Improving

Digital Wallet Design

by aligning the expertise of designers, users and academia

July 2025

SWINBURNE UNIVERSITY OF TECHNOLOGY
CENTRE FOR DES/GN /NNOVATION

sezoo

Improving digital wallet design by aligning the expertise of designers, users and academia

July 2025

A joint project between Swinburne University's Centre for Design Innovation[1] and Sezoo Pty Ltd[2].

[1]**Swinburne University's Centre for Design Innovation** (Future places for living) solves complex problems to generate new knowledge that delivers social, health, environmental, and economic benefits through client-focused community integrated research and commercial integration.

This research was funded by a Swinburne University Research Ecosystem Seed Grant (AUD$19,839)

[2]**Sezoo** provides expert services to help organisations, governments and international standards development bodies build trust, reduce risk, and enable trustworthy interactions.

Design by

bureau

designbureau@swin.edu.au

This report is relevant for the following stakeholder groups:

Stakeholder	Interest Area	Why it matters
Researchers	Design perspective in digital wallet design and the dissemination of user experience research	Helps understand how commercial factors influence digital wallet development ensuring that relevant future findings reach designers via relevant channels
Designers	User needs and design guidelines	Provides actionable insights for creating user-centric digital wallets
Policy makers	Evidence-based policy design	Supports creation of informed, user-focused digital wallet policies
Consortiums & peak bodies	Access to contemporary research	Enables alignment with current user expectations and adoption trends
Standards Bodies	Research-based standards and guidelines	Facilitates development of robust, evidence-backed digital wallet standards
Regulators	Regulation benchmarks	Offers clear standards to assess and enforce compliance in digital wallet design
Commercial organisations & consultancies	Framework for best practice and compliance	Guides development, advisory, and consulting efforts using research based evidence.

Research team:

Dr Jill Bamforth
Project Manager, School of Business, Law & Entrepreneurship

Professor Jeni Paay
Director, Centre for Design Innovation, School of Design

Dr David Mesa Saldarriaga
Project Manager, Swinburne Design Factory

Dr Daria Gradusova
Research Assistant

Dr Hassan Daronkola
School of Business Law & Entrepreneurship

Professor Hadi Ghaderi
Lead, Swinburne Supply Chain Decarbonisation Initiative, School of Business Law & Entrerpeneurship,

Report authors:

Acknowledgements - Thanks to Mr John Phillips and Dr Jo Spencer, Sezoo for their support and industry insights.

Executive summary

This report explores how to improve the design of digital wallets (DWs) to support users in making informed identity management decisions. As DWs become increasingly integrated into everyday activities—from banking and e-commerce to healthcare and government services—the need for secure, intuitive, and user-controlled experiences grows.

The research draws on three key sources: a literature review, student-led community projects, and interviews with commercial designers. The literature review identified critical factors influencing DW design, including cognitive psychology, behavioural science, trust theories, and User Experience (UX) principles. However, it also revealed a gap in the inclusion of commercial design considerations.

Student projects highlighted user challenges such as balancing convenience with security, low digital literacy, and access barriers. Their proposed solutions included simplified interfaces, offline access, gamification, and tailored education to promote safer identity behaviours.

Designer interviews revealed that while security, simplicity, and transparency are top priorities, commercial pressures often limit user feedback and influence design decisions. Designers also identified high-risk areas such as data sharing and security setup, and expressed mixed views on their responsibility to inform users about data usage and retention.

Three overarching themes emerged:

1. Comprehensive research is needed to better understand and validate the DW design process, especially from the designer's perspective.
2. Stronger alignment between academic and design priorities is essential to address user behaviour and identity management concerns.
3. Improved translation of complex regulatory and technical requirements into user-friendly, trust-building design is critical.

The report offers targeted contributions to stakeholders including researchers, designers, policymakers, regulators, standards bodies, and commercial organisations. It provides frameworks and insights to guide inclusive, evidence-based DW development that bridges gaps between policy, user needs, and commercial realities.

Table of Contents

Introduction

Introduction

This report builds off prior research into the social and psychological enablers and barriers to digital wallet usage (Bamforth et al 2020) to examine how to improve the trust aspects of digital wallet design, particularly in relation to identity management, by aligning the views of users, academics and industry designers. Digital wallets (DWs) are the online App extension of physical wallets and are used to save static information needed to support online identification processes. These processes support banking and finance (online banking), purchases and e-commerce (buying online); travel and hospitality (booking tickets and checking in); healthcare (aligning individuals with their medical records); online gaming; government services (social benefits and renewing licenses); accessing social media; applying for jobs etc. (Kagan 2024). Examples of static information include:

- Forms of identification (e.g., driving licenses, citizenship documents, birth certificates, passports)
- Health information (e.g., medical cards, health records)
- Educational achievements
- Personal items (e.g., photos, contacts)

The study of DWs is currently important due to their increasing global adoption (3.4 billion digital wallet users in 2025 (capitalshopping.com)) due to the rapid growth of financially focused DWs to support cashless payments in various industries (Alfie et al 2023) and growing location usage of digital wallets to manage individuals digital identities (see the EU Digital Identity Wallet initiative). This has increased the need for robust online identity verification for dynamic processes across several industries (Alfie et al 2023).

In 2023, Sellung & Kubach highlighted the crucial role identity management and the protection of confidential information now plays in financial and non-financial DWs as users and organisations verify their identity to gain access to particular products, services or personal resources. Recent DW developments are transferring personal identity management to individuals as evident in current initiatives, organisations, and projects with the EU Digital Identity Wallet [Eu22] being a prominent example (Sellung & Kubach; 2023).

Redirecting identity management from centralised authorities (government agencies, financial institutions, corporations) and intermediaries (identity providers, certification authorities) to individuals requires users to understand what level of identity information is relevant for what process and how to share that information in a low-risk way that they trust. Upskilling individuals understanding of what is needed to safely navigate this transfer of responsibility faces considerable hurdles (Sellung & Kubach 2023).

There is significant literature on factors (technical and non-technical enablers) affecting digital wallet adoption by end-users, particularly in relation to financial DWs (e.g. Chatterjee & Bolar 2019; Chuhan & Wojnas 2023; Čučko, Šumak & Turkanović 2023; Lukkien, de Reuver & Bharosa 2023, Shehu, Pinto & Correia 2023; Kim 2024; Sahir, Rosmawati, Listiorini & Pahlevi 2024; Satybaldy 2023; Alife et al 2023; Ansaroudi et al. 2023; Senali et al. 2023). This literature suggests adoption challenges occur in several areas: poor digital technologies awareness (weak digital literacy) (Lacity et al. 2024); technical issues (privacy, security, lack of infrastructure); social issues (trust, accessibility) (Lacity et al. 2024, Wang et al. 2023); economic issues (cost), and legal issues (cryptocurrency or DW legitimacy) (Khando et al 2022). Comprehensive strategies and guidelines for designers of DWs are also now emerging based on research into end user preferences (e.g. Selling & Kubach 2023; Alife et al 2023; Bowler et al 2023; Chuhan & Wojnas 2023; Peters 2023). However, several key gaps remain:

Firstly, there is little evidence of the designers' voices in the research i.e. what actual factors designers consider and what guides or constrains their DW design process. This missing piece in the discussion is important if academia is to offer research that aligns with and can meaningfully influence DW designers' outputs.

Secondly, limited attention has been paid to whether and how designers support end-users in high-risk and high-value decision-making during DW usage. Without filling these gaps there is an increasing likelihood that current omissions in safe DW design will persist, resulting in DW designs that do not support interoperability and ease of use across different countries and jurisdictions.

Thirdly, the role of trust in digital wallet adoption is complex and not fully understood. Many users have weak digital wallet literacy (Khando et al 2022) and are easily overwhelmed by poor design factors (see Selling & Kubach 2023). These can impact trust in the DW and, therefore, its take- up and usage e.g.:

- the use of inaccessible technical language which hinders user understanding;
- poor app structure that does not reflect established users' mental models and ways of doing things;
- non-transparency around user action and consequences;
- little support available when things go wrong e.g. insufficient backup methods in the event of digital systems crashing and a lack of portability of DWs across different countries and jurisdictions.

This project therefore aimed to contribute to a deeper understanding of factors affecting the provision of support to help individuals manage their digital identity safely and easily from both the user and the designer's perspective. The overarching research question explored in this project was

'How to improve the design of digital wallets to help users make informed identity management decisions?'

The project provides necessary groundwork to support future industry/academic grant application funding to bring together industry, academics and end users to fill gaps in current DW design practices. This was achieved by identifying:

1. What end users want from a DW, and what affects their trust in, and adoption of, DWs?This was achieved through a comprehensive literature review and undergraduate innovation students research projects.
2. Key factors affecting the design process of commercial app designers. This was explored via a short survey to commercial app designers.
3. Gaps in existing best practice DW design due to a misalignment of industry and end-user realities. This was addressed by aligning the findings from points 1 and 2.

