Exploring the Complexities of Passkey Revocation (Extended Version)

Anna Giacomello
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
anna.giacomello@cispa.de

Leona Lassak
Max Planck Institute for Security and Privacy
Bochum, Germany
leona.lassak@mpi-sp.org

Jonas Hielscher
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
hielscher@cispa.de

Maximilian Golla
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
golla@cispa.de

Abstract

The passkey ecosystem lacks a way to invalidate access across authenticators and relying parties, as required in scenarios such as device theft, offboarding, or account unsharing. Although cryptographic revocation protocols have been proposed, they are not yet part of the ecosystem. Currently, users must sign in to each service and manually delete passkeys while tracking them across devices and passkey providers. In this work, we investigate passkey revocation from both technical and user perspectives. We systematize existing passkey revocation proposals and derive four revocation mechanisms that abstract cryptographic protocols into user-facing interaction models. We then conduct an online survey (*n=308*) to examine when users would consider revoking access across scenarios, complemented by semi-structured interviews (*n=20*) exploring users' awareness, concerns, and preferences regarding the four revocation mechanisms. We find that revocation intention closely follows perceived severity, with high-risk scenarios eliciting near-universal willingness to revoke, while lower-risk scenarios show more varied responses. Our qualitative results show that users perceive the available revocation flow as cumbersome and difficult to manage at scale, but also share conflicting opinions on the proposed mechanisms, none of which represents a ready-to-use solution. Our results highlight the need to design more usable revocation mechanisms, for which we provide recommendations.

CCS Concepts

• **Security and privacy → Usability in security and privacy**.

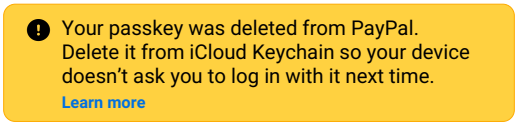
Keywords

Authentication, Revocation, Passkey, FIDO, Survey, Interview

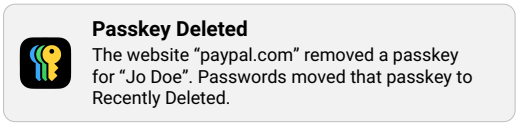
1 Introduction

Passkeys, which aim to reduce reliance on passwords [62], provide advantages such as phishing resistance and protection against credential reuse [66, 96]. Lately, they have seen increasing adoption across major platforms and services [1], with recent work identifying hundreds of passkey-enabled websites [43].

Despite their advantages, passkeys also introduce new challenges, especially around credential management and recovery [24, 62]. Among these, revocation is a critical yet understudied aspect [13]. Revocation differs from fallback authentication and account recovery, which aim to restore access [38, 61]. Instead, revocation is essential for mitigating ongoing threats, such as device theft or compromise, and is also relevant for less time-critical scenarios like device offboarding or unsharing accounts [24].



(a) PayPal reminding the user to *manually* delete the removed passkey from their passkey provider (iCloud Keychain).



(b) Signal API informing the user about the *automatic* removal of the passkey from their passkey provider (Passwords app).

Figure 1: The current state of the art in passkey removal.

While revocation is a well-established concept in computer security, it has traditionally been handled by expert users. Examples for this include public key infrastructures (PKIs) and certificate-based systems such as TLS [56], PGP and S/MIME [72, 78], software and code signing [47], secure boot [7], and API keys [27]. As a result, it has largely remained invisible to everyday users. Passkeys change this by making revocation a user-facing problem. Users may manage multiple credentials across devices and services, yet passkeys deliberately avoid global coordination. Unlinkability across relying parties is a core privacy property [31], achieved by scoping each credential to a specific relying party. While this prevents cross-site correlation [45], it also removes any central control point, requiring users to revoke access individually across services. This stands in contrast to commonly understood revocation, such as blocking a stolen credit card or reporting a lost passport, where a single authority can invalidate access.

In practice, passkey revocation is largely reduced to manual deletion. Users must (1) identify and remove multiple passkeys across relying parties, often via incomplete account security interfaces [25], and additionally (2) manage corresponding credentials across their authenticators and passkey providers to avoid stale credentials being suggested after removal (see Figure 1). This multi-step process is fragmented and burdensome, and most importantly,

CCS '26, The Hague, Netherlands

ACM ISBN 979-8-4007-2871-6/2026/11
https://doi.org/10.1145/3830454.3846647

does not scale to realistic usage scenarios or high-risk situations, such as device theft, where timely action is required [11].

Although revocation events are generally rare (e.g., below 4% for the Belgian eID [57]; 2-8% in the TLS ecosystem [51, 65]), their impact is significant at scale. In large-scale deployments with multiple credentials per service, even a revocation rate of only 1% could affect hundreds of millions of accounts.

Overall, there is currently no scalable and user-friendly mechanism for revoking passkeys, creating a mismatch between users' need to revoke access and their ability to do so effectively. In this work, we investigate this problem from both technical and user-centric perspectives by addressing the following research questions:

RQ1 *Which user-facing revocation models exist in the literature?*

RQ2 *When would users consider revoking access?*

RQ3 *How do users reason about the proposed revocation models?*

Our contributions are as follows:

(1) First, we **systematize existing passkey revocation proposals and derive four revocation mechanisms** that abstract underlying cryptographic protocols into user-facing interaction models (revocation code, backup device, centralized service, and eID). By doing so, we bridge the gap between protocol-level designs and their practical implications for users. Building on this, we conducted two empirical studies.

(2) We captured users' perceptions about credential revocation using an **online survey** ($n = 308$). Specifically, we investigated users' revocation intent in varying situations, distinguishing perceived situation severity and expected revocation difficulty.

(3) Through **semi-structured interviews** ($n = 20$), we then examine users' perceptions, mental models, and preferences regarding the four revocation mechanisms identified in the literature.

(4) Based on these findings, we give **recommendations** for more effective and usable revocation methods for industry and standardization bodies.

Our findings reveal that revocation intent closely follows perceived risk. In high-risk scenarios, such as a stolen device or a compromised password manager, 82% to 95% of participants report high intent to revoke access, whereas lower-risk situations show substantially reduced revocation intent. Qualitative results further show that users perceive current revocation practices as cumbersome, fragmented, and difficult to manage at scale, often expressing concerns about incomplete revocation. Across the evaluated mechanisms, no single approach clearly dominates, as users highlight trade-offs between usability, security, and trust. Notably, participants consistently express a preference for simple, low-effort solutions, ideally enabling centralized or one-click revocation, despite such approaches conflicting with the decentralized and privacy-preserving design of passkeys. Overall, our findings highlight the need for revocation mechanisms that meet security requirements while remaining low-effort for users, as otherwise they are unlikely to be used in practice. Passkeys' standardized structure and well-defined interfaces open up opportunities for more automated and scalable revocation approaches.

2 Background and Related Work

Next, we provide background on passkeys, focusing on credential management and revocation. Following, we summarize revocation in other domains and cover related work on both topics.

2.1 FIDO2 and Passkeys

FIDO2 is a public key-based passwordless authentication standard developed by the industry-led *FIDO Alliance* [30]. The term "*passkeys*" is the official user-friendly name for FIDO2 credentials [32]. FIDO2 comprises WebAuthn and CTAP2, which define communication between a user's browser (*client*) and the website (*relying party*) [20], and between the client and an *authenticator* (e.g., the user's device or a security key) [34], respectively. For registration, the authenticator generates a key pair and then securely stores the private key. Additionally, the public key is transmitted to the relying party. For authentication, the relying party sends a challenge that the authenticator signs with its private key. The user authorizes this by using a local unlock, e.g., biometrics or PIN, to their device.

Passkeys & Credential Management. FIDO2 credentials were originally device-bound and stored within a single authenticator, either as *platform* authenticators or *roaming* authenticators (e.g., security keys). Modern ecosystems increasingly support synchronization via cloud services (e.g., platform vendors or password managers), referred to as *passkey providers*. These systems manage, store, and synchronize passkeys across a user's devices (e.g., iCloud Keychain, Google Password Manager), allowing passkeys to be replicated across devices. While improving usability, this complicates revocation, as multiple copies may exist without an invalidation mechanism beyond platform features such as remote device wiping.

Important Security & Privacy Properties. FIDO2 credentials provide unlinkability across services by generating a unique key pair per account and relying party [31, 45]. They were also originally designed to be non-exportable and to always require user verification [59]. Synced passkeys weaken the first of these assumptions: credentials may be available on multiple devices and may be subject to provider-specific recovery, synchronization, and deletion mechanisms [99]. Some platforms further support controlled local migration mechanisms (e.g., Apple's AirDrop [5]), allowing offline credential transfer between devices.

User verification has also been weakened in practice: software-based authenticators such as password managers often remain unlocked after initial authentication, and attackers who obtain a mobile device and PIN (e.g., via shoulder surfing [8]) can access stored passkeys. While these features improve usability and recovery, they complicate the security model and increase the need for a scalable passkey revocation mechanism.

2.2 Revocation

Revocation invalidates previously issued credentials. While implementations vary, it is often designed for experts and embedded in complex infrastructures. Next, we briefly summarize existing approaches and explain why they are impractical for passkeys.

Web PKI (CRLs, OCSP, & Expiration). In X.509-based public key infrastructures, such as the TLS ecosystem, Certificate Authorities (CAs) revoke certificates by publishing their identifiers in Certificate Revocation Lists (CRLs) [22] or by making their status available via the Online Certificate Status Protocol (OCSP) [86].

Unfortunately, in practice, both approaches suffer from scalability, privacy, and availability limitations [21, 56]. OCSP in particular often fails open, allowing clients to accept a certificate when its revocation status is unavailable, effectively disabling revocation checking. As a result, browsers rely on workarounds (e.g., stapling or vendor-driven lists), weakening revocation guarantees. To improve the situation, the Web PKI increasingly relies on expiration as a lightweight complement, reflected in shorter certificate lifetimes [68]. While simple, expiration provides only coarse-grained control and leaves compromised certificates valid until expiry.

Secure Email. OpenPGP uses a decentralized model in which revocation is handled through signed revocation certificates shared via key servers. Each client decides how to enforce them [72]. In contrast, S/MIME follows a PKI-based approach with centrally managed revocation via CRLs and the OCSP [78].

Payment Systems. Credit cards provide user-facing mechanisms to report lost or stolen cards and unauthorized transactions. Account remediation and revocation are centrally enforced by the issuing institution [2]. Smartphone wallets support device-level revocation, e.g., by remotely removing payment credentials from devices marked as lost or stolen (e.g., via the "*Find My*"-network) [4, 39].

Electronic IDs. eID systems under the EU eIDAS framework rely on X.509 certificates protected by PINs. Revocation is centrally managed by issuing authorities via CRLs or OCSP [57, 94]. Many systems support user-initiated revocation (e.g., via hotlines or dedicated credentials), enabling rapid mitigation of misuse.

Instant Messaging Systems. Messengers use identity keys that can be replaced. WhatsApp automatically accepts replacements [63], whereas Signal requires users to explicitly consent [85].

2.3 Related Work

Revocation. Prior work on revocation focuses on X.509-based public key infrastructures in TLS and S/MIME [21, 56, 58], as well as electronic IDs [42, 57, 94], software and code signing [47], secure boot [7, 69], API keys [27, 52], and encrypted email [72, 78]. In these systems, certificate revocation has long been recognized as a fundamental challenge [19, 23, 50, 73] and is handled by experts.

In contrast, we study revocation from the user's perspective in the context of passkeys, where human factors are central. Prior work shows that revocation in user authentication is non-trivial [14]. In FIDO2, revocation is not supported: users must manually remove passkeys at each relying party [13], and existing mechanisms such as remote device wiping only partially address the problem, especially for roaming authenticators [11, 101]. Beyond security, passkey deletion can also be maliciously leveraged in interpersonal threat scenarios [24], highlighting that revocation itself can be misused.

Credential Management, Account Compromise, & Remediation. Past work has extensively studied credential management from a user-centric perspective [36, 90], particularly the role of password managers in reducing the burden of creating, remembering, and entering credentials [49, 76, 80]. Yet, revoking access by changing passwords and expiring sessions remains cumbersome, requiring users to navigate inconsistent account security interfaces (ASIs) [12, 53, 77, 105]. Related work suggests that unified interfaces may reduce this burden. For example, Smith et al. [89] created a framework for managing secondary authentication factors (SAFs). Their proposal encompasses the entire SAF life cycle, including removal, effectively enabling semi-automated revocation.

Prior work on remediation has examined user interactions with login notifications [67], security checkups [77], and ASIs [25], often finding them inconsistent, insecure, and ineffective. Studies analyze remediation protocols across services [64, 75], including FIDO2 [54] and password-based accounts [53]. Bhattacharya et al. [12] show that ASI logs and notifications are difficult to navigate even for expert users. Others demonstrated real-time phishing and client-side attacks against FIDO-based authentication, including downgrade attacks [96] and malicious browser extensions [35, 102], further motivating the need for effective revocation mechanisms.

While prior work focuses on service-specific remediation or revocation of other authentication factors, we study revocation of passkeys as a user-driven response to compromise (e.g., a compromised passkey provider or a stolen authenticator) and investigate when and how users resort to such measures.

Users' Understanding of Passkeys. A large body of prior work explores users' mental models, experiences, and understanding of FIDO2 authentication [59, 60, 66, 79, 100]. These studies mostly examine usability, misconceptions, and adoption challenges.

Early work primarily investigates device-bound credentials. Studies on hardware security keys show difficulties, particularly when configuring accounts, following setup instructions, and integrating the devices into existing authentication workflows [66, 84]. Research focused on smartphone-based authenticators highlights challenges related to cross-device usage and platform support [74, 79, 101]. In enterprise settings, work emphasizes integration challenges, organizational constraints, and deployment obstacles [29, 41, 46, 60, 62]. Across these settings, a recurring theme is the concern about losing access and the resulting difficulty of account recovery.

More recent work shifts toward synced passkeys. Büttner and Gruschka [18] show that syncing improves availability and mitigates device loss, but introduces new security risks and concentrates trust in passkey providers. Reittinger et al. [83] demonstrate improved usability compared to passwords and 2FA, but also identify adoption barriers and challenges related to cross-device synchronization. Similarly, Willis-Arnold et al. [100] find that concerns about portability and transferability persist, particularly among less technical users. Jannett et al. [43] find significant differences in how websites allow users to add, manage, and delete passkeys, with some sites restricting deletion or limiting users to a single passkey. Kupris and Schreck [55] compare synced passkeys, passkeys generated by hardware security keys, and passwords with OTPs in a university setting. Synced passkeys received the highest willingness to adopt, despite concerns about their use for sensitive accounts.

While prior work on users' understanding of passkeys focuses primarily on usability and adoption, we take a complementary perspective by examining passkey revocation, which is currently not supported at the ecosystem level. To this end, we explore users' perceptions, mental models, and preferences regarding revocation.

3 Systematization of Revocation Approaches

In this section, we (1) examine proposals for passkey revocation from the literature, summarize their underlying ideas, and systematize their envisioned user-facing interactions into four revocation mechanisms, and (2) compare the mechanisms based on *scalability*, *unlinkability*, and their estimated *time to revoke*.

Approach. To identify passkey revocation proposals, we conducted a targeted literature search between Oct. 2024 and Mar. 2025. We queried Google Scholar, DBLP, ACM DL, IEEE Xplore, and the IACR Archive using: "revocation" + "FIDO," "FIDO2," "passkey(s)," and "WebAuthn" and complemented this with backward and forward citation tracking. Among the results, we selected only the papers that mention revocation at least once. The schemes outlined in this section encompass all identified proposals.

As these proposals primarily focus on protocol design rather than user interaction, we abstracted each into a simplified, user-facing interaction model. In cases of underspecification (e.g., the distribution of the revocation list), we inferred missing details based on the system design, making conservative assumptions. Finally, some schemes are not primarily designed for revocation but target account recovery while still incorporating or discussing revocation. An overview is provided in Table 1.

Definition: Passkey Revocation. A relying party revokes a passkey by disabling or deleting its credential record and expiring any potentially compromised sessions. A complete process may additionally remove corresponding copies from authenticators and passkey providers to prevent stale credential prompts. We consider a revocation mechanism *scalable* if it enables timely revocation without requiring users to remove each affected passkey manually from every relying party and passkey provider.

