CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Exploring the Complexities of Passkey Revocation

ACM CCS 2026 | The Hague, NL

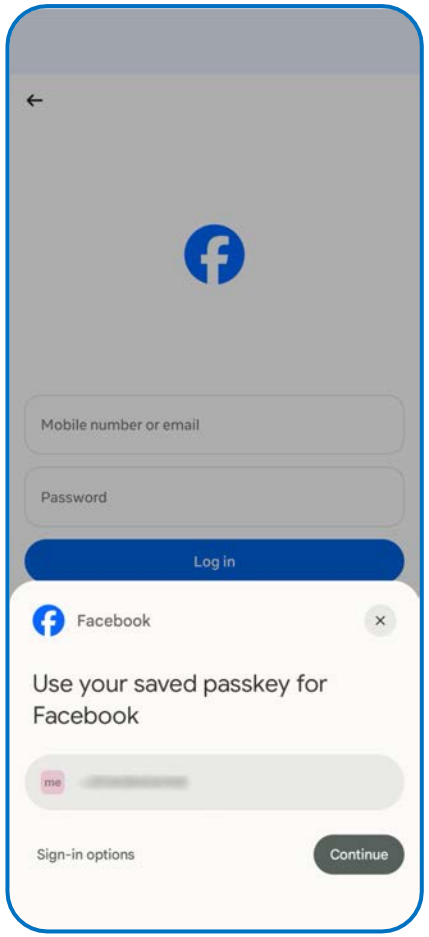
Anna Giacomello, Leona Lassak★, Jonas Hielscher, and Maximilian Golla

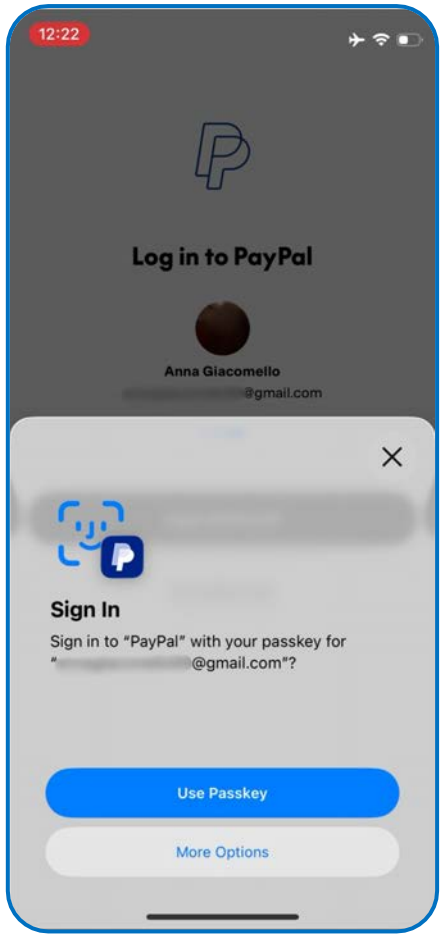
CISPA Helmholtz Center for Information Security, ★Max Planck Institute for Security and Privacy

