The wallet demarcation problem: developing a taxonomy for classifying digital wallets

Bert Lukkien [a*], Mark de Reuver [a], Nitesh Bharosa [a]

[a] Faculty of Technology, Policy, and Management, Delft University of Technology, Delft, the Netherlands, J.A.Lukkien@tudelft.nl, 0009-0005-0540-8771.

Submitted: 31 January 2025, Revised: 26 March 2025, Accepted: 21 April 2025, Published: 26 May 2025

Abstract. Digital wallets are emerging as new tools that provide citizens with control over their personal data while allowing innovation in service delivery. Wallets promise various functionalities, from authentication, authorisation, and signing, to storage and generating qualified electronic attestations. Given the potential, policymakers and service providers face significant challenges in selecting, developing, implementing, and regulating digital wallets due to the lack of clarity about their characteristics. This paper focuses on this lack of clarity. Through a socio-technical systems theory lens, we developed a comprehensive taxonomy for classifying digital wallets. Our empirical analysis reveals a taxonomy of 47 characteristics in 14 dimensions. The contribution of this taxonomy is two-fold. Firstly, it can help develop a more precise theory on specific types of wallets. Secondly, actors in the field can use the taxonomy for more granular communication on wallet development and adoption challenges, standardisation efforts, and policy development.

Keywords. wallet, digital identity, public value, privacy, taxonomy, responsible data sharing, eIDAS, Data Governance Act, policy instruments, personal data space, personal data.
Research paper, DOI: https://doi.org/10.59490/dgo.2025.1039

1. Introduction

Interactions in society are more digital than ever. In some countries, people order their groceries from the supermarket online; apply for a building permit via the municipality's app and book a trip via the travel agency's website. When interacting with (semi)public agencies, we also expect public values to be protected. In many cases, efficiency and ease of use have been the dominant values in the design of digital systems. Considering security scandals and privacy regulations, values such as privacy, choice, security, and trustworthiness have become increasingly important. One of the ways to promote privacy, choice, security, and trustworthiness in the digital exchange of personal data is the introduction of digital wallets. However, a digital wallet is an ambiguous concept. Research has revealed multiple types of wallets with various functionalities and objectives (Degen & Teubner, 2024).

The European Union is also introducing a digital wallet, the 'European Digital Identity Wallets (EUDI Wallet).' This wallet should offer private users and businesses a universal, trustworthy, and secure way to identify themselves when accessing public and private services across borders. Examples of how the EUDI wallet can be used include opening a bank account, proving one's age, renewing medical prescriptions, renting a car, or displaying their flight tickets."[1] EU Member states have been given the legal obligation to provide all citizens with a digital wallet upon request[2]. These can be provided by the Member State, on behalf of the Member State, by a private party, or by a private party with recognition from the Member State[3].

[1] https://digital-strategy.ec.europa.eu/en/news/commission-adopts-technical-standards-cross-border-european-digital-identity-wallets
[2] eIDAS Article 5a(1)
[3] eIDAS Article 5a(2)

However, despite the legal framework available, it is still unclear what that digital wallet under eIDAS will look like. This new legislation does not aim for uniform implementation but leaves EU Member States and wallet providers with relative freedom of choice. It describes a set of minimum requirements about functionality, interoperability, security, and respect for privacy, as formulated in the General Data Protection Regulation (GDPR)[4]. Therefore, we can expect a wide variety of implementations across member states, each with its own focus and user context. Requirements such as protocols and interfaces are also specified in the European Digital Identity Wallet Architecture and Reference Framework (ARF)[5] and in five implementation acts[6].

As discussed in previous work, public and private service providers are struggling with the development and implementation of digital wallets in general and the EUDI wallet in particular (Lukkien et al., 2023). An explanation can be found in the complex environment in which wallets must operate. According to the ARF, wallets must be implemented in a multi-actor ecosystem with various trust services, including authentication, electronic signing, and data exchange. These functionalities need to be orchestrated for end-to-end service delivery (Bharosa, 2022).

This leads to a demarcation problem: how can we distinguish the different manifestations of digital wallets and their components from each other in multi-actor ecosystems? The use of vague or ambiguous terms or concepts that are not contextualised with each other is one of the causes of this lack of clarity, which can lead to operational and conceptual problems (Podsakoff, MacKenzie & Podsakoff, 2016). Moreover, the multi-actor ecosystem embedding wallets exacerbates the publicness puzzle problem (Bozeman & Bretschneider, 1994).

The objective of this paper is to contribute to solving this demarcation problem by providing both scholars and policy makers with a scientifically grounded and empirically tested taxonomy for studying wallets. Our premise is that we need a socio-technical lens for the wallet demarcation problem. According to socio-technical theory, socio-technical systems are generically defined as systems that include social (people) and technical elements (Polojärvi, 2022). Socio-technological systems also require an institutional structure that coordinates the positions, relations, and behavior of the parties that own and operate the system (Koppenjan & Groenewegen, 2005). Accordingly, the research question we answer in this article is as follows: *Which social technical design dimensions constitute a taxonomy for digital wallets found in practice?*

The contribution of this paper is two-fold. First, this is the first paper to take the socio-technical lens on digital wallets. Based on a literature review of taxonomies and wallets, we conclude that taxonomies of digital wallets that contribute to the socio-technical design are lacking, in particular for institutional design dimension. Our study contributes to the existing body of knowledge by introducing a taxonomy for digital wallets that covers this. Second, we provide practitioners and scholars with a comprehensive overview of the socio-technical design dimensions of digital wallets. This overview helps address the problem of lack of clarity in the delimitation of digital wallets. On the one hand, it facilitates scholars in their research on conceptual clarity and, on the other hand, it supports practitioners such as policymakers in choosing existing or designing new policy instruments that helps to put together the publicness puzzle (Bozeman & Bretschneider, 1994).

The remainder of this article is structured as follows. Section 2 presents the research background, zooming in on the complexity of wallets. Next section 3 presents the taxonomy development approach applied in this study. Section 4 discusses the resulting taxonomy. Section 5 concludes this paper with suggestions for further research and policy making.

2. Background: The wallet as an evolving concept

The concept of a wallet is ambiguous and is characterised by a myriad of descriptors such as 'identity', 'digital', and 'data' wallets. Synonyms for the term wallet include e-Wallet, mobile wallet, virtual wallet, online wallet, cyber wallet, electronic wallet, digital payment wallet, cryptocurrency wallet, digital identity wallet, or blockchain wallet. In this chapter, we will examine the digital wallet as a concept that has evolved over time, with technological and functional advancements occurring over several decades.

The concept “wallet” emerged in the academic literature in the late 1970s and early 1980s, initially referring to electronic financial methods by banks to enhance efficiency. Berton (1983) emphasised digital storage over cheques and cash, and Even et al. (1984) introduced electronic wallets for managing funds. This era set the stage for smart cards, progressing payment and ID digitisation. Clifford (1986) identified smart card applications beyond finance, using decentralised data storage, while Frank (1988) noted secure access and data storage. In the 1990s, wallets became decentralised, bolstered by merging PDAs[7] and smartphones with apps. The World Wide Web increased service demand, challenging old authentication. Winslett et al. (1997) argued that traditional

[4] http://data.europa.eu/eli/reg/2016/679/oj.