3.1 Baseline

FIDO2 and passkeys do not provide a mechanism for scalable revocation across relying parties. As noted by Blessing et al. [13], "*the FIDO2 standard does not adequately address credential revocation at a global scale*" and instead relies on per-site removal of credentials (cf. Figure 1). Currently, the FIDO Alliance recommends that relying parties provide users with a clear interface for managing and removing passkeys. In particular, users should be asked to confirm passkey deletion and, optionally, be informed that credentials may still exist in their passkey providers (cf. Figure 1a). If the removed passkey is the last credential associated with an account, users should be warned about potential account lockout and reminded of available recovery mechanisms.

This way, passkey removal remains fundamentally decentralized. Users are responsible for identifying and removing corresponding credentials across all of their passkey providers. This challenge is exacerbated by current best practices that encourage registering multiple authenticators per account for recovery [54, 104].

To mitigate inconsistencies between server-side and client-side credential state, the recently proposed *WebAuthn Signal API* [48] enables relying parties to signal that a credential is no longer valid (cf. Figure 1b). Upon receiving such a signal, clients can update or remove stale passkeys from passkey providers, reducing the likelihood of outdated credentials being presented to users. However, this mechanism requires explicit support from the passkey provider and relying parties. As of today, support in Web browsers remains limited [71], and the API does not provide a revocation solution but rather a best-effort synchronization mechanism.

3.2 Revocation Code

Hanzlik et al. [40] propose a mechanism for global passkey revocation without requiring per-relying-party interaction. From a user's perspective, the proposed mechanism can be understood as a "revocation code:" a secret that must be stored and later disclosed to invalidate all associated passkeys. On a technical level, the mechanism relies on deterministic key derivation. Concretely, when a user initializes an authenticator, a revocation key rk is derived from the authenticator's master secret key msk.[1] The user needs to store this rk, '*externally, i.e., on a piece of paper as a QR code*." To revoke credentials, the user then publishes rk to a public *revocation list* which relying parties may, for example, periodically retrieve to update the status of registered authenticators. To preserve unlinkability, the scheme relies on deterministic key derivation (e.g., BIP32), where rk consists of a master public key and a chain code. This allows relying parties to recompute authenticator-specific public keys and efficiently check whether they should be revoked. However, after the revocation code is published, unlinkability is not maintained.

3.3 Backup Device

The following interaction model builds on prior work by Arora et al. [6] and Takakuwa et al. [92, 93], which explore mechanisms for managing and recovering FIDO credentials across multiple devices.

Group Signatures. Arora et al. [6] propose organizing authenticators into a group using managerless group signatures. Each device holds an individual signing key (gsk), while the relying party stores a shared group verification key (gvk). Authentication can be performed by any group member. Group membership is tracked in a public identity ledger (`Table`), which records additions and revocations. Authorized devices can update this state using a revocation key, enabling group-wide revocation. Compared to standard FIDO deployments, this approach provides a unified view of credentials across devices while maintaining unlinkability.

Transfer Access Protocols. Takakuwa et al. [92, 93] propose a family of protocols based on the idea that trust can be transferred via chains of signatures. In the *Transfer Access Protocol*, a new device obtains credentials by having its public keys signed by an already trusted device (primary authenticator A), forming a credential chain that the relying party can verify. Upon successful authentication with the new device, the relying party replaces the old device's (A) credentials, effectively revoking its access. Building on this construction, *Preemptively Synced Keys* introduce a dedicated backup device (BA), whose public keys are registered alongside the primary authenticator's A. Should A be lost, the backup device BA can sign keys for a completely new device, allowing it to authenticate and replace the lost one (A), thereby revoking its access. In real-world contexts, *Preemptively Synced Keys* encounter key storage limitations on authenticators. To mitigate this, the authors introduce the

[1] Hardware security keys can only store a limited number of keys; thus, they instead derive them on the fly using key wrapping or key derivation techniques [103].

Table 1: Comparison of Passkey Revocation Approaches and Their Interaction Models.

Interaction Model	Setup Phase	User Action	Mechanism	No 3^{rd} Party	Scalability	Unlinkability	Revocation Time
Baseline [33]	-	Remove individually	-	●	○	●	Hours to days[c]
Revocation Code [40]	Store code	Publish code	Revocation list	○	●	◐	Immediate[d]
Backup Device [6, 92, 93]	Pair devices	Auth. replacement device	Automatic removal at sign-in	◐[b]	○	◐	Hours to days[c]
Centralized Service [88]	Create account	Remove authenticator	Revocation list[a]	○	●	◐	Immediate
Electronic ID [87]	Present eID	Revoke eID	eID validity check at sign-in	○	●	●	Immediate to weeks[e]

[a]Enforcement unspecified; [b]Only for Online Recovery Storage Protocol; [c]Some accounts may be missed; [d]Once revocation code is obtained; [e]Depends on implementation & user-chosen revocation option.

Online Recovery Storage Protocol, which outsources pre-generated keys to an encrypted blob stored on an untrusted server. Authorized devices can then retrieve and update this state using a shared key, while the remainder of the protocol remains unchanged.

Across these protocols [6, 92, 93], changes to active credentials are authorized by a previously provisioned device. Takakuwa et al. use delegation chains to onboard a new authenticator [92, 93], while Arora et al. allow authorized devices to update a shared group state [6]. Building on this pattern, we consider a dedicated backup device that is provisioned during setup but cannot itself authenticate. If a primary authenticator is lost, the user establishes a secure channel between the backup device and a replacement. The backup device authorizes the replacement, allowing the relying party to add it and revoke the lost authenticator's passkey. For this to work, users must retain the backup device, authenticators must support secure device-to-device communication and signed replacement authorizations, while relying parties must verify these authorizations and replace the registered passkey accordingly.

3.4 Centralized Service

Using a trusted third party is common in various revocation contexts, such as federated identity and token-based systems, where central servers manage credential or session revocation. For FIDO2, Shiraishi et al. [88] propose *CloudAuthn*, an online service that manages certifying keys associated with a user's authenticators. The core idea is to introduce *certifying keys* (dsk, dpk) that serve as proxies for device credentials. Authenticators generate temporary keys that are signed using certifying keys held in the cloud, allowing relying parties to verify that the authenticator belongs to the user. Relying parties store both the FIDO2 public key and the corresponding certifying key dpk, allowing any authenticator certified by the same dsk to be recognized as belonging to the same user. To initiate revocation, the user authenticates to CloudAuthn using another available authenticator or an alternative identity verification method. CloudAuthn then deletes the inaccessible authenticator and adds the device to a revocation list. This list is shared with the relevant relying parties so that they can reject the revoked authenticator. However, the proposal does not specify how the distribution of this list is implemented and enforced. Additionally, the proposal does not discuss unlinkability.

3.5 Electronic ID (eID) or Passport

Schwarz et al. [87] propose *FeIDo*, a FIDO2-compatible authentication scheme based on electronic documents such as eIDs and ePassports. While primarily designed as a second factor, it can also be extended to passwordless scenarios. FeIDo leverages standardized interfaces (e.g., ICAO eMRTD) to extract verifiable user attributes from widely deployed identity documents. Instead of storing credentials on a device, FeIDo derives FIDO2 credentials from stable user attributes (e.g., name, date and place of birth) using a key derivation function inside a trusted execution environment (TEE). This allows credentials to be re-derived even if the physical document is replaced, enabling recovery without backup authenticators. The architecture consists of a remote credential service and a client-side middleware. The middleware reads the eID and forwards authenticated attributes to the credential service, which verifies them and deterministically derives per-relying-party credentials. No persistent user data is stored outside the TEE. Revocation in FeIDo is largely delegated to existing eID infrastructures and enforced during credential derivation. If an eID is reported as lost or stolen, it is added to trusted external databases (e.g., Interpol-like services), which the credential service consults during authentication. If the document is flagged as revoked, the credential derivation is denied. In addition, FeIDo supports eID-specific revocation certificates, which users can use on demand to invalidate a specific eID across all credential services.

3.6 Comparison

Next, we compare the approaches summarized in Table 1, focusing on scalability, unlinkability, and the estimated time to revoke.

Scalability refers to how easily a user can revoke all credentials associated with a compromised authenticator across relying parties. This is largely divided into individual, *per-site* revocation and *global* revocation, which removes access to all services at once. Neither the *baseline* nor the *backup device* are scalable. However, the backup device removes the need to visit each account's settings. All remaining proposals are scalable.

Unlinkability is a central privacy requirement of the FIDO specifications [31], aimed at preventing cross-site tracking [45]. Not all proposals achieve this property. The *baseline* is unlinkable by design, both before and after revocation. The *revocation code* proposal also provides unlinkability prior to revocation, but becomes linkable once the code is published, since two relying parties can then check whether two accounts link to the same code. For *backup device*-based revocation, unlinkability requires that backup devices themselves are indistinguishable. For credential chains, unlinkability is violated by the existence of two distinguishable modes: regular logins and recovery. In recovery mode, the service can link the previous primary authenticator to the new device. However, as long as access for the prior primary authenticator is deactivated, this is not a major concern. For constructions based on group signatures, unlinkability depends on the chosen signature scheme. Some provide built-in unlinkability [10]. Using a *centralized service* does not break unlinkability in the narrow sense. However,

the service itself inherently knows where users hold accounts and which authenticators are linked to them. For the *eID*-based mechanism, unlinkability is provided even after revocation. While, as with the backup device, the relying party may learn which eID was previously used, this provides no useful information as the old ID is deactivated by the government, outside the relying party's control.

Revocation time largely depends on the number of steps involved and whether third parties, such as government bodies, may delay the process. Revoking accounts manually (*baseline* and *backup device*) likely takes hours to days, depending on the number of accounts a user holds, and how easily they restore access via fallback mechanisms. Still, some accounts may be missed entirely. Both *revocation codes* and *centralized service* approaches promise immediate revocation. However, the revocation code must be obtained first. Additionally, revocation status must be distributed to relying parties. Hence, it also depends on the availability and timely synchronization of such "revocation lists." Lastly, *eID*-based revocation is highly implementation dependent. If user-issued revocation certificates are available, immediate revocation may be possible. However, when revocation relies on processes within government institutions, it is more likely to take days or weeks, depending on the infrastructure.

RQ1 – Proposed Revocation Models

Our *baseline* reflects current FIDO Alliance practice, relying on per-site removal. In contrast, we introduce four user-facing models based on academic proposals: (1) *revocation codes* (publish a revocation secret), (2) *backup devices* (use a pre-provisioned device as root of trust), (3) *centralized services* (delegate revocation to a trusted third party), and (4) *eID* (rely on external identity infrastructures). These approaches introduce coordination beyond individual relying parties, but differ in their trust assumptions and how revocation information is propagated.

4 Online Survey

To our knowledge, no prior work has examined users' perceptions of revocation or reactions to scenarios requiring it, either for passkeys specifically or credentials generally. We therefore conducted an online survey with 308 participants to investigate the importance users assign to revocation, their perceptions of it, and their likelihood of revoking access across scenarios, while establishing a foundational understanding of their beliefs for our interview study.

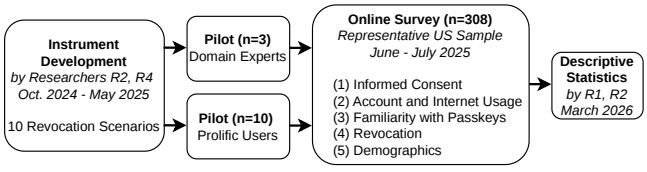


Figure 2: Overview of the survey, including instrument development, testing, and deployment, followed by descriptive analysis of participants' responses across scenarios.

4.1 Method

Each participant was presented with ten scenarios and asked to rate their likelihood of revoking access in each case, as well as assess the perceived severity and the effort required to revoke access. They were then asked to briefly explain their rating for two of the scenarios, chosen at random. This allowed us to analyze the factors influencing anticipated revocation behavior across different contexts. The scenarios were a (1) ***Stolen Device***, a (2) ***Security Checkup***, a (3) ***Hacked PWM***, a device (4) ***Shared w. Friend***, or (5) ***Shared w. Partner***, a device (6) ***Offboarding***, a (7) ***Compromised Account***, an account on a (8) ***Public Computer***, an (9) ***Unused Account***, and an (10) ***Old Device***.

Scenarios were chosen to reflect a broad range of situations in which revocation might be necessary or desirable. While generally based on heuristics, we prioritized representing a variety of account sensitivities, attacker types, and capabilities (i.e., the likelihood of an attacker getting access), varying numbers of affected accounts, and different revocation complexities. The scenario descriptions are available in Table 2. Figure 2 summarizes our method.

Table 2: Revocation Scenarios and Descriptions.

Scenario	Description
Stolen Device	Your device has been stolen. You are logged in to all of your accounts on that device, and the thief knows your PIN.
Security Checkup	During a check-up of one of your accounts, you see that a device that you do not use anymore is still logged in.
Hacked PWM	You use a service that stores all your passwords for you so you don't have to remember them. You receive a legitimate email from the service telling you they have been hacked and your passwords might have been leaked.
Shared w. Friend	You shared your streaming account with a friend. Now they don't want to use it anymore and no longer pay their share of the fee but they are still logged in on their devices.
Shared w. Partner	As many couples do, you shared some of your accounts with your partner and both of you know the passwords to these accounts. You now broke up with this partner.
Offboarding	You quit your job and have to return your work laptop to the company. You are still logged into some of your personal accounts on this device.
Compr. Account	You receive a legitimate email from a service where you have an account. They tell you that your account has been hacked.
Public Computer	You used a shared computer in a public library and accidentally clicked on "store password" when you logged in to one of your accounts.
Unused Account	You made an account on a shopping list website that helps you plan your groceries but did not end up using it.
Old Device	You got a new device and put the old one in a drawer. It's still signed in, but you're not using it anymore.

4.1.1 Study Protocol. Next, we present our survey, with references to individual questions. The full survey is provided in Appendix C.

(1) ***Informed Consent.*** We first collected participants' consent, clarifying study goals, data collection practices, and storage policies. Furthermore, participants formally agreed to complete the study without the use of generative AI.
(2) ***Account & Internet Usage.*** To start, we thoroughly explained the phrase "login in to an account," ensuring participants correctly understood the difference between online account logins and unlocking a device locally (**AA**). After that, we collected information about participants' account use and management

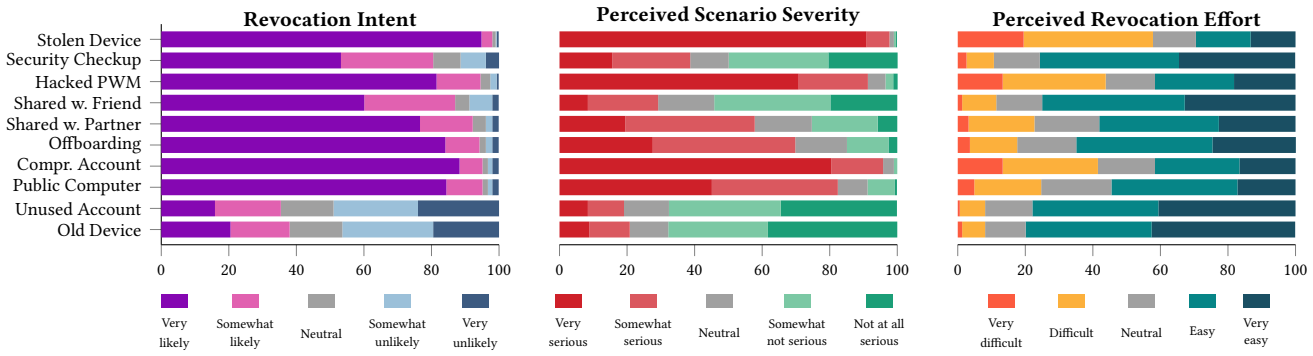


Figure 3: Participants' self-reported revocation intent, perceived scenario severity, and perceived revocation effort.

habits, e.g., the use of password managers, account sharing, and account security setups (**A1**–**A9**).