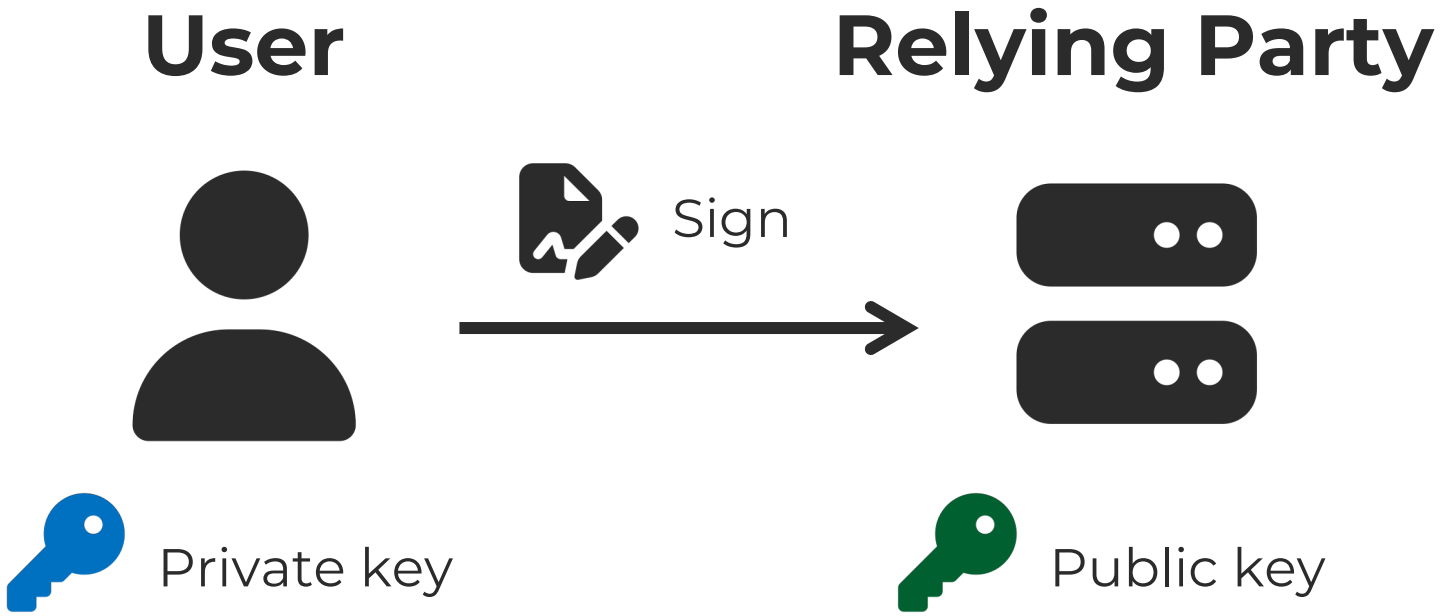


Your phone just got stolen! What now?

What are Passkeys?





