Design and Evaluation of Privacy-Preserving Protocols for Agent-Facilitated Mobile Money Services in Kenya

Karen Sowon[1], Collins W. Munyendo[2], **Lily Klucinec**[3], Eunice Maingi[4], Gerald Suleh[4], Lorrie Faith Cranor[3], Giulia Fanti[3], Conrad Tucker[5], Assane Gueye[5]

[1]Indiana University, [2]The George Washington University, [3]Carnegie Mellon University, [4]Strathmore University, [5]Carnegie Mellon University-Africa

CyLab Carnegie Mellon University Security and Privacy Institute

What is Mobile Money (MoMo)?

- Financial system tied to SIM cards/phone numbers



What is Mobile Money (MoMo)?

- Financial system tied to SIM cards/phone numbers
- Involves network of third parties called “agents”



What is Mobile Money (MoMo)?

- Financial system tied to SIM cards/phone numbers
- Involves network of third parties called “agents”
- Over 77 million MoMo accounts in Kenya[1]



1. Statista. Kenya: registered mobile money accounts 2021-2023. https://www.statista.com/statistics/1188510/registered-mobile-money-accounts-in-kenya/, 2025.

What is Mobile Money (MoMo)?

- Financial system tied to SIM cards/phone numbers
- Involves network of third parties called “agents”
- Over 77 million MoMo accounts in Kenya[1]
  - Exceeds 2023 population of ~51 million people[1]



1. Statista. Kenya: registered mobile money accounts 2021-2023. https://www.statista.com/statistics/1188510/registered-mobile-money-accounts-in-kenya/, 2025.

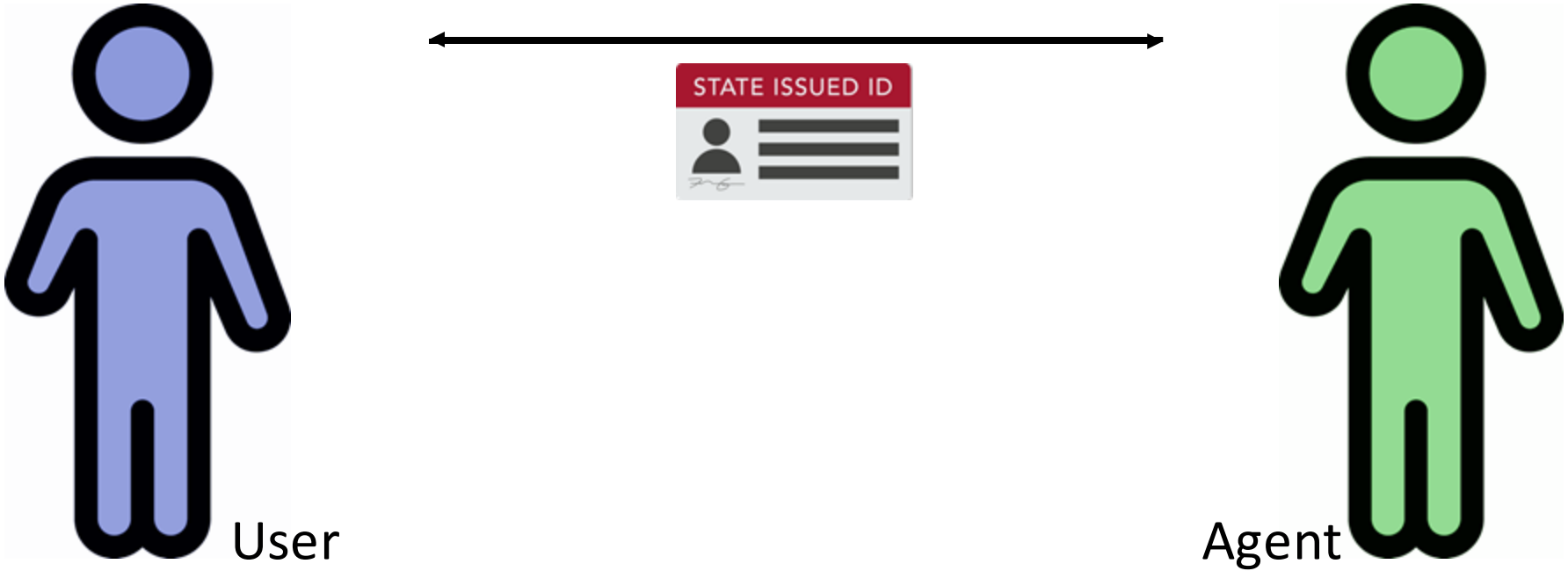
What is Mobile Money (MoMo)?