(3) ***Familiarity with Passkeys.*** Next, we investigated participants' passkey familiarity and knowledge, asking if and for which accounts they had used them before (**P1**–**P2-yes-2**).

(4) ***Revocation.*** This section was the main part of our survey. We started with a brief description of the term "revocation" to ensure a correct understanding, and verified this with an attention check (**RA**). Then, we presented participants with the ten scenarios (see Table 2), in which they might want to revoke access to their accounts, asking to rate their likelihood of revoking access on a 5-point Likert scale (**R1**). A follow-up open question then randomly presented two of the ten scenarios, asking participants to provide further reasoning for their ratings (**R2-1**–**R3-2**). Finally, we asked participants to rate the perceived effort required to revoke access (**R4**) and the perceived severity of each scenario on 5-point Likert scales (**R5**) to gather further insights into participants' reasons for their intent to revoke access.

(5) ***Demographics.*** We finished with demographic questions on age, gender, education, and IT background (**D1**–**D4**).

Pilot Testing. We tested our survey with three domain experts and 10 Prolific participants. As a result, we decided to add the perceived effort and severity Likert scale metrics (**R4**, **R5**). Additionally, we encountered AI-generated open answers. We therefore extended our participation requirements to prohibit generative AI and manually removed responses for which we suspected AI use.

Recruitment & Demographics. We recruited participants via Prolific and collected responses via a Qualtrics survey. We compensated $5.25 USD for an average duration of 21 minutes ($15 USD average hourly rate). In total, we collected $n = 322$ responses and retained $n = 310$ after sanitization (e.g., removing incomplete surveys and failed attention checks). Upon manual review, we removed two additional responses due to indications of AI use, totaling the final number to $n = 308$. Our sample was representative for the US public according to gender ($n = 148$ men, $n = 157$ women, $n = 3$ non-binary) and mostly representative for age and education. Only ages 75+ and low education (no high school completed) were underrepresented. The full demographics are provided in Appendix D.

Data Analysis. To analyze qualitative results from open answers, we applied thematic analysis following Braun & Clarke [15–17] using a purely inductive approach. First, two researchers independently coded and created codebooks for 10% of all answers. These were subsequently organized and merged in joint discussions. The remaining answers were then coded only by the main coder. The codebooks are provided in Appendices F and G.

To examine how perceived severity and required effort predict revocation likelihood, we fitted a linear mixed-effects model. Revocation likelihood served as the dependent variable. Severity and effort, as well as their interaction, were included as fixed effects. For easier interpretation of interaction effects, variables were centered before being entered into the analysis. To account for the hierarchical structure of the data, we included random intercepts for both participants and scenarios. This approach controls for baseline differences in revocation tendencies across individuals, as well as systematic differences between scenarios. Statistical significance was assessed using two-tailed tests with an alpha level of .05.

4.2 Results

Below, we present the results for the **(4)** ***Revocation*** section of the survey. We start with descriptive information on participants' revocation likelihood and later integrate it with the reasoning provided in open answers as well as statistical results.

4.2.1 General Revocation Intent. Across situations, the revocation intent was high. Particularly, in case a device was stolen (***Stolen Device***), an account was compromised (***Compromised Account***), or the password manager storing all credentials was hacked (***Hacked PWM***), the vast majority of participants reported the highest possible intent (82% to 95% were "Very likely to revoke"). Some situations were perceived as less severe, such as forgetting to log out of a public computer (***Public Computer***), sharing an account with an ex-partner (***Shared w. Partner***), and offboarding a work device (***Offboarding***), where 75% to 84% gave the highest possible rating. They reported being less likely to revoke (~60% "Very likely") if they shared an account with a friend (***Shared w. Friend***) or found an unused device in their list of logged-in devices (***Security Checkup***). They claimed to be unlikely to revoke (~50% "Unlikely" or "Very unlikely") an account they did not use (***Unused Account***) or an old device lying in a drawer (***Old Device***).

4.2.2 Interaction of Intent, Severity, & Effort. Below, we further analyze potential reasons for the revocation intent measured across different scenarios, integrating regression results and open answers. We focus on the three most severe and least severe scenarios.

Influence of Effort & Severity. The mixed-effects model revealed that *severity* ($b = 0.24$, 95% CI $[0.21, 0.28]$, $p < .001$) and *effort* ($b = -0.04$, 95% CI $[-0.08, -0.01]$, $p = .007$) predicted likelihood, but not the interaction between both of them ($b = 0.00$, 95% CI $[-0.02, 0.02]$, $p < .813$). The positive effect of severity indicates that participants are more likely to revoke access in scenarios perceived as more severe, reflecting increased motivation to act in riskier situations. The negative effect of effort indicates that higher perceived effort is associated with a lower likelihood of revocation, although the effect is small, suggesting that effort acts as a minor barrier to revoking access. The regression table can be consulted in Appendix E.

High-Risk Scenarios. ***Stolen Device***, ***Compromised Account***, and ***Hacked PWM*** scenarios were the ones in which the severity was perceived as the highest, with 91%, 81%, and 71% of the participants rating them as "Very serious," respectively. As shown above, these were also the scenarios with the highest possible revocation intent (82% to 95% were "Very likely to revoke"). Interestingly, these scenarios are also those for which perceived revocation effort is rated the highest (42% to 58% "Difficult" or "Very difficult"). This may be due to the fact that in such high-risk scenarios the attacker has significant power over one or many accounts, or the device itself, and regaining control may be perceived as more difficult by users, as reflected in open-text responses: *"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. [...] once that kind of data is out there, it's very hard to control who sees it, and I might not even have access to it anymore."* Most identified the perpetrator as either a thief (***Stolen Device***) or a hacker over the internet. Hence, their primary motivation to revoke was to prevent unauthorized access (*"I don't want hackers having access to my accounts and my information."*). Participants were concerned about monetary losses, identity theft, and access to sensitive information, particularly banking, especially in the ***Hacked PWM*** scenario (*"It could ruin my life by stealing my money and charging things to my credit cards and ruining my credit."*).

Low-Risk Scenarios. ***Old Device***, ***Shared w. Friend***, and ***Unused Account*** scenarios were perceived as less severe with only 8-9% of participants rating them as "Very serious." In all three cases, reported revocation likelihood was also relatively low compared to other scenarios (21%, 60%, and 16% were "Very likely to revoke," respectively). In the ***Old Device*** scenario, the reported low revocation likelihood was primarily justified by participants feeling safe as their devices' physical location was perceived as safe (*"If the device is just sitting in a drawer in my own house, there is no danger or possibility that someone else will get to it. Therefore, no one will be able to get into my accounts either. Without the risk, I do not see a reason to revoke."*). Additionally, some argued they may want to access and use the device later on, in which case revoking access would be inconvenient (*"I might need to use it again briefly."*). In the ***Shared w. Friend*** scenario, a major potential concern was the possibility of the account being shared with other people or the friend continuing to use the account without paying (*"I think that the worst that could happen is that he might share my password with his other friends. One more thing that could happen is that he still might use the account behind my back because he still has the account logged in into his devices without even paying his share."*). However, participants justified their low intention to revoke by wanting to prevent conflicts, particularly given the expected low monetary losses in the described scenario (*"I wouldn't want my friend to become upset with me if they got an email notification that I revoked access. I also don't really find it a big deal, as I am paying for the service anyway and if it isn't blocking me from logging in with new devices, I won't push the issue."*). Finally, the ***Unused Account*** scenario was perceived as non-critical as participants expected no sensitive information being stored on the account. Additionally, revocation might even be counterproductive in case of future account use (*"I may use it in the future, and it doesn't seem any sensitive information would be stored or accessible from there."*).

Some users who also expressed unwillingness to revoke rated the revocation effort as high, suggesting revocation in low-severity scenarios is perceived as unnecessary, and thus burdensome (*"The account is inactive and doesn't pose a security risk."*).

RQ2 – Revocation Intent

Participants show high revocation intent in scenarios that they perceive as very severe, i.e., scenarios where a threat or the presence of an attacker is clear (***Stolen Device***, ***Compromised Account***, ***Hacked PWM***). Moreover, when participants are able to clearly identify the attacker and their goal, such as in high-risk scenarios, expected potential consequences are relatively unanimous (namely, financial abuse, identity theft, and sensitive data exfiltration). In contrast, when participants perceive the situation as less severe, the attacker is more fuzzy (i.e., "someone"), and the imagined consequences become more vague and less threatening. Moreover, in these situations, participants rely on physical security measures (e.g., storing the old device in a drawer), on trusted relationships (e.g., friendship), or on the belief that the information stored in the account is not sensitive and that the potential consequences are mild.

5 Interview Study

Next, we describe our semi-structured interviews with $n = 20$ passkey users, where we discussed potential mechanisms for systematic passkey revocation, derived from the research proposals identified in Section 3. Figure 4 provides an overview of our method.

5.1 Method

In practice, regular users seldom interact with revocation. Additionally, none of the proposed passkey revocation mechanisms identified in Section 3 have been deployed in practice. Hence, we devoted substantial effort to translating technical proposals into descriptions that are easy to digest for regular users. Additionally, as highlighted by the survey, revocation can be relevant in numerous different scenarios, each involving varying stakeholders and accounts. Covering all would significantly complicate the

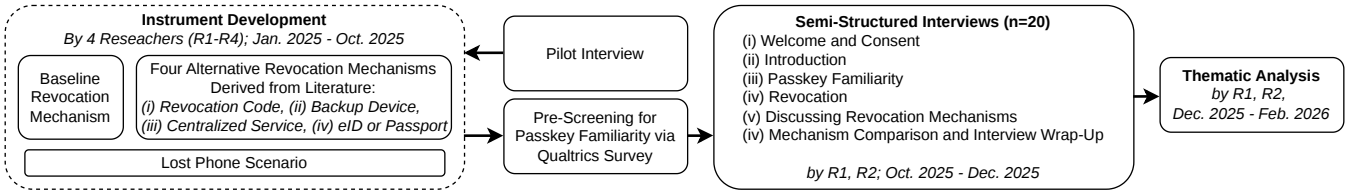


Figure 4: Overview of the semi-structured interview study, including instrument development, pilot testing, pre-screening, and interviews, followed by a thematic analysis of participants' perspectives on different revocation mechanisms.

demonstration of the mechanisms and likely overwhelm participants. Hence, we selected only one scenario, which was then used as the context for the following presentation of revocation mechanisms. Drawing on the survey findings, we jointly developed a "lost phone" scenario that retained the sense of urgency associated with the high-risk scenarios identified in the survey. Concretely, we envisioned a phone on which the user stores passkeys for several accounts. Subsequently, this phone is lost, and access needs to be revoked for all passkeys stored on the device.

5.1.1 Proposed Revocation Mechanisms. As mentioned before, we never presented any technical details to avoid overwhelming and potentially confusing participants. Concretely, we covered the following five mechanisms with their corresponding descriptions:

(i) **Baseline**. This revocation mechanism represents the current state of the art. If a person loses their device, they must log in to each account that stores passkeys, open the account security settings, and manually revoke the passkey associated with the lost device. This process must be repeated for all accounts for which passkeys are stored on the lost phone.
(ii) **Revocation Code** is based on Hanzlik et al. [40]. In this mechanism, each of the user's devices is assigned a so-called *revocation code* which the user can use to revoke all passkeys stored on the device at once.
(iii) **Backup Device** is based on Arora et al. [6] and Takakuwa et al. [92, 93]. Here, the user pre-configures a backup device by locally connecting it to their phone via a secure channel (e.g., Bluetooth). When the phone is lost, the user accesses each account with the backup device, which then automatically revokes the passkeys associated with the lost phone.
(iv) **Centralized Service** is based on Shiraishi et al. [88]. Here, the user has an account at an online service and registers all their devices on it. The service is responsible for managing the devices' registration at different relying parties. When the phone is lost, the user can simply access the platform on another device and revoke the lost phone.
(v) **eID or Passport** is based on Schwarz et al. [87]. For this mechanism, the user's issued FIDO credentials are derived from personal attributes stored on their eID or electronic passport. Hence, in this case, the eID is the authenticator and would be lost (as opposed to the phone, like in previous scenarios). To revoke, the user must report the eID as lost to official authorities; the document is then added to a list of compromised documents, invalidating its use for authentication.

Appendix H includes the full explanation of the revocation mechanisms as described to participants during interviews.

5.1.2 Study Protocol. The interviews were conducted online with one or two researchers present. During the online interviews, we shared Miro boards to showcase relevant concepts to participants. Overall, the interview consisted of six steps. After (i) **Welcome and Consent** as well as an (ii) **Introduction**, we collected information on participants' passkey usage habits in our (iii) **Passkey Familiarity** section. Questions covered experiences, platform usage, and the perceived purpose of passkeys. Moreover, we investigated participants' familiarity with passkeys' technical functionality. For participants with limited knowledge, we presented an explanation of passkeys on a Miro board and thoroughly clarified potential questions. Next, we introduced participants to the concept of (iv) **Revocation**, again on a Miro board. We then asked them to propose plausible revocation scenarios and specify the steps they would take to perform revocation. The main part was (v) **Discussing Revocation Mechanisms**. Here, we individually presented the passkey revocation mechanisms (cf. Section 5.1.1) and asked participants for their impressions and concerns. Finally, we asked participants for their preferred revocation mechanism and ended the interview. The full guide used for conducting interviews is available in Appendix H.

Pilots. We conducted two pilot interviews, prompting minor refinements to the interview script. Moreover, for the first five interviews, we presented revocation mechanisms in considerable detail, using diagrams on a Miro board as visual aids. However, those detailed explanations proved time-consuming, leaving less room for participants' thoughts and perceptions, so in subsequent interviews, we omitted the visual presentation.

5.1.3 Recruitment & Demographics. We recruited passkey users to ensure a certain baseline knowledge needed to introduce passkey-specific revocation mechanisms. We recruited participants via Prolific, screening for age (18 or older), US residency, and current or former passkey use. Participants first completed a pre-survey to confirm that they were passkey users and, if so, to book an interview slot via *Calendly* [9]. Participants received $0.50 USD for completing the pre-interview survey and $30 USD for participating in the interview. The interviews lasted between 40 min. and 1 hour. Participants were on average 43 years old, with 60% younger than 45. Eight participants were women and 12 were men. The majority (70%) reported no education or work experience in IT. Only three had a technical background, while the remainder chose not to provide this information. All demographics are provided in Appendix I.

5.1.4 Data Analysis. All interviews were audio-recorded and conducted in English. We utilized *noScribe* [28] for transcription and MAXQDA 24 for coding. For analysis, we applied thematic coding following Braun & Clarke [15–17] using a purely inductive approach. This method is well-suited for exploratory research like ours, where we prioritized contextualizing revocation ratings and understanding participants' reasoning about proposed mechanisms over frequency-based analyses. While all four researchers participated in discussions about interpreting the results throughout the process, the main coding was conducted by two researchers. In a first step, two interviews (10%) were jointly coded to establish an initial codebook. This was finalized through multiple discussion sessions, continuing until full agreement was reached between the two coders on each individual code. The remaining interviews were then coded by the main coder, expanding on the codebook as needed. Themes were then extracted from codes in joint sessions with all four researchers. The final codebook can be found in Appendix J.

5.2 Results

Here, we present the results of our qualitative analysis.

5.2.1 Familiarity with Passkeys. Most participants reported first enabling passkeys when offered by a service. The vast majority reported using their desktop or laptop and phone, with a minority also enabling passkeys on their tablet. Participants primarily used passkeys on financial platforms (e.g., PayPal and online banking), in online shops, and, to a lesser extent, for social media and other accounts. When asked about their impression of passkeys, several participants reported that *"It seems like a more secure method of authenticating a user."* Moreover, participants recognized passkeys as a convenience feature that allows them to streamline logins.

Concerns About Passkeys. A few participants reported issues with passkeys, such as unreliable biometric sensors or forgetting the fallback PIN. Some also expressed concerns about account recovery in case their device is lost or their biometrics are not recognized. As a result, they shared a desire for a fallback authentication method, for instance, a password. Other security and privacy concerns included the potential sharing of biometrics, the sale of data to third parties, or uncertainties about passkeys' resistance to hacking.