[5] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/v1.4.0/docs/arf.md

[6] https://digital-strategy.ec.europa.eu/en/news/commission-adopts-technical-standards-cross-border-european-digital-identity-wallets

[7] https://en.wikipedia.org/wiki/Personal_digital_assistant

authentication was inadequate for authorisation. Thus, wallets expanded beyond finances to include digital IDs and licenses, marking a shift to digital personal data, credentials, and entitlements.

In recent academic literature, a *digital wallet* has been defined in many ways. A prevalent definition posits that a digital wallet is an electronic application accessible via smartphones or other electronic devices, facilitating rapid and secure electronic commerce transactions (Podgorelec et al., 2022a). Digital wallets are recognised as a type of electronic payment instrument that can be operated on multiple electronic platforms, including computers, laptops, and mobile phones (Shah & Rathod, 2022). These wallets offer convenience and usability in routine activities and transactions, with perceived utility being a key factor influencing users' adoption intentions.
Another perspective accentuates wallets in the digital identity sphere, empowering users with authoritative control over their identity data (Nugroho et al., 2022). Such wallets are engineered to give users governance over their digital identities, incorporating functionalities to manage and authenticate identity and other personal data (Liswanty et al., 2023a). The '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 to provide them to relying parties and other users of European Digital Identity Wallets, and to sign using qualified electronic signatures or to seal using qualified electronic seals' (Article 3(42) eIDAS 2024).

The ambiguity surrounding the concept of a wallet is further illustrated when zooming in on how control over personal data can be exercised. Personal Information Management Systems (Janssen & Singh, 2022b), Personal Data Stores (Kim et al., 2025a; Min & Son, 2022), and Personal Data Spaces (Lehtiniemi, 2017a) all share this objective and hence may also be regarded as manifestations of the concept of digital wallets. These developments align with the escalating datafication of society, driven by advancements in the Internet of Things (IoT) and data analysis technologies (Mejias & Couldry, 2019). The consequences of such progress include the rapid expansion of personal data and the diminishing distinction between identity and personal data, on the one hand, and non-personal data, on the other (Purtova, 2018). To allow users to exercise control over their personal information, they need exclusive online environments from which data access and sharing can be steered[8]. Illustrative examples of these advancements include IoT wallets (Lomazina et al., 2021a; Soli´c et al., 2020) and Human Digital Twins (Chen et al., 2024; Lin et al., 2024; Miller & Spatz, 2022; Zibuschka et al., 2020).

How might one navigate these wallets from a policy perspective, and under what circumstances does it apply? Determining what is encompassed and the aspects that require design consideration is crucial. A taxonomy helps to identify the 'essences in the research territory and their relationships' (Iivari J., 2007 p. 46). They are particularly crucial for both practitioners and scholars, as without a classification framework, they find it challenging to "generalise, communicate, and apply research conclusions" (Glass & Vessey, 1995 p.65). If we look at the taxonomies available in academic literature, we found (January 2025) in Scopus with the query "wallet" AND "taxonomy"[9] (in the relevant context) 38 results. A taxonomy from a policy perspective is currently absent. In the next chapter, we will explain the development of this taxonomy.

3. Research Approach: Taxonomy development process

In pursuit of the research objective, we employed the established taxonomy development methodology of Nickerson et al. (2013). This is a tested method for taxonomy development (Pawlowski & Scholta, 2023). It facilitates the integration of conceptual-to-empirical (C2E) and empirical-to-conceptual (E2C) iterations to ensure a thorough and comprehensive investigation. The approach consists of the following steps:

[8] E.g. the DGA (preamble 30) gives substance to the principle of *'bringing the algorithm to the data'* as a privacy-preserving measure when it is stated that, 'in certain situations, it could be desirable to collate actual data within a personal data space so that processing can happen within that space without personal data being transmitted to third parties in order to maximise the protection of personal data and privacy.'

[9] (ALL (taxonomy) AND ALL (wallet)) AND (LIMIT-TO (EXACTKEYWORD , "Taxonomies") OR LIMIT-TO (EXACTKEYWORD , "Taxonomy")) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "ENGI") OR LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "ECON") OR LIMIT-TO (SUBJAREA , "DECI") OR LIMIT-TO (SUBJAREA , "BUSI"))

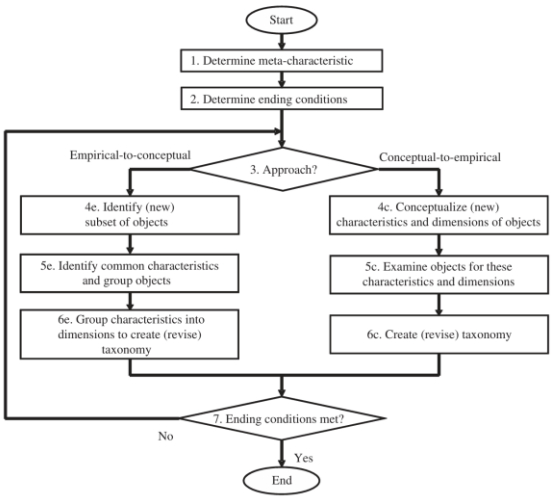

Fig. 1 The taxonomy development method (Nickerson et al., 2013)

We started by defining the purpose and expected use: differentiate digital wallets according to their characteristics for users, like practitioners, policy makers and scholars seeking to classify digital wallets. The second step was to define the objective ending conditions: The taxonomy consists of dimensions, each with mutually exclusive and collectively exhaustive characteristics. As subjective ending conditions, we followed Nickerson's recommendation: the taxonomy must be concise, robust, comprehensive, extensible, and explanatory (p. 344).

The initial iteration of the E2C encompassed a comprehensive examination of the design specifications relevant to the EUDI wallet. This examination was informed by European legislation, namely eIDAS 2.0, GDPR[10], and DGA[11], as well as Dutch legislation, ARF (which includes acknowledged standards such as the Verifiable Credentials Data Model v1.1), and Large Scale Pilots[12]. Seen through a socio-technical lens, we have concluded from this analysis that digital wallets contain the aspects of actors, capabilities, data, and infrastructure (including devices). We have delineated the following dimensions: 1- Identity model, 2- Guaranteed data, 3- Wallet provider, 4- Trust services, 6- Supervision, 7- Jurisdiction (territoriality), 8- Jurisdiction (organisation) and 9- Capabilities.

The objective of the second iteration was to perform an E2C analysis of a comprehensive set of existing digital wallets, utilising the dimensions established in the first iteration. The set compilation was informed by the description provided in Table 1 and three previous assessments by independent third-party entities. These entities were SIVI (88) [13], MyData (35) [14], and DUE (101) [15], amounting to a total of 224 digital wallets. These objects were analysed based on actors, capabilities, data, and infrastructure themes. The analysis was based on publicly accessible descriptions of the wallets, complemented by qualitative insights from interviews conducted during the initial inventories. The results of this iteration were a list of 13 characteristics on the dimension capabilities and adding the dimension transaction initiative, sector, and jurisdiction (organisation type). In addition, the characteristics of the first iteration have been supplemented.