- Financial system tied to SIM cards/phone numbers
- Involves network of third parties called “agents”
- Over 77 million MoMo accounts in Kenya[1]
  - Exceeds 2023 population of ~51 million people[1]
- Variety of transaction types offered



1. Statista. Kenya: registered mobile money accounts 2021-2023. https://www.statista.com/statistics/1188510/registered-mobile-money-accounts-in-kenya/, 2025.

Example MoMo Withdrawal Transaction



Example MoMo Withdrawal Transaction



User

Withdraw Ksh500 from agent.



Agent

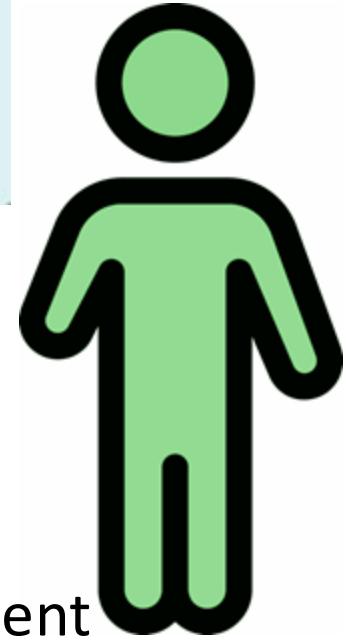
Example MoMo Withdrawal Transaction



User

Withdraw Ksh500 from agent.

Give KSH500.00 to Jasta Senda 0710456789.