Overview

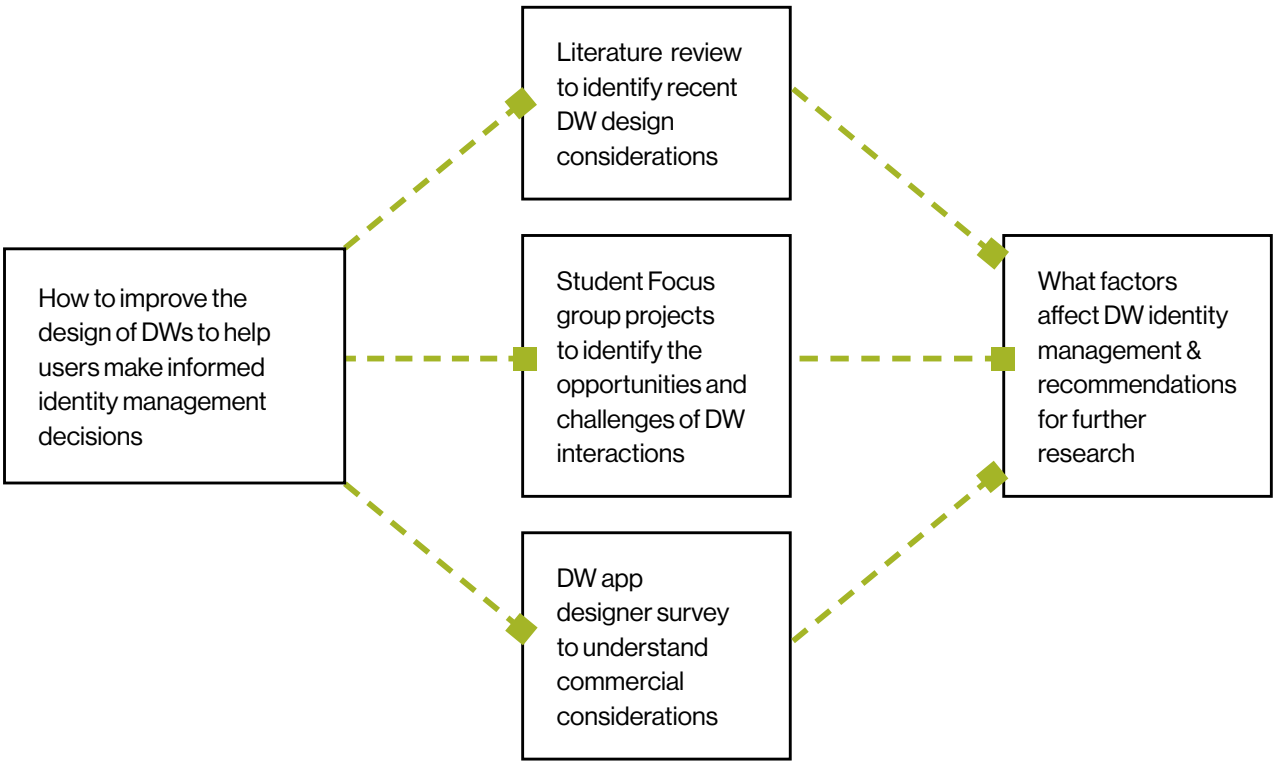
Project Overview and Methods Used

This section outlines the research approach used for the different aspects of the project process and the underpinning thinking behind those decisions (Diagram 1) using Gelo et al (2008). As the research sought to understand how DW should be constructed to build trust from a researcher, user and designer perspective an inductive qualitative approach was used. This allowed the researchers to build a comprehensive and contextualised socially and psychological understanding of how trust is built from the academic, designer and user perspectives. Purposive sampling was used to select research, users and designers who could help to answer the research question:

'How to improve the design of digital wallets to help users make informed identity management decisions?'.

Data was collected through a literature review, focus groups with specific demographic user groups and a descriptive survey with a small group of app designers. Data was analysed using thematic analysis and was interpreted to understand how user groups viewed key trust aspects affecting data management in particular contexts. The findings and insights from the literature review, focus groups and descriptive survey were compared and contrasted to ensure descriptive validity (i.e. the validity of the descriptions of settings and events), interpretative validity (i.e. the validity of statements about the meanings or perspectives held by participants), explanatory validity (i.e. the validity of claims about causal processes and relationships, including construct validity as well as causal validity), and process generalizability (i.e. the extent to which a researcher can generalize the account of a particular situation or population to other individuals, times, setting, or contexts) (Maxwell 1992; Maxwell & Loomis 2003).

Diagram 1



Literature review

To capture the most recent developments in digital wallet design and the factors affecting it, the literature review examined both peer-reviewed academic publications and grey literature published between 2008-2025. The literature search was conducted across four major databases: IEEE, Web of Science, Scopus, and Taylor and Francis. Two specific keyword search entries were used to query these databases:

1. ("UX" OR "UI" OR "UX/UI" OR "design" OR "user experience" OR "user centered") AND ("digital wallet" OR "digital identity wallet" OR "digital ID wallet")
2. ("digital wallet" OR "digital identity wallet" OR "digital ID wallet") AND ("trust" OR "trustworthiness" OR "trusted" OR "confidence" OR "perception of trust" OR "consumer trust" OR "user trust" OR "consumer perception" OR "user perception" OR "behavioral intention" OR "security") AND ("UX" OR "UI" OR "UX/UI" OR "design" OR "user experience" OR "user centered"

Appendix 1 provides a list of articles used in the systematic review.

The analysis focused on user trust in DWs, the models being used to understand the nature of this trust, currently proposed digital wallet design guidelines and key factors affecting how they can be used. The literature review showed a heavy academic and user focus with almost no inclusion of the voice of actual digital wallet designers from industry which limits the ability to view DW design from different perspectives.

Student projects

This project tasked student groups with exploring (as part of an industry-commissioned design brief), the needs of different demographics to identify opportunities and challenges associated with digital wallet interactions. First, the students conducted desktop research to identify key challenges and user pain points in DWs' usage to narrow down the project's scope. Some of the areas explored included identity theft, user-friendly interactions, new markets and uses for DWs, user education, and risk reduction during interactions. Each team then collected data from surveys and interviews to validate the issues they had identified and to gain a better understanding of user needs and behaviour. With a clear understanding of user pain points, the students refined the scope of their project to propose solutions to specific problems they found. Final proposals (pitch and report) of prototype (physical or digital) solutions were then presented to the industry client.

The data collection for the projects was undertaken under ethics approval No.20248160-19354. The industry partner (Sezoo) provided the project brief and feedback to the student teams at mid-semester and end-semester time points. The final solutions proposed were assessed against:

- desirability (how well it tackled stakeholders needs),
- feasibility (technically practical and possible),
- viability (economically, socially, and environmentally).

Industry app designer survey

The research team designed a survey to better understand the factors influencing the commercial app design process which was then administered to a small number of willing industry app designers in line with ethics approval Swinburne University no. 20248261-19964. The survey collected respondents demographic profile (age, gender, experience, Design technical and soft skills) and factors affecting their design priorities (their design priorities, legislation considerations and design areas of risk for end user and designer). Despite 40 participants being sourced through industry and research team connections only 7 participants completed the anonymous survey. As one potential respondent noted “a sizeable portion of the web3 wallet/UX devs will want to stay anonymous” Personal email communication, 28/01/25. This may be due to designers’ concerns about data privacy and the potential disclosure of commercial confidential information.

Alignment of findings from the literature review, student projects and industry app designer survey

The findings of the literature review, student projects and commercial app designer survey were compared to identify alignment and gaps in understanding re best practice DW design principles as they relate to factors affecting digital identity management. The remainder of this report captures this comparison and then reports research limitations, conclusions and future research recommendations.

Findings

Findings

3.1 Literature Review Findings

The literature review highlighted that the widespread adoption and effective utilisation of DWs is underpinned by User Experience (UX) and information security (InfoSec) considerations (Sauer et al 2024).

UX is defined as "user's perceptions and responses that result from the use and/or anticipated use of a system, product or service" [DIN EN ISO 9241-210:2020-03. 2020]. UX design seeks to minimise user errors and streamline operations by understanding user behaviour and needs. In digital wallets UX is impacted by poor end-user understanding of the wallet concept and DW usage difficulties due to non-intuitive design and lack of available support options (Sator et al 2022).

InfoSec refers to "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability" (Niels et al 2017). InfoSec design is concerned with preventing the misuse of personal data contained within verifiable credentials. A verifiable credential is a data record that contains a claim made by the holder that has been verified by another entity (the issuer) (Sauer et al 2024, p.36). InfoSec concerns in DW design include potential leaks of personal information and the possibility of data being mistakenly sent to other parties (Korir et al 2022).

3.1.1 Aspects influencing trust formation and DW take up and usage

Three key areas were identified as important to understanding UX, Infosec and related user behaviour. These were:

- Cognitive psychology theories for understanding how users perceive and process information in DW adoption and/or usage.
- Behavioural science and trust theories for understanding user behaviour (decision making, response to risk) and what factors affect user trust in DWs.
- Current UX design laws and principles underpinning DW design. These are largely derived from academic research on digital wallet users.

Cognitive Psychology Theories

Understanding how users think and process information is crucial. Cognitive psychology theories explore internal mental processes such as memory, perception, problem solving and learning. Examples of relevant theories include: Retention Theory which focuses on how long users can maintain attention on a task; Fitts's Law which predicts the time required to move to a target area (e.g. a button on a screen) and Hick's Law which describes how number of choices increases the time taken to make a decision. These insights help designers create processes that engage the user, make apps easier to use and reduce the amount of mental effort needed to use them.

Behaviour science and trust theories

Behaviour science theories are central to UX Design because they examine user behaviours and the environmental factors that influence them. Common theories relevant to this research are those affecting end-user digital wallet behaviour and trust formation.

