Improving Personal Data Protection Interaction in Digital Identity Wallets: A User-Centric Analysis

20th IFIP TC13 International Conference on Human-Computer Interaction

Shirlei Aparecida de Chaves, Fabiane Barreto Vavassori Benitti

Programa de Pós-Graduação em Ciência da Computação (PPGCC) - Universidade Federal de Santa Catarina (UFSC)

8 - 12 September 2025

Some Context

- Privacy regulations (e.g., GDPR, LGPD) require user-centred data protection
  - Yet, users rarely engage with privacy settings – the *privacy paradox*
- Digital identity begins at registration and is managed by Identity Providers (IdPs)
  - Centralised IdPs pose privacy risks; decentralised models (SSI) give users more control via digital wallets
  - However, SSI solutions face usability, trust, and transparency challenges
- This work proposes the use of **Transparency-Enhancing Tools (TETs)** to improve user understanding and control in decentralised identity systems

What is Digital Identity?

Definition

A **digital identity** is a unique set of attributes that identifies an individual or entity in a specific online context.

- Includes personal data used to recognise individuals in digital interactions
- Serves as the user's representation in online services and transactions
- Defined by standards (e.g., NIST 800-63-3) and regulations (e.g., GDPR)

Sources: NIST SP 800-63-3 (2020)[1] , Wilson & Hingnikar (2023)[2], GDPR (2016) [3]

[1] GRASSI, PAUL; GARCIA, MICHAEL; FENTON, JAMES. NIST SPECIAL PUBLICATION 800-63-3 DIGITAL IDENTITY GUIDELINES. 2020. Available from: <https://doi.org/10.6028/NIST.SP.800-63-3>.

[2] WILSON, YVONNE; HINGNIKAR, ABHISHEK. THE LIFE OF AN IDENTITY. In: SOLVING Identity Management in Modern Applications: Demystifying OAuth 2, OpenID Connect, and SAML 2. Berkeley, CA: Apress, 2023. P. 11–22. ISBN 978-1-4842-8261-8. DOI: 10.1007/978-1-4842-8261-8 2.

[3] EUROPEAN COMMISSION. 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) (TEXT WITH EEA RELEVANCE). European Commission, 2016. Available from: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

Digital Identity: Data Management & Ownership

- The Internet lacks a native identity layer
- Result: fragmented, service-specific identity systems
- Users must manage multiple accounts and credentials manually
- This fragmentation limits user control and hinders privacy

Source: Cameron, K. (2005). *The Laws of Identity*[4].

[4] http://myinstantid.com/laws.pdf

Digital Identity Management and Ownership

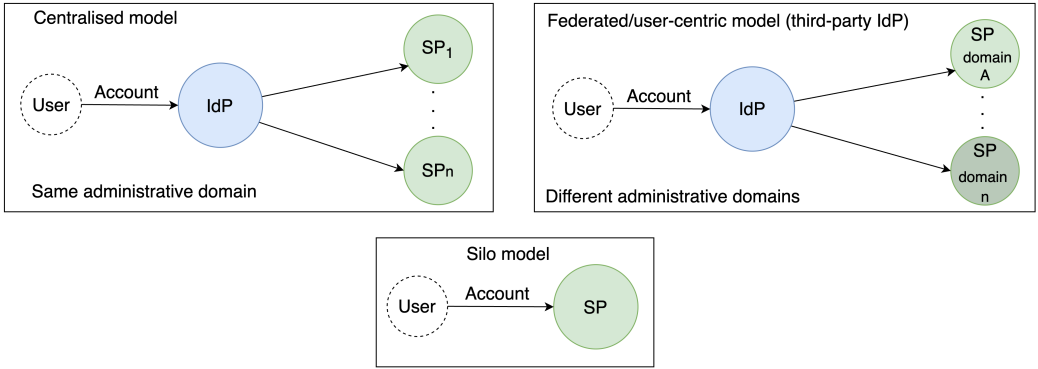


Figure: Identity Management (IdM) Models[5].