The source material utilised in the second iteration offered significant insight into capabilities, though it provided limited information regarding the technology employed. For instance, cryptocurrency wallets facilitate crypto transactions. The understanding of the foundational technology, blockchain, has been extracted from alternative sources. Therefore, the third iteration (C2E) comprised an analysis of the academic literature based on Table 1, and in this iteration, the Applicability and Data exchange initiative dimensions were added.

[10] 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).

[11] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (ELI: http://data.europa.eu/eli/reg/2022/868/oj)

[12] https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects/

[13] PDM-Monitor-Hoofdtekst-1-augustus-2021.pdf

[14] Understanding-Mydata-Operators-pages.pdf

[15] Top 101 Digital Wallet Companies - Due

Tab. 1 Literature Taxonomy and Wallet

Query	Literature selected on relevance
'taxonomy' AND 'wallet'(including e-wallet, electronic payment wallet, cryptocurrency wallet, identity wallet, IoT wallet)	(Amard et al., 2024; Degen & Teubner, 2024; Kersic et al., 2023a; Lama, 2022; Larsen et al., 2023; Liswanty et al., 2023; Lomazina et al., 2021b; Naik & Jenkins, 2020; Olsen et al., 2011; Podgorelec et al., 2022b; Sahmim et al., 2019; Sampath et al., 2022; Shah & Rathod, 2022; Stodt et al., 2024; Teng & Khong, 2021)

In the fourth iteration (C2E), we build on the technical insights of iteration 3. In this iteration, we used a selection of academic literature based on table 2, and in this iteration, the Platform dimension was added.

Tab. 2 Literature platform and infrastructure

Query	Literature selected on relevance
'taxonomy' AND 'digital platform', 'taxonomy' AND 'digital infrastructure' 'taxonomy' AND 'blockchain'	(Blaschke et al., 2019; da Silva Neto & Chiarini, 2023; Heurix et al., 2015; Rizk et al., 2018)
'digital platform', 'digital infrastructure', 'blockchain', 'digital ecosystem'	(Addo, 2022; Berndsen & Wandhöfer, 2020; Cammaerts & Mansell, 2020; de Reuver et al., 2020; Goertler et al., 2023; Hein et al., 2020; Lips, 2023; McIntyre et al., 2021; Ozalp et al., 2022; Rohn et al., 2021; Steffen et al., 2023; Susha et al., 2023)

The **fifth iteration** (C2E) focused on emerging concepts such as data spaces (e.g., eHealth data spaces[16]) and data intermediaries as described in the DGA[17]. Although these developments are still in progress, their inclusion allowed the identification of forward-looking characteristics and trends. The results of this iteration were adding the dimensions Data Intermediation.

Tab. 3 Literature data space and data intermediary

Query	Literature selected on relevance
Data Space	(Hägglund et al., 2024; Kim et al., 2025b; Lehtiniemi, 2017b; Marcus et al., 2022; Raab et al., 2023; Stellmach et al., 2022)
Data intermediary	(Bühler et al., 2023; de Rosnay & Stalder, 2020; Janssen et al., 2020; Janssen & Singh, 2022a, 2022c; Julia Hilberg, 2023; Micheli et al., 2023)

Digital wallets are, by their nature, only accessible to the user of the wallet. To analyse the implemented and working digital wallets and test our results so far, we chose the digital wallets that are accessible to the researcher. In the **sixth iteration** (E2C) we chose wallets provided by banks (ABN AMRO App using Apple Pay[18] and Triodos Mobiel Bankieren app[19],) and in the **final iteration** we chose wallets provided by the Belgium government (Itsme[20]) and Dutch government (Mijnoverheid.nl[21], and Mijn verzekeringsbericht[22]). These digital wallets were analysed to capture minute details of their functionalities, interfaces, and underlying architecture. No new dimensions or characteristics have emerged.

At each iteration, the characteristics and dimensions were validated, modified, or extended according to the findings of the data sets. This iterative process continued until the end objective conditions were met. The first version of the taxonomy yielded 83 characteristics in 20 dimensions. As subjective ending conditions, we followed Nickerson's recommendation: the taxonomy must be concise, robust, comprehensive, extensible, and explanatory (p. 344). Because we did not find 83 characteristics in 20 dimensions concise, we dropped the dimensions with characteristics related to functionalities as derived from the empirical analysis. We have renamed this dimension to one dimension functionality. The final list consists of 47 characteristics in 14 dimensions. These results are explained in more detail in the next section.

16 https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en

17 Compare DGA article 10.

18 https://www.abnamro.nl/nl/prive/internet-en-mobiel/abn-amro-app/index.html

19 https://www.triodos.nl/mobiel-bankieren

20 https://www.vlaanderen.be/uw-overheid/werking-en-structuur-van-de-vlaamse-overheid/hoe-werkt-de-vlaamse-overheid/informatie-en-communicatie/aanmelden/aanmelden-via-itsme

21 https://mijn.overheid.nl/?r=1

22 https://www.uwv.nl/nl/arbeidsverleden-loongegevens/verzekeringsbericht

4. Result: Proposed taxonomy of digital wallets

In this section, we introduce the proposed taxonomy for digital wallets. This taxonomy comprises 47 characteristics spread over 14 dimensions. Each dimension embodies an aspect or perspective of the digital wallet phenomenon. A characteristic delineates the potential values, derived from the analysis of the objects, that a dimension may assume concerning a digital wallet.

Dimension	Characteristics						
1-Identity model	1.1-centralised	1.2-decentralised	1.3-Federated	1.4-Self-sovereign			
2-Guaranteed data	2.1-non-EAA	2.2-EAA	2.3-QEAA	2.4-PuB-EAA			
3-Wallet provider	3.1-Member State	3.2-mandated organisation	3.3-recognised organisation	3.4-not recognised organisation			
4-Trust services	4.1-qualified	4.2-not qualified					
5-Data Intermediation	5.1-neutral DISP	5.2-Not-neutral DISP					
6-Supervision	6.1-present	6.2-not present					
7-Jurisdiction (territoriality)	7.1-only national territory	7.2-inside EU territory	7.3-outside EU territory				
8-Jurisdiction (organisation)	8.1-public	8.2-private	8.3-hybrid				
9- Funding model	9.1-public	9.2-privat	9.3-hybrid				
10-Applicability	10.1-open	10.2-brand open	10.3-bank-open	10.4-closed	10.5-semi-closed		
11-Functionality	11.1-high functionality	11.2-low functionality					
12-Data type	12.1-Regular personal	12.2-Special categories personal	12.3-Criminal records	12.4-Credential	12.5-Pseudo-nymized	12.6-Non-personal	12.7-Anonymous
13-Data exchange initiative	13.1-on initiative wallet user	13.2-on request relying party	13.3-at the initiative of the source				
14- Platform	14.1-Centralised	14.2-Decentralised	14.3-Distributed				

Fig. 2 Proposed taxonomy of digital wallets

In the subsequent sections of this chapter, the taxonomy will initially be presented, followed by an elucidation of each dimension alongside its corresponding characteristics. The numbering within the taxonomy aligns with that in the explanatory notes.