Theories that identify factors affecting user behaviour were:

- ***The Theory of Reasoned Action (TRA)*** (Fishbein & Ajzen 1975) examines how individuals form intentions to perform behaviours (e.g. DW adoption and usage). These intentions to behave are affected by attitude towards behaviour and social pressure to perform behaviour. TRA is used in research on understanding health behaviours, consumer behaviours, environmental actions and voting behaviour.
- ***The Theory of Planned Behavior (TPB)*** extends TRA (Ajzen, 1991.Chatterjee and Bolar, 2019) by introducing perceived behavioural control (ease/difficulty of performing behaviour) and attitude towards behaviour and social pressure to perform behaviour. i.e. the ease/difficulty of performing the behaviour. It highlights how users weigh psychological effort against perceived benefits when using DWs and is used extensively in health psychology, environmental psychology, education and tech adoption.
- ***The Technology Acceptance Model (TAM)*** (Davis, 1989) tailors TRA to technology. It focuses on user acceptance and intention to use technology (information systems, e-learning platforms, mobile apps such as DWs, e-commerce and AI and automation) to assess their perceived usefulness and ease of use of use.
- ***The Unified Theory of Acceptance and Use of Technology model (UTAUT)*** (Venkatesh, et al. 2003) integrates multiple theories, including TPB and TAM, and focuses on four main constructs: performance expectancy, effort expectancy, social influence, and facilitating conditions. It is widely used in UX to predict user acceptance and usage behaviour been applied by several authors (e.g. Sukaris et al 2021, Chatterjee & Bolar 2019)

Theories that identify factors affecting trust formation were:

- ***The Personal Propensity to Trust concept (PPT)*** (Mayer, Davis & Schoorman 1995) helps UX designers understand users' willingness to trust others in different contexts and organisational settings and users propensity to trust new services and technologies. It is therefore useful for understanding DW adoption and use.
- ***Initial trust formation theory*** (McKnight & Chervany 2000; Harrison, McKnight & Chervany 2001) explores how trust is formed based on factors like reputation, perceived security and user interface design.
- ***Institution-based trust*** (McKnight, Cummings & Chervany 1998) emphasises the role of institutions (e.g. banks, government bodies, app providers) in building trust.

These theories underpin several key UX design laws and principles used to design user-friendly DW experiences which are discussed below.

UX design guidelines and principles

Digital identity wallets have the potential to empower users and enhance trust in digital identity management by bringing together learnings from cognitive psychology, behavioural science and trust theories such as those identified above. If DWs and identity management are difficult to understand, use and apply, users are likely to perceive them as less trustworthy (Sellung & Kubach 2023; Yang et al. 2015, Kim, Ferrin & Rao 2008). DW design guidelines and principles therefore seek to develop DW apps that are user-centric (i.e. meet user needs and preferences) and prioritise transparency, control, security, and usability in the UX experience (Wang et al. 2023). This requires minimising user errors and streamlining operations by

- Ensuring ease of use of DW (UX Design)
- helping individual users control their personal data and its security (Infosec Design)

In 2023 Sellung & Kubach drew upon recent literature to identify areas of poor DW design and resolution guidelines for UX design; security and privacy; identity management and the DW user interface. In the analysis below these have been aligned with Sauer et al's (2024, pp.354-359) heuristics for UX design and Infosec to comprehensively map the relationship between the different aspects to understand the opportunities and challenges faced by DW UX designers (see Appendix 2, Table 1).

3.1.2 Supporting User experience and interaction

How information in the DW app is presented, structured and communicated is critical to ease of use and building of trust. Presented information must support user mental models and expectations. Mapping Sellung & Kubach (2023) and Sauer et al (2024)'s work provides the following recommendations:

User interface design guidelines (UX Design)

A well-designed DW prioritises transparent functionality and processes to reduce significant cognitive load for users. A minimalist and aesthetic DW design supports users' primary goals by providing information in a logical information structure with user-tailored customisable elements.

A straightforward, minimalistic and simple design that incorporates readable text sizes, high contrast colours, intuitive buttons and easily identifiable help guides tailored to users' specific tasks improves users' navigation and usage. Accessibility features should be included to support users with disabilities or conditions requiring additional assistance.

Uniform clear terminology across the DW improves user understanding. Unavoidable technical terms should be clearly explained. Onboarding should be smooth, with guidance offered. Back-up options should be user-friendly and have transparent and straightforward processes. Users should be able to navigate freely within the DW, with exit, cancel, and back features that enable the continuation of cancelled processes. The DW should be designed to prevent incorrect operations, warn users before errors occur, and offer solutions if they happen. Effective channels for user feedback and managing errors should be provided.

Finally, the DW interface must work seamlessly across different devices and contexts, providing a familiar and dependable user experience that ensures user autonomy and control. Consistent interaction patterns and terminology, that adhere to uniform design standards, should be used within the wallet and across applications.

Security & privacy design guidelines (Infosec Design)

Ensuring access to security-relevant information is crucial for building user trust. The DW should be properly secured and its functions protected using robust security protocols to keep user data and transactions safe. Sensitive user data should be secured with standardised authentication methods (e.g., finger scan) to ensure users are authenticated and authorised. Security updates should be automatically installed and users notified and reminded to be vigilant to maintain security. Data should also be automatically backed up to ensure data availability, prevent data loss, and enable data recovery.

Transparent information about what data is stored and how it is stored helps users understand the security measures in place. This transparency should extend to user data storage practices so users are fully aware of how their information is being handled. Informing users about the terms of use and requiring explicit agreement to them is essential to prevent security-critical actions being overlooked. These steps are important for enabling users to safely access their data independently, manage their identity profiles, consent to data use (Burkhardt et al. 2023,

Lindegren et al. 2021) and transfer data between wallets. By clearly communicating these aspects, users can make informed decisions and feel confident in the application's security protocols.

Identity data management design guidelines (UX & Infosec design)

A comprehensive system language that is understandable and familiar to users is essential for effective communication. Information should be strategically placed to ensure it is easily accessible and understandable. Interaction flows should be intuitive - the DW should be easy to navigate and offer search and filter options to find and organise information efficiently. For example, credentials should be able to be grouped, sorted, filtered, and searched, and automation functions should be provided to increase efficiency. Users should be able to transfer their data seamlessly between different digital wallets, enhancing flexibility and convenience. Providing users with the ability to delete their accounts easily is crucial for maintaining user autonomy and control. Visible reminders to back up data regularly helps users protect their information. Additionally, showing system status and providing feedback on actions performed ensures users are informed about the application's operations and their interactions with it.

3.1.3 Laws, Standards and Protocols also affecting DW design

The following universal/country/regional regulations and protocols also impact DW design. They are essential for maintaining the security and reliability of digital wallets and for ensuring they operate within legal boundaries and provide safe services to users. Below are some examples of regulations and legal frameworks affecting DW design:

- Anti-Money Laundering (AML) Regulations: Digital wallets must comply with AML laws to prevent money laundering and other illicit activities. This includes verifying user identities and monitoring transactions
- Data Protection Laws: Regulations such as the General Data Protection Regulation (GDPR) in Europe mandate strict data protection measures, ensuring user data is handled securely and transparently e.g. GDPR enhances data control and gives owners control over their personal data.
- Consumer Protection Laws: These laws ensure that digital wallet providers offer fair and transparent services, protecting users from fraud and ensuring their rights are upheld. In the UK the Financial Conduct Authority oversees digital wallet providers, ensuring they adhere to financial regulations and maintain consumer trust. In the US the Consumer Financial Protection Bureau regulates digital wallets to protect consumers from unfair practices and to ensure financial stability. In Europe the European Banking Authority provides security and consumer protection guidelines and regulations for digital wallets within the European Union.
- Digital ID and related initiatives: examples of initiatives used around the world are: Australia's AGDIS legislature, the European electronic identification, the authentication and trust services (eIDAS) regulatory framework, New Zealand's DISTF, the UKs DIATF, Age Assurance regulations and the implementation of the ISO mDL mobile driving licence.

Below are some examples of standards and protocols developed by peak bodies, foundations and governments to guide DW development:

- The Open Wallet Foundation's standards on DW technology collaboration.
- Examples of protocols, DW functional aspects and requirements are:

Trust services

- The eIDAS (electronic Identification, Authentication and Trust Services) Regulatory framework provides a legal framework to support decentralization and security requirements necessary for cross-sectional application.
- eIDAS2 updates the eIDAS regulation to include the EU Digital Wallet (EUDI) Architecture and Reference regulatory and requirement Framework (ARF). These are necessary for EU members to offer an individual DW to all EU member state citizens.

Identity management

- The European Identity EcoSystem (ARIES) is a framework for identity management.
- The functional concepts of IDM (1.0), IDM (2.0), and IDM (3.0) refer to the evolution of identity management models, with IDM (3.0) being user-centered.
- The Federated identity management (FIM) is the protocol/architectural framework for technical standards & practices that support a User-centric identity DW model.
- Decentralised Identifiers (DIDs) are Protocols for secure identity management.
- Verifiable Credentials (VCs) are Standards/protocols for credential verification.

- Cryptographic Mechanisms: Digital wallets use cryptographic protocols to secure data transfer and storage, preventing unauthorized access and ensuring data integrity. Secure Authentication Methods such as biometric scans, are used to protect sensitive user data and ensure secure access E.g. OpenID Connect (OIDC) has been developed by the OpenID Foundation for secure authentication. Strong data encryption techniques protect user data during storage and transmission and use key pairs and decentralized identifiers (DIDs) for secure access.

3.1.4 Summary of key findings

This brief literature review linked theories from cognitive psychology and behavioural science to DW design that supports take-up and usage. It brought together recent research by Sellung & Kubach (2023) and Sauer et al. (2024) to map recent best practices guidelines and design principles in the UX and InfoSec areas. This section also called out the role of regulations, legal frameworks and protocols on DW design within which both developers and designers are tasked to create trustworthy and intuitive DWs. The review showed that the current literature is heavily academic and user-focused, with almost no inclusion of the voice of actual DW designers from industry. This suggests a blind spot in understanding of the actual design processes and pressures faced by DW designers in industry.