[5] Adapted from PREUKSCHAT, ALEX; REED, DRUMMOND. SELF-SOVEREIGN IDENTITY. Manning Publications, 2021. ISBN 9781617296598.

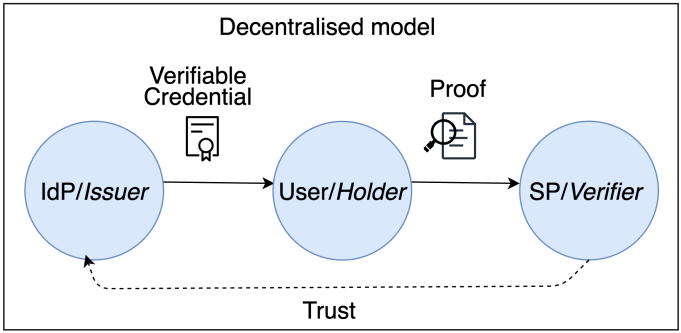


Figure: From Centralised to Decentralised Identity Models[5]

.

[5] Adapted from PREUKSCHAT, ALEX; REED, DRUMMOND. SELF-SOVEREIGN IDENTITY. Manning Publications, 2021. ISBN 9781617296598.

- We conducted a **Rapid Review** to map user-facing tools and challenges in decentralised identity systems.[6]

Scopus Search (30 Nov 2023)

Filter	Values
Document type	Conference Paper, Journal Article
Language	English
Keywords	`("review" OR "map*" OR "survey") AND ("self-sovereign identity" OR "decentralised identity")`

Research Questions

- **RQ1:** What are the main tools of user interaction in decentralised IdMs?
- **RQ2:** What are the challenges of decentralised IdMs?

[6] Cartaxo, B. et al. (2020). Rapid Reviews in Software Engineering. In: *Contemporary Empirical Methods in SE*, Springer.

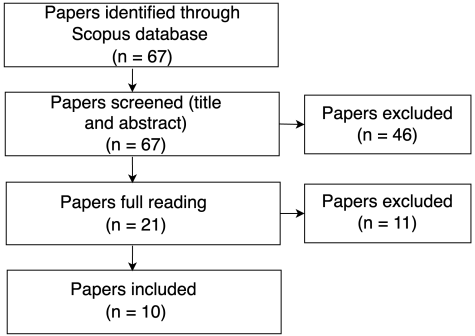


Figure: Paper selection flow.

Inclusion and Exclusion Criteria

Inclusion Criteria
(i) Secondary study
(ii) Peer-reviewed
(iii) Written in English
(iv) Covers solutions and challenges from the user perspective
Exclusion Criteria
(i) Not secondary study / not relevant
(ii) Duplicate
(iii) Not in English
(iv) Not peer-reviewed

- **Main Tool:** Digital Identity Wallets
- Used for secure storage and management of:
  - Identity attributes
  - Cryptographic keys
- Enable user interaction with online services

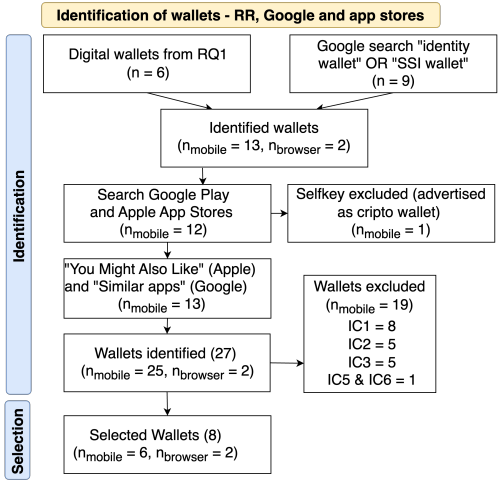
Figure: EU Digital Identity Wallet[7]

[7] ec.europa.eu/digital-building-blocks/...

A digital identity wallet provides secure, user-controlled storage and usage of identity data for interaction with online services.

