal definition, the most practical approach is a legal classification based on function and the applicable regulatory regime. From an EU law perspective, a "wallet" is a technical and organisational construct. Its legal effects depend on whether it covers the following:

A. Digital wallet for the tokenisation of an existing payment instrument (pass-through): it stores data/credentials of a payment instrument (e.g. tokenised card data), but it does not hold funds and it does not "issue" the instrument in an economic sense. Typically, such a digital wallet operates within a chain of contracts controlled by the issuer of the instrument and the payment scheme. The draft PSR expressly indicates that, in such a scenario, the digital wallet is not treated as a payment instrument, and the provider

of such a wallet “does not provide a payment service of issuing a payment instrument”².

B. A wallet that holds funds (staged / stored-value): the wallet provider comes into possession of the funds before the payment and executes the payment as a second stage. The draft PSR characterises this as a “funding-stage” and a “payment-stage” model, and indicates that the provider of such a wallet “issues the payment instrument”³.

C. A crypto-asset wallet: the relevant subject matter is crypto-assets and/or the “means of access” (keys), and the legal regime is based on Markets in Crypto-Assets Regulation (MiCA). MiCA does not build obligations on the concept of a “wallet” as such, but on the classification of the crypto-asset service provider’s (CASP’s) services, in particular the service of “custody and administration of crypto-assets on behalf of clients”⁴.

D. An identity wallet (identity wallet): the core subject matter is identity attributes and qualified credentials. The centrepiece of the regime is eIDAS, introducing the European Digital Identity Wallet.

3. Pass-through wallets

3.1. General concept of a pass-through wallet

The most precise account of a pass-through wallet is provided in the draft PSR (recital 24 in the Commission proposal; a similar functional approach is reflected in working documents): such a wallet, involving the tokenisation of an existing payment instrument, for example a payment card, are to be considered as technical services and should thus be excluded from the definition of payment instrument as a token cannot be regarded as being itself a payment instrument but, rather, a ‘payment application’⁵. In turn, Bank for International Settlements defines electronic wallet services as arrangements enabling end users to “access, manage and use” payment instruments “issued by one or more PSPs” via an app/website [Ehrentraud and others 2021: 10].

² Draft PSR, recital 24.

³ Draft PSR, recital 24.

⁴ Art. 3(1)(17) MiCA.

⁵ Recital 24 of the draft PSR.

The essential construction of such a wallet is, that the wallet is “passing through” the transaction to the relevant issuer of the instrument (e.g. the card issuer), which remains the payment service provider vis-à-vis the payer.

Under the current legal framework, PSD2 does not use the term pass-through wallet. Strictly speaking, the draft PSR also does not contain a legal definition. It only sets out the distinction in the recitals⁶. The legal classification therefore relies on the distinction between (i) a payment service and (ii) a purely technical service supporting the provision of payment services⁷. In addition, PSD2 provides a separate regime for third-party providers (TPPs) offering account access services (AIS), which are not subject to authorisation procedures, and payment initiation services (PIS), which involve initiating transactions from a payment account and require authorisation as a payment institution [Hallak 2025:3]. These services may be sometimes confused with pass-through wallet services.

Typical examples of pass-through wallets (in a functional sense) are wallets that store tokenised payment card data and make it available for contactless or online payments (provided it is not a “stored value” product) [Financial Conduct Authority and Payment Systems Regulator 2025]. Their common features include the following:

1. the underlying payment instrument (card / account) is issued or offered by a regulated institution (the issuer),
2. the wallet involves tokenisation of the payment instrument and strong customer authentication,
3. settlement takes place within an existing payment scheme for that payment instrument (e.g. Visa/Mastercard) and within the existing clearing and settlement infrastructure.

In a card-based model, a pass-through wallet stores the card data/credentials (often a token), while the transaction is authorised and settled as a card transaction. European Payments Council documents show that the “payment component” (the authentication application / credentials) remains “under the responsibility of the payer’s payment services provider (PSP)”, whereas

⁶ Because the “pass-through wallet” and “staged wallet” concepts are derived primarily from PSR recitals rather than operative provisions, supervisory practice may interpret and enforce them divergently across Member States, so this taxonomy should be read as a best-fit interpretive framework rather than a fully determinate legal rule.

⁷ Art. 3 (j) PSD2.

the wallet may aggregate multiple instruments and interfaces [European Payments Council 2014: 33].

As a rule, the mere storage of credentials and the provision of an interface does not amount to the provision of payment services. The key issue is whether the wallet provider comes into possession of funds (in which case the service moves to a staged wallet), or whether it initiates the transfer of funds or issues payment orders in its own name (which creates a risk of qualification as payment initiation services or other payment services).