5.2.2 Understanding Revocation. After explaining revocation, we asked for situations in which participants would revoke. Most frequently, *account sharing* was mentioned, prompting concerns about sensitive information being shared with the other person, the possibility for the other person to generate new passkeys for additional devices, or relationship breakdowns. Several also referenced *changes in device availability*, e.g., losing or switching them, or the device being damaged. Some mentioned revoking access in response to *fraudulent behavior*, such as account violations or a website becoming untrustworthy. One participant suggested the possibility of creating time-bound passkeys to grant temporary access, thus eliminating the need for revocation in this scenario: *"[...] or even being able to give a friend, someone that you're not as close to, a very temporary access to a shopping account or something."* Participants' overall impression of revocation was positive, as they recognized the usefulness and importance of being able to revoke a passkey when necessary. When asked how they would revoke, most participants indicated that they would go to the account's security settings, while others mentioned using another device.

5.2.3 Evaluating Revocation Scenarios.

Baseline. The majority of participants expressed negative reactions to the current state of revocation. They perceived it as annoying, cumbersome, and time-consuming, e.g., *"I mean, obviously it's cumbersome and annoying depending on how many passkeys you have saved."* They also pointed out that the process is high-friction and not manageable, especially the effort required to navigate to the individual settings of different websites. In addition, one participant noted that *"on each website, all their UI is different and you have to kind of figure out where the options are."* The primary concern was the risk of forgetting some accounts for which passkeys are stored on the lost device (e.g., due to cross-ecosystem use). Additionally, one user expressed concern about potential technical challenges: *"I have difficulty just with the basics."* Considering a future in which passkeys are (more) ubiquitous, one participant pointed out the lack of scalability of the mechanism *"If you've got two or three, fine. If you've got 20, not going to happen."*

Revocation Code. Many participants reacted positively to this mechanism, emphasizing its convenience and ease of use. Participants noted that the solution allows users to rely on a single code to revoke all passkeys on the corresponding device at once. *"I guess (option) one is kind of the nuclear option."* On the other hand, one participant observed that requiring only one code to revoke all the passkeys makes this solution less secure *"It's one number that covers all those different accounts. So maybe that would make it less secure."* The main concern reported regards code storing, losing it or forgetting it, or choosing an insecure method of storing that would result in it getting into malicious hands. Even when users are properly informed about its importance, the risk of loss remains *"Even if something's super important, it wouldn't stop people from losing it. People lose important documents all the time."* Beyond concerns about storing or losing the code itself, participants also expressed uncertainty about the consequences of using such a powerful revocation mechanism. In particular, participants questioned the scope of revocation in the presence of synced passkeys. *"So, if you do that on your phone, is that also going to revoke all [...] of your passkeys on your computer?"*. Another participant was concerned about the irreversibility of the process if the supposedly lost device were later recovered. *"What happens if you do find your phone [...] a couple days later, [...] how do you turn everything back on?"*. When asked what method they would prefer for storing the revocation code, participants were pretty equally divided between saving it in a digital location, either the phone/computer notes, a spreadsheet, a password manager, or on another device of theirs, and storing it in a physical location, by printing it/writing it down and then placing it in a trusted location at home, or storing it in a location where it can be easily accessed in case of need, such as a wallet. For some participants, this storage requirement represented an additional burden, effectively requiring them to securely maintain another credential-like information. *"So, now suddenly I'm back to managing a password problem. I know it's not a password, but I'm back to another problem of managing data."*

Backup Device. Opinions about this mechanism were divided. One participant noted that this mechanism would not trump the baseline: *"It feels like it's not really saving me much time or effort. So yeah, probably not worth the hassle to have an external device."* Overall, participants' primary concern regarded the device's integrity and the potential loss or theft of it. Moreover, they expressed dislike towards still having to access every account manually, especially given a future with wider passkey adoption: *"Having to go to every website would add a fair amount of time. That is the one drawback, I guess."* When asked which device, most reported a preference for an already-owned device as backup, e.g., *"It almost feels like a waste to have a device just for that."* Most favored laptops, desktops, tablets, or phones, rather than security keys, as they feared that *"There's certainly a chance of losing it, if it's small."* However, one participant also reported not wanting the device to be too big *"I said small mainly because [...] it shouldn't take up too much room in your house."* Keeping devices at home was generally favored, primarily to keep them safe. Conversely, participants who preferred carrying the device emphasized the benefit of prompt access: *"Probably with me, just in case [...] I need to do any kind of instant verification. I would want it to be something that I could access quickly."* One participant suggested a wearable device to minimize the risk of device loss. Several participants also ruminated about elaborate ways of storing the device, such as in a safe: *"Maybe in some sort of a locker where the main security is pretty good."* However, they recanted when asked whether they would actually do so: *"I don't feel like what I'm storing is so essential that I would need to go through that extra step. If I had a bank account with thousands of dollars, or, you know, cryptocurrency, it would make sense."* Overall, participants faced a trade-off when considering where to store the backup device: keeping it in a protected location reduced concerns about loss or theft, whereas carrying it with them ensured that it would be readily available when needed. Additionally, there is a gap between ideal storage and the realistic effort participants are willing to invest, which also highly depends on the perceived value of the accounts. One participant suggested that this solution may be a better fit for enterprises. *"I can see it being useful for big corporations where they want extra security [...],"* underlining that the additional security and management burden is easier to justify in an organization.

Centralized Service. Reactions to this mechanism were mostly positive, with participants pointing out its convenience and ease of use and understanding: *"This is the easiest, I think, to understand at least and probably to actually do."* However, some participants complained that it would be *"an extra layer that you have to go through if you have to log in to another central website."* One participant mentioned the burden of having an additional service to manage: *"I don't like the idea of having to be bothered calling yet another place."* Reported benefits of the service were the ability to track all passkeys, e.g.,*"I think that it's a much cleaner option to have a centrally stored system,"* and the possibility to revoke them all at once, e.g., *"You can just click it, revoke or simply on the bottom, it shows revoke all. And then boom, it goes quickly."* Moreover, participants pointed out the benefits of not having a solution tied to a specific device, e.g., *"I think not having a physical device and then yeah, basically having a service which we can log into from any device, [...] I think this sounds good."* Participants raised concerns about access to login information as well as data collection and sale. Additionally, some participants were concerned about what would happen *"if that [service's] database gets broken into."* They described it as a potential single point of failure, e.g., saying *"then someone just wipes all my passkeys or something."* Additionally, participants asked whether *"you [should] trust that person or that company or that entity?"* Participants viewed the service as a third party they had to trust with the protection of their data and accounts, making them wary of the mechanism's potential misuse. One participant said: *"I don't like that. [...] Because it's a loss of control. Can I trust these people? Well, [...] what if that database gets broken into?"* However, some participants dismissed the privacy and security issues, noting that a certain degree of exposure is inevitable, e.g., *"You're always going to be compromised no matter what."* Several stated that they prefer a service that would be *"rather [...] integrated with what I already use,"* such as Google or Apple. Other participants leaned towards an independent company, e.g., *"I think that some people would prefer to have something that was independent."* Participants preferring an established company valued convenient integration with their existing ecosystem (*"So if it was an existing service that I use, I would be more willing to adapt to it and trust it as opposed to a new company I've never heard of"*), as well as, relying on their reputation and familiarity for security and trust (*"So I would trust Google with it, but I would be hesitant to trust smaller services."*). On the other hand, one participant praised the greater independence of a separate company *"I think that some people would prefer to have something that was independent. So that there isn't a bias."* These preferences reflect how participants balanced familiarity and existing trust against provider independence.

eID. Opinions about this mechanism were split. Several participants reacted positively, emphasizing its security, e.g., *"I think the part that makes it attractive to me, uh, that's hard to spoof"*, suggesting that using eIDs for authentication is perceived as robust: *"I'm assuming it's not easy to duplicate or gain unauthorized access to."* Moreover, participants pointed out the convenience of the mechanism: *"It'd be easier to revoke that single thing to have everything else revoked at once, because it's going to take care of all of them."* However, other participants expressed hesitation and distrust toward the mechanism due to the involvement of a government ID (e.g., *"I get very nervous with IDs"*), and noted a *"whole number of red flags."* This hesitation was partially linked to general beliefs about central authorities, such as: *"Whenever the government gets involved, I feel like it adds another layer of complexity, like, corruption,"* suggesting that negative perceptions of governments may act as an adoption barrier for the mechanism. Several participants pointed out that there would be *"a barrier to entry for the US, because [...] there are lots of people who don't have passports and there is an anti-centralized-identification-card-philosophy."* This may reflect a US cultural bias: passports are not universal, whereas driver's licenses, a common replacement, are issued at the state rather than the federal level [98]. Opinions may differ in other populations. Further concerns mainly focused on privacy, ID management, and the general revocation procedure. Many participants were concerned that data may be visible to government authorities or that their browsing history may be linked to their identity, e.g., *"I wouldn't want to use my passport or my driver's license to sign in to websites*

like this. [...] I want to stay anonymous on like Amazon or Uber." Some were also concerned about carrying around important ID documents. This mechanism elicited more varied responses, partly due to differing interpretations and misconceptions. Some, for example, questioned what would happen while the ID is re-issued, raising concerns about account access availability: *"It seems like it leaves you locked out of the world, you know, no ID and no, no access to, to apps, you know, and no device."* Overall, the mechanism was perceived as challenging and opaque in how the personal data is used for passkey generation, leading to a sense of mistrust.

RQ3 – Proposal Perceptions and Preferences

Users reason in terms of trade-offs between usability, security, and trust. The *baseline* is perceived as cumbersome and unscalable, requiring manual per-account actions. Mechanisms that simplify revocation, such as *revocation codes* and *centralized services*, are generally preferred due to their low effort and ability to revoke access across multiple accounts. In contrast, *backup devices* are seen as less beneficial due to setup overhead and limited perceived advantages over the baseline, while *eID*-based approaches introduce strong guarantees but raise concerns about reliance on external authorities. Across all mechanisms, users express concerns about single points of failure, loss of control, and trust. No approach is seen as clearly superior, highlighting a gap between users' desire for simple, low-effort revocation and the constraints of secure, decentralized designs.

6 Discussion

Next, we discuss the implications of our findings for the design and deployment of future passkey revocation mechanisms.

6.1 Central Findings

Users Want to Revoke. Users recognize the need to revoke access in high-risk scenarios, but perceive the process as cumbersome, time-consuming, and error-prone. This indicates that the core challenge is not a lack of motivation, but the absence of mechanisms that enable scalable revocation. Unfortunately, the current baseline requires users to manually remove passkeys across relying parties, authenticators, and passkey providers, resulting in a fragmented process, which interview participants rejected almost unanimously.

Novel Mechanisms Introduce Novel Challenges. Users consistently prefer mechanisms that reduce effort and enable revocation across multiple accounts. Unfortunately, reducing the burden of manual per-account revocation often introduced new forms of reliance, whether on securely stored information, an additional device, a service provider, or an external identity infrastructure. **Backup Devices** slightly reduce the effort of revocation but still require per-account deletion. Hence, the additional effort of acquiring, storing, and maintaining a backup device was particularly difficult to justify. For some, this burden appeared more acceptable in higher-stakes or enterprise contexts, but most reported a tension between keeping the backup device secure and ensuring that it remained readily available when needed. Such fear of loss, as well as availability concerns, also echo previous work on the adoption challenges of physical security keys and second factors [66, 84, 95].

Mechanisms that enable global revocation were generally favored. For example, participants perceived the **Revocation Code** as a convenient and powerful mechanism. Yet, they also raised concerns about the consequences of losing or misusing the code, and about restoring account access *after* revocation. Moreover, securely storing and retaining the code was perceived as an additional management burden, suggesting that the mechanism may shift, rather than eliminate, the challenge of managing login-related information. These concerns reflect challenges identified in prior work, including the loss and secure storage of E2EE recovery codes [13].

A **Centralized Service** bundles revocation in a single location, making it both easy to understand and convenient to use [37]. However, centralization raises concerns about loss of control, privacy, and single points of failure. Accordingly, trust in the service provider becomes a key factor for acceptance [82, 91].

The **eID** mechanism was appreciated for its perceived security and robustness by some users, but faced concerns about privacy and government involvement by others. In part, acceptance depended on general attitudes toward governmental identification, which reflects results of prior work on using the German ID card with FIDO [44]. Participants also struggled with the complexity of the mechanism, given it conceptually differs from other approaches. This finding aligns with prior work where users struggle to grasp the concept of passwordless logins compared to passwords [59].

Overall, our results reveal a tension between the need for scalable and simple revocation and the decentralized design of passkeys, as well as the trust, privacy, and management challenges introduced by mechanisms designed to provide it.

6.2 Recommendations

Scale Beyond Per-Account Deletion. Manual passkey management is not a novel concern per se. For example, emerging mechanisms such as the WebAuthn Signal API [48] already aim to streamline credential cleanup by removing and preventing stale credentials in passkey providers. However, even with such support, our findings suggest that this model does not scale in practice. For synchronized passkeys, users may also "revoke access" by deleting them from their passkey provider. This enables removal even on inaccessible devices. However, an attacker in physical control of the stolen device may still evade the deletion attempt by disabling network access and then exporting the passkeys locally (e.g., on iPhone, with knowledge of the PIN via AirDrop [5]).

Users Favor Simple and Global Revocation. Participants consistently preferred low-effort approaches that enable global control, such as revocation codes or centralized services, and favored solutions that are simple, fast, and device-independent. Centralized models align well with these expectations, as they provide a clear and intuitive way to revoke access across accounts. At the same time, several participants raised concerns about such services becoming single points of failure, collecting sensitive data, and requiring additional trust. Our results suggest that effective mechanisms must bridge this gap, providing the usability benefits of global actions without introducing unnecessary central points of control.

Avoiding Technical and Social Failures. Users look for revocation options that work reliably in high-risk situations such as device

theft or account compromise. In these cases, revocation must be timely. Similar challenges exist for the Web PKI, where certificate revocation mechanisms suffer from latency, availability issues, and weak enforcement [21, 56]. Yet, the scale and distribution of passkeys differ, as credentials are spread across relying parties without central coordination. Our findings suggest that mechanisms must ensure reliable, decentralized coordination across the ecosystem.

Beyond technical failures, revocation may also introduce risks of misuse. Daffalla et al. [24], for example, show how abusive partners may abuse revocation in interpersonal threat scenarios, by removing a victim's access. This concern aligns with our findings, where participants identified account sharing and relationship breakdowns as plausible revocation scenarios. Revocation mechanisms should prevent silent lockout, for example, through clear notifications, recovery options, and safeguards against misuse.

Lessons from Passwords. Passwords and passkeys currently share a limitation: invalidating credentials across services requires users to act manually, service by service. For passwords, this means changing the credentials to prevent future use. However, prior work shows that users are often reluctant to change passwords [53, 77, 105], largely because the process is cumbersome and manual, and needs to be repeated across websites, often through different interfaces and requirements [12, 53]. A passkey mechanism that reproduces these usability problems is unlikely to see broad adoption. A key design challenge for future proposals is therefore to avoid the friction and burden still limiting password-change behavior today.

Semi-Automated Approaches. As discussed in Section 2.3, Smith et al. [89] propose a unified dashboard that interfaces with individual services to manage second factors. Applied to passkey revocation, such a dashboard could reduce the need to visit services individually. Because each relying party implements passkey management independently, this approach relies on service-specific scripts. Such script collections already exist in similar contexts [3, 81]. Replacing them with a common passkey-management API could make the approach more scalable, as discussed next.

Toward API-Based Passkey Management. Centralized solutions conflict with the decentralized design of passkeys and raise trust and privacy concerns. Instead, revocation should remain decentralized while presenting a unified interface to users. The WebAuthn Signal API [48] demonstrates that coordination between relying parties and passkey providers is feasible, suggesting a practical path to deploying more advanced revocation mechanisms. Extending this model to support bidirectional or user-initiated signaling could enable scalable revocation without requiring fundamentally new infrastructure. Standardized passkey management APIs could provide the foundation for such coordination, following efforts in the password ecosystem [26, 70]. However, partial deployment risks reproducing fragmentation, leaving users with a mix of automated and manual processes. Passkey providers are a natural integration point, as they already manage passkeys across devices and could integrate management and revocation APIs exposed by relying parties into a unified interface. Future mechanisms should therefore build on standardized APIs to enable decentralized coordination while shifting complexity away from users.