- Enhancing User Experience and Usability;
- SSI Ecosystem Growth, Adoption, and Interoperability;
- Security, Recovery, and Key Management Challenges.

Identification, Selection, and Analysis of User Tools



#	Inclusion Criteria (IC)	Description
(IC1)	Availability	Available for public use, with documentation and use case tutorial
(IC2)	Regularly updated	At least one update within six months and releases for both the Google Play and Apple App Stores
(IC3)	Usage	For mobile apps, over 1,000 downloads
(IC4)	Versioning	If version differs from one store to another, the newest one is considered
(IC5)	Identity lifecycle	Covers all the identity lifecycle
(IC6)	Personal data	Capable of handling personal data, including verifiable credentials storage and maintenance

Figure: Identification and selection of wallets using inclusion criteria (IC1–IC6).

Digital Identity Life Cycle

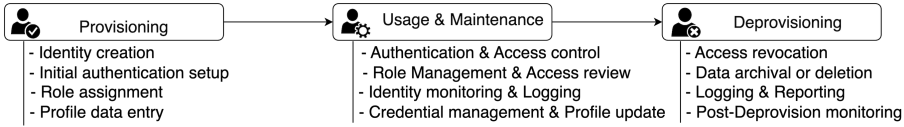


Figure: Main phases with main events of a digital identity life cycle[8].

[8] Adapted from WILSON, YVONNE; HINGNIKAR, ABHISHEK. THE LIFE OF AN IDENTITY. In: SOLVING Identity Management in Modern Applications: Demystifying OAuth 2, OpenID Connect, and SAML 2.

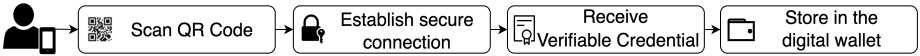


Figure: User journey to receive a Verifiable Credential using a digital wallet.

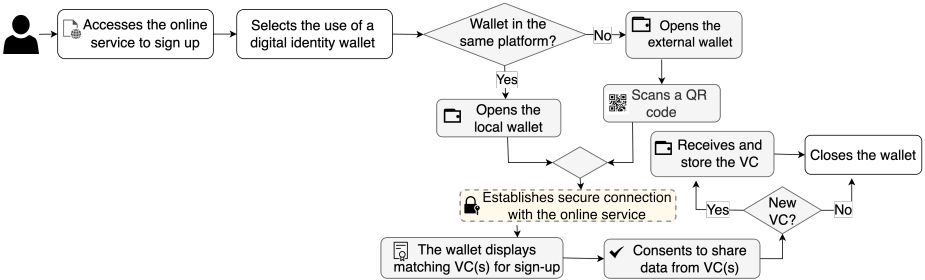


Figure: Overview of using a digital wallet to sign up with Verifiable Credentials.

- Delete individual credentials
- Some allow deleting all wallet data
- One allows the request of data deletion from verifiers

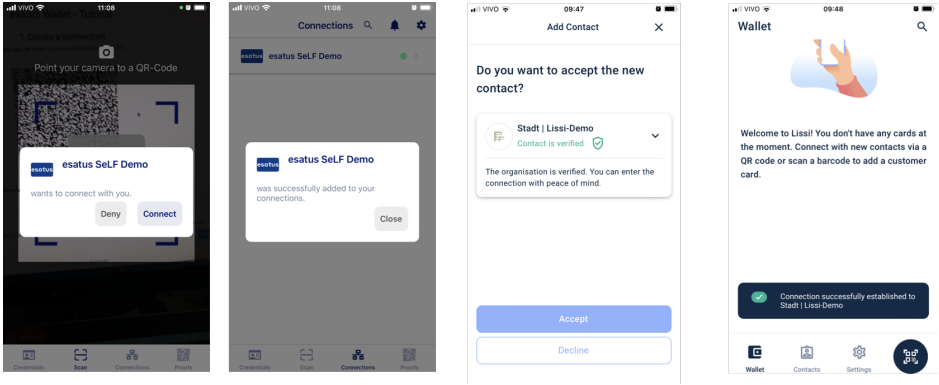
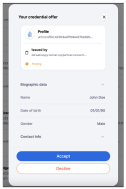


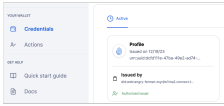
Figure: Examples of new contact connection.