In an “account-based” variant, the wallet (a third party) provides the user with access to a payment account (or to multiple accounts) and may integrate account-to-account (A2A) payment initiation functions [Financial Conduct Authority 2024: 10]. This model is close to third-party provider services, namely payment initiation services or account information services within the meaning of PSD2, based on access to a “payment account” with the user’s consent [Hallak 2025: 33].

If, in practice, the wallet initiates a transaction on the user’s behalf (i.e. it transmits a payment order to the account servicing payment services provider (ASPSP), it is difficult to maintain a qualification solely as a technical service provider. In such a case, the wallet may operate as a technology provider of a licensed payment initiation services provider (PISP), based on a contract and an outsourcing model on the PISP’s and/or the ASPSP’s side. Otherwise, the digital wallet provider must hold authorisation as a payment service provider providing PIS under the PSD2 regime and, in the future, under the PSR/PSD3 framework.

3.2. The role of a pass-through wallet as a credentials provider in an AI agent payment protocol

The legal function of a “digital wallet” is also present in AI agentic payment protocols. These protocols underpin end-user services that enable payments to be made using an artificial intelligence system. The protocol assumes that a so-called Credentials Provider (which cooperates with an AI Payment Provider) stores information about the user’s payment instruments and, with the user’s consent, participates in activities aimed at initiating payment transactions⁸.

⁸ For example: Google Agent Payments Protocol. There are also press releases indicating the introduction of the service in EEA: Revolut is the first to use it in the EEA.

Where such a wallet remains credential-based, meaning that the Credentials Provider stores the payment instrument data and supports tokenisation and/or strong customer authentication (SCA), but does not initiate payments in its own name, there are grounds to treat such services as pass-through wallets.

However, if the agentic payments provider in fact initiates the transaction, or holds the user's funds, the question arises whether the relevant licensing requirements are met (PIS or another payment service). It also raises the issue of what types of agreements with the issuer and/or the acquirer are required.

3.3. Legal issues associated with pass-through wallets

The legal qualification of a given digital wallet service as a payment service depends primarily on the functions performed by the solution. Where the wallet provider carries out activities that constitute a payment service (for example, initiating payments, operating a payment account, or accepting funds), the service may be classified as a payment service. If, by contrast, the provider merely supplies technology (UX, tokenisation, secure storage of credentials), does not come into possession of funds, and payment transactions are executed with the involvement of a licensed payment service provider, the wallet may be treated as a "technical service provider" within the meaning of Article 3(j) PSD2. Such services do not constitute payment services and do not require authorisation to provide payment services.

A separate, but practically important, issue is whether offering a pass-through wallet could be classified as operating a payment system⁹ or a payment scheme¹⁰. The mere fact that a wallet is "used for payments" does not in itself determine such a qualification. A typical pass-through wallet does not establish either the infrastructure for the transfer and settlement of funds or a complete set of rules for the execution of transactions. It operates within existing payment rails, including the acceptance and clearing/settlement infrastructure and the rules of the relevant payment scheme (for example, a card scheme). The wallet functions as a credential layer and an interface. It "connects" the user to an instrument issued by the issuer, and to the rules and infrastructure that already exist on the scheme's side and on the side

⁹ As defined in Art. 4(7) PSD2.

¹⁰ A concept not defined in PSD2, but appearing in the draft PSR and as a 'payment card scheme' in Article 2(16) of Regulation (EU) 2015/751.

of payment service providers. In this sense wallets are considered to be solutions incorporating existing schemes [European Commission 2022:13].

As a result, a standard credential-based wallet does not “become” a payment scheme merely because it aggregates instruments and provides a single user interface. A payment scheme is, as a rule, a set of rules organising the execution of transactions (who participates, what the roles are, authorisation and settlement rules, liability, fees, communication standards). By contrast, in a pass-through model the wallet usually only implements the scheme’s and the issuer’s requirements in its user experience and in the tokenisation and SCA flows. Similarly, a wallet does not “become” a payment system simply because it transmits transaction data or technically initiates execution, where the actual transfer and settlement of funds occurs in existing systems (for example, in clearing systems and in the scheme’s infrastructure).

The risk of qualification as a payment system or a payment scheme may arise only in configurations where an entity simultaneously: (i) sets transaction-execution rules for participants in an independent and binding manner, and (ii) provides the infrastructure for the transfer or settlement of funds, or at least organises it in a functionally equivalent way (for example, through centralised routing, its own participation rules, and its own settlement between participants). In such a model, the wallet ceases to be merely an access layer to others’ rails and others’ rules. It begins to perform the role of a scheme organiser or a system operator. This is not, however, a feature of typical pass-through wallets, which remain dependent on the issuer, the acquirer, and the scheme, and whose role focuses on credential storage, tokenisation, and support for authentication.