3.2 Findings from the Students digital wallet project

3.2.1 Concerns emerging from the digital wallet projects and the solutions provided

The four student teams identified the following concerns and project solutions:

Security and privacy Concerns

The first team explored how to enhance transparency and convenience in Digital Wallets. They focused on surveying and interviewing Gen Z users, collecting data from 34 participants. Despite being largely ignorant about data safety and how their data is used, most users continued to prioritise convenience over security. Most also admitted to agreeing to the terms and conditions without reading them, largely due to a blind trust in large corporations like Samsung and Apple, who they saw as responsible for their data. They either blindly trusted big corporations or felt powerless to prevent companies from collecting their information. The team found that most users had limited understanding of how to manage their data safely.

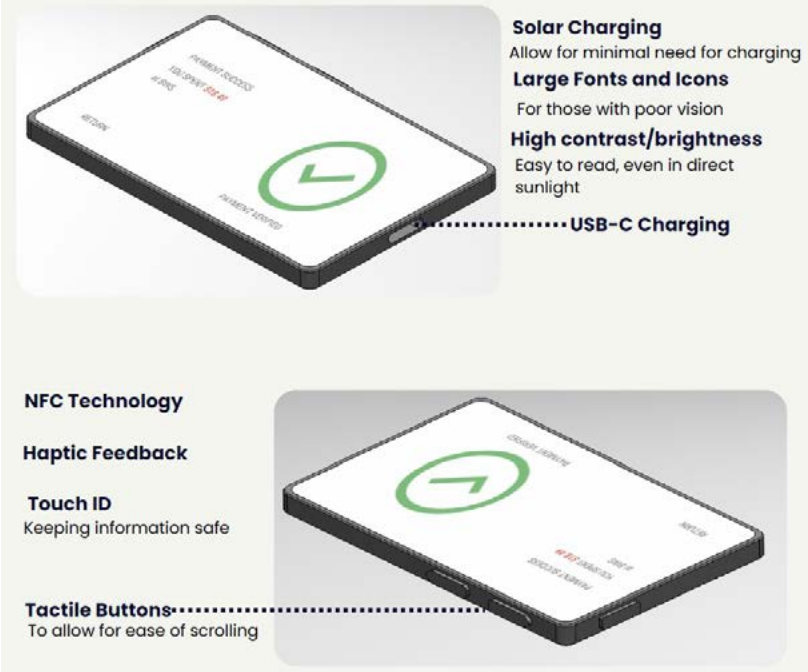


Figure 1. Clippy Conceptual Prototype.

The second group focused on the DW interactions of older demographics as they showed less adoption than younger people. They surveyed 28 participants aged 60 and above. The students found that older users were more hesitant to adopt DWs due to a lack of technological literacy and confusing user interfaces. Older users therefore needed easy-to-understand setup processes, guided support and products tailored to their needs.

The following solutions were developed by the student groups to deal with various privacy and security concerns:

1. Privy Buddy, an internet browser extension to make privacy and security more convenient and transparent. This was achieved through an AI powered user-friendly user terms and conditions reviewer browser extension, and a “hub” with tools to protect personal data and provide tips on email protection. This solution addressed issues uncovered by the first group.
2. Clippy, a user-friendly digital wallet for older adults which combined a physical card with a digital interface, so the users would have payment interactions more familiar to them (see Figure 1). This solution addrssed issues uncovered by the second group.

Money management concerns

The third student group explored ways to enhance digital wallet security and usability, with a focus on mitigating risks such as overspending and fraud. They surveyed 45 participants and conducted 12 interviews with participants aged 18 and above. Half of their survey respondents generally lacked awareness and understanding of digital privacy and security risks, with the main security concerns related to phishing, malware, and Wi-Fi snooping. Most participants expressed overspending using DW due to the simplicity of WX (Wallet experience) interactions, due to the lack of visibility of financial habits compared to using cash. This student team discovered that disparities between different bank applications

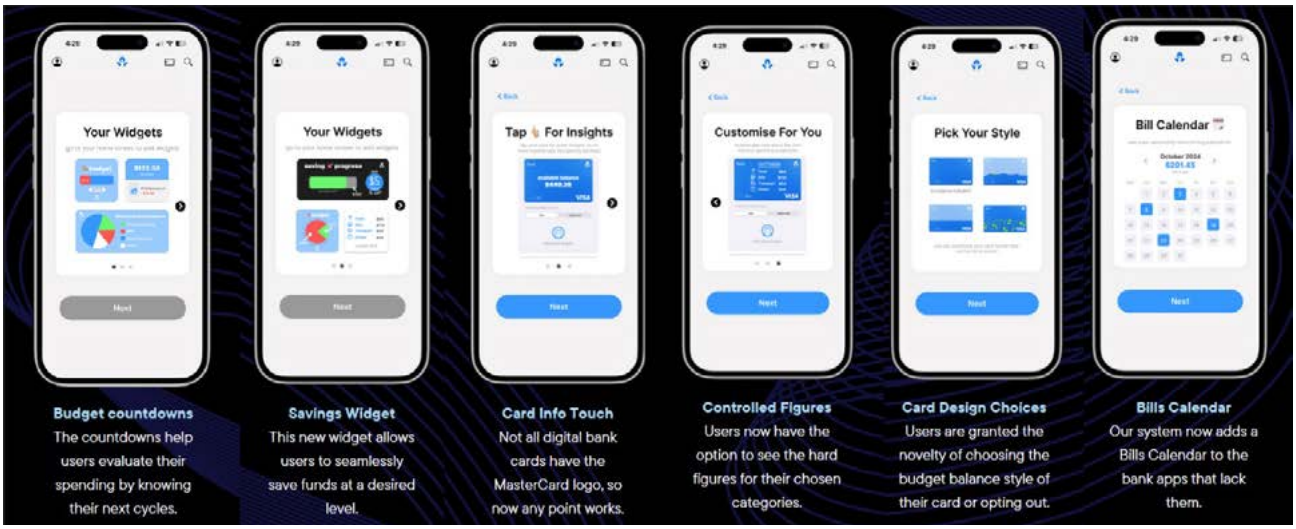


Figure 2. BANKME UX Conceptual Prototype

resulted in inconsistent user experiences.

Also, this team found that older users were more concerned about privacy and security than younger users. Younger users were therefore more open to DWs, valuing its efficiency and convenience.

Regarding money management, this group found that the ease of digital transactions could also encourage their participants to overspend. They highlighted the need for improved and consistent budgeting tools from banks, as current options were often seen as inadequate. This underscores the importance of developing more effective financial management solutions to help users of all ages control their spending and manage their finances more efficiently. This student group proposed the following solution (illustrated in Figure 2).

BANKME, a yearly subscription service for banks to integrate into their apps. It acts as a “bank revamp” system and includes:

- Widgets: Depicting receipts, budget trackers, and a savings button.
- Proactive security defences: Alerting users to various risks, with seven types of defences available.
- Security defence history: Providing transparency on security measures used.
- Desaturating digital card: Visually indicating budget status and providing balance information.
- Intelligent analysis for budgeting and tracking bills: Offering budgeting assistance and bill tracking features.

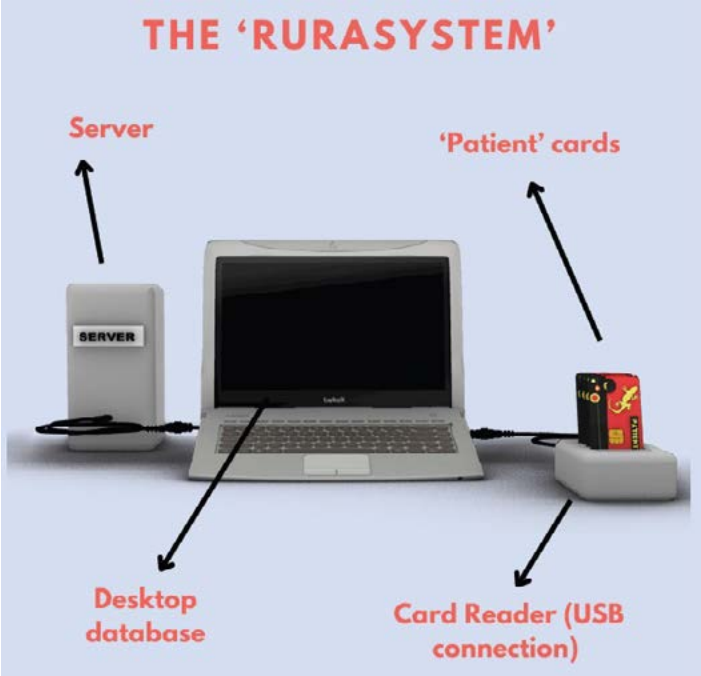


Figure 3. RURASYSTEM Conceptual Prototype.

Digital wallets and indigenous communities

The fourth and final team looked at the lack of accessibility to digital wallets in rural and remote Australia. They focused on analysing DW in indigenous communities. Their research, which included 15 interviews, indicated that indigenous communities face unique healthcare challenges, like limited access to comprehensive patient records, lack of access to advanced healthcare procedures, and historical distrust in institutions. Outstation residents, in particular, experienced inadequate and outdated care, restricted autonomy, and a historical lack of trust in institutions and healthcare providers. Nurses in remote outstations generally struggled with a lack of resources and large workloads. This was exacerbated by a lack of access to patient databases, requiring overworked nurses to rely heavily on their memory for patient information. Additionally, limited internet access compounded the issues. The team proposed the following solution to use DWs in healthcare as a means to provide better service and increase trust (illustrated in Figure 3).

RuraSystem, a decentralised database system designed to support indigenous nurses in outstations.