Analysis considering user interaction with the wallets

Examples



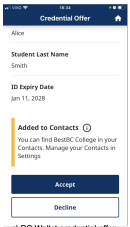
a) Trinsic ID credential offer



b) Trinsic ID credential accepted and stored

c) wwWallet select credential to receive

d) wwWallet credential received and stored



e) BC Wallet credential offer

f) BC Wallet credential accepted and stored

g) Data Wallet credential offer

h) Data Wallet credential offer details

i) Data Wallet credential accepted and stored

Figure: Examples of storing a new VC.

Table: Selected Privacy Attributes[9].

Attribute	Description
Collection	How wallets **inform users** about **data collection** and limit unnecessary data sharing.
Correctness	Mechanisms to ensure the **accuracy** and **up-to-date** status of **user data**.
Control	**User autonomy** over **data sharing and management** through features like consent and revocation.
Transparency	**Clear communication** of data handling, including policies and audit logs.
Security	Protection of sensitive information from **unauthorised access**.
Right to be forgotten	Allows users to **delete or revoke access to their data**, reflecting the dynamic nature of privacy needs.

[9] Adapted from BARTH, SUSANNE; IONITA, DAN; HARTEL, PIETER. UNDERSTANDING ONLINE PRIVACY—A SYSTEMATIC REVIEW OF PRIVACY VISUALIZATIONS AND PRIVACY BY DESIGN GUIDELINES. ACM Comput. Surv., Association for Computing Machinery, New York, NY, USA, v. 55, n. 3, Feb. 2022. DOI: 10.1145/3502288.

Analysis Considering Data Protection

	Collection	Correctness	Control	Right to be forgotten	Transparency	Security
BC	✧ Informs how many credentials are involved in the data collection ✦ Shows information to be shared ☆ Supports selective disclosure	N/A	✶ Consent for accepting credentials and responding to proof requests ✶ Notifies credential offers and proof requests.	✸ VC removal from the wallet	✪ Wallet privacy policy ✨ VC receiving and sharing history is available under "Contacts" menu ✶ Informs what will be lost and what will be kept when a VC is deleted ✷ When storing a VC, inform about the new contact under Contacts ✶Encourages users to review the specific details of the proof request ✹ Guide on wallet use upon opening	✳ Secure connection with issuers and verifiers ✹ Authentication with PIN or biometrics
Data Wallet	✦ Shows information to be shared	N/A	✶ Consent for accepting credentials and responding to proof requests ✳ Consent when establishing a new connection ☆ Notifies new credential offers, proof requests and connections. ✦ Cloud backup data	✸ VC removal from the wallet	✪ Wallet privacy policy ✨ VC receiving and sharing history under "My Shared Data" ✪ Explicitly shows the establishment of a connection ✦ Shows verifier privacy policy	✳ Secure connection with issuers and verifiers ☆ Authentication with biometrics
Esatus	✦ Shows information to be shared	N/A	✶ Consent for accepting credentials and responding to proof requests ✳ Consent when establishing a new connection ☆ Backup as a local encrypted file ✮ Notifies new credential offers, proof requests and connections ✯ Deletion requests for shared data and notifies upon success ✪ Allows auto-acceptance of credentials/request proofs	✸ VC removal from the wallet ✯ Deletion requests for shared data	✨ VC receiving and sharing history is available under "Connections" menu ✪ Explicitly shows the establishment of a connection	✳ Secure connection with issuers and verifiers ✹ Authentication with PIN or biometrics ✷ Backup as an encrypted file using a seed of 12 words

Figure: Privacy attributes analysis of selected wallets. Showing the first three wallets.