Even a recital in the draft PSR indicates that, in a pass-through scenario, it may be necessary for the wallet provider and the payment service provider that issued the payment instrument to enter into an outsourcing arrangement¹¹. What is decisive is the scope and nature of the tasks entrusted to the pass-through wallet provider. The outsourcing regime (including DORA for ICT outsourcing) is triggered on the side of the regulated entity (issuer/acquirer/PSP) that entrusts the wallet provider with critical functions (tokenisation, the SCA workflow, and the storage of credentials).

¹¹ Recital 24 of the draft PSR.

Accordingly, a pass-through wallet, as such, will not constitute a payment instrument within the meaning of Article 4(14) PSD2. However, it may form part of a payment instrument issued to the user by a licensed provider, namely the issuer [European Banking Authority 2025]. In that case, the agreement between the issuer and the pass-through wallet provider may require the application of an outsourcing regime.

4. Staged wallets

4.1. Definition and constitutive elements of staged wallets

The draft PSR, as amended by the Council of the European Union, describes a staged wallet as a wallet characterised by a “funding-stage and a payment-stage”. In this model, the wallet provider “comes into possession of the funds... and then transfers those funds to the payee”, while at the same time “the wallet provider issues the payment instrument”.

The funding stage consists in funds being paid into the staged wallet, which are then used to execute the transaction [Górka 2026: 55]. The funds may be paid in via a payment card transaction, direct debit, or a credit transfer. If the staged wallet provider is technically involved in initiating the “top-up” transaction, it may be required to apply strong customer authentication [European Banking Authority 2021].

The payment stage, in turn, consists in executing a payment transaction initiated from the wallet. This step may also require strong customer authentication. At the same time, the “funding” and “payment” stages may be performed simultaneously. This may resemble “decoupled debit transactions”, i.e. transactions in which, for example, a card payment triggers a direct debit, and that direct debit is used to provide the funds to cover the card transaction.

According to the EBA's position, the Commission Delegated Regulation on regulatory technical standards for strong customer authentication (SCA-RTS) does not contain specific provisions for wallet solutions. Under the current legal framework, wallets are therefore “plugged into” the SCA and liability regimes through the roles of the issuer/acquirer/merchant and the payment architecture, rather than through an autonomous “wallet” regime [European Banking Authority 2021].

In the case of staged wallets, two aspects are particularly legally relevant: (i) the wallet provider's possession of funds (even if only temporarily), and (ii) the wallet provider's issuance of a payment instrument within the meaning of PSD2 and the draft PSR.

Examples of staged wallets (in a functional sense) include stored-value solutions, where the user funds the wallet and then pays from the wallet balance (e.g. typical e-money wallets; in market practice, also quasi-account models in payment apps). For the purposes of legal classification, the key issue is whether the balance takes the form of:

1. funds held in a payment account (scriptural money),
2. electronic money (e-money),
3. in the future – possibly central bank digital currency (CBDC)
4. or another type of value (e.g. crypto-assets, loyalty points) that may not fall within “funds” under PSD2. In that case, such solutions would not qualify as staged wallets under PSD2 and the draft PSR.

4.2. Categories of “funds” held in a staged wallet

The basic category of “funds” within the meaning of PSD2 is so-called “scriptural money”¹². This is money held in payment accounts maintained by banks and payment service providers, and it is the equivalent of cash in the form of banknotes and coins. In practice, commercial bank money held on payment accounts functions as the standard settlement asset for retail non-cash payments, with discharge effects determined by national law and payment execution rules.

If a staged wallet provider offers a user an account in scriptural money, this entails the performance of (at least) payment services related to operating a payment account and transferring funds. This requires the status of a PSP under the PSD2 regime (and, in the future, under PSD3/PSR).

Another type of “funds” is electronic money. The definition of electronic money in the second Electronic Money Directive (EMD2) refers to electronically, stored monetary value, representing a claim on the issuer, issued on the receipt of funds. If a staged wallet holds the balance as e-money, the wallet provider should

¹² According to art. 4(25) PSD2, ‘funds’ means banknotes and coins, scriptural money or electronic money. This definition is extended in the draft PSR (Art. 3 (30)): ‘funds’ means central bank money issued for retail use, scriptural money and electronic money, including electronic money tokens.

hold authorisation as an electronic money institution (EMI). If the wallet operates in a model where the e-money is issued by a separate EMI and the wallet functions as a type of access interface, this may constitute a pass-through wallet service.

As regards treating crypto-assets as “funds”, PSD2 generally does not cover this category. An exception concerns e-money tokens (EMTs) as a specific form of e-money introduced by MiCA [European Banking Authority 2025:4]. MiCA defines an e-money token as a crypto-asset that purports to maintain a stable value by reference to the value of one fiat currency (for example, the euro).

If a staged wallet holds EMTs, the MiCA regime (issuance of EMTs) and the e-money regime overlap in practice [European Banking Authority 2025: 3, 29–30]. From a doctrinal and systemic perspective, this means that a “staged wallet” in the sense used in the draft PSR may cover crypto value only insofar as it constitutes e-money (i.e. an EMT). By contrast, “other” crypto-assets (asset-referenced tokens, utility tokens, etc.) are not “funds” under PSD2.