1- Identity Model

An identity model refers to how personal identity data are managed and shared. The similarity is that they all aim to manage and use them to provide access to services or systems. They distinguish themselves in the aspects managed by the issuer, user control level, privacy protection, single point of failure, trust by relying party, interoperability, and technology. An overview is explained in Annex 1. This taxonomy distinguishes the dimension Identity model between **centralised, decentralised, federated, and self-sovereign identity**.

2- Guaranteed data

An attribute can be defined as information that describes a certain quality, right, or permission of an identified subject (natural or legal person) or object. For a relying party that wants to rely on the accuracy of the data, guarantees concerning at least the following elements are central: (1) the accuracy of the identified subject and (2) the accuracy of the value of the attribute, and (3) the accuracy of the relationship between the identified subject and the attribute, and (4) the identity of the issuer. Electronic Attestation of Attributes (EAA) refers to the process of electronically verifying and confirming attributes of a subject. If an EAA is provided by a Qualified Trust Service Provider (QTSPs), it is called a Qualified Electronic Attestation of Attributes[23]. EAA issued by or on behalf of a public body responsible for an authentic source. A PuB-EAA is an EAA that is legally trusted by default[24]. For this taxonomy, we distinguish between **non-EAA, EAA, QEAA,** and **PuB-EAA**.

3- Wallet provider

A digital wallet provider facilitates the provision of a digital wallet to the end user. A provider can be a public or a private organisation whose location can, in principle, be worldwide. A provider can be part of a group (e.g. Google, Apple) or an independent organisation that provides its services to others. To increase trust in these parties, the eIDAS (2024) novel certification framework by the Member States to recognise providers (Article 5c).

[23] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference- framework/blob/v1.4.0/docs/arf.md (section 3.5)

[24] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference- framework/blob/v1.4.0/docs/arf.md (section 3.6)

Consequently, until recognition is granted, all digital wallet providers are classified as 'not recognised.' Upon implementation, three variants of EUDI Wallet Providers emerge: those instituted by Member States, those mandated by Member States, or those recognised by Member States, all of which provide the EUDI Wallet for end users[25]. For this taxonomy, we distinguish the dimension Wallet provider between **Member State, mandated organisation, recognised organisation**, and **not recognised organisation**.

4- Trust services

This dimension focuses on a trust service provider's level of trustworthiness. A trust service is defined as 'an electronic service normally provided for remuneration that consists of (a) the creation, verification, and validation of electronic signatures, electronic seals, or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification, and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals, or certificates related to those services' (eIDAS 2024 article 3(16).). Article 3 (17) defines a 'qualified trust service' as a trust service that meets the applicable requirements set out in the eIDAS Regulation. For this taxonomy, we distinguish between a **qualified trust service provider** and a **non-qualified trust service provider**.

5- Data Intermediation Services Provider

The emergence of the concept of inclusive data governance[26] stems from broader discussions of data ethics and human rights within academic literature and international organisations, among others. It aims to promote equitable, ethical, and participatory data management, considering various stakeholders' needs, rights, and perspectives. Data Intermediation services aim to give substance to this concept, whereby it should be noted that 'at the current time the landscape is still dynamic, and governance practices have not yet crystallised' (Centre et al., 2023). The DGA, article 2(11) defines 'data intermediation service' as 'a service which aims to establish commercial relationships for data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal, or other means, including to exercise the rights of data subjects in relation to personal data'. Data Intermediation Services Providers include data cooperatives, data trusts, data unions, data marketplaces, and data sharing pools (Centre et al., 2023). The DMS draws up rules in Article 12, among other things, to safeguard the neutral position of that provider. For example, these rules provide restrictions on use, clarity about fees, etc. For this taxonomy, we distinguish between a **neutral DISP** (complying with the set DGA rules) and a **non-neutral DISP** (not complying with the set DGA rules).

6- Supervision

The deployment of independent and mandated agents is frequently employed to promote cooperation and trust among participants within an ecosystem[27]. These agents are entrusted with the responsibility of facilitating the integration of other participants into a trust-based system. Their duties include evaluating compliance with established regulations and, when required, enforcing adherence to these standards (encompassing admission, recognition, and enforcement processes). The existence of such supervisory entities ensures the effective operation of the ecosystem. For this taxonomy, we distinguish, therefore, between a **mandated supervisor present** and **no mandated supervisor present**.

7- Jurisdiction (territoriality)

A fundamental legal principle dictates that cooperating entities adhere to agreements, and such adherence can be enforced in the event of noncompliance. The commitment to the agreements made is paramount to this principle (*pacta sunt servanda:* "agreements must be kept")[28]. According to (Ryngaert (2008), jurisdiction is understood as individuals or entities' obligation to adhere to state regulations. Within international law, jurisdiction denotes the authority and capacity of a state to enact legislation, implement enforcement measures, and administer justice within a specified territory or concerning specific individuals or entities. Various principles of international and domestic law define a state's jurisdiction.

The primary foundational principle is the principle of territoriality, in which a state possesses jurisdiction over events, actions, or individuals within its territory (Ryngaert, 2008). Jurisdiction is further established through international treaties, as exemplified by the European Union. Given the simultaneity of these jurisdictional forms (territorial and treaty-based), an entity may encounter national and European regulations. Therefore, this taxonomy distinguishes between a digital wallet ecosystem that operates **only in national territory, inside EU territory**, and **outside EU territory.**

8- Jurisdiction (organisation type)

Digital wallets are made available by both public and private organisations. These organisations are distinguished by their purpose, ownership structure, and financing methods. Public organisations primarily prioritise the public interest, whereas the commercial interests of their owners drive private organisations. Such distinctions also

[25] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference- framework/blob/v1.4.0/docs/arf.md (section 3.2)

[26] https://www.unescap.org/events/inclusive-data-charter-making-everyone-count

[27] E.g. https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-33.html and https://www.regulations.gov/agencies

[28] https://www.britannica.com/topic/pacta-sunt-servanda

impact the regulatory framework to which these entities are subject. Public law governs the relationships between government agencies and citizens and addresses the internal organisation of the government, intending to safeguard public interest and maintain public order. On the contrary, private law refers to the legal relationships between private entities.

The EUDI wallet represents a digital ecosystem that can be implemented jointly by public and private entities. Public entities within this framework are subject to public law, whereas private entities comply with private law. This regulatory discrepancy is evident, for example, in the guidelines concerning the procurement of services from third parties, as delineated by European competition law. Furthermore, both public and private organisations are engaging in innovative hybrid organisational forms by collectively owning an entity dedicated to providing digital wallets for use by citizens and businesses. For this taxonomy, we distinguish between **public, private**, and **hybrid** organisations involved in the wallet ecosystem.