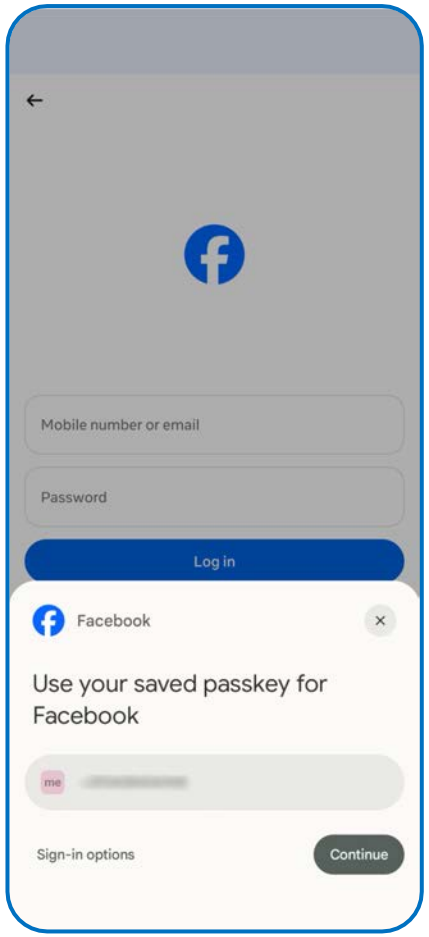


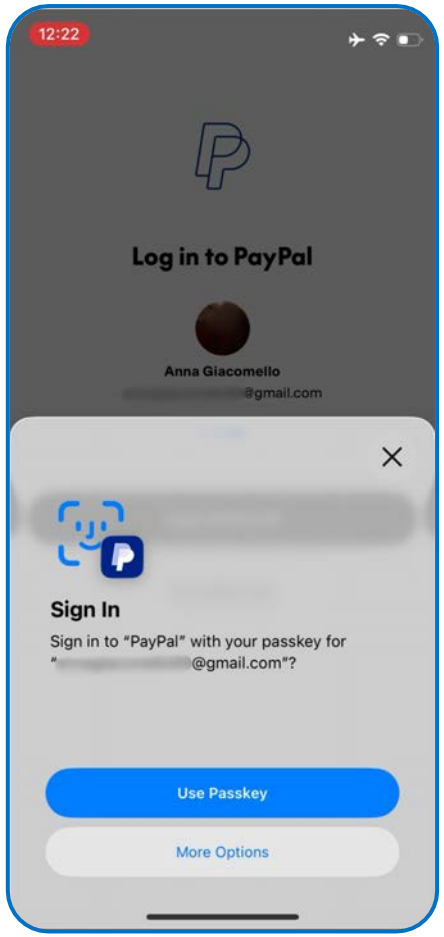


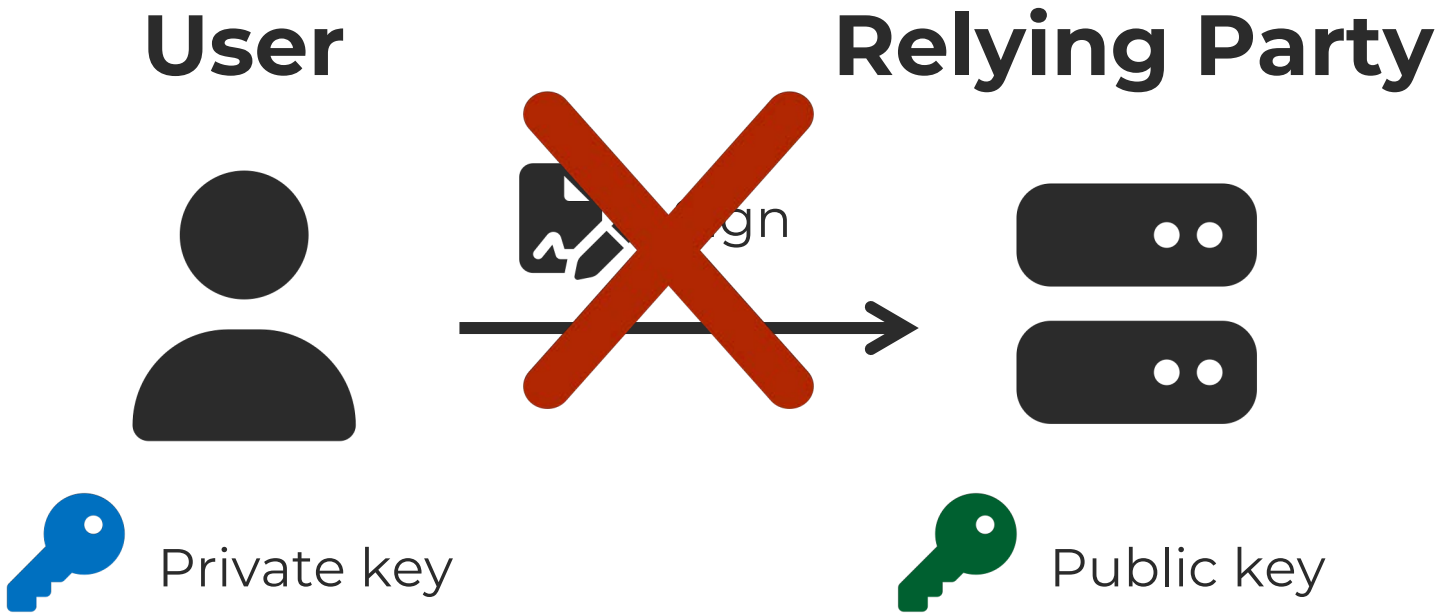
“re...what?