Features:

- Local, secure, and offline database accessible without an internet connection.
- Personal patient cards containing health records.
- Card reader for accessing and updating records.
- Temporary DWs for patients to carry health information to central hubs for further treatment.
- Integrated support tools at hubs to assist with training.

3.2.2 Digital wallet guidelines emerging from the student projects

The following key findings emerged from the student projects and captured user needs and preferences.

Digital Wallet Guidelines

1. Balance Security and Convenience: Ensure security features are robust but seamlessly integrated into the user experience. Features like biometric authentication, tokenisation, and multi-factor authentication should not hinder ease of use. Users often prioritise convenience but expect security to function in the background without unnecessary friction. Balancing these aspects builds trust and reduces the risk of data breaches or unauthorised access. Security features such as biometric logins or encrypted QR codes for transactions should be implemented with minimum additional steps for users. For example, auto-login for recognised devices can offer security without creating barriers.

2. Enhance Transparency About Data Usage: Clearly communicate how user data is stored, shared, and protected. Introduce dashboards or summaries to give users a visual representation of their data usage and permissions. Enhancing transparency builds trust and empowers users by giving them control over their information thereby addressing common concerns about privacy and misuse. Adding features like a “Data Transparency Hub” helps users view their data sharing history, adjust privacy settings, and understand how their data is used through simple, non-technical language.

3. Design for Demographic-Specific Needs: Customise DWs to cater to diverse user groups, such as older adults, rural users, or those with limited digital literacy. This could include simplified interfaces, hybrid physical-digital options, or offline functionality. By addressing the unique needs of specific demographics, DWs can increase adoption and usability while reducing frustration or exclusion. Create modular interfaces that adapt to user preferences. For older users, include large text, high-contrast designs, and tutorial videos. For rural users, design offline features or allow transactions to queue until connectivity is restored.

4. Incorporate Behavioural Insights for Financial Management: Add tools that help users track spending, set budgets, and receive personalised financial advice. Behavioural insights can guide users toward better financial habits. Features like spending alerts and budget tracking reduce overspending and provide value beyond transactions, encouraging more frequent use. Include real-time budget trackers, notifications for unusual spending patterns, and gamified savings goals to engage users in managing their finances more effectively.

5. Foster Intergenerational Collaboration: Implement programs or features that encourage younger users to assist older adults in adopting DWs, such as incentive schemes for teaching or assisting family members. Build a supportive ecosystem where tech-savvy users can help non-tech-savvy users bridge the digital divide, increasing overall adoption. Include referral programs or shared family accounts where younger users can assist with setup and troubleshooting, earning points or rewards for their support.

6. Ensure Accessibility in Low-Connectivity Environments: Incorporate offline capabilities, such as locally stored tokens for transactions and minimal reliance on continuous internet access. This addresses the challenges faced by users in rural or underserved areas, ensuring inclusivity. Enable functionality like storing encrypted transaction tokens locally that sync with the Cloud once connectivity is restored. Partner with telecom providers to optimise for low-bandwidth environments.

7. Integrate Education and Support Tools: Provide users with clear, accessible guides and tutorials to build confidence, especially for new adopters. Include multi-language support and assistive technologies. This increases digital literacy and reduces the barriers to entry for new users or those unfamiliar with DWs. Embed interactive onboarding guides, FAQ sections, and chatbots for instant support. Use step-by-step tutorials during the setup process to familiarise users with features.

8. Gamify Security and Usage: Introduce gamification elements to encourage secure behaviours, such as enabling two-factor authentication or reviewing account settings. This increases user engagement while subtly reinforcing secure habits and improving the overall experience. Offer badges or rewards for actions like setting up biometric authentication, securing accounts with strong passwords, or completing security reviews.

3.3 Factors affecting commercial digital wallet designers

The literature on DW design is dominated by the academic and end user perspectives with little input from industry app designers. This increases the likelihood of misalignment between academics, end users, and industry app designers, limiting the cross-pollination of ideas and best practice between these key groups. This could result in academics having limited understanding of the commercial constraints App designers work under and App designers having limited understanding of end user issues that academics are identifying. This section examines the commercial challenges App designers face.

3.3.1 Demographic profile of respondents

The seven respondents to the survey were predominantly aged 25 – 44 years (85% of participants) and predominantly female (71%). All had higher education qualifications and identified as either advanced or expert in problem solving, with strong verbal and written communication skills and capable of leading development teams. 57% felt they had a good understanding of cybersecurity principles and practices. 43% classified themselves as experts in User Interface (UI)/UX design. Most respondents identified themselves as beginners in programming languages and mobile development (71%).

Type of employment organisation and roles

43% of respondents currently worked in multinationals; 29% currently worked for an independent contractor or consultant and 28% worked for either a national organisation or a start-up. 86% of these organisations were in either North America or Europe – the remaining 14% did not indicate their work location.

86% had prior experience working in multinationals and 57% had worked for either an SME, Start-up or independent contractor/ consultant.

80% of respondents had planning and detailed design experience, 60% had experience in the areas of research & analysis; development support; product testing and validation, launch and monitoring.

Type of digital wallet experience

All respondents had been involved in conceptual wallet design and had worked in user interface/ user experience (UI/UX) design. Almost all (80%) had worked on data holding wallet designs on functionality, features and personalisation activities. Examples of work done included designing data wallet UX/UI; defining features for credential wallets and defining features for AI embedded into wallets. Their experience covered areas such as: improving payments functionality uplift within utilities; working on the Global Legal Entity Identifier Foundation ecosystem; working in education space startups, supporting country specific digital identity initiatives; working on the European digital wallet program (eIDAS) and assisting other companies with their wallet aspirations.

3.3.2 Legislation guidelines

The most popular legislative guidelines followed were 1) the General data protection regulation 2) electronic identification authentication and trust services legislation and 3) digital ID acts. One respondent noted that constant updates in legislation made wallet app design complicated, difficult to develop and maintain, and slowed development and release plans.

3.3.3 Areas of risk and priority

Most designers ranked security, simplicity, and transparency (clear and understandable information about transactions) as top design priorities. Their employers' top design priority was security.

The top high-risk priority areas in DW design from a user perspective were sharing information digitally and setting up security. Medium risk areas identified were online and in-app purchases. The lowest concern area was in-store purchases.

Designers predominantly viewed most design risks as falling in the medium risk range with the most important being explaining how data should be protected. The next most important areas were making in store purchases, online and in-app purchases and sharing information safely.

High risk areas of lower concern were using clear language and visuals to communicate risk, providing clear options for security, and explaining the use of encryption for sharing key data.

All designers felt it important users be notified of the type of information being asked by a party to validate their digital wallet actions and how that information would be used. However, designers were split on whether it was the designers' responsibility to notify users about what information was being asked and how long personal data would be retained.

3.3.4 Gaps in the design process

60% of respondents identified gaps in the design process within their organisations as due to:

1. pressure to get product to market without real user feedback
2. political agendas affecting the design process
3. design teams defining their own design principles.

One respondent noted that in Europe, eIDAS regulations were starting to dictate how wallets should be designed due to impending eIDAS compliant certification. The respondent commented that whilst the requirements were still being formed, they were comprehensive and were setting the standard for others to follow. Responses from designers on whether there were varying gaps in legislative requirement guidelines depended on what design aspect was being pursued (the survey question design unfortunately did not provide further data to explain this).

In summary, the app designers who completed the survey mainly worked in multinationals and national organisations in North America or Europe. They were predominantly young, educated and experienced in UI/UX design in wallet design, development and optimisation but not in programming languages and mobile development. Commercial factors affecting their design process were pressure to get product to market, political agendas affecting the design process and design teams defining their own design process. The app designers respondents' work was predominantly influenced by data protection and reliable identity authentication regulations. Their employers' top priority was security. The designers' interests were in UX/UI design that was secure, simple to use and supported data transparency. Their top design concerns from a user perspective were setting up security and information sharing. While all 7 designers felt it important users be notified of the type of information being asked by a party to validate their digital wallet actions and how that information would be used, they were split on the level of disclosure as designers they were responsible for providing in this area.

Discussion

Discussion on how to Optimise Digital Wallet Design for Identity Management

The research question brought together academic, user and wallet designers' perspectives on aspects shaping digital wallet design to identify

'How to improve the design of digital wallets to help users make informed identity management decisions?

The response to this question focused on identifying risky areas in DW design and usage and how to address these through UX design and the influencing of user identity management behaviour.

Identifying risky areas in DW design and DW usage

The literature review relating to informed identity management decisions concerned digital wallet design (UX design) and data security and privacy (InfoSec). Together these shape how and where users perceive risk in DW decision-making which in turn affects their trust in what personal information they share with others. How users manage their personal identity information in DW decision making is particularly important at high-risk information exchange points in the DW usage process.

Designers felt users were most at risk when setting up security and sharing information digitally. Two of the student projects offer deeper insights. The Privy Buddy project showed Gen Z's, active users of DWs, were largely ignorant about data safety and how their data was used. This weakness was exacerbated by their prioritisation of convenience over security (i.e. they shared their personal data readily) and agreed to large corporation terms and conditions without reading them. In contrast the Clippy Project showed older adults were more hesitant to adopt DWs due to poor technological literacy indicating easy-to-understand setup processes and guided support and products tailored/customisable to their needs were important. This level of attention is also needed for communities where there is an ingrained distrust of institutions and also for those that support these communities (see RuraSystem project). Fostering intergenerational collaboration where tech savvy and supportive respected community members act as DW user champions is also important. Creating and building opportunities for designers to work in a respectful way with end user community groups is likely to be integral to DW acceptance (Bowler et al., 2023).

