An Empirical Study of a Decentralized Identity Wallet: Usability, Security, and Perspectives on User Control

Maina Korir\textsuperscript{1}, Simon Parkin\textsuperscript{2}, Paul Dunphy\textsuperscript{3}
\textsuperscript{1}University of Bedfordshire
\textsuperscript{2}TU Delft
\textsuperscript{3}OneSpan Innovation Centre
Identity Online

- Challenges
  - Identity fraud
  - Lack control over collection and use of personal information

- User centric identity
  - European Digital Identity
  - Microsoft

- Identity wallets
  - Evernym, LISSI, uPort
Problem and Research Question

• Identity wallets combine multiple security and privacy processes
  • Complex to understand and use

• Perception that control over disclosure of personal data will drive user acceptance
  • Untested

• Few trials or experiments focused on the user experience

RQ – What are the user-centered privacy and security challenges facing decentralized identity wallets?
Study Protocol

• Carry out three tasks
  • Make a connection
  • Obtain a credential from the identity provider
  • Build an identity proof

• Semi-structured interview with mental model scale

• System Usability Scale
Participants

• Mix of professionals, students, and retired individuals

• 15 male, 15 female

• 17 based in the US; 13 in the UK

• Had an Android phone, version 10 and above
Results

• User journey issues
  • QR codes – e.g., focusing phone camera
  • Misunderstanding regarding security and privacy
  • Uncertainty around device switching
  • Authentication challenges

• SUS
  • ‘Acceptable’ - 71
Qualitative Results - Overview

Security, Privacy and Trust in Decentralized Identity

- Current Challenges with Identity
  - Oversharing of data
  - Time identity processes take
  - Perceptions of forgery
  - Onboarding improvements
  - Life changing problems

- Assurances about the Identity Wallet Service
  - Who controls what? (Roles)
  - Foundations of trust
  - Privacy and security evaluations
  - Sharing violations
  - Bad actors

- Expectations of the Identifier
  - Assurances about security
  - Confidential identifier
  - Why generate own identifier?
  - Confusing procedure

- Examining Stakeholders and Their Roles
  - Weighing up the interaction
  - App’s value
  - Confidence in fallbacks
  - Interpretations of minimization
Resigned to oversharing data
“You know I work in information technology already and part of me says the idea that you keep your information secure and people not knowing it is a ship that has probably already sailed.” [P22]

Comfort while oversharing data
“Because it doesn't happen as often, I’m comfortable sharing that information.” [P16]

Current Challenges with Identity

Convenience and ease of use
“It’s no longer, oh, yeah, like I need a copy of your driver’s licence, proof of address and utility bill. Here’s your account details and that’s it. Oh my god that used to take like a week.” [P14]

Life changing problems
“And so, when I bought my first House you know 10-12 years ago. They were not able to give me my the keys after the closing had to wait a few days, I think, was three or four days, because my name comes up in some kind of watch list or something.” [P10]
User does not perceive that they are in control
“I think Alpaca Bank are deciding what this Bank of Carpathia can know about me, so I would say they are in control because they’re the ones that are divulging information to the second party involved. So, I would think that they could potentially withdraw your social security number if that’s what they chose to do.” [P23]

Fear of bad actors
“Oh man, I can see just a whole new breed of hackers. Oh God, as we speak they’re breeding.” [P11]

Assurances about the Identity Wallet Service

Foundations of trust
“I don’t know if I trust my device as being as secure as like potentially you know, the bank’s devices or network or their security is probably more enhanced than just my phone.” [P10]

Separation of concerns
“I don't think that the Bank needs to have any idea that I'm doing something with a different bank. That that's my private business, so I like that it kind of mentions that and I think that's important.” [P3]
Expectations of the Identifier

Identifier encodes identity
“When I looked at the identifier I have here, it always shows a unique set of characters and didn’t show my address, my birth date or any of that other information that’s usually shown on a physical ID.” [P6]

Confidentiality
“You don’t give out your password, so why would you go on sharing your unique code for your identifier.” [P16]

Confusing procedure
“So I will say that I am used to things like these really long string of numbers and letters. But I think that would probably throw off the average user.” [P5]

Confusion about generating an identifier
“Wait … is it a … I’m not even sure if it’s an identifier that I actually have to remember, or if it’s something that the app will automatically show me.” [P18]
Examining Stakeholders and their Roles

Confidence in fallbacks
“So, because, like, I mean at the end of the day, all these I’m assuming that all these data points are feeding into IdentiCorp’s like their, whatever, their database for something like that. So I think it’s the first, I think they are respon… like they are going to be the one that I should reach out to instead of other organizations.” [P13]

Unfamiliar process
“I think it’s still a bit. It’s definitely different than a lot of other apps that are used, so there is a learning curve, especially for someone that, I think I'm pretty technologically competent and I think I would still have a bit of a difficulty with this here and there.” [P24]

Varying interpretations of minimization
“If think if Carpathia wanted to know exactly how much I make a month, they would ask for it. … And I wouldn't be able to say no.” [P5]
Conclusions

• Perception of security
  • Trust in key actors in the study scenario instead of technical mechanisms

• User understanding of entities in control is a challenge
  • Complex technologies, hidden from users

• Complete user autonomy (and thus, responsibility) is unanticipated

• ID wallets need good usability
  • E.g., use terms that are easier to understand
Thank you!

Questions?

maina.korir@beds.ac.uk