6.3 Limitations

Systematization. Not all proposals we analyzed were designed primarily as revocation mechanisms. Several focus on adjacent problems, such as account recovery, credential transfer, or key management, and treat revocation only as a secondary or implicit capability. Consequently, revocation components are often underspecified or not articulated as user-facing interactions. Despite our best efforts at abstraction, interpretations of the proposals may vary.

Online Survey. Survey results reflect best-case revocation intent rather than actual behavior, as hypothetical scenarios may overestimate follow-through under real-world constraints such as time pressure, competing priorities, uncertainty, or effort. We applied extensive filtering to detect AI-generated survey responses (Section 4.1). However, given the inherent limitations of such approaches, some AI-generated survey responses may remain.

Interview Study. Interview findings concern hypothetical rather than deployed mechanisms. Participants sometimes expressed initial support but hesitated when considering real-world use. Thus, our findings reflect perceived benefits and concerns, not evidence of adoption. We intentionally focused on a high-risk lost-device scenario, so findings may not generalize to lower-risk contexts with less urgent revocation. Future work should examine a broader range of scenarios. Although most participants had no IT background or technical passkey knowledge, recruiting passkey users might still select for individuals with greater technology affinity than the general population. Lastly, two participants (P07, P13) described experiences that suggest possible confusion between passkeys and password manager functionalities. For those, we excluded interview segments on passkey experience but retained contributions to the revocation-mechanism discussion, which followed a shared explanation of passkeys and revocation.

Finally, our US-only samples may not reflect other cultural or societal backgrounds, particularly regarding the eID mechanism. Additionally, survey and interview methods are also prone to social desirability biases, which we sought to mitigate by emphasizing our interest in participants' true opinions. Moreover, Prolific participants may not fully represent the broader population.

7 Conclusion

In this work, we investigated passkey revocation from both technical and user-centric perspectives. We systematized existing approaches into four user-facing mechanisms and conducted a mixed-methods study to examine when users claim they would revoke access and how they reason about different designs. Our results show that revocation intent closely follows perceived risk. Participants described current practices as cumbersome and unscalable, and no proposed mechanism clearly met user expectations. Instead, users reason about revocation as a trade-off between usability, security, and trust. This suggests that scalable revocation cannot rely on users manually visiting each relying party. Taken together, our findings suggest that usable passkey revocation requires (i) **simple, global** user actions, (ii) **decentralized coordination** that avoids introducing new trust assumptions, and (iii) **integration into passkey providers** to enable cross-account management.

Future mechanisms should build on standardized APIs that coordinate revocation across relying parties, passkey providers, and

authenticators while preserving the decentralized design of passkeys. Overall, our findings reveal a gap between users' willingness to revoke and their ability to do so effectively. Addressing this gap requires mechanisms that reduce user effort while preserving key security and privacy properties. As passkeys gain adoption, usable and scalable revocation will be essential in practice.

Acknowledgments

We thank Lars Richter for his contributions to the ideas and materials used in this study, and Lucjan Hanzlik for his expertise and advice on cryptographic matters, as well as his general feedback. We also thank our shepherd and the reviewers for their valuable and constructive feedback, which helped us improve the paper. Finally, we thank the participants for sharing their thoughts and experiences.

References

[1] AgileBits, Inc. 2026. Passkeys.Directory: A Community-Driven Index of Websites That Offer Signing in with Passkeys. https://passkeys.directory, as of September 14, 2026.

[2] Eman Alashwali, Ragashree Mysuru Chandrashekar, Mandy Lanyon, and Lorrie Faith Cranor. 2024. Detection and Impact of Debit/Credit Card Fraud: Victims' Experiences. In *European Symposium on Usable Security (EuroUSEC '24)*. ACM, Karlstad, Sweden, 235–260.

[3] Apple, Inc. 2020. Password Manager Resources. https://opensource.apple.com/projects/password-manager-resources/, as of September 14, 2026.

[4] Apple, Inc. 2026. iPhone User Guide: Remove Your Cards from Apple Pay If Your iPhone Is Lost or Stolen. https://support.apple.com/guide/iphone/iph3dd32dffe/, as of September 14, 2026.

[5] Apple, Inc. 2026. Share Passkeys Securely with Airdrop. https://support.apple.com/guide/iphone/iph0dd1796bb/, as of September 14, 2026.

[6] Sunpreet S. Arora, Saikrishna Badrinarayanan, Srinivasan Raghuraman, Maliheh Shirvanian, Kim Wagner, and Gaven Watson. 2022. Avoiding Lock Outs: Proactive FIDO Account Recovery using Managerless Group Signatures. *Cryptology ePrint Archive* 2022/1555 (Nov. 2022), 1–46.

[7] Paul Asadoorian. 2022. Firmware Security Realizations: Secure Boot and DBX. https://eclypsium.com/research/firmware-security-realizations-part-1-secure-boot-and-dbx/, as of September 14, 2026.

[8] Adam J. Aviv, John T. Davin, Flynn Wolf, and Ravi Kuber. 2017. Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Annual Conference on Computer Security Applications (ACSAC '17)*. ACM, Orlando, Florida, USA, 486–498.

[9] Tope Awotona. 2026. Calendly: Free Online Appointment Scheduling Software. https://calendly.com, as of September 14, 2026.

[10] Michael Backes, Lucjan Hanzlik, and Jonas Schneider-Bensch. 2019. Membership Privacy for Fully Dynamic Group Signatures. In *ACM Conference on Computer and Communications Security (CCS '19)*. ACM, London, United Kingdom, 2181–2198.

[11] Divyanshu Bhardwaj, Sumair Ijaz Hashmi, Katharina Krombholz, and Maximilian Golla. 2025. Understanding How Users Prepare for and React to Smartphone Theft. In *USENIX Security Symposium (SSYM '25)*. USENIX, Seattle, Washington, USA, 5987–6005.

[12] Arkaprabha Bhattacharya, Alaa Daffalla, Kevin Lee, Rosanna Bellini, Nicola Dell, and Thomas Ristenpart. 2026. Inconsistent, Incomplete, and Insecure: A Survey of Account Security Interfaces. In *USENIX Security Symposium (SSYM '26)*. USENIX, Baltimore, Maryland, USA, 5533–5552.

[13] Jenny Blessing, Daniel Hugenroth, Ross J. Anderson, and Alastair R. Beresford. 2025. SoK: Web Authentication and Recovery in the Age of End-to-End Encryption. In *Privacy Enhancing Technologies Symposium (PETS '25)*. PoPETS, Washington, District of Columbia, USA, 560–589.

[14] Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *IEEE Symposium on Security and Privacy (SP '12)*. IEEE, San Jose, California, USA, 553–567.

[15] Virginia Braun and Victoria Clarke. 2019. Reflecting on Reflexive Thematic Analysis. *Qualitative Research in Sport, Exercise and Health* 11, 4 (July 2019), 589–597.

[16] Virginia Braun and Victoria Clarke. 2021. One Size Fits All? What Counts as Quality Practice in (Reflexive) Thematic Analysis? *Qualitative Research in Psychology* 18, 3 (July 2021), 328–352.

[17] Virginia Braun, Victoria Clarke, and Nikki Hayfield. 2024. *Thematic Analysis: A Reflexive Approach* (4 ed.). SAGE Publications, London, United Kingdom, Chapter 8, 168–196.

[18] Andre Büttner and Nils Gruschka. 2025. Device-Bound vs. Synced Credentials: A Comparative Evaluation of Passkey Authentication. In *International Conference on Information Systems Security and Privacy (ICISSP '25)*. SciTePress, Porto, Portugal, 651–659.

[19] Jan Camenisch and Anna Lysyanskaya. 2002. Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials. In *Advances in Cryptology – CRYPTO 2002 (CRYPTO '02)*. Springer, Santa Barbara, California, USA, 61–76.

[20] Tim Cappalli, Akshay Kumar, Emil Lundberg, Matthew Miller, Pascoe, and Nina Satragno. 2026. Web Authentication: An API for Accessing Public Key Credentials – Level 3. https://www.w3.org/TR/2026/REC-webauthn-3-20260825/, as of September 14, 2026.

[21] Laurent Chuat, AbdelRahman Abdou, Ralf Sasse, Christoph Sprenger, David Basin, and Adrian Perrig. 2020. SoK: Delegation and Revocation, the Missing Links in the Web's Chain of Trust. In *European Symposium on Security and Privacy (EuroSP '20)*. IEEE, Virtual Conference, 624–638.

[22] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. 2008. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280. RFC Editor. 1–151 pages. https://datatracker.ietf.org/doc/html/rfc5280

[23] David A. Cooper. 1999. A Model of Certificate Revocation. In *Annual Computer Security Applications Conference (ACSAC '99)*. IEEE, Scottsdale, Arizona, USA, 256–264.

[24] Alaa Daffalla, Arkaprabha Bhattacharya, Jacob Wilder, Rahul Chatterjee, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. 2025. A Framework for Abusability Analysis: The Case of Passkeys in Interpersonal Threat Models. In *USENIX Security Symposium (SSYM '25)*. USENIX, Seattle, Washington, USA, 7819–7838.

[25] Alaa Daffalla, Marina Bohuk, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. 2023. Account Security Interfaces: Important, Unintuitive, and Untrustworthy. In *USENIX Security Symposium (SSYM '23)*. USENIX, Anaheim, California, USA, 3601–3618.

[26] Dashlane, Inc. 2021. Password Changer .well-known [DRAFT]. https://github.com/Dashlane/password-changer-well-known, as of September 14, 2026.

[27] Nurullah Demir, Yash Vekaria, Georgios Smaragdakis, and Zakir Durumeric. 2026. Keys on Doormats: Exposed API Credentials on the Web. In *ACM Conference on Computer and Communications Security (CCS '26)*. ACM, The Hague, Netherlands.

[28] Kai Dröge. 2025. noScribe v0.7: Free Interview Transcription with AI. https://noscribe.de/en/, as of September 14, 2026.

[29] Florian M. Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. 2020. "You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company. In *Symposium on Usable Privacy and Security (SOUPS '20)*. USENIX, Virtual Conference, 19–35.

[30] FIDO Alliance. 2018. WebAuthn and FIDO2. https://fidoalliance.org/fido-alliance-and-w3c-achieve-major-standards-milestone-in-global-effort-towards-simpler-stronger-authentication-on-the-web/, as of September 14, 2026.

[31] FIDO Alliance. 2022. FIDO Security Reference. https://fidoalliance.org/specs/fdo-security-requirements/FDO-security-requirements-v1.0-fd-20220913.html, as of September 14, 2026.

[32] FIDO Alliance. 2024. Passkeys. https://fidoalliance.org/passkeys/, as of September 14, 2026.

[33] FIDO Alliance. 2024. Remove Passkeys from Service Provider Account Settings. https://www.passkeycentral.org/design-guidelines/optional-patterns/remove-passkeys-from-service-provider-account-settings, as of September 14, 2026.

[34] FIDO Alliance. 2026. FIDO2 Specifications: Client to Authenticator Protocol. https://fidoalliance.org/specifications/download/, as of September 14, 2026.

[35] Anuj Gautam, Tarun Yadav, Garrett Smith, Kent Seamons, and Scott Ruoti. 2025. Passwords and FIDO2 Are Meant To Be Secret: A Practical Secure Authentication Channel for Web Browsers. In *ACM Conference on Computer and Communications Security (CCS '25)*. ACM, Taipei, Taiwan, 1859–1873.

[36] Shirley Gaw and Edward W. Felten. 2006. Password Management Strategies for Online Accounts. In *Symposium on Usable Privacy and Security (SOUPS '06)*. ACM, Pittsburgh, Pennsylvania, USA, 44–55.

[37] Mohammad Ghasemisharif, Amrutha Ramesh, Stephen Checkoway, Chris Kanich, and Jason Polakis. 2018. O Single Sign-Off, Where Art Thou? An Empirical Analysis of Single Sign-On Account Hijacking and Session Management on the Web. In *USENIX Security Symposium (SSYM '18)*. USENIX, Baltimore, Maryland, USA, 1475–1492.

[38] Maximilian Golla and Markus Dürmuth. 2015. Analyzing 4 Million Real-World Personal Knowledge Questions (Short Paper). In *International Conference on Passwords (PASSWORDS '15)*. Springer, Cambridge, United Kingdom, 39–44.

[39] Google, Inc. 2025. Android's Safety Features: What You Should Do If You Lose Your Phone. https://www.android.com/articles/what-to-do-if-your-phone-is-lost-or-stolen/, as of September 14, 2026.

[40] Lucjan Hanzlik, Julian Loss, and Benedikt Wagner. 2023. Token meets Wallet: Formalizing Privacy and Revocation for FIDO2. In *IEEE Symposium on Security and Privacy (SP '23)*. IEEE, San Francisco, California, USA, 1491–1508.

[41] Jan-Ulrich Holtgrave, Sabrina Klivan, Karola Marky, and Sascha Fahl. 2025. A Qualitative Study of Adoption Barriers and Challenges for Passwordless Authentication in German Public Administrations. In *ACM Conference on Human Factors in Computing Systems (CHI '25)*. ACM, Yokohama, Japan, 1090:1–1090:16.

[42] Michael Hölzl, Michael Roland, Omid Mir, and René Mayrhofer. 2018. Bridging the Gap in Privacy-Preserving Revocation: Practical and Scalable Revocation of Mobile eIDs. In *Symposium on Applied Computing (SAC '18)*. ACM, Pau, France, 1601–1609.

[43] Louis Jannett, Andreas Mayer, Maximilian Westers, Vladislav Mladenov, Christian Mainka, and Jörg Schwenk. 2026. The State of Passkeys: Studying the Adoption and Security of Passkeys on the Web. In *USENIX Security Symposium (SSYM '26)*. USENIX, Baltimore, Maryland, USA, 5039–5058.

[44] Markus Keil, Philipp Markert, and Markus Dürmuth. 2022. "It's Just a Lot of Prerequisites": A User Perception and Usability Analysis of the German ID Card as a FIDO2 Authenticator. In *European Symposium on Usable Security (EuroUSEC '22)*. ACM, Karlsruhe, Germany, 172–188.

[45] Michal Kepkowski, Lucjan Hanzlik, Ian Wood, and Mohamed Ali Kaafar. 2022. How Not to Handle Keys: Timing Attacks on FIDO Authenticator Privacy. In *Privacy Enhancing Technologies Symposium (PETS '22)*. PoPETS, Sydney, Australia, 705–726.

[46] Michal Kepkowski, Maciej Machulak, Ian Wood, and Dali Kaafar. 2023. Challenges with Passwordless FIDO2 in an Enterprise Setting: A Usability Study. In *IEEE Secure Development Conference (SecDev '23)*. IEEE, Atlanta, Georgia, USA, 37–48.

[47] Doowon Kim, Bum Jun Kwon, Kristián Kozák, Christopher Gates, and Tudor Dumitraş. 2018. The Broken Shield: Measuring Revocation Effectiveness in the Windows Code-Signing PKI. In *USENIX Security Symposium (SSYM '18)*. USENIX, Baltimore, Maryland, USA, 851–868.

[48] Eiji Kitamura. 2024. The WebAuthn Signal API. https://developer.chrome.com/docs/identity/webauthn-signal-api, as of September 14, 2026.

[49] Sabrina Klivan, Sandra Höltervennhoff, Nicolas Huaman, Yasemin Acar, and Sascha Fahl. 2023. "Would You Give the Same Priority to the Bank and a Game? I Do Not!" Exploring Credential Management Strategies and Obstacles during Password Manager Setup. In *Symposium on Usable Privacy and Security (SOUPS '23)*. USENIX, Anaheim, California, USA, 171–190.

[50] Paul C. Kocher. 1998. On Certificate Revocation and Validation. In *Financial Cryptography and Data Security (FC '98)*. Springer, Anguilla, United Kingdom, 172–177.

[51] Nikita Korzhitskii and Niklas Carlsson. 2021. Revocation Statuses on the Internet. In *Conference Passive and Active Measurement (PAM '21)*. Springer, Virtual Conference, 175–191.