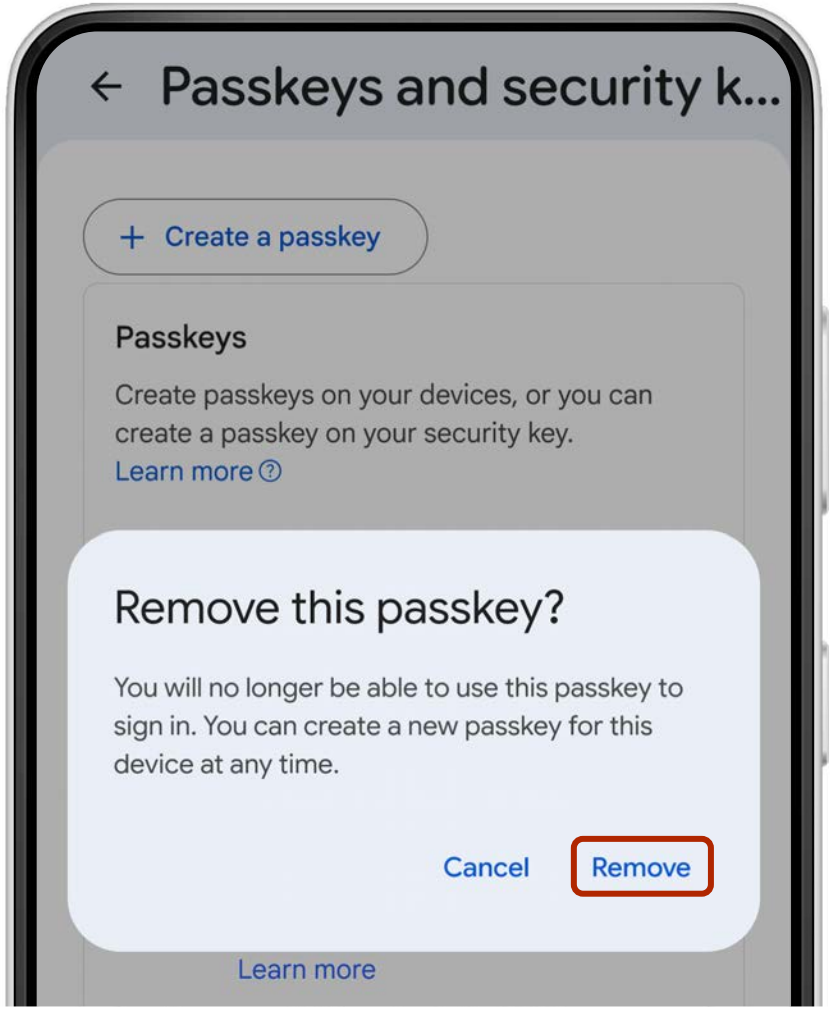
Can you please repeat the word for me?”

What is Passkey Revocation?









Passkey revocation:

manual

time consuming

burdensome



“You have to remember which websites to go to, and figure out where the options are. So yeah, it’s super, super painful.”



Research Questions

Research Questions



RQ 1: Revocation Need

When do users want to revoke?