Observations	Suggested Improvements	ID
All wallets require consent for storing VCs, but only some ask for consent before secure connections.	Explicit user consent before establishing any secure connection.	Ctrl-01
Some wallets lack export options; others support JSON or encrypted backup.	Provide data export and backup functionality to enhance control.	Ctrl-02
Users cannot easily revoke consent once granted.	Add features to request consent revocation.	Ctrl-03
Wallets do not clearly display the requested data or its purpose.	Display the requested data and the verifier's purpose for informed consent.	Ctrl-04
Auto-acceptance may reduce control if settings are too coarse.	Provide granular settings for auto-acceptance with periodic confirmations.	Ctrl-05

Table: Control attribute: observations and suggested improvements.

Analysis Considering Data Protection

- From the detailed analysis of **8 selected wallets** considering the privacy attributes:
  - No comprehensive set of features to support users in managing their digital identities in a personal data-protective manner;
  - 21 suggested features;
    - 14 existing features
    - 7 non-existing features

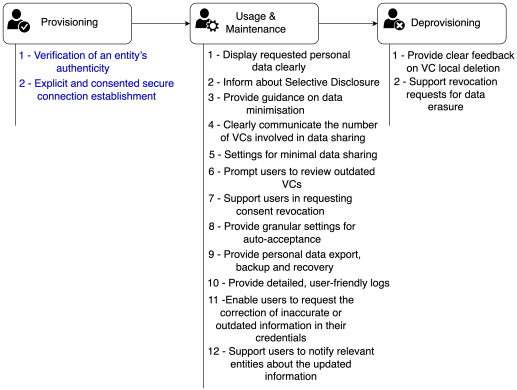


Figure: User stories based on suggested improvements.

- 16 user stories to inform TETs design and development.

TETs - tools designed to give users insight into the collection, storage, processing, and disclosure of their personal data[a].

[a] JANIC, MILENA; WIJBENGA, JAN PIETER; VEUGEN, THIJS. TRANSPARENCY ENHANCING TOOLS (TETS): AN OVERVIEW. In: 2013 Third Workshop on Socio-Technical Aspects in Security and Trust. 2013. P. 18–25. DOI: 10.1109/STAST.2013.11.

- **(US2) - Explicit and consented secure connection establishment**: *As a user, I want to be explicitly informed when a secure connection is to be established with an entity so that I can be aware of the trust relationship and provide my consent before proceeding.* **Improvements**: *Ctrl-01*; *Transp-03*.

- **(US10) - Provide granular settings for auto-acceptance**: *As a user, I want to have granular control over auto-acceptance settings for new VCs or proof requests from my connections so that I can configure which types of requests I want to accept automatically and which I want to review manually.* **Improvements**: *Ctrl-05*.

Threats to Validity

- **Rapid Review limitations:** – Single database (Scopus); – Few reviewers: possible study omissions
- **Temporal validity:** – Search updated (May 2025): 105 results, 38 new; – 4 new relevant studies: confirm but do not expand challenges
- **Tool analysis:** – Findings may not generalise to all implementations or future versions
- **Proposed features:** – User stories + TETs based on conceptual analysis; – Empirical validation still needed (prototypes in development)

Conclusion

- Rapid Review of decentralised Identity Management (IdM) challenges
- Analysis of 8 digital wallets: **21 suggested improvements**
  - 14 enhancements to existing features
  - 7 novel features
- Improvements grouped into **16 user stories** across the identity lifecycle
- User stories will inform design of **Transparency-Enhancing Tools (TETs)** for privacy-aware wallets
- Decentralised IdM aligns with GDPR/eIDAS 2.0 principles but wallets remain in early stages
- Future work: develop and empirically validate prototypes

Final remarks/Acknowledgements

Supplementary material available at:
https://github.com/shirlei/didm-sop-dpa

Special thanks to:

INSTITUTO FEDERAL
Santa Catarina

UFSC

ifip TC 13

Email: shirlei@gmail.com
Website: https://shirlei.me

Thank you!