[52] Alexander Krause, Jan H. Klemmer, Nicolas Huaman, Dominik Wermke, Yasemin Acar, and Sascha Fahl. 2023. Pushed by Accident: A Mixed-Methods Study on Strategies of Handling Secret Information in Source Code Repositories. In *USENIX Security Symposium (SSYM '23)*. USENIX, Anaheim, California, USA, 2528–2544.

[53] Alexander Krause, Jacques Suray, Lea Schmüser, Marten Oltrogge, Oliver Wiese, Maximilian Golla, and Sascha Fahl. 2026. An Analysis of the Security, Usability, and Automation Capabilities of Password Update Processes on Top-Ranked Websites. In *Symposium on Usable Privacy and Security (SOUPS '26)*. USENIX, Hannover, Germany, 1–20.

[54] Johannes Kunke, Stephan Wiefling, Markus Ullmann, and Luigi Lo Iacono. 2021. Evaluation of Account Recovery Strategies with FIDO2-based Passwordless Authentication. In *Open Identity Summit (ODI '21)*. GI, Copenhagen, Denmark, 59–70.

[55] Erwin Kupris and Thomas Schreck. 2026. The Passkey Promise: A Comparative Usability Study of MFA Methods. In *IEEE Symposium on Security and Privacy (SP '26)*. IEEE, San Francisco, California, USA, 3647–3666.

[56] Hyunsoo Kwon, Doowon Kim, Hodong Kim, Changhee Hahn, and Junbeom Hur. 2026. Certificate Revocation in the TLS Ecosystem: A Survey. *Comput. Surveys* 58, 7 (Feb. 2026), 178:1–178:36.

[57] Jorn Lapon, Markulf Kohlweiss, Bart De Decker, and Vincent Naessens. 2011. Analysis of Revocation Strategies for Anonymous Idemix Credentials. In *International Conference on Communications and Multimedia Security (IFIP CMS '11)*. Springer, Ghent, Belgium, 3–17.

[58] James Larisch, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. CRLite: A Scalable System for Pushing All TLS Revocations to All Browsers. In *IEEE Symposium on Security and Privacy (SP '17)*. IEEE, San Jose, California, USA, 539–556.

[59] Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. 2021. "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In *USENIX Security Symposium (SSYM '21)*. USENIX, Virtual Conference, 91–108.

[60] Leona Lassak, Nicklas Lindemann, and Marvin Kowalewski. 2025. From TOTPs to Security Keys: Studying the Reality of Passwordless FIDO2 Authentication With PIN and Biometrics in a Corporate Environment. In *Symposium on Usable Privacy and Security (SOUPS '25)*. USENIX, Seattle, Washington, USA, 371–389.

[61] Leona Lassak, Philipp Markert, Maximilian Golla, Elizabeth Stobert, and Markus Dürmuth. 2024. A Comparative Long-Term Study of Fallback Authentication Schemes. In *ACM Conference on Human Factors in Computing Systems (CHI '24)*. ACM, Maui, Hawaii, USA, 970:1–970:19.

[62] Leona Lassak, Elleen Pan, Blase Ur, and Maximilian Golla. 2024. Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication. In *USENIX Security Symposium (SSYM '24)*. USENIX, Philadelphia, Pennsylvania, USA, 7231–7248.

[63] Sean Lawlor and Kevin Lewi. 2023. WhatsApp: Key Transparency Overview. https://www.whatsapp.com/security/WhatsApp-Key-Transparency-Whitepaper.pdf, as of September 14, 2026.

[64] Jeongho Lee, Hyoung-Kee Choi, Jin Hee Yoon, and Seongjune Kim. 2023. An Empirical Analysis of Incorrect Account Remediation in the Case of Broken Authentication. *IEEE Access* 11 (Dec. 2023), 141610–141627.

[65] Yabing Liu, Will Tome, Liang Zhang, David Choffnes, Dave Levin, Bruce Maggs, Alan Mislove, Aaron Schulman, and Christo Wilson. 2015. An End-to-End Measurement of Certificate Revocation in the Web's PKI. In *Internet Measurement Conference (IMC '15)*. ACM, Tokyo, Japan, 183–196.

[66] Sanam Ghorbani Lyastani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. 2020. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. In *IEEE Symposium on Security and Privacy (SP '20)*. IEEE, Virtual Conference, 268–285.

[67] Philipp Markert, Leona Lassak, Maximilian Golla, and Markus Dürmuth. 2024. Understanding Users' Interaction with Login Notifications. In *ACM Conference on Human Factors in Computing Systems (CHI '24)*. ACM, Maui, Hawaii, USA, 853:1–853:17.

[68] Matthew McPherrin. 2025. Let's Encrypt: Decreasing Certificate Lifetimes to 45 Days. https://letsencrypt.org/2025/12/02/from-90-to-45, as of September 14, 2026.

[69] Microsoft, Corporation. 2025. Windows Secure Boot Certificate Expiration and CA Updates. https://support.microsoft.com/kb/5062710, as of September 14, 2026.

[70] Ricky Mondello and Theresa O'Connor. 2024. W3C Working Draft: A Well-Known URL for Changing Passwords. https://www.w3.org/TR/change-password-url/, as of September 14, 2026.

[71] Mozilla Developer Network. 2026. MDN Web Docs: WebAuthn Signal API. https://developer.mozilla.org/en-US/docs/Web/API/PublicKeyCredential/signalAllAcceptedCredentials_static, as of September 14, 2026.

[72] Tobias Mueller. 2022. Let's Re-Sign! Analysis and Equivocation-Resistant Distribution of OpenPGP Revocations. In *International Conference on Information Networking (ICOIN '22)*. IEEE, Jeju-si, South Korea, 34–39.

[73] Moni Naor and Kobbi Nissim. 1998. Certificate Revocation and Certificate Update. In *USENIX Security Symposium (SSYM '98)*. USENIX, San Antonio, Texas, USA, 217–228.

[74] Florian Nawrath. 2021. Quantitative Analysis of FIDO2 Client Support. In *Who Are You?! Adventures in Authentication Workshop (WAY '21)*. USENIX, Virtual Conference, 1–5.

[75] Lorenzo Neil, Elijah Bouma-Sims, Evan Lafontaine, Yasemin Acar, and Bradley Reaves. 2021. Investigating Web Service Account Remediation Advice. In *Symposium on Usable Privacy and Security (SOUPS '21)*. USENIX, Virtual Conference, 359–376.

[76] Sean Oesch, Scott Ruoti, James Simmons, and Anuj Gautam. 2022. "It Basically Started Using Me:" An Observational Study of Password Manager Usage. In *ACM Conference on Human Factors in Computing Systems (CHI '22)*. ACM, New Orleans, Louisiana, USA, 33:1–33:23.

[77] Sanghak Oh, Heewon Baek, Jun Ho Huh, Taeyoung Kim, Woojin Jeon, Ian Oakley, and Hyoungshick Kim. 2025. Understanding and Improving User Adoption and Security Awareness in Password Checkup Services. In *ACM Conference on Human Factors in Computing Systems (CHI '25)*. ACM, Yokohama, Japan, 386:1–386:32.

[78] Gurur Öndarö, Jonas Kaspereit, Samson Umezulike, Christoph Saatjohann, Fabian Ising, and Sebastian Schinzel. 2025. S/MINE: Collecting and Analyzing S/MIME Certificates at Scale. In *USENIX Security Symposium (SSYM '25)*. USENIX, Seattle, Washington, USA, 6737–6756.

[79] Kentrell Owens, Olabode Anise, Amanda Krauss, and Blase Ur. 2021. User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators. In *Symposium on Usable Privacy and Security (SOUPS '21)*. USENIX, Virtual Conference, 57–76.

[80] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why People (Don't) Use Password Managers Effectively. In *Symposium on Usable Privacy and Security (SOUPS '19)*. USENIX, Santa Clara, California, USA, 319–338.

[81] Jay Peters. 2021. Dashlane Is Giving Its One-Click Password Changer a Big Upgrade. https://www.theverge.com/2021/3/11/22320467, as of September 14, 2026.

[82] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2021. Why Older Adults (Don't) Use Password Managers. In *USENIX Security Symposium (SSYM '21)*. USENIX, Virtual Conference, 73–90.

[83] Tobias Reittinger and Günther Pernul. 2026. No Password, No Problem? A Large-Scale Field Study of Passkey Adoption and Usage. In *IEEE Symposium on Security and Privacy (SP '26)*. IEEE, San Francisco, California, USA, 3607–3626.

[84] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent E. Seamons. 2018. A Tale of Two Studies: The Best and Worst of YubiKey Usability. In *IEEE Symposium on Security and Privacy (SP '18)*. IEEE, San Francisco, California, USA, 872–888.

[85] Matthew Rosenfield. 2016. Signal: Safety Number Updates. https://signal.org/blog/safety-number-updates/, as of September 14, 2026.

[86] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. 2013. *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. RFC 6960. RFC Editor. 1–41 pages. https://datatracker.ietf.org/doc/html/rfc6960

[87] Fabian Schwarz, Khue Do, Gunnar Heide, Lucjan Hanzlik, and Christian Rossow. 2022. FeIDo: Recoverable FIDO2 Tokens Using Electronic IDs. In *ACM Conference on Computer and Communications Security (CCS '22)*. ACM, Los Angeles, California, USA, 2581–2594.

[88] Momoko Shiraishi and Takahiro Shinagawa. 2023. Poster: Toward Cloud-based FIDO Authentication with Secure Credentials Recovery. In *Annual Conference on Computer Security Applications (ACSAC '23)*. ACM, Austin, Texas, USA, 1–2.

[89] Garrett Smith, Tarun Yadav, Jonathan Dutson, Scott Ruoti, and Kent Seamons. 2023. "If I could do this, I feel anyone could:" The Design and Evaluation of a Secondary Authentication Factor Manager. In *USENIX Security Symposium (SSYM '23)*. USENIX, Anaheim, California, USA, 499–515.

[90] Elizabeth Stobert and Robert Biddle. 2014. The Password Life Cycle: User Behaviour in Managing Passwords. In *Symposium on Usable Privacy and Security (SOUPS '14)*. USENIX, Menlo Park, California, USA, 243–255.

[91] San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. 2013. Investigating Users' Perspectives of Web Single Sign-On: Conceptual Gaps and Acceptance Model. *ACM Transactions on Internet Technology* 13, 1 (Nov. 2013), 2:1–2:35.

[92] Alex Takakuwa. 2019. *Moving from Passwords to Authenticators*. Ph. D. Dissertation. University of Washington.

[93] Alex Takakuwa, Tadayoshi Kohno, and Alexei Czeskis. 2017. *The Transfer Access Protocol – Moving to New Authenticators in the FIDO Ecosystem*. Technical Report UW-CSE-17-06-01. University of Washington.

[94] Valentyna Tsap, Silvia Lips, and Dirk Draheim. 2020. Analyzing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia. In *Electronic Government and the Information Systems Perspective (EGOVIS '20)*. Springer, Bratislava, Slovakia, 69–88.

[95] Mark Turner, Martin Schmitz, Morgan Masichi Bierey, Mohamed Khamis, and Karola Marky. 2023. Tangible 2FA – An In-the-Wild Investigation of User-Defined Tangibles for Two-Factor Authentication. In *USENIX Security Symposium (SSYM '23)*. USENIX, Anaheim, California, USA, 245–261.

[96] Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. 2021. Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols. In *USENIX Security Symposium (SSYM '21)*. USENIX, Virtual Conference, 3811–3828.

[97] U.S. Department of Homeland Security. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/, as of September 14, 2026.

[98] U.S. Department of State. 2025. U.S. Passports: Statistics. https://travel.state.gov/content/travel/en/about-us/reports-and-statistics.html, as of September 14, 2026.

[99] W3C Web Identity & Credentials Adoption Community Group and the FIDO Alliance. 2026. Passkey Device Support: Synced Passkeys. https://passkeys.dev/device-support/, as of September 14, 2026.

[100] Brandon Willis-Arnold, Paul Vickers, and James Nicholson. 2025. Are Passkeys the Key? Older Adults' Perceptions of Passwordless Authentication. In *European Symposium on Usable Security (EuroUSEC '25)*. IEEE, Manchester, United Kingdom, 40–48.

[101] Leon Würsching, Florentin Putz, Steffen Haesler, and Matthias Hollick. 2023. FIDO2 the Rescue? Platform vs. Roaming Authentication on Smartphones. In *ACM Conference on Human Factors in Computing Systems (CHI '23)*. ACM, Hamburg, Germany, 68:1–68:16.

[102] Tarun Kumar Yadav and Kent Seamons. 2024. A Security and Usability Analysis of Local Attacks Against FIDO2. In *Symposium on Network and Distributed System Security (NDSS '24)*. ISOC, San Diego, California, USA.

[103] Yubico, Inc. 2014. Yubico: Yubico's Take on U2F Key Wrapping. https://www.yubico.com/blog/yubicos-u2f-key-wrapping/, as of September 14, 2026.

[104] Yubico, Inc. 2026. Yubico: WebAuthn Deployment Best Practices. https://developers.yubico.com/WebAuthn/WebAuthn_Developer_Guide/Best_Practices.html, as of September 14, 2026.

[105] Yixin Zou, Khue Le, Peter Mayer, Alessandro Acquisti, Adam J. Aviv, and Florian Schaub. 2024. Encouraging Users to Change Breached Passwords Using the Protection Motivation Theory. *ACM Transactions on Computer-Human Interaction* 31, 5 (Nov. 2024), 63:1–63:45.

A Open Science

In alignment with the guidelines of open science, we provide the artifacts to support the work we conducted, in order to make it reproducible and verifiable by the community. Below we provide a list of the artifacts that are available at the following link: https://doi.org/10.5281/zenodo.22307146.

- **Consent Form for the Survey.** The consent form participants have to agree to in order to proceed with the survey.
- **Consent Form for the Interview.** The consent form participants have to agree during the pre-interview questionnaire in order to proceed with the interview.
- **Survey Instrument.** The complete structure of the survey taken by participants on Qualtrics
- **Survey Codebooks.** The qualitative analysis for the open answers to the questions **R2-1**, **R2-2**, **R3-1**, **R3-2**.
- **Survey Data.** The data collected from the survey, as well as the data used for the stacked bar plots and the demographics.
- **Interview Guide.** The full guide that was used to conduct the interviews.
- **Interview Codebook.** The qualitative analysis of the interviews.

Moreover, we decided not to share the following artifacts:

- **Raw Survey Data from Qualtrics.** This dataset contains sensitive information, such as participants' Prolific IDs and potentially de-anonymizing responses.
- **Interview Recordings and Transcripts.** In compliance with the data policy we presented to participants in the consent form for the interviews, we decide not to share interview recordings and transcripts. Moreover, in the interviews participants may have shared personal experiences that affected them or some of their loved ones. Therefore, only the interview codebook is going to be shared as it is believed to be a faithful representation of the content of the interviews.

B Ethical Considerations

Stakeholders. We identify several stakeholders affected by this work, including study participants, end users, service providers implementing passkeys and passkey revocation mechanisms, and relevant standardization bodies such as the FIDO Alliance.

Study participants are directly involved in the research process, while end users may be affected by the security and usability of revocation mechanisms.

Service providers and standardization bodies are responsible for designing and deploying such mechanisms, and may be impacted by the recommendations derived from this work.

Potential Impacts. Our research could result in several potential impacts on these stakeholders. For study participants, the main risk is represented by potential re-identification of de-identified data, as well as possible discomfort when discussing personal or sensitive experiences related to passkey revocation.

When it comes to end users, implications of our work are substantial, as lacking to address the development of global and usable revocation mechanisms could result in millions of accounts, and therefore end users, being affected in the foreseeable future.

However, we recognize that revocation could also be weaponized in contexts such as intimate partner violence (IPV), as mentioned by Daffalla et al. [24] and as discussed in Section 6, being utilized as an abuse vector to lock the victim out of their own accounts.

Mitigation Measures. To mitigate these risks, we implemented several safeguards throughout the research process.

Our institution's ethical review board (ERB) approved our study design, survey materials, and interview guidelines. The interview and survey study were approved individually.