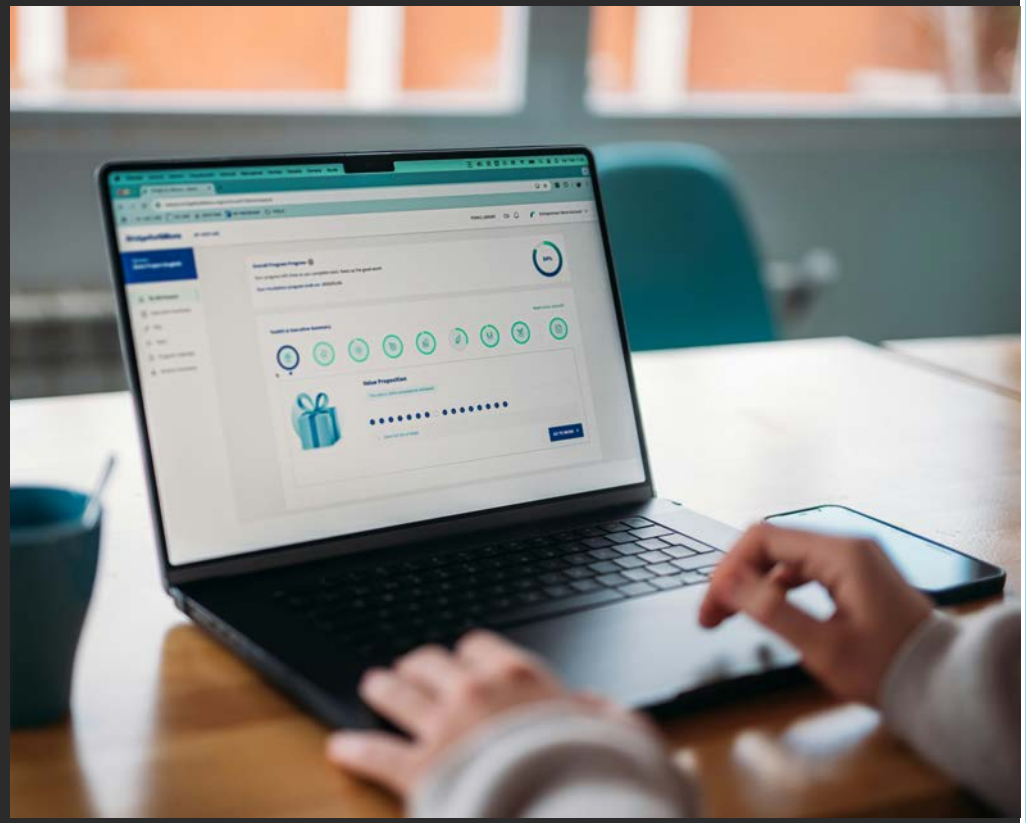
RQ 2: Literature

Which user-facing passkey revocation models exist in the literature?



RQ 3: Users' Perception

How do users feel about the proposed revocation mechanisms?