9- Funding model

Introducing a digital wallet requires significant investment in development and operation. Governments will finance this from taxes, while for private actors in the digital ecosystem, this will often be an investment that must be compensated for to achieve an acceptable return on investment (ROI). This funding model relates to the business model for digital wallets and covers investments in development and operation on the one hand and monetisation of value transfer. Public business models are aimed at creating value for society, are publicly funded, and are aimed at cost reduction rather than profit maximisation. On the other hand, private business models are aimed at creating financial profit for shareholders or owners, have private financing, and are competitively driven by innovation, cost reduction, or customer loyalty. Hybrid models in which public and private parties work together combine characteristics of both domains. For this taxonomy, we distinguish the dimension funding model between **public**, **private**, and **hybrid**.

10- Applicability wallet

An organisation often provides digital wallets as an extension of their business processes to facilitate personalised transactions with the wallet user. For the retail sector and related payments, Levitin (2018) differentiates digital wallets into "open", "brand-open," "bank-open," "closed", and "semi-closed", concerning payments and acceptance. These differ in varying degrees of freedom of use for wallet users, vendor adoption, and interoperability between wallets. A similar distinction can also be found in other sectors where digital wallets are used. Because these wallets are also often provided as an extension of business processes, they will be more likely to support the personal data set, user interface, business rules, and functions required for that specific business process.

Examples of industries with sector-specific digital wallets include: Finance (ING Mobiel Bankieren App[29]), Health (SelfPass[30]), Real Estate (Zorgeloos Vastgoed[31], Property Wallet[32]), Education (Eduwallet[33]), Media (Datakluis[34]), Government (Digid[35]), Rental (Qii[36]), Telecom (Finacle[37]), Energy (EnergieID[38]), Agrifood (Agri-Wallet[39]) and Travel/Tourism (GrabPay[40]). These sector-specific digital wallets exist alongside more generically applicable ones, such as the EUDI wallet, which will offer identification, authentication, and a limited set of (verified) personal data. We follow the characteristics set by Levitin (2018) and generalise them to other digital wallets in the explanatory descriptions.

Tab. 5 Applicability wallet

10	System	Explanation	Example
1	Open	Can be used for managing personal data at a wide range of actors and often supports multiple capabilities like signing, sealing, sharing, storage, and so on. This wallet is also free of any brand or industry restrictions.	EUDI wallet
2	Brand-open	Developed and managed by a specific brand, but offers the ability to share data with other companies, often integrated into the brand's ecosystem but not limited to use within that ecosystem.	MyQii app
3	Bank-Open	Integrated with the user's bank account, it can be used to make payments from a variety of actors, like an open wallet, and often also	ING app

[29] https://www.ing.nl/particulier/digitaal-bankieren/app/downloaden-en-activeren

[30] https://www.selfresearch.org/

[31] https://www.zorgeloosvastgoed.nl/

[32] https://www.propertywallet.pk/

[33] https://npuls.nl/wp-content/uploads/2024/09/Wegen-naar-wendbaar-sessie-eduwallet.pdf

[34] https://www.datakluis.nl/

[35] https://www.digid.nl/

[36] https://www.qii.nl/

[37] https://www.finacle.com/

[38] https://www.energyid.eu/en/

[39] https://agri-wallet.com/

[40] https://www.grab.com/sg/consumer/finance/pay/

		supports bank transfers and other banking services.	
4	Closed	Can only be used with a specific actor or group of actors that are part of the same ecosystem and has no interoperability with other digital wallets or networks outside of its own system.	MijnOverheid.nl
5	Semi-closed	Can be used with multiple actors, but only within a specific network or group of contracted actors, but has limited interoperability with other systems.	Vidua Vastgoed

For this taxonomy, we distinguish the dimension **applicability** between **open, brand-open, bank-open, closed, and semi-closed** digital wallets.

11- Functionality wallet

The results of the digital wallet analysis showed a set of functionalities that can be part of a digital wallet. The first group relates to Identification and Authentication Management (management of identification, authentication, authorisation, representation, and consent). The second group relates to Customer Relation Management (management of preference, loyalty, and contact). The third group relates to Transactions (order service, execution transactions, payment service, and monetise data). Finally, the fourth group relates to additional services (digital diary for diabetes, personal finance management, lifestyle management, Know Your Customer check, billing, and payment request).

Digital wallets can support one or more of these functionalities depending on the intended use. This distinguishes between low-functionality digital wallets (limited to a few functionalities) and high-functionality digital wallets (supporting multiple functionalities). DigID (limited to identification, authentication, and representation) is an example of a low-functionality digital wallet. Examples of high-functionality digital wallets can be found in the Asia-Pacific region. WeChat Pay[41] and Alipay[42] (China), GrabPay[43] (Singapore), and Kakao Pay[44] (South Korea) combine various functionalities such as payment, order service, and execute transactions into multi-functional digital wallets. For this taxonomy, we distinguish the dimension functionality wallet between **high-functionality** and **low-functionality** digital wallets.

12- Data Type

Within the data type dimension, we distinguish between different forms of (personal) data. The starting point here is the European context, in which this distinction has been elaborated in the GDPR. For this taxonomy, we distinguish for the dimension data type between:

Tab. 6 Data Type

12	Data Type	Meaning:
1	Regular personal data	Any information relating to an identifiable or identified natural person. (Article 4(1) GDPR)
2	Special categories Personal Data	personal data concerning a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetic data, and biometric data.
3	Criminal record data	are data relating to criminal convictions and offences or to security measures related to them.
4	Credentials	personal data as a digital proof of qualities, training, or experience that make you suitable for doing something[45]
5	Pseudonymised Data	Identifying data with a certain algorithm is replaced by encrypted data (the pseudonym) so that someone's identity can be concealed. Because a link can be established between pseudonymised data and identifying data, pseudonymised data is full personal data. (defined in Article 4(5) GDPR)
6	Non-personal data	Any data that is not personal data.
7	Anonymous Data	Non-personal data, as these data cannot be traced back to an identified or identifiable natural person.