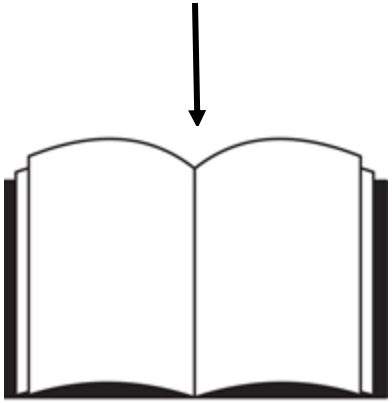
Agent

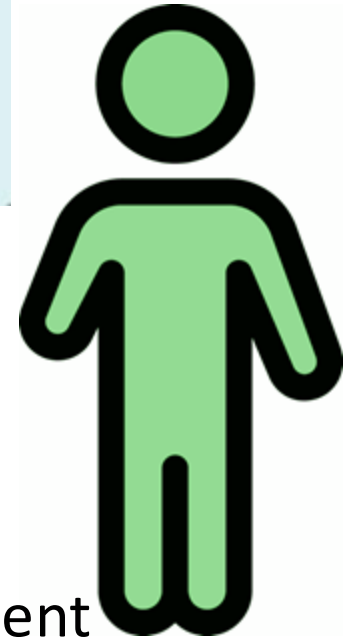
Example MoMo Withdrawal Transaction



User

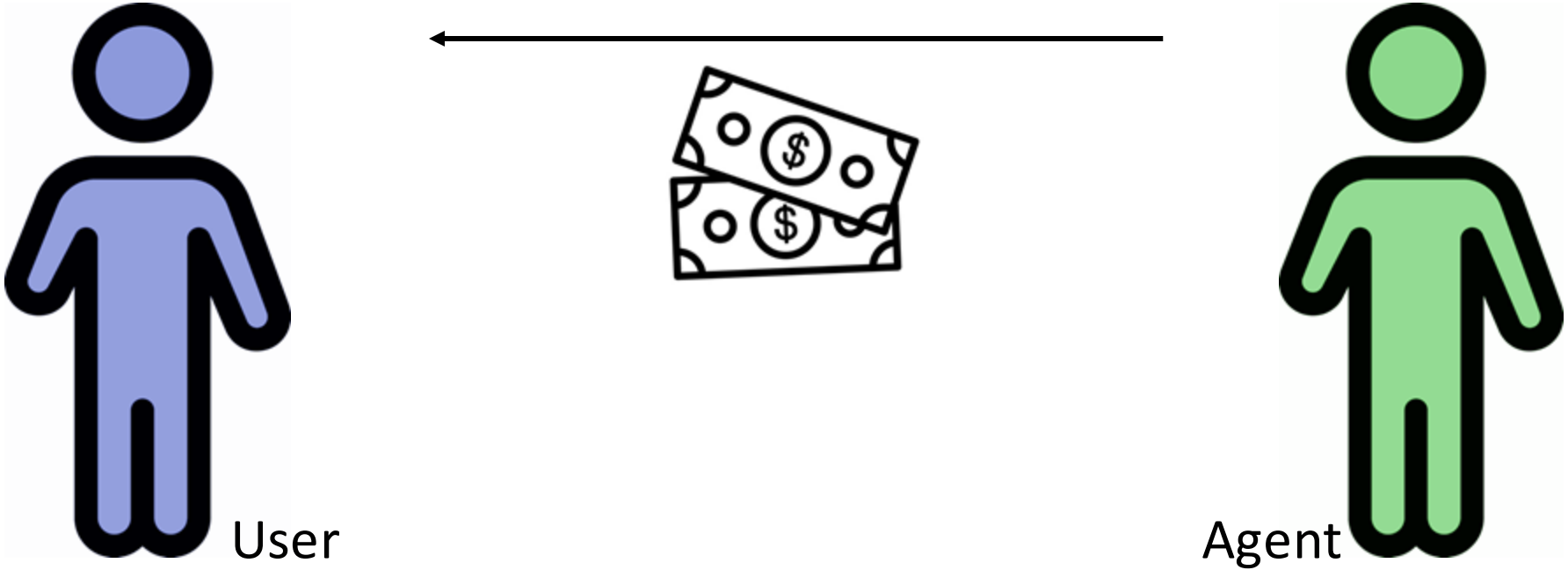
Give KSH500.00 to Jasta Senda 0710456789.





Agent

Example MoMo Withdrawal Transaction



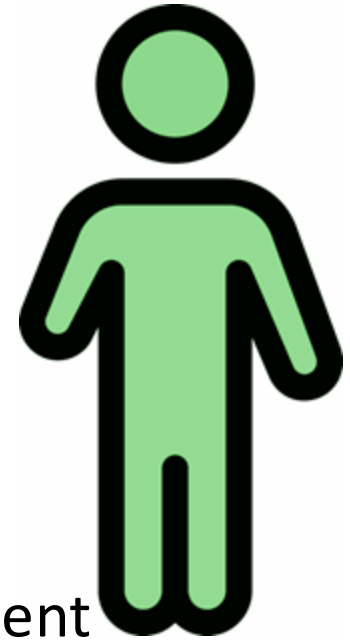
Privacy Concerns in the Current Process



User



"If someone has my ID number, they can track my [retirement fund, healthcare fund, and] my ID number links me to my bank and my family details." -U18



Agent

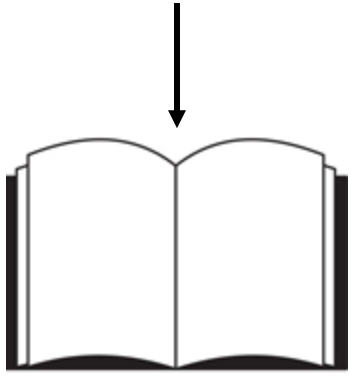
Privacy Concerns in the Current Process

Give KSH500.00 to Jasta Senda 0710456789.