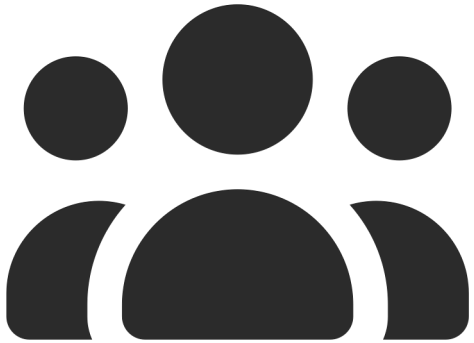


Online Survey

RQ 1: Revocation Need

Survey Method

308 US Participants



10 Scenarios

Stolen Device

Shared Account

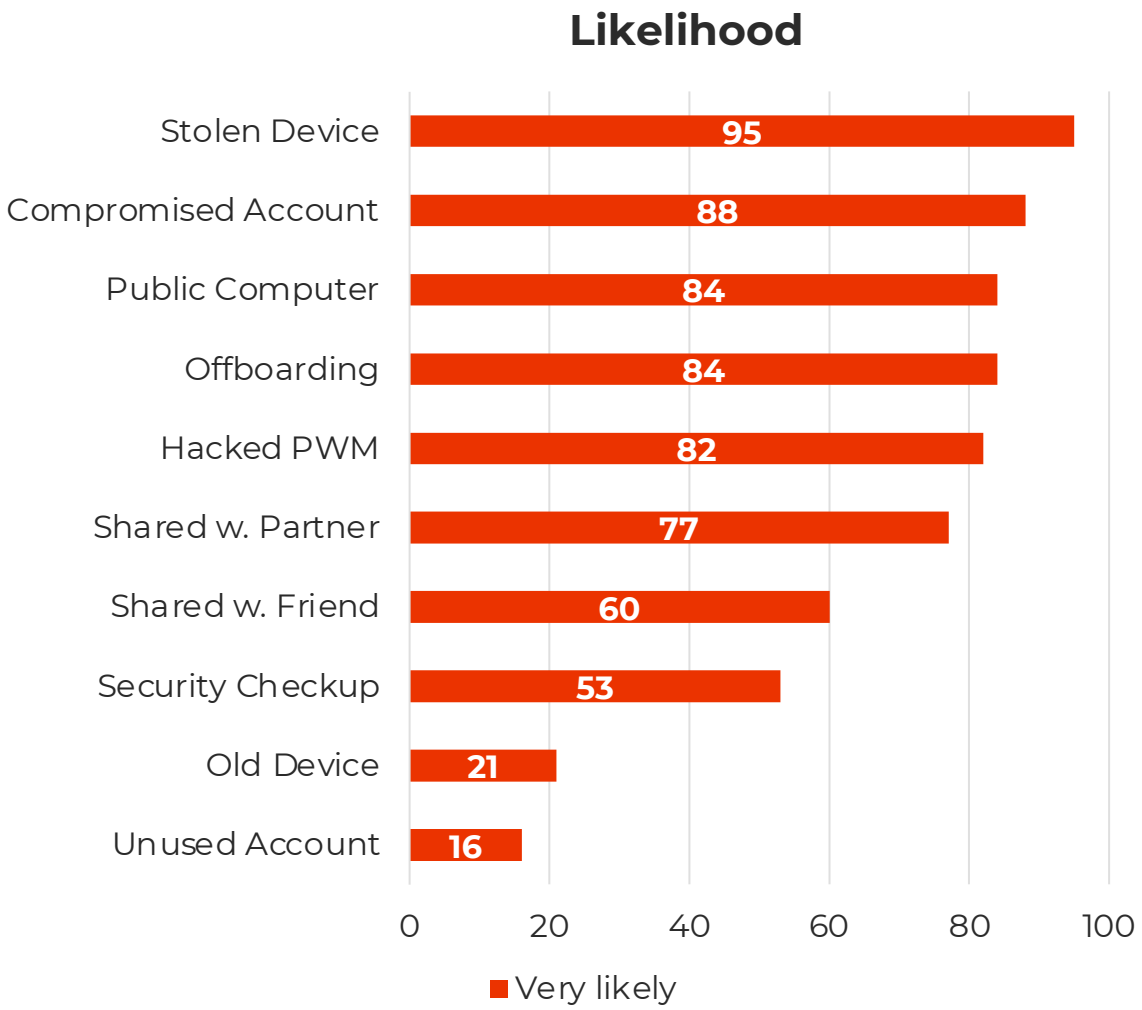
Users Rate

Likelihood

Severity

Effort

Revocation Intent Follows Perceived Severity



High-Risk Scenarios

Actor: thief or hacker

Consequences: money loss, data theft



“If I don’t revoke access in that situation, that could lead to identity theft, financial loss, or even someone locking me out of my own accounts.”