13- Data Exchange Initiative

The dimension data exchange initiative refers to the entity that is undertaking the initiative to insert, access, or extract data from the wallet. A transaction may necessitate this within the framework of an agreement or in adherence to a legal obligation. Furthermore, data exchanges are increasingly occurring autonomously, without

[41] https://pay.weixin.qq.com/index.php/public/wechatpay_en/

[42] https://www.adyen.com/nl_NL/betaalmethoden/alipay

[43] https://www.grab.com/sg/consumer/finance/pay/

[44] https://www.kakaocorp.com/page/service/service/KakaoPay?lang=en

[45] https://www.oxfordlearnersdictionaries.com/definition/english/credentials

the necessity for direct human intervention. This phenomenon results from the growing datafication (encompassing personal data generated by sensors (IoT)), the deployment of algorithms that autonomously ascertain with whom and when data exchange transpires, and contactless data exchange (embracing Near Field Communication (NFC), Radio Frequency Identification (RFID), Bluetooth, Wi-Fi Direct, and Ultra-Wideband (UWB)). These systems are not identified as independent actors yet, but rather as technological instruments employed on behalf of a human actor. For this taxonomy, we distinguish for the dimension data exchange initiative between:

Tab. 7 Data Exchange Initiative

13	Initiative	Meaning:	Example
1	on initiative wallet user	The wallet user obtains data from an external source or provides/presents data to a relying party.	The user needs the last income data.
2	on request of the relying party	The relying party obtains data from the digital wallet, direct from the internal storage, or indirectly from the external source with the consent of the wallet user.	The user buys a house and provides data to the broker.
3	at the initiative of the source;	The source (human actor or systems) can provide data to the digital wallet	Automatically send when there is an update in the source.

14- Platform

A digital platform plays a central role in data exchange between actors. For this taxonomy, we distinguish for the dimension platform between centralised, decentralised, and distributed. Table 10 provides an overview.

Tab.10 Platform

Platform	is characterised by:
Centralised	All data and control are managed by a single entity or authority, leading to a dependency on a central system for operations and decision-making (Kersic et al., 2023b). They often have a single point of failure, making them vulnerable to security breaches and downtime if the central entity is compromised.
Decentralised	They distribute data and control across multiple nodes or entities, reducing the need for a single central authority for management and decision-making. They emphasise self-custodial and self-sovereign management of digital identities, enabling users to control their identifiers and related data without centralised entities (Kersic et al., 2023b).
Distributed	They involve a network of interconnected nodes that work together to achieve a common goal, sharing data, and processing tasks across multiple nodes in a peer-to-peer fashion (Sahmim, 2019). No single point of control or failure exists as the network operates collectively, improving resilience and scalability (Sahmim et al., 2019).

5. Conclusions and future research

This paper addresses the lack of clarity in the demarcation of digital wallets by developing a taxonomy for digital wallets. The demarcation problem amplifies the struggle of private and public service providers in their journey to develop and implement digital wallets. The research question we answered in this paper is: Which social-technical design dimensions constitute a taxonomy for digital wallets found in practice?

We first took the socio-technical lens on digital wallets to answer this question. We applied the methodological theory of Nickerson et al. (2013) to develop a taxonomy for digital wallets. This is a tested method for providing practitioners and researchers with a comprehensive overview of digital wallets' social and technical design dimensions.

The taxonomy developed in this study contains 14 dimensions and 47 variables that characterise a wallet. Our study contributes to the existing body of knowledge by introducing a taxonomy for digital wallets that covers the socio-technical design dimensions. Additionally, it facilitates scholars in their research on conceptual clarity, and, on the other hand, it supports practitioners such as policymakers in choosing existing or designing new policy instruments that support the launch of wallets.

Given the social impact of these wallets, more research is encouraged. We identify three main research directions. First, the proposed taxonomy can be further validated and developed by applying it to other empirical cases across the globe. Second, applying the taxonomy could help identify governance challenges for digital wallets. Studies looking into the governance of wallets are lacking, mainly focusing on safeguarding public values. What policy instruments and regulatory tools can effectively address specific challenges? Finally, we applied the

methodological theory of Nickerson to develop a taxonomy for digital wallets. We have combined this methodology with socio-technical design theory for a taxonomy-driven digital wallet design approach. We encourage the further development of the theory of taxonomy-driven policy instrument design.

References

Addo, A. (2022). Orchestrating a digital platform ecosystem to address societal challenges: A robust action perspective. Journal of Information Technology, 37(4), 359–386. https://doi.org/10.1177/02683962221088333

Amard, A., Hartwich, E., Lu, E. H., Hoess, A., Lu, A. H., Rieger, A., Roth, T., Fridgen, G., & Lu, G. F. (2024). Designing Digital Identity Infrastructure: A Taxonomy of Strategic Governance Choices. https://hdl.handle.net/10125/106646

Berndsen, R., & Wandhöfer, R. (2020). To Centralize or Decentralize: What is the Question? An Application to Digital Payments. In IFIP Advances in Information and Communication Technology (Vol. 555, pp. 105–118). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-64246-4_9

Berton, L. G. (1983). Putting Intelligence In Your Wallet.

Bharosa, N. (2022). The rise of GovTech: Trojan horse or blessing in disguise? A research agenda. https://doi.org/10.1016/j.giq.2022.101692

Blaschke, M., Haki, K., Aier, S., & Winter, R. (2019). Taxonomy of Digital Platforms: A Platform Architecture Perspective. https://aisel-aisnet-org.tudelft.idm.oclc.org/wi2019/track06/papers/3/

Bozeman, B., & Bretschneider, S. (1994). The 'Publicness Puzzle' in Organization Theory: A Test of Alternative Explanations of Differences between Public and Private Organizations The 'Publicness Puzzle' in Organization Theory: A Test of Alternative Explanations of Differences between Public and Private Organizations*. Public Administration Research and Theory: J-PART, 4(2), 197–223.

Bühler, M. M., Calzada, I., Cane, I., Jelinek, T., Kapoor, A., Mannan, M., Mehta, S., Micheli, M., Mookerje, V., Nübel, K., Pentland, A., Scholz, T., Siddarth, D., Tait, J., Vaitla, B., & Zhu, J. (2023). Data Cooperatives as Catalysts for Collaboration, Data Sharing, and the (Trans)Formation of the Digital Commons. https://doi.org/10.20944/preprints202304.0130.v1

Cammaerts, B., & Mansell, R. (2020). Digital Platform Policy and Regulation: Toward a Radical Democratic Turn. In International Journal of Communication (Vol. 14). http://ijoc.org.

Centre, E. C. J. R., Micheli, M., Farrell, E., Carballa-Smichowski, B., Posada-Sánchez, M., Signorelli, S., & Vespe, M. (2023). Mapping the landscape of data intermediaries – Emerging models for more inclusive data governance. Publications Office of the European Union. https://doi.org/doi/10.2760/261724

Chen, J., Yi, C., Du, H., Niyato, D., Kang, J., Cai, J., & Shen, X. (2024). A Revolution of Personalized Healthcare: Enabling Human Digital Twin with Mobile AIGC. IEEE Network. https://doi.org/10.1109/MNET.2024.3366560

Clifford, B. (1986). Smart Card. Electronics , 59(37), 55–58.

da Silva Neto, V. J., & Chiarini, T. (2023). The Platformization of Science: Towards a Scientific Digital Platform Taxonomy. Minerva, 61(1), 1–29. https://doi.org/10.1007/s11024-022-09477-6

de Reuver, M., van Wynsberghe, A., Janssen, M., & van de Poel, I. (2020). Digital platforms and responsible innovation: expanding value sensitive design to overcome ontological uncertainty. Ethics and Information Technology, 22(3), 257–267. https://doi.org/10.1007/s10676-020-09537-z

de Rosnay, M. D., & Stalder, F. (2020). Digital commons. Internet Policy Review, 9(4), 1–22. https://doi.org/10.14763/2020.4.1530

Degen, K., & Teubner, T. (2024). Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. Electronic Markets, 34(1). https://doi.org/10.1007/s12525-024-00731-1

Even, S., Goldreich, O., & Yacobi, Y. (1984). Electronic Wallet. In D. Chaum (Ed.), Advances in Cryptology: Proceedings of Crypto 83 (pp. 383–386). Springer US. https://doi.org/10.1007/978-1-4684-4730-9_28

Frank, A. U. (1988). Requirements for a Database Management System for a GIS.