User

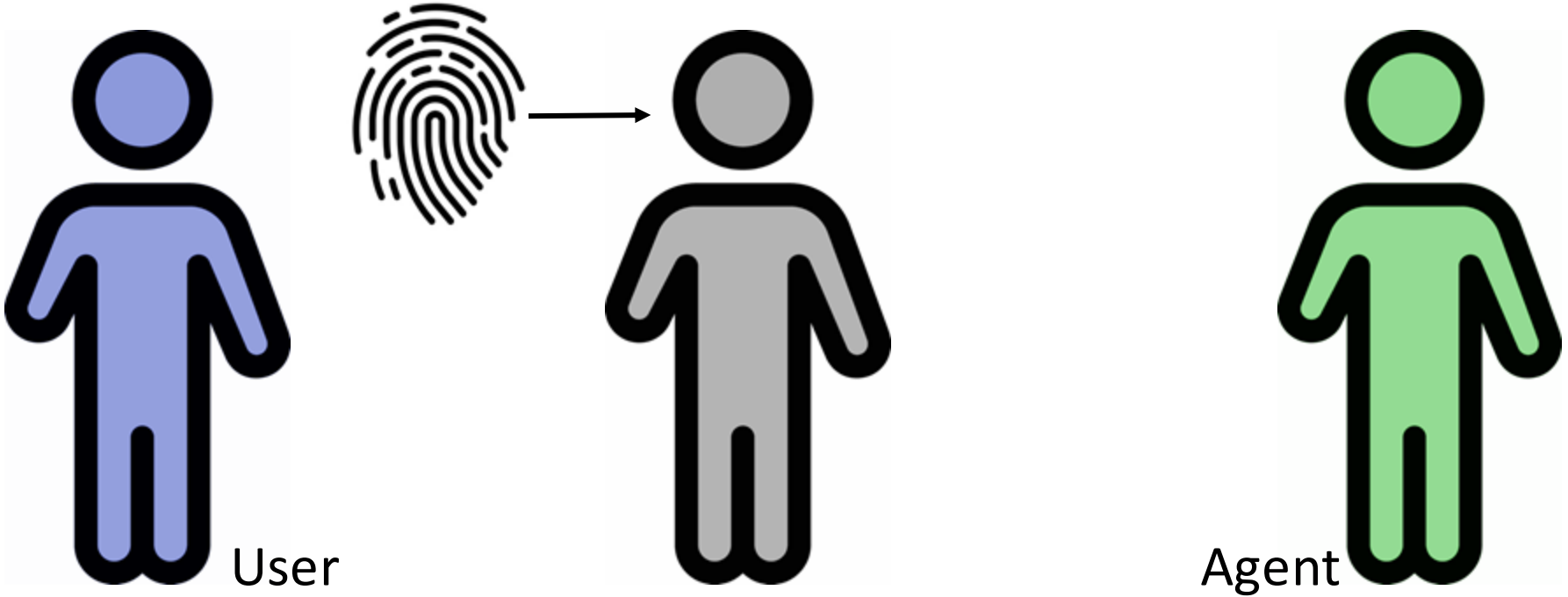
"[The agent] might try calling me and stalking me, and so I wouldn't want them to have a name and phone number to avoid that." -U19