Throughout the research, we took steps to minimize the collection of personally identifiable information (PII) and restricted access to non-anonymized data to a limited number of individuals. We ensured that all data storage and processing complied with GDPR requirements. We followed the Menlo report [97] and determined that de-identifying participants was the primary threat to their safety. Hence, multiple safeguards were put in place:

- During the interview scheduling process, we ensured that we did not collect personal information, such as name and email address.
- We only collected the audio of the interview, and we did so after receiving explicit consent by the participants at the beginning of the interview.
- We used GDPR-compliant software to record the interviews and transcribe the audio.

The topics discussed the interviews rarely touched the participants' sensitivity. However, in the few cases that the participants reported intimate personal experiences regarding passkey revocation, or a lost or stolen device, we reassured them that they were under no obligation to share further details if they didn't feel comfortable doing so.

To address the aforementioned societal risks, we derive and present design recommendations aimed at preventing the misuse of revocation mechanisms (see Section 6), for example by suggesting to introduce safeguards against unauthorized or coercive revocation.

Justification of Research. We believe that conducting and publishing this research is justified by the need to address the issue of passkey revocation, and to bring the attention of the service providers and FIDO Alliance to the topic. By identifying potential misuse and abuse of passkey revocation, this work provides significant contribution to the design of safer and more usable authentication systems. The potential benefits of the outcomes of our research outweigh the identified ethical risks, which have been mitigated thanks to the measures described above.

C Survey Instrument

Study 1: Passkey Familiarity and Revocation Scenarios

Important Note on AI Use
This survey is intended to collect your personal views and experiences. The use of AI tools (e.g., ChatGPT, Copilot, etc.) to generate answers is not allowed! Submissions that appear to be AI-generated or lack genuine personal input will not be approved or compensated in Prolific. As long as you answer honestly and in your own words, there's nothing to worry about. Thank you for your cooperation!

Consent Form
Thanks a lot for your interest to participate in this study. Before we can start, please take a minute to read our consent form and confirm that you are eligible and willing to participate in this study.

By giving your consent below, you confirm that
- you are at least 18 years old
- you have read or have been read this declaration of consent and information on data protection[1]
- your questions on this have been answered to your satisfaction
- you are voluntarily participating in this survey

[1] *The full consent form is left out for space reasons.*

○ Yes, I consent to participate in this survey.
○ No, I do not consent to participate in this survey.

Account/Internet Usage
First, we would like to learn about some general aspects surrounding your internet and account usage. There are no right or wrong answers - we are interested to learn how you behave in real life, not how you think you should behave! Please note: When we talk about "logging in to an account" we refer to logins on websites such as your Gmail, your Amazon, or your online banking account. This does not include logging in to your computer when you turn it on or typing your PIN to unlock your phone.

AA Please confirm that you have understood what we mean by "logging in to an account" by selecting the correct answer below. "Logging in to an account" means...
○ Typing my PIN to unlock my phone ○ Logging in on websites such as my Gmail, my Amazon, or my online banking
○ Logging in to my computer

A1 Great, now let's begin with the questions. Think about your average day. Approximately, how often do you log in to your accounts manually, meaning you type in your password (instead of it being automatically filled in for you)?
○ More than 10 times per day ○ More than 5 times per day
○ About 3 times per day ○ About once every day
○ Once every other day ○ Once a week
○ Once every two weeks ○ Once a month ○ Once a year
○ I never log in manually

A2 Do you use a password manager?
A password manager is any tool that stores and manages your passwords and can fill in login forms automatically. This includes the password storage integrated in your browser (e.g., passwords saved in Chrome, Edge, Firefox, etc.), password storage provided by your operating system (e.g., Apple's Passwords App/iCloud Keychain), and third-party services (like 1Password, Bitwarden, or LastPass).
○ Yes ○ No ○ I don't know

*If participant selected "Yes" in **A2**:*

A2-yes Which type of password manager do you use? (You can select multiple answers)
□ The password manager provided by my browser (e.g., Chrome, Edge, Firefox) □ The password manager provided by my operating system (e.g., Apple's Passwords app/iCloud Keychain)
□ A third-party password manager (e.g., 1Password, Bitwarden, LastPass) □ Other: _____

*If participant selected "No" in **A2**:*

A2-no How do you usually keep track of your passwords?
○ I remember them ○ I write them down on paper
○ I write them down digitally (i.e., in the notes app)
○ Someone else keeps track of them for me ○ Other: _____

*If participant selected "I don't know" in **A2**:*

A2-uns. How do you usually keep track of your passwords?
Answer: _____

A3 Do you share accounts with others?
○ Yes ○ No ○ I don't know

*If participant selected "Yes" in **A3**:*

A3-yes-1 With whom do you share accounts? (You can select multiple answers)
□ Partner □ Friends □ Children □ Parents
□ Other family members □ Co-workers □ Others: _____

*If participant selected "Yes" in **A3**:*

A3-yes-2 What type of accounts do you share with others? (You can select multiple answers)
□ Mail □ Banking □ Shopping □ Streaming/Video
□ News/Blogs/Information □ Social Media □ Other: _____

A4 Think of your online accounts. In the account settings, many websites show which devices are currently logged in. On average, how often do you check which devices are logged in on your accounts?
○ Once a week ○ Once a month ○ Every six months
○ Once a year ○ Rarely ○ Never ○ Other: _____

*If participant did **not** selected "Never" in **A4**:*

A4-1 For which type of account do you check which devices are logged in? (You can select multiple answers)
□ Mail □ Banking □ Shopping □ Streaming/Video
□ News/Blogs/Information □ Social Media □ Other: _____

A5 Have you ever suspected that someone knows your password, or were you worried that someone might have unwanted access to one of your accounts?
○ Yes ○ No

*If participant selected "Yes" in **A5**:*

A5-yes Did you take any action when you suspected that someone knows your password, or you were worried that someone might have account access?
○ Yes - Why?: _____ ○ No - Why not?: _____

A6 On average, how regularly do you buy new devices? Devices could be a phone, laptop, tablet, or any other device that has an account associated with it (i.e., smart TVs).
○ Several times a year ○ 1-2 times per year ○ Less than once a year ○ Every three years ○ Every five years ○ Almost never

A7 Do you reset your devices before selling or giving them away? A device could be a phone, laptop, tablet, or any other device that has an account associated with it (i.e., smart TVs).
○ Yes, I reset every time ○ Yes, but I do not reset every device
○ I have reset a device before but don't do it regularly
○ I have never reset a device

A8 Have you ever switched the operating system or vendor of your devices? For example from Samsung to Apple, from Windows to macOS, or vice versa.
○ Yes ○ No ○ I don't know

A9 Have you ever changed or adjusted any security settings in one of your online accounts? (e.g., enabling two-factor authentication, checking active sessions, or setting up recovery options like phone number)
○ Yes ○ No ○ I don't know

*If participant selected "Yes" in **A9**:*

A9-yes Which of the following security features have you used or adjusted? (You can select multiple options)
□ Two-factor authentication (2FA)
□ Viewing or managing logged-in devices
□ Setting up account recovery options
□ Security alerts or login notifications
□ Session timeout settings □ Password change or reset
□ I don't remember □ Other: _____

Familiarity with Passkeys
Next, we would like to learn more about your experience with a new login method known as "Passkeys".

P1 Have you ever heard of passkeys or FIDO2 before?
○ Yes ○ No ○ I don't know

*If participant selected "Yes" in **P1**:*

P1-yes Briefly explain what you know about passkeys.
○ Answer: _____

*If participant selected "Yes" in **P1**:*

P2 Have you ever used passkeys to login to an account?
○ Yes ○ No ○ I don't know

*If participant selected "Yes" in **P2**:*

P2-yes-1 How often do you use passkeys?
○ I use them anywhere it is possible ○ I use them every now and then ○ I just tried it once but don't use them regularly
○ Other: _____

*If participant selected "Yes" in **P2**:*

P2-yes-2 On which accounts have you already used passkeys? (You can select multiple answers)
□ Mail □ Banking □ Shopping □ Streaming/Video
□ News/Blogs/Information □ Social Media □ Other: _____

Revocation
Next, we will continue with the topic of revocation, which is the main focus of our study. Please pay special attention to these questions as they are very important for our research.

First, we would like to explain what exactly we mean by revocation. Please take a minute to read this brief introduction.

Revocation
Generally speaking, revocation is the process of canceling a previously granted permission. Here's a simple example: Imagine you have a key card that lets you into your office building. If you leave the company or your key card gets lost or stolen, the security team can revoke this key card, meaning the card will no longer work to open the doors.

In the context of account logins, revocation means invalidating the access to an account. For example, if you forget your password, or it gets compromised, you might reset it. The old password is revoked, meaning it can no longer be used to access your account.

You can also revoke access only for certain users, such as friends/family that you don't want to continue sharing accounts with or devices you no longer use accounts on.

RA Please confirm that you have understood what we mean by "revocation" for accounts. "Revocation" means...
○ Deleting my account ○ Returning my key card ○ Invalidating the access to an account ○ Sharing accounts with my family or friends

On the following pages, we describe scenarios where revocation could be considered. We are interested in learning whether you think revocation is necessary in those scenarios.

Note: There are no right or wrong answers - we are interested to learn how you would behave in real life, not how you think you should behave.

In some scenarios, we refer to a "legitimate" email. This means that the email you receive actually comes from the service you use and contains accurate information. It is not phishing or spam.

R1 For each scenario below, please indicate how likely you would be to revoke the access to your account.
Remember: There are no right or wrong answers!
For every scenario, the participant had to rank the likelihood of revocation on the following Likert scale:
○ Very unlikely to revoke ○ Somewhat unlikely to revoke ○ Neither likely nor unlikely to revoke ○ Somewhat likely to revoke
○ Very likely to revoke

The scenarios were the following:
○ **Stolen Device:** Your device has been stolen. You are logged in to all of your accounts on that device, and the thief knows your PIN.
○ **Security Checkup:** During a check-up of one of your accounts, you see that a device that you do not use anymore is still logged in.
○ **Hacked PWM:** You use a service that stores all your passwords for you so you don't have to remember them. You receive a legitimate email from the service telling you they have been hacked and your passwords might have been leaked.
○ **Shared w. Friend:** You shared your streaming account with a friend. Now they don't want to use it anymore and no longer pay their share of the subscription fee but they are still logged in on their devices.

○ **Shared w. Partner:** As many couples do, you and your partner shared some accounts and both of you know the passwords to these accounts. You now broke up with this partner.
○ **Offboarding:** You quit your job and have to return your work laptop to the company. You are still logged into some of your personal accounts on this device.
○ **Compromised Account:** You receive a legitimate email from a service where you have an account. They tell you that your account has been hacked.
○ **Public Computer:** You used a shared computer in a public library and accidentally clicked on "store password" when you logged in to one of your accounts.
○ **Unused Account:** You made an account on a shopping list website that helps you plan your groceries but did not end up using it.
○ **Old Device:** You got a new device and put the old one in a drawer. It's still signed in, but you're not using it anymore.

Now, we would like to learn more about your thoughts on revocation. We have selected two of the scenarios you just ranked. Please explain your reasoning in more detail.

We picked two scenarios from the previous question at random and used it for the next question:

R2-1 Scenario: *{Scenario 1}*. You answered that you would be *{Likelihood 1}*. Why is that? ○ Answer: _____

R2-2 What do you think is the worst that could happen if you do **not** revoke access in this situation? ○ Answer: _____

R3-1 Scenario: *{Scenario 2}*. You answered that you would be *{Likelihood 2}*. Why is that? ○ Answer: _____

R3-2 What do you think is the worst that could happen if you do **not** revoke access in this situation? ○ Answer: _____

R4 Lastly, let's have a look at all the situations again.
How much effort do you think would it take to revoke access in these situations?
For every scenario, the participant had to rank the effort of revocation on the following Likert scale:
○ Very easy ○ Easy ○ Neither easy nor difficult ○ Difficult ○ Very difficult

R5 How serious do you consider these situations to be? (e.g., in terms of potential consequences such as data loss, misuse, or loss of control) *For every scenario, the participant had to rank the serious of the scenario on the following Likert scale:*
○ Not at all serious ○ Somewhat not serious ○ Neither serious nor not serious ○ Somewhat serious ○ Very serious

Demographics

Finally, we would like some demographic information.

D1 How old are you?
○ 18–24 ○ 25–34 ○ 35–44 ○ 45–54 ○ 55–64 ○ 65–74 ○ 75+
○ Prefer not to answer

D2 What gender do you identifiy with?
○ Woman ○ Man ○ Non-binary
○ Prefer to self-describe: _____
○ Prefer not to answer

D3 What is the highest degree or level of school you have completed?
○ No schooling completed ○ Some high school, no diploma
○ High school graduate, diploma, or equivalent ○ Some college
○ Trade, technical, or vocational training ○ Associate's degree
○ Bachelor's degree ○ Master's degree ○ Professional degree
○ Doctorate ○ Prefer not to answer
○ Other (please specify): _____

D4 Which of the following best describes your educational background or job field?
○ I have an education in, or work in, the field of computer science, computer engineering or IT. ○ I do not have an education in, nor do I work in, the field of computer science, computer engineering or IT. ○ Prefer not to answer

End of Study

Thank you for participating in our study. You can now head back to Prolific by following the link below.

D Demographic Table for Survey Participants

Table 3: Demographics of Survey Participants (n = 308).

	Count	(%)
Age		
18–24	40	13
25–34	52	17
35–44	50	16
45–54	51	16
55–64	48	16
65–74	61	20
75+	6	2
Gender		
Woman	157	51
Man	148	48
Non-Binary	3	1
Education		
Low[1]	19	6
Medium[2]	165	54
High[3]	124	40
IT Background		
Yes	77	25
No	222	72
No answer	9	3

[1] "No schooling completed", "Some high school, no diploma."
[2] "High school graduate, diploma, or equivalent", "Some college", "Trade, technical, or vocational training."
[3] "Associate's degree", "Bachelor's degree", "Master's degree", "Professional degree", "Doctorate."

E Regression Analysis

Table 4: Results of the Linear Mixed-Effects Model Predicting Revocation Likelihood.