Glass, R. L., & Vessey, I. (1995). Contemporary application-domain taxonomies. IEEE Software, 12(4), 63–76. https://doi.org/10.1109/52.391837

Goertler, T., Papert, M., Schmidt, M., & Fischer, I. (2023). Designing Digital Platform Ecosystems: A Synthetization of Relevant Design Topics for Ecosystems from a Literature Review Digital Business Models View project DESIGNING DIGITAL PLATFORM ECOSYSTEMS A SYNTHETIZATION OF RELEVANT DESIGN TOPICS FOR ECOSYSTEMS FROM A LITERATURE REVIEW. https://www.researchgate.net/publication/371576799

Hägglund, M., Kharko, A., Bärkås, A., Blease, C., Cajander, Å., DesRoches, C., Fagerlund, A. J., Hagström, J., Huvila, I., Hörhammer, I., Kane, B., Klein, G. O., Kristiansen, E., Moll, J., Muli, I., Rexhepi, H., Riggare, S., Ross, P., Scandurra, I., … Johansen, M. A. (2024). A Nordic Perspective on Patient Online Record Access and the European Health Data Space. Journal of Medical Internet Research, 26(1). https://doi.org/10.2196/49084

Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2020). Digital platform ecosystems. Electronic Markets, 30(1), 87–98. https://doi.org/10.1007/s12525-019-00377-4

Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. Computers and Security, 53, 1–17. https://doi.org/10.1016/j.cose.2015.05.002

Iivari J. (2007). A Paradigmatic Analysis of Information Systems As a Design Science. Scandinavian Journal of Information Systems, 2007, 19(2):39-64, 19(2), 39–64.

Janssen, H., Cobbe, J., Norval, C., & Singh, J. (2020). Decentralized data processing: personal data stores and the GDPR. https://www.hubofallthings.com

Janssen, H., & Singh, J. (2022a). Data intermediary. Internet Policy Review, 11(1), 1–9. https://doi.org/10.14763/2022.1.1644

Janssen, H., & Singh, J. (2022b). Personal Information Management Systems. Internet Policy Review, 11(2). https://doi.org/10.14763/2022.2.1659

Janssen, H., & Singh, J. (2022c). Personal Information Management Systems. Internet Policy Review, 11(2). https://doi.org/10.14763/2022.2.1659

Julia Hilberg, S. (2023). Impulse Paper, October 2023 Reflections on the DGA and Data Intermediaries Key messages. www.internationaldataspaces.org//1

Kersic, V., Vidovic, U., Vrecko, A., Domajnko, M., & Turkanovic, M. (2023a). Orchestrating Digital Wallets for On- and Off-Chain Decentralized Identity Management. IEEE Access, 11, 78135–78151. https://doi.org/10.1109/ACCESS.2023.3299047

Kersic, V., Vidovic, U., Vrecko, A., Domajnko, M., & Turkanovic, M. (2023b). Orchestrating Digital Wallets for On- and Off-Chain Decentralized Identity Management. IEEE Access, 11, 78135–78151. https://doi.org/10.1109/ACCESS.2023.3299047

Kim, T. M., Ko, T., Hwang, B. W., Paek, H. G., & Lee, W. Y. (2025a). Self-sovereign management scheme of personal health record with personal data store and decentralized identifier. Computational and Structural Biotechnology Journal, 28, 16–28. https://doi.org/10.1016/j.csbj.2024.11.036

Kim, T. M., Ko, T., Hwang, B. W., Paek, H. G., & Lee, W. Y. (2025b). Self-sovereign management scheme of personal health record with personal data store and decentralized identifier. Computational and Structural Biotechnology Journal, 28, 16–28. https://doi.org/10.1016/j.csbj.2024.11.036

Lama, D. (2022). Role of Distributed Ledger Technology for the EU Digital Identity Wallet.

Larsen, B., El Kassem, N., Giannetsos, T., Krontiris, I., Vasileiadis, S., & Chen, L. (2023). Achieving Higher Level of Assurance in Privacy Preserving Identity Wallets. Proceedings - 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications,

TrustCom/BigDataSE/CSE/EUC/ISCI 2023, 1049–1059. https://doi.org/10.1109/TrustCom60117.2023.00146

Lehtiniemi, T. (2017a). Personal Data Spaces: An Intervention in Surveillance Capitalism? Surveillance & Society, 15(5), 626–639. http://library.queensu.ca/ojs/index.php/surveillance-and-society/index|

Lehtiniemi, T. (2017b). Personal Data Spaces: An Intervention in Surveillance Capitalism? Surveillance & Society, 15(5), 626–639. http://library.queensu.ca/ojs/index.php/surveillance-and-society/index|

Lin, Y., Chen, L., Ali, A., Nugent, C., Cleland, I., Li, R., Ding, J., & Ning, H. (2024). Human digital twin: a survey. In Journal of Cloud Computing (Vol. 13, Issue 1). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1186/s13677-024-00691-z

Lips, S. (2023). A Multifaceted Assessment Framework for Electronic Identity Schemes.

Liswanty, I., Muda, I., & Kesuma, S. A. (2023). Systematic Literature Review Intention to Use E-Wallet. International Journal of Social Service and Research, 3(3), 650–655. https://doi.org/10.46799/ijssr.v3i3.300

Lomazina, T. A., Surovtsova, T. G., & Ivanov, D. A. (2021a). Development of a Cryptocurrency IoT wallet with Automatic Authentication. Proceedings of the 2021 IEEE International Conference 'Quality Management, Transport and Information Security, Information Technologies', T and QM and IS 2021, 318–323. https://doi.org/10.1109/ITQMIS53292.2021.9642727

Lomazina, T. A., Surovtsova, T. G., & Ivanov, D. A. (2021b). Development of a Cryptocurrency IoT wallet with Automatic Authentication. Proceedings of the 2021 IEEE International Conference 'Quality Management, Transport and Information Security, Information Technologies', T and QM and IS 2021, 318–323. https://doi.org/10.1109/ITQMIS53292.2021.9642727

Lukkien, B., De Reuver, M., & Bharosa, N. (2023). Barriers for developing and launching digital identity wallets. https://doi.org/10.1145/3598469

Marcus, J. S., Martens, B., Carugati, C., Bucher, A., & Godlovitch, I. (2022). The European Health Data Space Subtitle (optional) Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies.

Martin, J. (1983). Managing the data-base environment. USA: Prentice Hall.