Agent

Proposed Privacy-Preserving Withdrawal



Proposed Privacy-Preserving Withdrawal



User

Withdraw Ksh500
from agent.
Code: **23PPW**



Agent

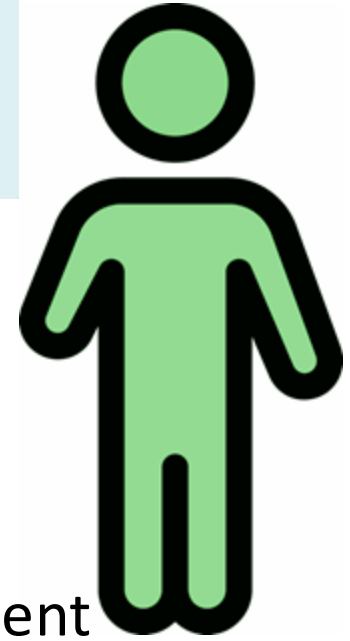
Proposed Privacy-Preserving Withdrawal



User

Withdraw Ksh500
from agent.
Code: **23PPW**

Give KSH500.00
to person with code:
23PPW



Agent

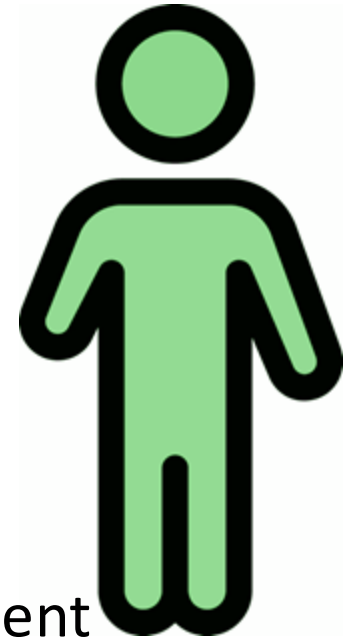
Proposed Privacy-Preserving Withdrawal



User

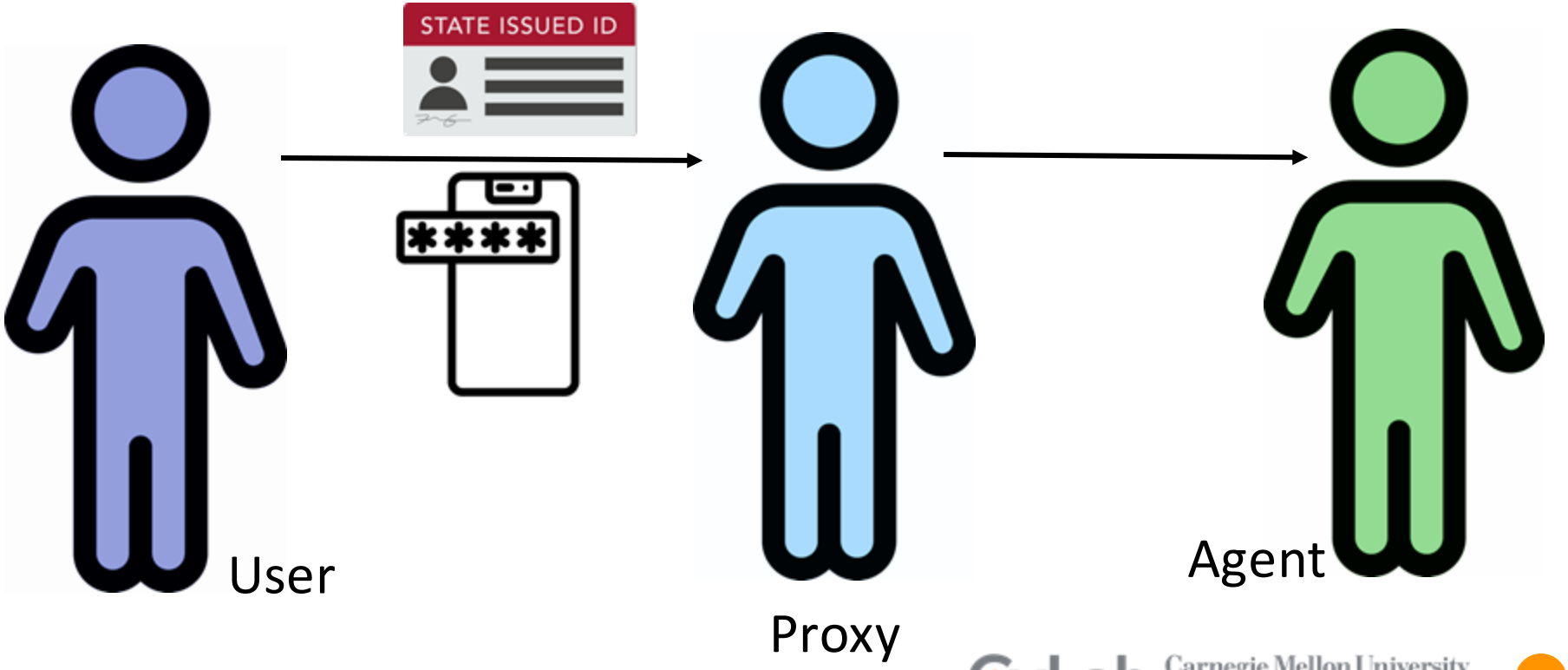






Agent

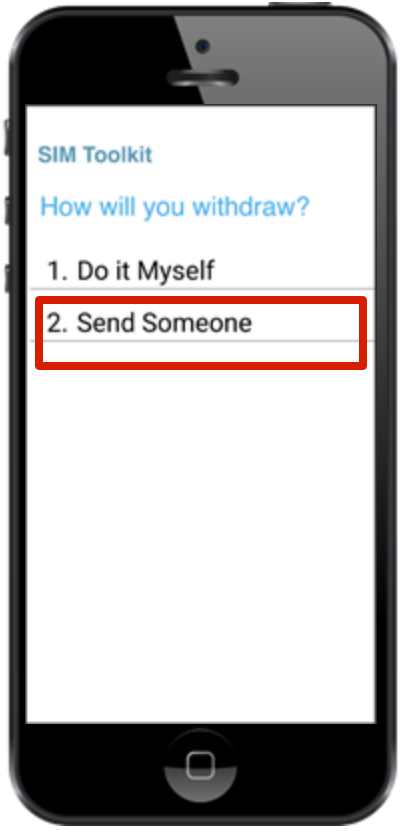
Formalizing Delegated Transactions



Formalizing Delegated Transactions



User



Formalizing Delegated Transactions

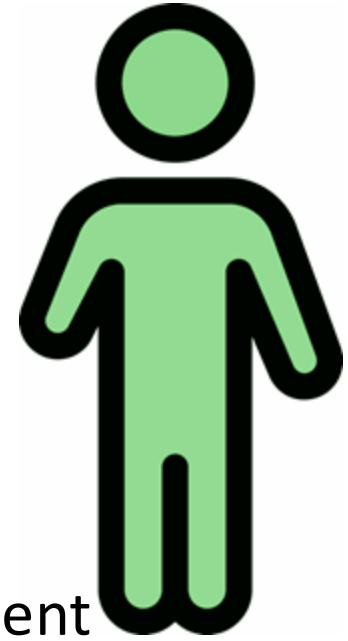


User



Proxy

Collect Ksh500 from agent for Mimi Koleta. Code: **23PPW**



Agent

Formalizing Delegated Transactions



User



Proxy

Give KSH500.00
to person with code:
23PPW

Collect Ksh500
from agent for
Mimi Koleta.
Code: **23PPW**



Agent

Research Questions

1. What are users' **privacy perceptions** and what factors influence their **data sharing attitudes** in the **context of agent-facing mobile money transactions**?
2. What **security, privacy, and usability factors** influence user and agent **preferences and concerns** for our **alternative, privacy-preserving protocols**?
3. What other design considerations arise with the use of privacy-preserving protocols?