Potentially, another category of “funds” may in the future be central bank digital currency (CBDC). This concerns in particular the digital euro, which is intended to constitute legal tender¹³. This is envisaged both by the draft PSR and by the Proposal for a Regulation on the establishment of the digital euro (draft Digital Euro Regulation). The PSR draft indicates that the definition of funds should cover all forms of central bank money issued for retail use, including banknotes and coins, and any possible future central bank digital currency, as well as e-money and commercial bank money. Central bank money issued for use between the central bank and commercial banks, i.e. for wholesale use, should not be covered¹⁴. Where a digital wallet offers access to an account on which such a type of CBDC is held, that wallet will qualify as a staged wallet. This will imply that the wallet provider must have the status of a payment service provider providing a digital euro payment service, in accordance with Annex I to the draft Digital Euro Regulation¹⁵.

¹³ Art. 7(1) of the draft Digital Euro Regulation.

¹⁴ Recital 28 and Art. 3 (30) of the draft Payment Services Regulation.

¹⁵ E.g. basic digital euro payment services consist i.a. of opening, holding and closing of a digital euro payment account.

4.3. Legal issues associated with staged wallets

Offering a staged wallet generally requires a licence (as a PSP/EMI/credit institution), because it entails holding users' funds and executing payment transactions. This feature distinguishes a staged wallet from a pass-through wallet.

Where a staged wallet is offered by a third party, but the "actual" e-money issuer or the account provider is a regulated institution, the arrangement will in most cases qualify as a pass-through wallet. It may imply the need to conclude an outsourcing agreement. DORA and the EBA outsourcing guidelines would then be triggered on the side of the regulated institution.

The draft PSR expressly qualifies a staged wallet as a "payment instrument" and links this to the payment service of "issuing" provided by the wallet provider¹⁶.

5. Wallets for crypto assets

With regard to crypto-assets, EU law does not treat the notion of a "wallet" as the key concept. What matters is control over the means of access (keys) and the type of service provided¹⁷. MiCA defines the service of "custody and administration of crypto-assets on behalf of clients" as the safekeeping or controlling, on behalf of clients, of crypto-assets or of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys¹⁸.

In practice, this corresponds to the market notion of a custodial wallet, where the provider controls the keys or the means of access¹⁹. *A non-custodial wallet is a solution in which the means of access remain exclusively with the user; the software provider does not "safekeep or control" the keys for the client.*

Examples of custodial wallets include wallets offered by exchanges and crypto platforms, which maintain a user "account" and execute transfers upon the user's instruction while controlling the keys or the means of access

¹⁶ Recital 34 draft Payment Services Regulation.

¹⁷ In hybrid key-management models (eg MPC, smart-contract wallets with recovery, delegated signing, or hosted key-shards), "control" may be shared or shifting, so these structures are hard cases for whether the provider is "safekeeping/controlling the means of access" within the meaning of MiCA.

¹⁸ Art. 3.1.(17) of MiCA.

¹⁹ Recital 83 of MiCA.

[Zetzsche, Sinnig, Nikolakopoulou 2024: 214]. By contrast, non-custodial wallets are self-hosted wallet applications (eg software wallets) in which the user retains the seed/private key and the provider supplies only a tool for signing and broadcasting transactions [Berkun 2025: 1–3].

Accordingly, the term “digital wallet” may be used in market practice, but MiCA allocates obligations differently, along the axes of (i) custody/means of access, (ii) transfer as a service, (iii) execution of orders, (iv) exchange, and so forth, rather than by reference to a “wallet institution”. From a legal perspective, a “crypto wallet” is therefore a shorthand for a bundle of services, which may (but need not) qualify as crypto-asset services.

Where an entity safeguards or controls the means of access for clients, it falls within the scope of custody and administration under MiCA. In that case, authorisation as a CASP is, as a rule, required.

Conversely, where the provider supplies software only and the keys remain exclusively with the user, the legal assessment will instead rest on the “purely technical” character of the service provided [Berkun 2025: 1–2]. That assessment may, however, be exceeded if the entity in fact organises the execution of transactions “on behalf of” the client (eg by implementing mechanisms that control the means of access, signing, routing, or the execution of orders) [See as to the understanding of control over cryptographic keys [Ciach, Prokopowicz 2025: 81–82].

6. Identity wallets

A digital identity wallet (European Digital Identity Wallet) is defined as an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals²⁰. Identity wallets are subject to a legal regime separate from payment wallets (and, potentially, crypto-asset wallets). Their subject matter is not “funds”, payment instruments, or crypto-assets, but identity credentials, and their purpose is interoperable authentication and the use of attributes.

²⁰ Art. 3 (42) eIDAS.