Systematization of Revocation Approaches

RQ 2: Literature

Literature Method

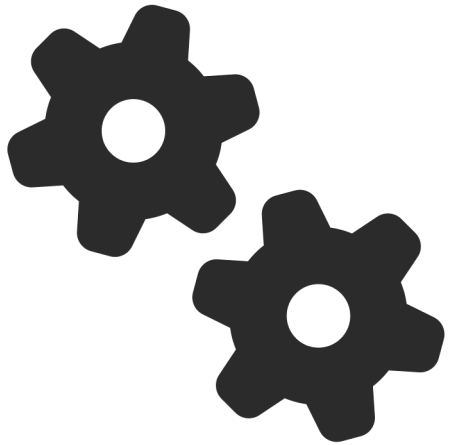
Literature Search



User-Facing Models

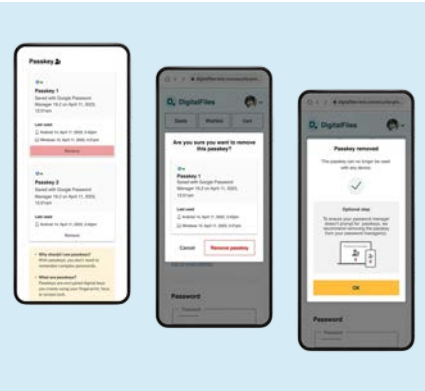


5 Revocation Mechanisms



Revocation Mechanisms

Baseline



Remove individually

Revocation Code



Publish code

Backup Device



Authorize replacement device

Central Service

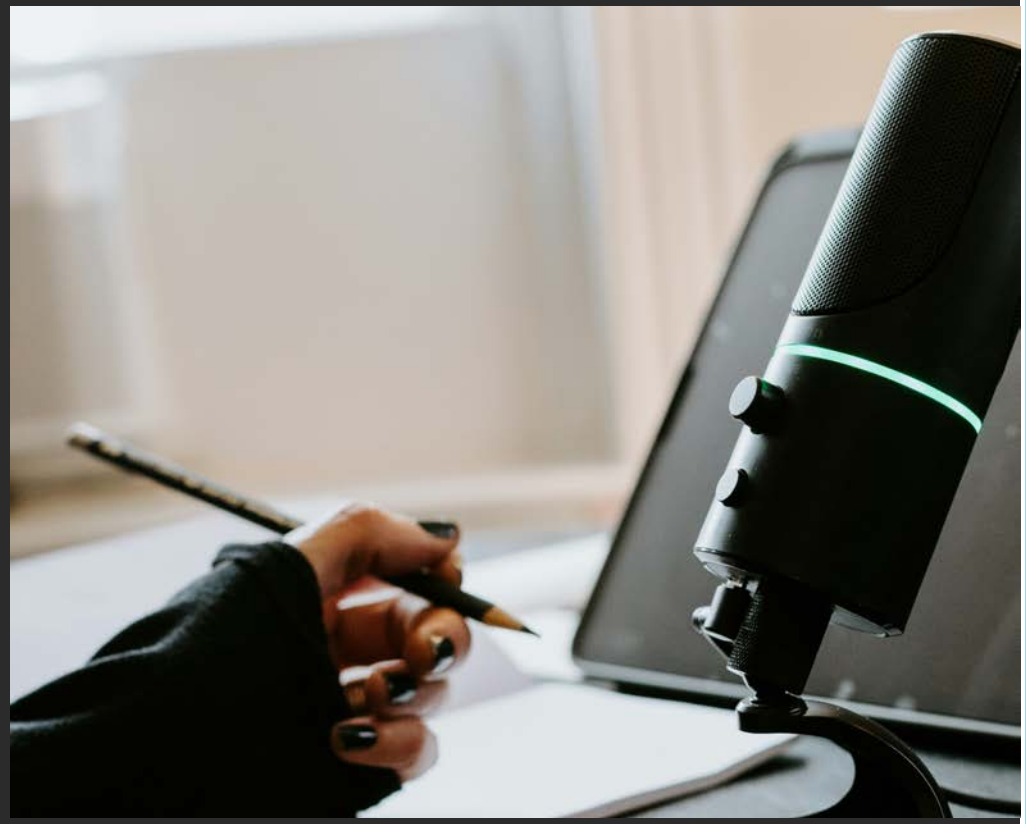


Remove authenticator

Electronic ID



Revoke eID

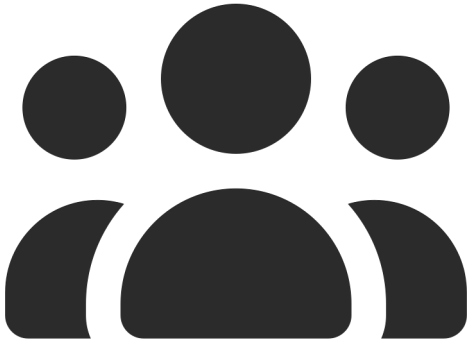


Semi-Structured Interviews

RQ 3: Users' Perception

Interview Method

20 Passkey Users



Discuss 5 Revocation Mechanisms



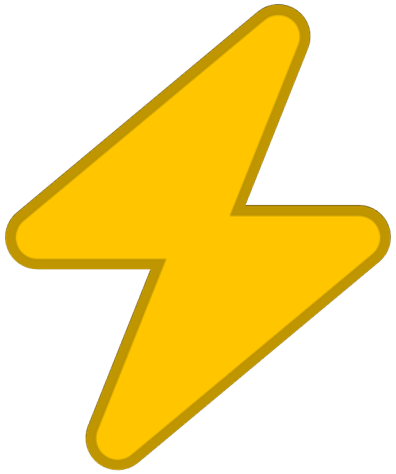
Thematic Analysis



Users' Reasoning



Scalability



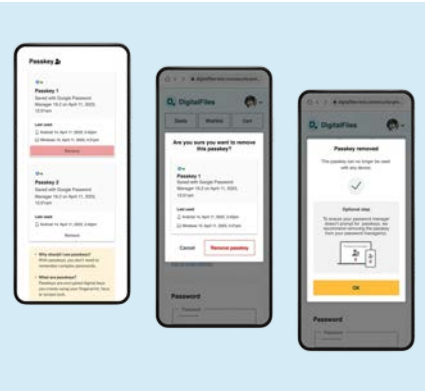
Convenience



Privacy, Security, and Trust

Overall – No Silver Bullet

Baseline



- Per-account deletion
- Cumbersome
- No concerns

Revocation Code



- Revoke all at once
- Managing code
- No concerns

Backup Device



- Login to each account
- Managing device
- No concerns

Central Service



- Revoke all at once
- Nothing to manage
- Security and trust

Electronic ID



- Revoke all at once
- Revoking and re-issuing eID
- Distrust for authority



“If you’ve got two or three saved passkeys, fine. If you’ve got twenty, not going to happen.”