Research Questions

1. What are users' **privacy perceptions** and what factors influence their **data sharing attitudes** in the **context of agent-facing mobile money transactions**?
2. What **security, privacy, and usability factors** influence user and agent **preferences and concerns** for our **alternative, privacy-preserving protocols**?
3. What other design considerations arise with the use of privacy-preserving protocols?

Interview Methods and Recruitment

- In-person interviews with paper prototypes
  - n=32 users, n=15 agents
  - Wizard-of-Oz style for users
  - Process walkthroughs for agents
- Conducted by 2nd author in English and Kiswahili



Recruitment

- Recruited from 5 neighborhoods in Nairobi
  - Posted flyers in agent shops
  - Also used snowball sampling



RQ1: User privacy perceptions and data sharing attitudes

What data-sharing risks concern users?

- 4 main categories:
  - Fraud/theft
  - Unauthorized data use
  - Physical harm
  - Economic judgements
- **Almost all users viewed agents as the threat actor**

What data-sharing risks concern users?

- 4 main categories:
  - Fraud/theft
  - Unauthorized data use
  - Physical harm
  - Economic judgements
- **Almost all users viewed agents as the threat actor**

"I came to learn that my ID number had registered another SIM card and I didn't know" -U18

Why do users share information?

- 4 main reasons:
  - Utility of shared data
  - Perceptions about data sensitivity
  - Trust (in providers)
  - Obligatory compliance

Why do users share information?

- 4 main reasons:
  - Utility of shared data
  - Perceptions about data sensitivity
  - Trust (in providers)
  - Obligatory compliance

"They are the service providers offering the service. I trust them to keep my information secret" -U22

Why do users share information?

- 4 main reasons:
  - Utility of shared data
  - Perceptions about data sensitivity
  - Trust (in providers)
  - Obligatory compliance

"There are details they might need and even if they are personal…I am going to give [them]" -U26

RQ2: Security, privacy, and usability factors

What did users and agents **like** about the new processes?

- Less PII shared with agents
- Code and biometrics offer better security
- More convenient to authenticate without ID
- Formalized proxy process

What did users and agents **like** about the new processes?

- Less PII shared with agents
- Code and biometrics offer better security
- More convenient to authenticate without ID
- Formalized proxy process

"...there is also no way [the agent] can use my details [unlike] the [existing] one [where they] can get my phone number and start calling and harassing me" -U9

What did users and agents **like** about the new processes?

- Less PII shared with agents
- Code and biometrics offer better security
- More convenient to authenticate without ID
- Formalized proxy process

"…someone will not be able to remove your money because they will not have your fingerprints"-U12

What did users and agents **like** about the new processes?

- Less PII shared with agents
- Code and biometrics offer better security
- More convenient to authenticate without ID
- Formalized proxy process

"…I remain with my phone and my details and he uses his phone and his details."-U9

What did users and agents **dislike** about the new processes?

- Voice authentication might be less private
- Accessibility concerns
- Agents' lack of trust in self-authentication

What did users and agents **dislike** about the new processes?

- Voice authentication might be less private
- Accessibility concerns
- Agents' lack of trust in self-authentication

"Maybe [the person] is a construction worker and their fingerprints are not quite clear…and it fails."
- A5

What did users and agents **dislike** about the new processes?

- Voice authentication might be less private
- Accessibility concerns
- Agents' lack of trust in self-authentication

"...for my security purposes, how do you really trust the customer…to do self-service?"
- A13

What did users and agents **dislike** about the new processes?

- Voice authentication might be less private
- Accessibility concerns
- Agents' lack of trust in self-authentication
- **These are mostly process misconceptions**

Conclusions and Recommendations

- Generally, users and agents prefer our processes
  - Some shared accessibility and security concerns
- Future work should:
  - Implement and pilot new protocols
  - Investigate fraud targeted at MoMo agents and privacy violations of MoMo users



Scan for full paper!

Presenter Email: laklucin@andrew.cmu.edu