The EUDI Wallet is intended, inter alia, to enable the storage of identification data and attributes and their presentation in relationships with public and private entities (eg onboarding, access to services) [Baldini 2024:306]. In this sense, it may “co-exist” with payment wallets, but legally it remains an eIDAS construct [Roman-Jakob, Vieira, James 2024: 9].

Key obligations for identity wallet providers arise under eIDAS (including requirements relating to the functioning of the wallet, trust, and security). This is not a “payment” licence, but rather a regime of trust services and electronic identification. From the perspective of this article, it is relevant that market solutions may combine identity and payment functionalities (e.g. in a “one app” model), but this does not automatically mean that those functionalities are subject to the same legal regime.

A specific role for the EUDI Wallet is envisaged in the draft Digital Euro Regulation. The proposal assumes that the EUDI Wallet may support user identification and authentication when using the digital euro. The recitals state that users should be able to onboard and authorise payments with the digital euro by using the European Digital Identity Wallets.²¹ The proposal also adds that PSPs distributing the digital euro should be required to accept the EUDI Wallet for identity verification and for the authorisation of payments, where the payer wishes to use the wallet for authorisation.

The proposal also introduces a functional requirement on the “front-end” side. It provides that front-end services shall be interoperable with or integrated in the European Digital Identity Wallets.²² As a consequence, the EUDI Wallet may become one of the access channels to digital euro services, alongside other technical solutions offered by payment service providers. The proposal also envisages an obligation to ensure that users can rely on the functionalities of their European Digital Identity Wallets²³. It is also being considered to allow the use of the EUDI Wallet to store digital euro on a payment device for contactless payments in an offline model²⁴. Such a function could imply that the EUDI Wallet would perform the role of a staged wallet.

²¹ Draft Digital Euro Regulation, recitals (57)–(58)

²² Draft Digital Euro Regulation, Art. 25(1).

²³ Draft Digital Euro Regulation, Art. 25(2).

²⁴ Draft Digital Euro Regulation, recital 58.

7. Other types of digital wallets

There are also arrangements that are sometimes referred to in the market as “wallets”, but legally do not perform the function of a digital wallet in the legal sense. An example is solutions offered within a limited network, which fall under the exemption set out in PSD2 [European Banking Authority 2022]. Examples may also include “merchant wallets” and loyalty wallets [European Payments Council 2014], provided that they do not involve the storage of, or the execution of transactions using, “funds” within the meaning of PSD2 or do not develop into general-purpose instruments [Bairros 2023:84]. Such solutions nevertheless require a cautious legal assessment, in particular as to whether they amount to the issuance of e-money or the provision of payment services.

Given the premise of this article (clarifying the notion of a digital wallet across the PSR/PSD2, eIDAS and MiCA regimes), these categories are of auxiliary relevance. They illustrate that the term “wallet” is also used in relation to instruments that are not payment instruments.

8. Combined wallets

Technically, combining different types of digital wallets is possible. The EPC explicitly describes the coexistence of multiple wallets and a shared “umbrella UI”, as well as wallets with some components hosted in the cloud [European Payments Council 2014:31]. Legally, however, this implies an accumulation of legal regimes applying to a single solution. With regard to pass-through wallets, there is an outsourcing risk and a set of requirements related to the security of the solution. With regard to staged wallets, an authorisation to provide payment services, and potentially an authorisation to issue e-money, is required. With regard to crypto-asset (custodial) wallets, authorisation as a CASP may be required [see e.g. Stolarski 2025], while for an identity wallet the applicable regime is eIDAS.

Consequently, a “super-wallet” combining all functionalities is more likely to operate as a bundle of services provided by different entities (supported by contractual arrangements and outsourcing) than as a single service offered by one entity without a licence.

A key practical issue is therefore the separation of roles and ensuring that the user understands which component constitutes a payment service and which constitutes an identity service.

9. Conclusions

9.1. Legal issues related to the concept of a digital wallet

The absence of a uniform definition of a “digital wallet” in PSD2 means that the legal qualification depends on the actual function of a given solution. In practice, the same label is used for payment wallets, stored-value wallets, crypto-asset wallets and identity wallets, even though they are subject to different EU law regimes.

The draft PSR (however, only in the recitals) clarifies the situation in the area of payments by distinguishing between pass-through wallets and staged wallets and by linking these categories to the notion of a payment instrument. In particular, the draft indicates that a pass-through wallet “holds” payment instrument credentials, but does not “issue” them. By contrast, a staged wallet covers both a funding stage and a payment stage and is linked to the “issuance” of the instrument by the wallet provider.

The licensing boundary runs primarily where the wallet provider comes into possession of the user’s funds, even temporarily, or where it initiates the transfer of funds in its own name. In the first case, the model approaches a staged wallet and, as a rule, requires the status of a regulated entity (PSP/EMI/credit institution), depending on the type of value stored in the wallet. In the second case, the risk of qualification as payment initiation services, or another payment service, increases, especially for so-called account-based wallets that in fact transmit payment orders to the account servicing payment service provider.