Parameter	Estimate	95% CI	p
Fixed Effects:			
Intercept	4.28	[3.90, 4.66]	$< .001$
Perceived Effort	-0.04	[-0.08, -0.01]	.007
Perceived Severity	0.24	[0.21, 0.28]	$< .001$
Effort × Severity	0.00	[-0.02, 0.02]	.813
Random Effects (Standard Deviation):			
Intercept: Participants	0.37		
Intercept: Scenarios	0.60		

F Survey Codebook – Revocation Intent Explanation

Codes	Description
Reasons to Revoke	The participant expresses reasons why they would revoke in the given scenario
Protect privacy	Prevent exposure or misuse of personal information
Public computer	Avoid residual access on shared or untrusted devices
Security risk	Mitigate perceived or potential compromise or threats
No right/need for continued access	Remove unnecessary or outdated permissions
Relationship status	Reflect changes in personal or professional relationships
Device changes owner	Revoke access after transfer or resale of device
No future use	Remove credentials that are no longer needed
Negative past experience	Act based on prior security or privacy incidents
Best practice/common sense	Follow general security hygiene practices
Physical access	Prevent misuse by someone with physical device access
Prevent	The participant mentions situations they aim to prevent by resorting to revocation
Account misuse/takeover	Avoid unauthorized control of accounts
Blackmail/revenge	Prevent malicious or coercive personal exploitation
Financial loss/abuse	Avoid fraud or unauthorized transactions
Identity theft/impersonation	Prevent misuse of identity or credentials
Personal/sensitive data leak/theft	Protect confidential or private data
Sharing account with third persons	Avoid unintended access propagation
Online abuse (snooping, stalking)	Prevent invasive monitoring or harassment
Prevent Access To	The participant mentions assets they aim to prevent access to by resorting to revocation
Account(s)	Restrict access to user accounts
Banking	Protect financial services and funds
Browser history	Hide browsing activity
Email/Messages	Protect private communications
Sensitive/personal data/info	Secure confidential data
Prevent Access By	The participant mentions actors they aim to prevent getting access to their assets
Others/strangers	Block unknown or unauthorized individuals
Work-related actors	Restrict colleagues or organizations
Ex-partner	Prevent access by former partners
Housemates	Limit access by cohabitants
New owner/next user	Block access by future device users
Thief	Prevent access by a device thief
Reasons Not to Revoke	The participants expresses reasons why they would not revoke in the given scenario
Automatic account deletion/session timeout	Rely on built-in expiration mechanisms
Burglary unlikely	Low perceived risk of theft
Device gets wiped	Expect data removal via reset
Routinely changes passwords	Trust existing security habits
Still in possession	Maintain control over device
No priority	Low urgency to act
No sensitive data/info	Limited perceived impact
Potential future use	Keep access for convenience
Inconvenience/effort	Avoid time or effort required
No/low risk	Minimal perceived threat
Relationship status	Reflect changes in personal or professional relationships
Additional Steps	The participant mentions security steps they would go through in addition to revocation
Revocation for other accounts	Extend action across related services
Update important accounts	Strengthen security of critical accounts
Alternative Action	The participant mentions actions they would perform instead of revocation
Delete account	Permanently remove the account
Delete password from computer	Remove stored credentials
Establish recovery plan	Prepare backup recovery options
Just log out	End current sessions
Monitor account activity	Track for suspicious behavior
Remove device from account settings	Deauthorize specific devices
Verify extent of breach	Assess impact before acting

G Survey Codebook – Revocation Intent Worst Case

Codes	Description
Access To	The participant mentions the assets an attacker may have access to if they do not revoke
Account(s)	Access to user's online accounts and services
Apps	Access to installed or linked applications
Banking	Access to financial accounts and transactions
Personal/confidential information	Access to sensitive personal data (e.g., ID, health)
Credit card information	Access to stored payment and card details
Device	Access to the physical device and its contents
Email	Access to email accounts and communications
Files/documents	Access to stored files and documents
Friend's device	Access through a device owned by someone else
Login details	Access to usernames, passwords, or credentials
Damage	The participant mentions the type of damage if they do not revoke
Abuse of subscription	Unauthorized use of paid services or benefits
Account takeover/misuse	Unauthorized control or use of an account
Anything one can imagine	Broad, unspecified potential harm
Blackmailing	Coercion using sensitive or private information
Company information leaked	Exposure of confidential business data
Damaged reputation	Harm to personal or professional image
Device lost/stolen	Loss of control over the physical device
Emotional damage	Psychological distress or discomfort
Famil in peril	Risk or harm extending to family members
Financial loss/abuse	Monetary loss, fraud, or unauthorized spending
Forget about account	Loss of access due to missing credentials
Hacking	Unauthorized intrusion into systems or accounts
Identity theft/impersonation	Misuse of identity for fraudulent purposes
Inconvenience	Effort, or loss of time
Non-sensitive information leaked	Exposure of less critical personal data
Password leaked/stolen	Compromise of authentication credentials
Personal information leaked/stolen/misused	Exposure or misuse of sensitive data
Data deleted/lost	Permanent loss of stored information
Privacy violation	Unauthorized access to personal/private data
Relationship problems	Conflict caused by misuse or exposure
Online abuse (scam, snooping, spam, stalking)	Harmful online behaviors
Unfairness	Perceived unjust or disproportionate use of online accounts
Prerequisite	The participant mentions additional conditions necessary for the worst case to happen
Theft	Device is stolen by another party
Device lost/stolen	Loss of control over the physical device
Device sold/given away	Ownership transferred to another person
Forget account	User forgets login or account information
Hacking	Unauthorized intrusion into systems or accounts
Physical device access	Someone can directly use the device
Site gets hacked	Service provider suffers a security breach
Who	The participant mentions the actor that they believe would be responsible
Anyone	Any individual, regardless of relationship
Close relationship (ex-partner, friend, family member)	Trusted or previously trusted person
Housemate	Person sharing the same living space
Malicious actor (scammer, hacker, thief)	Individual with harmful intent
Other device owner/user	New or secondary user of the device
Someone	Unspecified or unknown individual
Someone at company	Insider within the work environment
Someone with physical device access	Person holding or using the device
The website	The service or platform itself
Unauthorized person	Individual without legitimate permission

H Interview Guide

Part	Section	Goal	Questions
1	Greetings and Consent	Warming up. Asking for the participant's permission to record the audio of the interview.	Hello, thank you for joining our study. Can you hear and see me properly? If you feel comfortable, I would appreciate it if you could turn on your camera, but it is not required. As mentioned in the consent form, we will audio record this session. We will not record the video. Please let me know if you are okay with me starting the audio recording now.
2	Introduction	Providing the participant with an overview of the interview.	Do you have any questions before we start? First of all, I would like to highlight: This isn't a test, there are no wrong answers. Instead, we are here to understand your thoughts, expectations, and preferences, so please share whatever is on your mind. The interview consists of two main parts: First, we will talk a bit about your familiarity with passkeys, and then we will talk about how you can manage and remove your passkeys in certain situations. Any questions before we start?
3	Passkey Familiarity	Making sure that the participant is in fact a passkey user. Get information on the participant's passkey usage habits.	**Passkey use** Great! So, you mentioned you have used passkeys before, right? • Where did you use them? • For what type of accounts? • Do you use the, regularly or just as a "one time" thing? • Do you use them for personal or professional purpose? **Experiences** • How have you liked passkeys so far? • Have you encountered any issues? If so, how did you overcome them? • Have you ever decided against enabling passkeys when they were offered to you? If so, for which accounts and why? • Are there accounts where you would not use them? • Cross-device/cross-platform: Do you use multiple ecosystems (e.g., Android + Mac)? Have you ever tried login on multiple of those devices? • Comparison with other login mechanisms used in the past (just passwords, 2FA with SMS OTP, 2FA with TOTP) **Passkey mechanism knowledge** • How familiar do you feel with how passkeys work? • **Mental model** – In your own words, what do you think a passkey is? – Where do you think your passkeys are stored? – Please (try to) explain what you think happens when you log in with a passkey – Where do you think biometrics are stored? – If you got a new device, how would you expect to get your passkeys onto it? ***[Optional, depending on the participant's knowledge on the topic]*** We are going to show you a brief definition of passkeys as well as a high-level explanation of how passkeys work. *Passkeys are a new way to sign in to websites without using a password. Instead, your device, for example your phone or computer, creates a digital key, which is stored securely on your device. To sign in, you use the same steps that you use to unlock your device, for example, a fingerprint, face recognition, or a PIN. In the background, a cryptographic method ensures you are securely signed in to the website. Passkeys can also be synchronized across your devices.*
4	Revocation	Introducing and establishing a shared understanding of revocation. Collecting participants unbiased initial thoughts on revocation for passkeys.	Have you ever heard the term "revocation"? If so, what do you consider as revocation? To make sure everyone has the same understanding of the term, please read the following definition. Afterwards, we can talk about it more and answer any questions you might have. Just let me know when you finish reading. *On a high level, revocation means taking away a permission that was given before. Revocation can take place in various different situations, also in the context of online accounts, but here is a simple example from the physical world:* *Imagine you have a key card to get into your office building. If you leave the job or lose the card, the company can stop the card from working, or in other words, revoke the card. That way, no one can use it any longer to enter the building.* *In comparison, in the digital world, for account logins, revocation simply means stopping someone (or something) from getting into your account by removing the permission to log in that was previously granted. You could, for example, revoke access for certain people, like friends or family, whom you shared an account with but no longer want to have access. Or you could revoke access for an old device by logging it out and removing it from the account, so it cannot be used to access your account anymore.*

Part	Section	Goal	Questions
4	Revocation	Introducing and establishing a shared understanding of revocation. Collecting participants unbiased initial thoughts on revocation for passkeys.	• Do you have any idea if and when you would have to use revocation with passkeys? • Are there situations where you could imagine it would be important to revoke a passkey? • If you think of your personal passkeys and the situations you just mentioned, what practical steps would you follow in order to revoke a passkey?
5	Discussing Revocation Mechanisms	Communicating the high level concept of the different mechanisms and collecting first impressions and concerns.	***Initial Scenario*** Imagine you have a phone, and you have several accounts for which you have passkeys stored on this phone. Now imagine that you lost your phone. In that case, you would need to revoke the passkeys stored on the device to prevent anyone from potentially being able to access your accounts. We are going to present you the first option, which represents what you would need to do as of now, and four alternative mechanism. ***0. Baseline*** If you now want to revoke the access to your accounts on your lost phone, you need to log into each and every one of your accounts individually on another device. There you would need to go into the security settings and find the section for your logins. You then click on "delete" for that passkey. If you want to, for example, make sure that you can still access the account from a new device, you have to register a new passkey on that new device. • Would you be able to list all services for which you have activated passkeys right now? • Imagine a scenario where passkey are as widespread as passwords are right now. How would you keep track of the accounts you have? How difficult would that be? ***1. Revocation Code*** With this revocation mechanism, you would have a very long number associated to each of your devices. In case your phone is lost, you can use the number associated to your phone to automatically revoke all the passkeys stored on it. • Where would you store this number? ***2. Backup Device*** In the case of this mechanism, you would have a backup device that can be used to revoke the passkeys that are stored in your phone. However, in order to revoke the passkeys on your phone, you would have to manually log into each account, for which you have passkeys on your lost phone, with the backup device. • What would your preference be for this device? • Would you prefer a device that you carry around with you at all times or would you prefer to leave that device at home? ***3. Centralized Service*** With this revocation mechanism, you would have an account on an online service. This service keeps track of all the passkeys deployed for a certain device,. In case of a lost device, you can access this account from another device and revoke all the passkeys associated to the device you lost. • Do you have any thoughts on the fact that this service knows the websites on which you have accounts? • What do you think about the centralized nature of this service? ***4. Electronic ID or Passport*** With this mechanism, you would use your electronic ID or passport in order to generate passkeys for your accounts. In case you lost this document, you would need to report it as stolen in order to revoke the passkeys that are associated to it. • Do you have any thoughts associated to using a document to generate passkeys? • How do you think the revocation process would look like? • Do you have any thoughts about the involvement of the authorities in the revocation process?
6	Final Mechanism Comparison and Interview Wrap-up	Collecting final considerations on the mechanisms and passkey revocation in general.	After having seen and discussed all the revocation mechanism, do you have any final consideration on them? Is there one in particular that caught your attention? Could you please rank them according to your opinion and impression about them? Do you have any final remarks? Thank you so much for taking part in our study. We greatly appreciate your contribution.

I Demographics and Passkey Usage for the Interviews

Table 7: Participant Demographics and Passkey Usage ($n = 20$).

ID	Age	G	Education	IT Backgr.	Accounts with Passkeys	Passkey Usage Frequency
P01	25–34	M	Bachelor's Degree	No	Mail, Banking, Shopping	Anywhere Possible
P02	35–44	W	Associate Degree	No	Mail, Banking, Shopping, Streaming, Social Media	Anywhere Possible
P03	25–34	M	Some College	No	Mail, Banking	Every Now and Then
P04	55–64	M	Some College	Yes	Mail, Shopping	Anywhere Possible
P05	25–34	M	Some College	NA	Mail, Banking	Every Now and Then
P06	65–74	M	Master's Degree	No	Banking	Tried Once
P07	35–44	M	Master's Degree	No	Banking, Shopping	Every Now and Then
P08	45–54	W	Bachelor's Degree	No	Mail, Banking, Shopping, Social Media	Anywhere Possible
P09	55–64	W	Vocational Training	No	Banking, Shopping	Every Now and Then
P10	55–64	W	Bachelor's Degree	No	Mail, Banking	Every Now and Then
P11	35–44	M	Master's Degree	NA	Banking, Social Media	Every Now and Then
P12	45–54	W	NA	NA	Mail, Banking, Shopping, Streaming, News, Social Media	Anywhere Possible
P13	35–44	M	Master's Degree	Yes	Mail, Banking, Shopping, Streaming, News, Social Media	Anywhere Possible
P14	18–24	M	Bachelor's Degree	Yes	Mail, Banking, Shopping, Social Media	Anywhere Possible
P15	55–64	W	Bachelor's Degree	No	Banking	Every Now and Then
P16	25–34	M	Bachelor's Degree	No	Mail, Social Media	Every Now and Then
P17	65–74	W	Associate Degree	No	Banking	Anywhere Possible
P18	18–24	M	No Diploma	No	Mail, Banking, Shopping, Streaming, News, Social Media	Anywhere Possible
P19	25–34	M	Bachelor's Degree	No	Mail, Banking, Shopping, Social Media	Anywhere Possible
P20	35–44	W	High School	No	Mail, Shopping, Streaming, Social Media	Anywhere Possible

J Interview Codebook

Codes	Description
Passkey Familiarity	
Impression	The participant's opinion about passkeys
Concerns	The participant's perceived barriers and skepticism related to passkeys
Passkey tracking method	The participant's preferred method for keeping track of their deployed passkeys
Enables passkeys	How/when the participant chooses to enable passkeys for a certain service
Unlocking mechanism	Participant mentions the device's unlocking mechanism
Compares to passwords	Participant compares passkeys to passwords
Compares to unlock	Participant compares passkeys to app or device unlock
Knows it's login	The participant mentions passkeys being a login method
Passkey usage	The participant's habits on passkey usage
First usage	How and when they first started using passkeys
Cross-device syncing	Whether they used synced passkeys
Account type	Types of account for which passkeys are activated (personal, work)
Frequency of usage	How often the participant uses passkeys to access their accounts
System used	Type of operating system on which they use passkeys (both mobile and desktop)
Device usage	The types of devices on which they use passkeys
Service usage	The types of services for which they use passkeys
Issues	Whether they ever experienced any issues in using a passkey
Decided against	Whether they ever decided against using a passkey
Passkey understanding	
Familiarity with passkey function	The participant's prior knowledge of the way passkeys work
Mechanism understanding	The participant's understanding and misunderstandings of the inner working of passkeys
Concerns	The participant's skepticism regarding the functioning of passkeys
Compares to 2FA	Participant compares passkeys to 2FA
Mentions password manager	The user mentions using or not using a password manager
Mentions biometrics	Participant's concerns about biometrics, and their beliefs on where they are stored
Revocation Explanation	
Doubts	The participant's uncertainties regarding the concept of revocation
Impression	The participant's impression regarding the concept of revocation
Passkey revocation option	Where the participants would look for an option to revoke a passkey
Revocation scenarios	The participant's idea of a scenario in which they think revocation could be enacted/useful
Revocation Mechanisms	
Baseline	
Reaction	The participant's initial response to the mechanism
Concerns	The participant's perceived barriers and skepticism related to the mechanism
Keeping track of accounts	The way participants would keep track of the accounts for which they have deployed passkeys
Revocation Code	
Reaction	The participant's initial response to the mechanism
Concerns	The participant's perceived barriers and skepticism related to the mechanism
Availability of revocation code	The participant's perceived importance of the availability of the revocation code
Keeping track of revocation code	How the participant would keep track of the revocation code
Backup Device	
Reaction	The participant's initial response to the mechanism
Concerns	The participant's perceived barriers and skepticism related to the mechanism
Device availability	The participant's perceived importance of the availability of the backup device
Device preference	The participant's preferred device to use for revocation purposes
Location preference	The participant's opinion on the preferred location where to store the device
Centralized Service	
Misconceptions	The participant's misconceptions regarding the mechanism
Certain exposure inevitable	Participant mentions that they would accept a privacy/security tradeoff in exchange for the service
Pros	The benefits that participants perceive regarding the revocation mechanism
Preferred operator company	The participant's preferred company to implement this mechanism
Concerns	The participant's perceived barriers and skepticism related to the mechanism
Reaction	The participant's initial response to the mechanism
eID	
Misconceptions	The participant's misconceptions regarding the mechanism
Authority involvement	The participant's opinion regarding the authorities' involvement in the revocation mechanism
Preferred document	The participant's preferred document to use for authentication
Idea of functioning	The participant's understanding of the mechanism's functioning
Reaction	The participant's initial response to the mechanism
Concerns	The participant's perceived barriers and skepticism related to the mechanism
Comparison Between Mechanisms	
Last choice	The participant's least preferred revocation mechanism
First choice	The participant's preferred revocation mechanism
Comparison with baseline	The participant's comparison of the revocation mechanism with the baseline