Designers identified users' identity management at medium risk during online and in-app purchases and making in-store purchases. Designers believed they were at medium risk when designing the processes related to the storage of additional information, adding payment information, making in-store purchases, online and in-app purchases and sharing information digitally. No high-risk areas were identified. The student projects discussed above suggest designers may need to reconsider this risk weighting for high-risk users such as those with poor connectivity, low digital technology skills, low DW trust or high compulsive behaviour addictions (e.g. gambling, shopping, gaming, drug/alcohol, smartphone or social media addiction) to ensure appropriate support is provided to support them. For example, the BANKME project which surveyed adults over 18 years, found half the participants identified that overspending behaviour was aggravated by easy payment interactions when no visibility of financial impact was provided. Given that 30% of Americans self-identified as addicted to social media (addictiongroup.org), 48% reported an addiction to digital devices (Thenestledrecovery.com) and over 50% showed signs of problematic internet use (Thenestledrecovery.com), helping users manage their weaknesses during DW usage is an important designer consideration.

UX Design considerations:

This area incorporates findings on communication & information (how information is presented, the clarify of messages and feedback mechanisms); user support and assistance (help features, onboarding, troubleshooting and guidance during use) and user experience & interaction (design elements, ease of navigation, responsiveness and accessibility). Differences arising from the different research stream perspectives can be explained by their different foci. The literature review identified design principles, underpinning theories and captured the academic focus on user related trust perspectives reflecting the focus of this study. In contrast the student projects studied specific demographic needs and behavioural insights relating to data management and DW usage in specific case study areas e.g. banking and payments, health and identity management. In contrast the designers focused on commercial design considerations such as possible gaps in the design of DW processes and functions.

All three research areas identified user accessibility as key to DW take up and usage with simple to use interfaces a top priority. The literature and student projects held DW designers responsible for encouraging appropriate DW usage behaviour (understanding and navigation) through interface design and the inclusion of education and support tools. Academics, users and designers all agreed that transparent functionality, and minimalistic and aesthetic design were important intuitive navigation and user customisation. However, designers noted pressure to get product to market, team autonomy and political agendas often resulted in a lack of real user feedback in the design process.

Security & privacy

This area focused on the security and privacy of user data, ensuring safe transactions and helping users manage their behaviour and identity information.

All three research areas indicated security of personal data and transparency about how it is used are important for user trust. Whilst the literature review provided a comprehensive overview of key aspects relating to these areas, the top prioritisation for DW designers and their employers was security. Most designers indicated their second priority was data request transparency whilst their employers focused on their employers who focused on personalisation and a mobile-first design. In contrast the literature and student projects focused on the balance between security and user behaviour with the student projects suggesting gamification as one way to tackle the issue of low user engagement in these areas.

DW designers felt it important that users be notified of the type of information being asked by a party to validate their digital wallet actions and how that information would be used. However, designers were split on whether it was their responsibility to notify users about what actual information was being asked for and how long that personal data would be retained by the requester.

Identity management

The literature review's user perspective and industry designers' commercial drivers focus highlighted the importance of easily accessible clear communication information and processes. Both highlighted the need to inform users about the type of information being requested and its usage. The projects focused on DW usage in particular contexts and confined identity management insights to user concerns about security and information sharing reflecting the tension between usability and protection. Privy Buddy, an internet browser extension, provided an option for making data privacy and security more convenient and transparent. Clippy sought to combine a physical card with a digital interface to help older users make payment interactions more familiar to them and promoted inter-generational collaboration as a way to bridge the divide between different experience and age levels of user groups. BANKME, a bank app integrating multiple apps, sought to offer more effective financial management solutions to help users of all ages control their spending and manage their finances more efficiently. RuraSystem sought to support nurses working in rural indigenous communities through a decentralised database system of patient health record data. All three research areas touched on the need to balance security with convenience which requires finding the right trade-off between protecting data and ensuring usability.

Designers identified the process of notifying users of the type of information being requested and encouraging informed consent in high-risk areas reflecting discussions in the literature about how to encourage privacy behaviour (Burkhardt et al. 2023) and data protection and identity authentication regulations. Designers universally supported notifying users about the type of personal identifiers being asked by a third party to validate service support requests and the reasons for request of particular personal information/ types. Most supported informing users of where their personal identifiers were being held and what happened to that data once the action was complete. However, opinions were divided on whether designers were responsible for notifying users about the type of information being asked by a party to validate actions. This suggests universal guidelines in this area would be useful for designers.

How to improve the design of digital wallets to help users make informed identity management decisions?

DW UX design and data security and privacy shape how and where users perceive risk in DW decision-making which in turn affects their trust in what personal information they share with others. UX design must be simple, intuitive and easy to use but it also needs to provide alerts to users when their decision making, and behaviour may detrimentally affect their DW usage outcomes (e.g. sharing personal details with third parties for unknown usage). To ensure consistent accessibility DWs need to be easily customisable to the needs of specific user groups and to their connectivity status (e.g. variations in internet access or different legislation requirement).

Contributions

Key Contributions

To researchers:

- Identification of the need to incorporate the commercial designer perspective into digital wallet design to understand how commercial considerations shape DW design.
- Identification of the need to promote the findings from their research into DW user needs and wants through media channels accessible and relevant to designers.

To designers, policy makers, regulators, consortiums and peak bodies researching DW adoption & usage:

- Raising awareness of alternative sources where designers, policy makers, regulators, consortiums and peak bodies researching DW adoption and usage can access contemporary research on user expectations and needs.

To commercial organisations and consultancies

- Providing commercial organisations and consultancies with a research-based framework against which to develop, advise and consult on best practice and compliance.

Researchers

- Highlighted to researchers the need to incorporate commercial designer perspectives into digital wallet (DW) design.
- Emphasised to researchers the need to promote research findings promoting research findings on user needs through accessible media channels.

Designers

- Provided designers with research-based guidelines for effective DW design.
- Raised awareness of alternative sources for contemporary user research.
- Identified risk areas in the DW process that could impact user outcomes.

Policy Makers

- Offered evidence-based insights to inform digital wallet policy development.
- Supported alignment between user expectations and regulatory frameworks.

Consortiums and Peak Bodies

- Shared access to current research on user needs and expectations.
- Encouraged the use of academic findings to shape adoption strategies.

Standards Bodies

- Delivered research-backed material to inform the creation of standards and guidelines for DW design.

Regulators

- Provided standards and benchmarks to support regulatory oversight of digital wallets

Commercial Organisations and Consultancies

- Introduced a research-based framework to guide best practice, compliance, and advisory services in DW development.

Limitations

Limitations

This research was limited by the low response rate by commercial designers to the survey and the limiting capturing of the perspectives of digital wallet (DW) designers in the academic literature. This affects the broader generalisability of the analysis findings and discussion. In addition, the low number of designer respondents may not reflect the diversity of views and experience of the entire DW designer population which can affect the determination of meaningful patterns or differences and trust in those findings.

Conclusion

Conclusion and Recommendations

This report set out to identify ways to improve digital wallet (DW) design to support users in making informed identity management decisions. The literature review underscored the importance of integrating user experience (UX) and information security (InfoSec) principles, supported by behavioural theories and regulatory frameworks, to foster trust and informed consent.

Insights from student projects revealed diverse user needs and challenges, including digital literacy gaps, access barriers, and generational differences. Their proposed solutions—such as simplified interfaces and offline access—highlighted the value of inclusive, user-centred design.

Designer surveys further illuminated how regulatory and commercial pressures shape DW development, often limiting user feedback and introducing risk areas that could undermine adoption.

Together, these findings emphasise the need for a holistic inclusive approach to DW design—one that aligns academic research, user experience, and designer perspectives. By grounding design in behavioural insight and inclusive principles, digital wallets can better support users in managing their identities with confidence and clarity.

Based on the above the following recommendations are made:

1. Comprehensive research on DW design and implementation
    a. Qualitative research is needed to more comprehensively understand the designer's perspective and the nuances of the DW design process
    b. Quantitative research is needed to validate and explore relationships between factors influencing DW design
    c. Diverse designer perspectives are needed to bridge gaps between policy, user needs and commercial realities
2. An alignment of academic and design priorities
    a. Better understanding of user behaviour through the research of how social and psychological factors influence online identity management, particularly in the DW context.
    b. Stronger collaboration between designers and academics to improve mutual understanding of user needs and design priorities.
3. A better articulation of how to translate complex requirements into user-friendly design
    a. Context relevant dialogue between multiple stakeholders groups (regulators, users, academics and designers) is needed on how to
        i. translate technical and regulatory requirements into intuitive, user-controlled secure experiences.
        ii. Design experiences that foster user trust in digital identity systems

    Incorporating a broader range of stakeholder perspectives could help bridge the gap between policy, user needs, and the commercial realities underpinning digital wallet design. This would help to foster context relevant dialogue that more accurately translates complex digital identity requirements into intuitive, user-controlled experiences that engender trust.

Bringing together designer and academics perspectives on user needs and priorities through research and case study examples is important if DW design is to shape users' identity management decisions. As findings from a recent research commissioned report by the EU Digital Wallet Consortium noted "Security and privacy are seen as key features ... but wallets are not fully delivering on this benefit yet with users wanting clear signposting of security (trustmarks) and greater control of the data they share" (EU Digital Identity Wallet Consortium 2025, June, slide 3).

References

References used in this report

Addiction Group.org, (2025, Feb 17), Statistics on Social Media Addition, available at https://www.addictiongroup.org/resources/social-media-addiction-statistics/

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211.