In the pass-through model, the key issue is whether the service can be qualified as a purely technical service rather than a payment service. If the wallet provider limits itself to “credential” functions (tokenisation, secure storage of data, support for SCA), and the transaction is executed by a licensed PSP within existing schemes, it is easier to maintain the qualification as a technical service provider. If, however, the wallet “enters” the payment

initiation process in a manner functionally equivalent to PIS, the qualification as a technical service becomes difficult to defend.

Outsourcing is a key legal mechanism in typical market configurations. Both the PSR draft and market practice for credential wallets indicate that cooperation between a wallet provider and a regulated entity (issuer/acquirer/ASPSP or PISP) may need to be framed as outsourcing, especially where functions essential for security and continuity are entrusted (eg tokenisation, elements of the SCA workflow, storage of credentials). As a result, the regulatory compliance burden materialises mainly on the side of the regulated entity. The wallet often becomes part of the outsourcing chain, including ICT outsourcing.

For staged wallets, the decisive factor is the type of “funds” stored. If the wallet covers scriptural money, this in practice entails the provision of payment services related to the operation of a payment account and the transfer of funds. If the wallet covers electronic money, the relevant regime for issuance, distribution and the execution of payment transactions using e-money applies. If the wallet covers crypto-assets, they are, as a rule, not “funds” under PSD2, except for EMTs, where elements of the e-money regime and MiCA overlap.

Crypto-asset wallets do not form an autonomous normative category in MiCA. MiCA allocates obligations primarily by reference to the qualification of the service, in particular “custody and administration ... on behalf of clients” and control over the “means of access”, rather than by the label “wallet” as such. For that reason, the market notions of custodial and non-custodial have legal relevance only insofar as they reflect actual “safekeeping or controlling” of crypto-assets or of the means of access.

Identity wallets, including the EUDI Wallet, are subject to the separate eIDAS regime. Their core consists of identity attributes and attestations, rather than “funds” or payment instruments. In market practice, solutions combining identity and payments in a single application may emerge, but this does not remove the separation of legal regimes and requires a clear allocation of roles and clear communication towards the user.

Digital euro and identity wallets add a further layer to the wallet taxonomy. If digital euro becomes available, a wallet may provide access to CBDC holdings. This reinforces the staged wallet logic, because CBDC holdings

are connected to a digital euro payment account held with a payment service provider. A “wallet” that provides access to that account is therefore unlikely to be neutral from a regulatory perspective. It will typically be part of a regulated distribution model.

The draft Digital Euro Regulation also makes the EUDI Wallet relevant for payment flows. It links identity and payments through onboarding and authentication. In practical terms, EUDI becomes an identity layer for access to digital euro services. The proposal also requires technical interoperability or integration between front-end services and EUDI Wallets. This creates a structural bridge between eIDAS and the payment services framework.

At the same time, EUDI Wallet does not become a payment wallet by default. Its core function remains identity credentials and qualified trust services. The fact that EUDI can be used to authorise payments does not mean it issues a payment instrument or holds funds. The legal regimes therefore remain distinct, even if the user experience is “one app”.

The offline model raises a specific classification risk. The proposal text considers using the EUDI Wallet for storing digital euro on a payment device for offline proximity payments. If such a model were adopted, it could move EUDI closer to a staged wallet function in operational terms. This would not automatically change the legal basis of eIDAS. It would, however, require a clear separation of roles and liability in the distribution chain, because offline holdings are economically equivalent to stored value.

The qualification of a digital wallet as a payment system or a payment scheme does not follow automatically from the fact that the wallet is used for payments. In typical models, the wallet operates within existing infrastructure and the rules of a payment scheme and does not create them itself. The risk of such a qualification may arise only where an entity both sets the rules for executing transactions and provides the infrastructure for their execution or settlement, which is not a feature of standard credential wallets.

Overall, the analysis supports a general finding that wallets increasingly act as regulatory interfaces. The same user interface may combine payment credentials, stored value, identity attributes, and crypto access. This increases the likelihood that a single product triggers multiple regulatory regimes. It also strengthens the practical need for transparency and clear allocation of responsibilities. Users should understand which component constitutes

a payment service, which component constitutes an identity service, and which entity is responsible for each component.

A further practical risk, especially in “combined” models, is “functional drift” across regulatory boundaries. A wallet that is designed as a technical service may, in an account-based configuration, become hard to distinguish from payment initiation services. This risk arises where the wallet controls the user journey and transmits payment orders to the account servicing payment services provider, even if it does not hold funds. A credential wallet may also evolve into a staged wallet if it adds prefunding or top-ups. This is the case where the provider comes into possession or control of users’ funds, even temporarily. A wallet presented as “non-custodial” may still amount to custody under MiCA if the provider effectively safeguards or controls the means of access, for example through recovery or signing arrangements. An identity wallet used for payment authorisation may also move closer to stored-value logic in offline models. This can occur where it enables storage of payment value on a device. Therefore, the legal assessment should not focus on branding. It should focus on who controls payment orders, funds, authentication flows, and access credentials, as shown by the technical design and the contractual allocation of roles.