McIntyre, D. P., Srinivasan, A., & Chintakananda, A. (2021). The persistence of platforms: The role of network, platform, and complementor attributes. Long Range Planning, 54(5). https://doi.org/10.1016/j.lrp.2020.101987

Mejias, U. A., & Couldry, N. (2019). Datafication. Internet Policy Review, 8(4). https://doi.org/10.14763/2019.4.1428

Micheli, M., Farrell, E., Carballa-Smichowski, B., Posada-Sánchez, M., Signorelli, S., & Vespe, M. (2023). JRC SCIENCE FOR POLICY REPORT Mapping the landscape of data intermediaries Emerging models for more inclusive data governance. https://doi.org/10.2760/8943

Miller, M. E., & Spatz, E. (2022). A unified view of a human digital twin. Human-Intelligent Systems Integration, 4(1–2), 23–33. https://doi.org/10.1007/s42454-022-00041-x

Min, S. H., & Son, K. H. (2022). MyData Personal Data Store Model(PDS) to Enhance Information Security for Guarantee the Self-determination rights. KSII Transactions on Internet and Information Systems, 16(2), 587–608. https://doi.org/10.3837/tiis.2022.02.012

Naik, N., & Jenkins, P. (2020). Self-Sovereign Identity Specifications: Govern Your Identity through Your Digital Wallet using Blockchain Technology. Proceedings - 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2020, 90–95. https://doi.org/10.1109/MobileCloud48802.2020.00021

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. European Journal of Information Systems, 22(3), 336–359. https://doi.org/10.1057/ejis.2012.26

Nugroho, T. C., Pubra, E. H., & Helwani, R. M. K. (2022). Analisis Pengalaman Penggunaan Dompet Digital (Studi Kasus : Shopeepay). IJAcc, 3(1), 26–31. https://doi.org/10.33050/jakbi.v3i1.2155

Olsen, M., Hedman, J., & Vatrapu, R. (2011). E-wallet properties. Proceedings - 2011 10th International Conference on Mobile Business, ICMB 2011, 158–165. https://doi.org/10.1109/ICMB.2011.48

Ozalp, H., Ozcan, P., Dinckol, D., Zachariadis, M., & Gawer, A. (2022). "Digital Colonization" of Highly Regulated Industries: An Analysis of Big Tech Platforms' Entry into Health Care and Education. California Management Review, 64(4), 78–107. https://doi.org/10.1177/00081256221094307

Pawlowski, C., & Scholta, H. (2023). A taxonomy for proactive public services. Government Information Quarterly, 40(1). https://doi.org/10.1016/j.giq.2022.101780

Podgorelec, B., Alber, L., & Zefferer, T. (2022a). What is a (Digital) Identity Wallet? A Systematic Literature Review. Proceedings - 2022 IEEE 46th Annual Computers, Software, and Applications Conference, COMPSAC 2022, 809–818. https://doi.org/10.1109/COMPSAC54236.2022.00131

Podgorelec, B., Alber, L., & Zefferer, T. (2022b). What is a (Digital) Identity Wallet? A Systematic Literature Review. Proceedings - 2022 IEEE 46th Annual Computers, Software, and Applications Conference, COMPSAC 2022, 809–818. https://doi.org/10.1109/COMPSAC54236.2022.00131

Raab, R., Küderle, A., Zakreuskaya, A., Stern, A. D., Klucken, J., Kaissis, G., Rueckert, D., Boll, S., Eils, R., Wagener, H., & Eskofier, B. M. (2023). Federated electronic health records for the European Health Data Space. In The Lancet Digital Health (Vol. 5, Issue 11, pp. e840–e847). Elsevier Ltd. https://doi.org/10.1016/S2589-7500(23)00156-5

Rizk, A., Bergvall-Kåreborn, B., & Elragal, A. (2018). Towards a Taxonomy of Data-driven Digital Services. http://hdl.handle.net/10125/50022

Rohn, D., Bican, P. M., Brem, A., Kraus, S., & Clauss, T. (2021). Digital platform-based business models – An exploration of critical success factors. Journal of Engineering and Technology Management - JET-M, 60. https://doi.org/10.1016/j.jengtecman.2021.101625

Ryngaert, C. (2008). The Territoriality Principle. In Jurisdiction in International Law (pp. 42–84). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199544714.003.0003

Sahmim, S., Gharsellaoui, H., & Bouamama, S. (2019). Edge computing: Smart identity wallet based architecture and user centric. Procedia Computer Science, 159, 1246–1257. https://doi.org/10.1016/j.procs.2019.09.294

Sampath, S., Sanjay, M., Ahmed, N., Bhagavath, A., & Nanjesh, B. R. (2022). Decentralized Digital Identity Wallet using Principles of Self-Sovereign Identity Applied to Blockchain. 7th IEEE International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2022 - Proceedings, 337–341. https://doi.org/10.1109/ICRAIE56454.2022.10054286

Shah, S., & Rathod, K. (2022). A Study On Consumer Perception On E-Wallet In Ahmedabad. International Journal of Management, Public Policy and Research, 1(2), 56–60. https://doi.org/10.55829/ijmpr.v1i2.47

Soli´c, P. S., Loji´c, A., Kapetanovi´ckapetanovi´c, L., Tomislavˇ, T., Tomislavžupanovi´c, T., Kovačevi´c, I. K., Perkovi´c, T. P., & Popovski, P. (2020). IoT Wallet: Machine Learning-based Sensor Portfolio Application. https://www.thethingsnetwork.org/

Steffen, B., Möller, F., & Stachon, M. (2023). Success Factors of Digital Platform Design. ITM Web of Conferences, 51, 05001. https://doi.org/10.1051/itmconf/20235105001

Stellmach, C., Muzoora, M. R., & Thun, S. (2022). Digitalization of Health Data: Interoperability of the Proposed European Health Data Space. Studies in Health Technology and Informatics, 298, 132–136. https://doi.org/10.3233/SHTI220922

Stodt, F., Reich, C., & Stodt, F. (2024). Digital Wallets and Identity Management: Pioneering Advances for Cloud Service Evolution. In International Journal on Advances in Software (Vol. 17). http://www.iariajournals.org/software/2024,

Susha, I., van den Broek, T., van Veenstra, A. F., & Linåker, J. (2023). An ecosystem perspective on developing data collaboratives for addressing societal issues: The role of conveners. Government Information Quarterly, 40(1). https://doi.org/10.1016/j.giq.2022.101763

Teng, S., & Khong, K. W. (2021). Examining actual consumer usage of E-wallet: A case study of big data analytics. Computers in Human Behavior, 121. https://doi.org/10.1016/j.chb.2021.106778

Winslett M., Ching N., Jones V., & Slepchin I. (1997). Using digital credentials on the World Wide Web. Journal of Computer Security, 5(3), 255–267.

Zibuschka, J., Ruff, C., Horch, A., & Roßnagel, H. (2020). A Human Digital Twin as Building Block of Open Identity Management for the Internet of Things.