Alfie, N. A., Sidi, J., Junaini, S. N., Chai, W. Y., Mit, E., & Gedat, R. (2023, October). Bridging the Digital Gap: **A Systematic Review on UI/UX Design Considerations for Elderly-Friendly Digital Wallets.** In *2023 6th International Conference on Applied Computational Intelligence in Information Systems (ACIIS)* (pp. 1-6). IEEE.

Ansaroudi, Z. E., Carbone, R., Sciarretta, G., & Ranise, S. (2023). Control is Nothing Without Trust a First Look into Digital Identity Wallet Trends. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).

Bamforth et al 2020, Digital wallets: impact, implications and issues, APO, available at https://apo.org.au/node/309504.

Bowler, R., Goodell, G., Revans, J., Bizama, G., & Speed, C. (2023). A non-custodial wallet for digital currency: design challenges and opportunities. https://doi.org/10.48550/arxiv.2307.05167

Capital One Shopping , Digital Wallet Statistics (2025, 23 June): Users, Growth Rate & Trends, available at https://capitaloneshopping.com/research/digital-wallet-statistics/ .

Čučko, S., Šumak, B., & Turkanović, M. (2023). Identification and Analysis of Self-Sovereign Identity User Interface and User Experience Design Patterns. Proceedings - 2023 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2023.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.

DIN EN ISO 9241-210:2020-03. 2020. DIN EN ISO 9241-210:2020-03, Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems (ISO 9241-210)

EU Digital Identity Wallet Consortium, (2025, June) GEN, EWC Phase 2 (P2) End User Pilot Report, Travel and Hospitality, available at https://eudiwalletconsortium.org/wp-content/uploads/2025/07/Phase-2-end-user-pilot-report_v1.1.pdf

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behavior. Reading, MA:Addison-Wesley.

Gelo, O., Braakmann, D., & Benetka, G. (2008). Quantitative and qualitative research: Beyond the debate. Integrative psychological and behavioral science, 42(3), 266-290.

Harrison McKnight, D., & Chervany, N. L. (2001). Trust and distrust definitions: One bite at a time. In *Trust in cyber-societies: Integrating the human and artificial perspectives* (pp. 27-54). Springer Berlin Heidelberg.

Kagan, J, (2024). What is a digital wallet?, Investopedia, Available at What Is a Digital Wallet?

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision support systems, 44(2), 544-564.

Korir, M., Parkin, S., & Dunphy, P. (2022). An empirical study of a decentralized identity wallet: Usability, security, and perspectives on user control. In *Eighteenth symposium on usable privacy and security (SOUPS 2022)* (pp. 195-211).Lacity, M. C., Schuetz, S. W., Kuai, L., & Steelman, Z. R. (2024). IT's a matter of trust: Literature reviews and analyses of human trust in information technology. Journal of information technology. https://doi.org/10.1177/02683962231226397

Lukkien, B., de Reuver, M., & Bharosa, N. (2023, Jul 11-14). Barriers for developing and launching digital identity wallets. [Together in the unstable world: Digital government

and solidarity]. 24th Annual International Conference on Digital Government Research (DGO) - Together in the Unstable World - Digital Government and Solidarity, Gdansk, POLAND.

Sauer, M., Becker, C., Oberweis, A., Pfeifer, S., Stark, A., & Sürmeli, J. (2024, November). User Experience and Information Security Implications of Digital Identity Wallets. In *Proceedings of the 2024 14th International Conference on Information Communication and Management* (pp. 36-45).

Sellung, R., & Kubach, M. (2023). Research on User Experience for Digital Identity Wallets: State-of-the-Art and Recommendations. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI),

Sukaris, S., Renedi, W., Rizqi, M. A., & Pristyadi, B. (2021). Usage Behavior on Digital Wallet: Perspective of the Theory of Unification of Acceptance and Use of Technology Models. Journal of Physics: Conference Series.

The nestled Recovery Centre, Internet/ Cyber Addition Statistics in the United States, available at https:// thenestledrecovery.com/rehab-blog/ internet-addiction-statistics/#:~:text=Key%20 Takeaways%3A,criteria%20for%20 problematic%20internet%20use

Burkhardt, G., Boy, F., Doneddu, D., & Hajli, N. (2023). Privacy behaviour: A model for online informed consent. Journal of business ethics, 186(1), 237-255.

Chatterjee, D., & Bolar, K. (2019). Determinants of mobile wallet intentions to use: The mental cost perspective. International Journal of Human–Computer Interaction, 35(10), 859-869.

Chuhan, S., & Wojnas, V. (2023, July). Designing and evaluating a resident-centric digital wallet experience. In International Conference on Human-Computer Interaction (pp. 591-609). Cham: Springer Nature Switzerland.

Khando, K., Islam, M. S., & Gao, S. (2022). The emerging technologies of digital payments and associated challenges: a systematic literature review. Future Internet, 15(1), 21.

Kim, G. H. (2024, July). A study on universal digital wallet for web 3. In 2024 Fifteenth International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 70-72). IEEE.

Lacity, M. C., Schuetz, S. W., Kuai, L., & Steelman, Z. R. (2024). IT'sa matter of trust: Literature reviews and analyses of human trust in information technology. Journal of Information Technology, 02683962231226397.

Lindegren, D., Karegar, F., Kane, B., & Pettersson, J. S. (2021). An evaluation of three designs to engage users when providing their consent on smartphones. Behaviour & Information Technology, 40(4), 398-414.

Maxwell, J. A., & Loomis, D. M. (2003). Mixed methods design: An alternative approach. Handbook of mixed methods in social and behavioral research, 1(2003), 241-272.

Maxwell, J. (1992). Understanding and validity in qualitative research. Harvard educational review, 62(3), 279-301.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of management review, 20(3), 709-734.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. Academy of Management review, 23(3), 473-490.

McKnight, D. H., & Chervany, N. L. (2000). What is trust? A conceptual analysis and an interdisciplinary model.

Nieles M., Dempsey K., Pillitteri, V. Y. (2017). NIST Special Publication 800-12: An introduction to information security. https://doi.org/10.6028/ NIST.SP.800-12r

Peters, D. (2023). Wellbeing Supportive Design - Research-Based Guidelines for Supporting Psychological Wellbeing in User Experience. International journal of human-computer interaction, 39(14), 2965-2977. https://doi.org/ 10.1080/10447318.2022.2089812.

Sahir, S. H., Rosmawati, R., Listiorini, L., & Pahlevi, M. (2024). The influence of user experience using digital wallets on consumer behavior. AIP Conference Proceedings.

Sartor, Sebastian; Sedlmeir, Johannes; Rieger, Alexander; and Roth, Tamara, "Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets" (2022). ECIS 2022 Research Papers. 46. https://aisel.aisnet.org/

ecis2022_rp/46.

Satybaldy, A. (2023). Usability Evaluation of SSI Digital Wallets. IFIP Advances in Information and Communication Technology.

Sauer, M., Becker, C., Oberweis, A., Pfeifer, S., Stark, A., & Sürmeli, J. (2024, November). User Experience and Information Security Implications of Digital Identity Wallets. In Proceedings of the 2024 14th International Conference on Information Communication and Management (pp. 36-45).

Sellung, R., & Kubach, M. (2023). Research on User Experience for Digital Identity Wallets: State-of-the-Art and Recommendations. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI).

Senali, M. G., Iranmanesh, M., Ismail, F. N., Rahim, N. F. A., Khoshkam, M., & Mirzaei, M. (2023). Determinants of Intention to Use e-Wallet: Personal Innovativeness and Propensity to Trust as Moderators. International Journal of Human–Computer Interaction, 39(12), 2361-2373. https://doi.org/10.1080/10447318.2022.2076309.

Shehu, A. S., Pinto, A., & Correia, M. E. (2023). SPIDVerify: A Secure and PrivacyPreserving Decentralised Identity Verification Framework. 2023 International Conference on Smart Applications, Communications and Networking, SmartNets 2023.

Sukaris, S., Renedi, W., Rizqi, M. A., & Pristyadi, B. (2021). Usage Behavior on Digital Wallet: Perspective of the Theory of Unification of Acceptance and Use of Technology Models. Journal of Physics: Conference Series.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS quarterly, 425-478.

Wang, R., Bush-Evans, R., Arden-Close, E., Bolat, E., McAlaney, J., Hodge, S., Thomas, S., & Phalp, K. (2023). Transparency in persuasive technology, immersive technology, and online marketing: Facilitating users' informed decision making and practical implications. Computers in human behavior, 139, 107545. https://doi.org/10.1016/j.chb.2022.107545

Yang, Y., Liu, Y., Li, H., & Yu, B. (2015). Understanding perceived risks in mobile payment acceptance. Industrial management + data systems, 115(2), 253-269. https://doi.org/10.1108/IMDS-08-2014-0243.

Appendices

Appendix 1 – List of articles in Systematic Review:

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211.

Alfie, N. A., Sidi, J., Junaini, S. N., Chai, W. Y., Mit, E., & Gedat, R. (2023, October). Bridging the Digital Gap: **A Systematic Review on UI/UX Design Considerations for Elderly-Friendly Digital Wallets.** In *2023 6th International Conference on Applied Computational Intelligence in Information Systems (ACIIS) (pp. 1-6).* IEEE.

Ansaroudi, Z. E., Carbone, R., Sciarretta, G., & Ranise, S. (2023). Control is Nothing Without Trust a First Look into Digital Identity Wallet Trends. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).