9.2. De lege ferenda proposals within EU law

First, it is worth maintaining the pass-through/staged distinction in the PSR, but the criteria for “issuance” of a payment instrument in the staged model need to be clarified. In particular, “issuance” should be clearly linked to the holding of “funds” and to economic control over the payment stage, in order to reduce supervisory divergence and regulatory arbitrage. This clarification should be placed in binding provisions rather than only in recitals.

Second, the boundary between a technical service and AIS/PIS needs to be clarified in the context of account-based wallets. In practice, the market will develop models in which the wallet acts as a technology provider for a licensed PSP, and such models should be predictable across the EU. A consistent approach is needed as to when an entity “initiates” a transaction in a functional sense, including where the entity controls the user journey, transmits orders to the ASPSP, or orchestrates authentication flows.

Third, better conceptual coordination is needed between PSR/PSD3, eIDAS (EUDI Wallet) and MiCA. Super-apps will combine payments, identity and crypto, and the lack of coherent reference points increases the risk of misclassification and inconsistent compliance requirements. Coordination should reduce the risk that one function “masks” the obligations triggered by another function. This could include a clearer “mapping” of wallet explanations in recitals across the instruments, and consistent terminology for credentials, means of access, and stored value.

Fourth, wallet outsourcing should be explicitly and practically embedded in the DORA regime and in the EBA outsourcing guidelines. Operational criteria are needed for when wallet functions should be treated as critical or important, especially in relation to tokenisation, the SCA workflow and the storage of credentials. This would facilitate consistent implementation and reduce the risk of formally shifting responsibility to non-licensed entities.

Fifth, the emergence of the digital euro should be reflected consistently in payment law classification tools. Where CBDC is treated as “funds” for retail use, EU law should ensure that the allocation of responsibilities between PSPs, front-end providers, and identity wallet providers is transparent. This is particularly relevant for offline payments and for any model in which identity wallets are used in connection with CBDC holdings.

References

- Baldini, D.: The Impact of the Right to Personal Data Protection on the Design of the European Digital Identity Wallet, *Italian Journal of Public Law*, No 1, Vol. 16, 2024.
- Bairros, R. P.: The Licensing Principle and Innovation in Payments, in D. Moura Vicente, D. Pereira Duarte and C. Granadeiro (eds), *Fintech Regulation and the Licensing Principle*, European Banking Institute, 2023.
- Berkun, J.: Why Self-Custody Wallet Platforms Are Not Brokers Under the Securities Exchange Act of 1934, *Business & Finance Law Review Essays*, Vol. 8, 2025.
- Carrillo, R.: Seeing Through Money: Democracy, Data Governance, and the Digital Dollar, *Georgia Law Review*, No 3, Vol. 57, 2023.
- Cavagnoli Micali, G.: When Organised Crime Turns to Cryptocurrency: The Compatibility of Italian Patrimonial Preventive Measures with Cryptocurrency, *European Journal of Law and Technology*, No 3, Vol. 15, 2024.

Ciach, S., Prokopowicz, K.: Selected issues related to crypto-asset custody services in light of Markets in Crypto-Assets Regulation, *Safe Bank*, No 2, Vol. 99, 2025.

Górka, J.: *Finanse cyfrowe: tesseract* [Digital finance: tesseract], Wydawnictwo Uniwersytetu Warszawskiego [University of Warsaw Publishing House]: Warszawa, 2025.

Júnior, D. L. and Lopes, E. L.: Defining a Super App and Analyzing It from an Ecosystemic Perspective
Available at: <https://doi.org/10.21203/rs.3.rs-4542297/v1>, accessed: 11th March 2026.

Kohlbach, M.: Making Sense of Electronic Money, *Journal of Information, Law and Technology (JILT)*, No 1, 2004.

Roman-Jakob, S., Vieira, J. and James, E.: Bytes & Pieces: Reflections on Digital Identity, *La Revue des Juristes de Sciences Po (Sciences Po Law Review)*, No 25, 2024.

Schwarz, N. et al.: Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations, *FinTech Notes* 2021, vol. 1, no. 2.

Stolarski, K.: The area of the interplay of crypto-asset and payment services in EU law, *Safe Bank*, No 2, Vol. 99, 2025.

Tu, K. V.: Perfecting Bitcoin, *Georgia Law Review*, No 2, Vol. 52, 2018.

Veerpalu, A.: Shareholder Ledger Using Distributed Ledger Technology: The Estonian Perspective, *Masaryk University Journal of Law and Technology*, No 2, Vol. 13, 2019.