Discussion

Recommendations

Avoid reliance on central services



Integration into credential managers

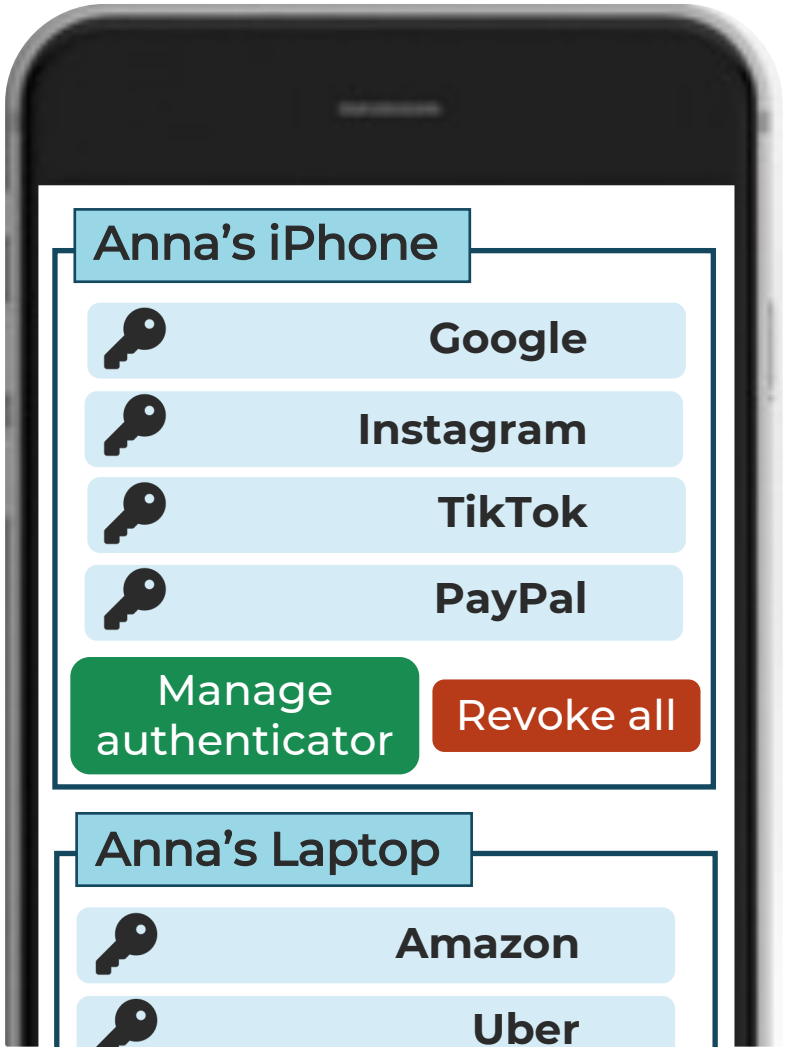


Safeguards against weaponization[1]



[1] Daffalla et al., A Framework for Abusability Analysis: **The Case of Passkeys in Interpersonal Threat Models**, USENIX 2025.

A Standardized, Cohesive Solution



Passkey Management API

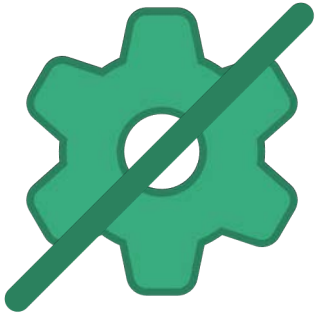
Exploring the Complexities of Passkey Revocation

Revocation is now user-facing



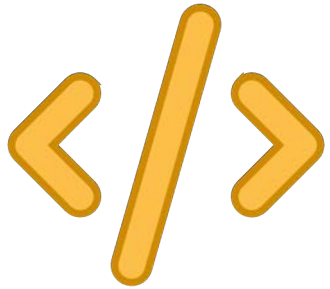
Passkeys bring revocation to the everyday user

Strong intent, weak options



People want to revoke, but current mechanisms are burdensome

APIs could bridge the gap



Credential managers could implement the full lifecycle



Anna Giacomello
anna.giacomello@cispa.de



Leona Lassak
leona.lassak@mpi-sp.org



Jonas Hielscher
hielscher@cispa.de



Maximilian Golla
golla@cispa.de









Read More