Bazarhanova, A., Smolander, K.: The review of non-technical assumptions in digital identity architectures. In: Hawaii International Conference on System Sciences (2020). https://doi.org/10.24251/HICSS.2020.785

Berbecaru, D. G., Lioy, A., & Cameroni, C. (2021). On enabling additional natural person and domain-specific attributes in the eidas network [Article]. IEEE Access, 9, 134096-134121. https://doi.org/10.1109/ACCESS.2021.3115853

Bowler, R., Goodell, G., Revans, J., Bizama, G., & Speed, C. (2023). A non-custodial wallet for digital currency: design challenges and opportunities. https://doi.org/10.48550/arxiv.2307.05167

Burkhardt, G., Boy, F., Doneddu, D., & Hajli, N. (2023). Privacy Behaviour: A Model for Online Informed Consent. Journal of business ethics, 186(1), 237-255. https://doi.org/10.1007/s10551-022-05202-1

Caraban, A., Karapanos, E., Gonçalves, D., & Campos, P. (2019). 23 Ways to Nudge: A Review of Technology-Mediated Nudging in Human-Computer Interaction. New York, NY, USA.

Chatterjee, D., & Bolar, K. (2019). Determinants of Mobile Wallet Intentions to Use: The Mental Cost Perspective. International Journal of Human–Computer Interaction, 35(10), 859-869. https://doi.org/10.1080/10447318.2018.1505697

Chuhan, S., & Wojnas, V. (2023). Designing and Evaluating a Resident-Centric Digital Wallet Experience. HCI for Cybersecurity, Privacy and Trust, Cham.

Čučko, S., Šumak, B., & Turkanović, M. (2023). Identification and Analysis of Self-Sovereign Identity User Interface and User Experience Design Patterns. Proceedings - 2023 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2023.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.

Harrison McKnight, D., & Chervany, N. L. (2001). Trust and distrust definitions: One bite at a time. In *Trust in cyber-societies: Integrating the human and artificial perspectives* (pp. 27-54). Springer Berlin Heidelberg.

Khando, K., Islam, M. S., & Gao, S. (2022). The emerging technologies of digital payments and associated challenges: a systematic literature review. Future Internet, 15(1), 21.Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Systems, 44(2), 544-564. https://doi.org/10.1016/j.dss.2007.07.001

Kim, G. H. (2024, 2-5 July 2024). A Study on Universal Digital Wallet for Web 3*. 2024 Fifteenth International Conference on Ubiquitous and Future Networks (ICUFN).

Korir, M., Parkin, S., & Dunphy, P. (2022). An empirical study of a decentralized identity wallet: Usability, security, and perspectives on user control. In *Eighteenth symposium on*

usable privacy and security (SOUPS 2022) (pp. 195-211).Lacity, M. C., Schuetz, S. W., Kuai, L., & Steelman, Z. R. (2024). IT's a matter of trust: Literature reviews and analyses of human trust in information technology. Journal of information technology. https://doi.org/10.1177/02683962231226397

Lepore, C., Laborde, R., & Eynard, J. (2024). Aligning eIDAS and Trust Over IP: A Mapping Approach. ACM International Conference Proceeding Series,

Lindegren, D., Karegar, F., Kane, B., & Pettersson, J. S. (2021). An evaluation of three designs to engage users when providing their consent on smartphones. Behaviour & Information Technology, 40(4), 398-414. https://doi.org/10.1080/0144929X.2019.1697898

Lukkien, B., de Reuver, M., & Bharosa, N. (2023, Jul 11-14). Barriers for developing and launching digital identity wallets. [Together in the unstable world: Digital government and solidarity]. 24th Annual International Conference on Digital Government Research (DGO) - Together in the Unstable World - Digital Government and Solidarity, Gdansk, POLAND.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review,* 20(3), 709-734.

Maxwell, J. A. (1992). Understanding and validity in qualitative research. Harvard Educational Review, 62(3), 279–300.

Maxwell, J. A., & Loomis, D. M. (2003). Mixed methods design: An alternative approach. In A. Tashakkori, & C. Teddlie (Eds.), Handbook of mixed methods in social and behavioral research. Thousand Oaks, CA: Sage

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management review,* 23(3), 473-490.

McKnight, D. H., & Chervany, N. L. (2000). What is trust? A conceptual analysis and an interdisciplinary model.

Nieles M., Dempsey K., Pillitteri, V. Y. (2017). NIST Special Publication 800-12: An introduction to information security. https://doi.org/10.6028/NIST.SP.800-12rl

Peters, D. (2023). Wellbeing Supportive Design - Research-Based Guidelines for Supporting Psychological Wellbeing in User Experience. International journal of human-computer interaction, 39(14), 2965-2977. https://doi.org/10.1080/10447318.2022.2089812

Satchell, C Shanks, G. Howard, S. & Murphy, J. *"Beyond security: Implications for the future of federated digital identity management systems," in Proc. 20th Conf. Comput.-Hum. Interact. Special Interest Group (CHISIG) Aust. Comput.-Hum. Interact., Design: Activities, Artefacts Environ. (OZCHI), 2006, pp. 313316, doi: 10.1145/1228175.1228231*

Sauer, M., Becker, C., Oberweis, A., Schork, S., & Sürmeli, J. (2024, November). User experience and information security heuristics for digital identity wallets. In *International Conference on Computer-Human Interaction Research and Applications* (pp. 339-361). Cham: Springer Nature Switzerland.

Sahir, S. H., Rosmawati, R., Listiorini, L., & Pahlevi, M. (2024). The influence of user experience using digital wallets on consumer behavior. AIP Conference Proceedings.

Sartor, Sebastian; Sedlmeir, Johannes; Rieger, Alexander; and Roth, Tamara, "Love at First Sight? A User Experience Study of Self-Sovereign Identity Wallets" (2022). ECIS 2022 Research Papers. 46. https://aisel.aisnet.org/ecis2022_rp/46

Satybaldy, A. (2023). Usability Evaluation of SSI Digital Wallets. IFIP Advances in Information and Communication Technology.

Sauer, M., Becker, C., Oberweis, A., Pfeifer, S., Stark, A., & Sürmeli, J. (2024, November). User Experience and Information Security Implications of Digital Identity Wallets. In *Proceedings of the 2024 14th International Conference on Information Communication and Management* (pp. 36-45).

Sellung, R., & Kubach, M. (2023). Research on User Experience for Digital Identity Wallets: State-of-the-Art and Recommendations. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI),

Appendix 2

UX design issues and resolution guidelines

Table 1 – UX design Issues and resolution guidelines

Areas of UX design	Poor aspects in areas	UX design guidelines	Security & Privacy design guidelines	Identity data management design guidelines	User interface design guidelines	UX heuristics (Sauer et al. 2024)	Infosec heuristics (Sauer et al. 2024)
Communication and information	Technical language usage that users may not understand. The omitting of explicit information for users on how their data is stored	Use of understandable terms that are clear and easy to understand. Use of consistent terms to maintain uniform terminology across app. Transparent information on data storage and how user data is stored.	Transparent information on data storage: Clear and detailed information about how user data is stored, ensuring users understand the security measures in place	User-friendly and transparent backup options Clear and easy-to-understand backup methods Visible user reminders to back up data regularly.	Placement of information strategically so it is easily accessible and understandable.	Placement of information strategically so it is easily accessible and understandable.	Placement of information strategically so it is easily accessible and understandable.
User support and assistance	Little user support and guidance and a lack of mechanisms to retrieve lost or forgotten credentials	Offer guidance and channels for user feedback. Managing errors effectively to assist users. Facilitate a smooth introduction to and onboarding to the app.		Adopt user-friendly account recovery that follows users' mental models. Implement recovery processes that align with users' expectations and mental models.	Use text sizes that are readable for all users. Use high contrast colours for better visibility and intuitive buttons which are easily identifiable and guide users to improve navigation. Use a minimalistic and simple design that is straightforward.	Providing help and documentation tailored to users' specific tasks, including help requests and detailed guides.	Provide recovery options to ensure data availability, prevent data loss, and enable data recovery through automated backups.
User experience during interaction	Poor DW app structuring that don't support user mental models and expectations. No ability to transfer accounts and credentials to other wallets	Design intuitive and predictable interaction flows. Allow users to tailor the application to their preferences. Ensure app is easy to navigate and provide search & filter options to find and organize information. Ensure interface works well across different devices and contexts. Design app to feel familiar and dependable.		Allowing users to transfer their data seamlessly between different digital wallets. Provide users with the ability to delete their accounts easily.		Ensure app is accessible to users with disabilities or conditions that require additional features. Allow users to navigate freely within the wallet by supporting exit, cancel, and back features that also enable continuation of cancelled processes. Use consistent interaction patterns and terminology within the wallet and across applications that follow uniform design standards. Design app to prevent incorrect operations, warn users before errors occur, and offer solutions if errors happen. Support flexible use, allowing credentials to be grouped, sorted, filtered, and searched, and provide automation functions to increase efficiency. Use a minimalist and aesthetic design that supports users' primary goals, with a logical information structure and customizable elements.	Securing sensitive user data with standardized authentication methods (e.g., finger scan) and ensuring users are authenticated and authorized. Automatically install required security updates and notifying users to maintain security.
Data management and security	Insufficient implementation of backup methods	Properly secure app and its functions by implementing robust security measures to protect user data.	Properly secure app and its functions by implementing robust security protocols that, ensure user data and transactions are safe.	Ensuring data is backed up automatically to prevent loss.		Provide adaptive interfaces to other ecosystems to create opportunities for using the wallet. Provide user autonomy and control by Allowing users to access their data independently, manage identity profiles, consent to data use, and transfer data between wallets.	Use cryptographic mechanisms and secure protocols to protect data during transmission and to detect unauthorized changes. Implementing secure encryption and decryption of data stored in the app by using key pairs and decentralized identifiers (DIDs).

Improving

Digital Wallet Design

by aligning the expertise of designers, users and academia

July 2025