Vezzoso, S.: 'Super-apps' and the Digital Markets Act, *Journal of Antitrust Enforcement*, No 2, Vol. 12, 2024.

Zetsche, D. A., Sinnig, J. and Nikolakopoulou, A.: Crypto custody, *Capital Markets Law Journal*, No 3, Vol. 19, 2024, pp. 207–228.

Legal Acts

Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, OJ L 69.

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ L 267.

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, OJ L 257.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, OJ L 150.

Other official documents

Council of the European Union: Payment services: Council and Parliament agree to step up the fight against fraud and increase transparency, Press release, Available at: <https://www.consilium.europa.eu/en/press/press-releases/2025/11/27/payment-services-council-and-parliament-agree-to-step-up-the-fight-against-fraud-and-increase-transparency/>, accessed: 11th March, 2026.

European Banking Authority: Applicability of SCA to wallet solutions, Single Rulebook Q&A, Q&A ID 2018_4133, published as final on 21 May 2021. Available at: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicld/2018_4133, accessed: 11th March, 2026.

European Banking Authority: EBA clarifies the application of strong customer authentication requirements to digital wallets, Press release. Available at: <https://www.eba.europa.eu/publications-and-media/press-releases/eba-clarifies-application-strong-customer-authentication>, accessed: 11th March, 2026.

European Banking Authority: Guidelines on the limited network exclusion under PSD2 (EBA/GL/2022/02, 24 February 2022). Available at: https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2022/EBA-GL-2022-02%20GL%20on%20limited%20network%20exclusions/1027516/Final%20report%20on%20draft%20Guidelines%20on%20the%20limited%20network%20exclusion%20under%20PSD2.pdf, accessed: 11th March, 2026.

European Banking Authority: Interpretation of payment instrument, Single Rulebook Q&A, Q&A ID 2023_6910, published as final on 11 July 2025. Available at: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicld/2023_6910, accessed: 11th March, 2026.

European Banking Authority: Opinion of the European Banking Authority on the interplay between Directive (EU) 2015/2366 (PSD2) and Regulation (EU) 2023/1114

(MiCA) in relation to crypto-asset service providers that transact electronic money tokens (EBA/Op/2025/08, 10 June 2025).

Available at: <https://www.eba.europa.eu/sites/default/files/2025-06/e2958c99-a1b0-4b07-9d31-bcba0a28dbe7/Opinion%20on%20the%20interplay%20between%20PSD2%20and%20MiCA.pdf>, accessed: 11th March, 2026.

European Commission: Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) No 260/2012 and (EU) No 2021/1230 as regards instant credit transfers in euro, SWD(2022) 546 final.

Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0546>, accessed: 11th March, 2026.

European Commission: Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010, COM(2023) 367 final.

Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0367>, accessed: 11th March, 2026.

European Commission: Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, COM(2023) 369 final.

Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0369>, accessed: 11th March, 2026.

European Commission: Settlement finality.

Available at: https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/financial-markets/post-trade-services/settlement-finality_en, accessed: 11th March, 2026.

European Payments Council: White Paper Mobile Wallet Payments (EPC163-13 v2.0, 21 January 2014).

Available at: <https://www.europeanpaymentscouncil.eu/sites/default/files/KB/files/EPC163-13%20v2.0%20White%20Paper%20Mobile%20Wallet%20Payments.pdf>, accessed: 11th March, 2026.

Financial Conduct Authority and Payment Systems Regulator: FS25/1: Big tech and digital wallets, Feedback Statement.

Available at: <https://www.fca.org.uk/publication/feedback/fs25-1.pdf>, accessed: 11th March, 2026.

Google Cloud: Announcing agents-to-payments AP2 protocol.

Available at: <https://cloud.google.com/blog/products/ai-machine-learning/announcing-agents-to-payments-ap2-protocol>, accessed: 11th March, 2026.

Payment Systems Regulator: Big tech and digital wallets: Call for Information (CP24/9). Available at:

<https://www.psr.org.uk/media/yqinyhnn/cp24-9-cfi-digital-wallets-july-2024-v2.pdf>, accessed: 11th March, 2026.

Revolut: Revolut to enable frictionless checkout across all agentic commerce platforms for the UK and EEA.

Available at: https://www.revolut.com/en-PL/news/revolut_to_enable_frictionless_checkout_across_all_agentic_commerce_platforms_for_the_uk_and_eea/, accessed: 11th March, 2026.

Internet Resources

Ehrentraud, J. and others: Fintech and payments: regulating digital payment services and e-money.

Available at: <https://www.bis.org/fsi/publ/insights33.pdf>, accessed: 11th March, 2026.

Hallak, I.: Payment services framework.

Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775891/EPRS_BRI%282025%29775891_EN.pdf, accessed: 11th March, 2026.