

As companies like Arena Plus, Houzz, and Houzz Pro lead the charge toward a more secure, passwordless future, the concept of **passkey adoption** continues to gain momentum. Passkeys—essentially cryptographic credentials stored securely on devices—are transforming how users authenticate, offering convenience through technologies like fingerprint authentication and significantly reducing password-related risks.

However, one persistent challenge remains: *how can organizations effectively measure passkey adoption without forcing it on every user?* Forcing passkey implementation prematurely risks alienating customers who aren't ready or able to use the new technology, damaging trust and engagement. In this blog post, we'll explore pragmatic strategies to evaluate adoption rates while respecting user preferences and maintaining smooth experiences across the entire digital identity lifecycle.

The Digital Identity Lifecycle Beyond Login

Adopting passkeys is not just about making login passwordless—it's about reimagining the entire digital identity lifecycle, which includes:

- **Registration:** Collecting minimal, essential information to create new accounts.
- **Authentication:** Offering options such as passkeys, fingerprint authentication, and fallback methods.
- **Verification & Recovery:** Balancing security and usability during identity verification and account recovery.
- **Step-Up Authentication:** Adding risk-based checks when performing sensitive actions.

Companies like Arena Plus have been pioneers in implementing clear, streamlined registration fields, which pave the way for easier adoption of advanced authentication methods like passkeys. Simplifying early user input also reduces friction when prompting users to register passkeys later in their journey.

Clear, Minimal Registration Fields Set the Stage

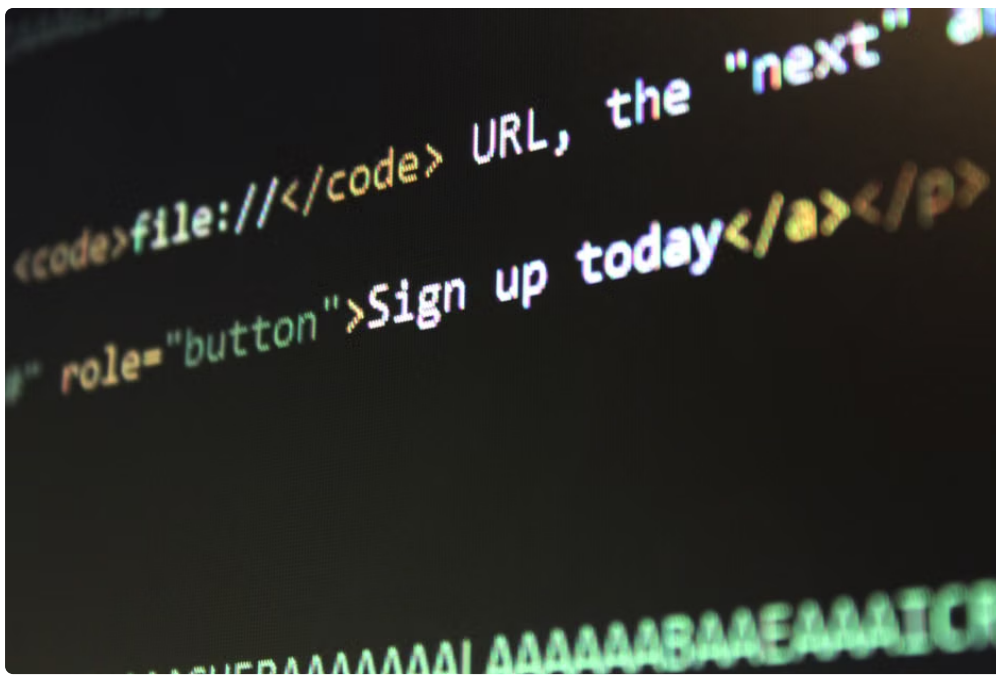
One common pain point in digital identity management is overwhelming users with long registration forms. This unnecessarily raises abandonment rates. Houzz and Houzz Pro, for example, focus on minimal initial data capture to encourage user onboarding and make subsequent authentication upgrades feel less intrusive.

Why does this matter for passkey adoption? Because adding friction at the registration stage can negatively impact opt-in rates later on. Instead, consider these best practices:

1. **Ask only for essential information:** Email address or phone number, full name, and minimal profile data.
2. **Defer noncritical data collection:** Collect additional preferences after first login or during ongoing profile updates.
3. **Educate users:** Use succinct, clear messaging about the benefits of passwordless login and passkeys upfront.

Passwordless Access: How Passkeys and Fingerprint Authentication Work Together

Passkeys improve security and user experience by relying on public-key cryptography and device-based credential storage. A user registers their device, which stores the private key, while the server holds the matching public key. When authenticating, the system challenges the user to verify possession via biometric methods like fingerprint authentication or device PINs.



For example, Houzz Pro integrates fingerprint authentication as an easy biometric layer for passkey sign-ins, providing both strong security and familiar user interaction. This synergy makes passkey adoption smoother, especially on mobile devices where biometrics are common.

Key benefits include:

- **Reduced phishing and credential stuffing risks:** No shared secrets to steal.
- **Faster, frictionless login experiences:** No need to remember or type passwords.
- **Greater user control:** Credentials stay on the user's trusted devices.

Respecting Users: The Importance of Fallback Options

Despite the advantages, not every user can immediately move to passkeys. Some may lack compatible devices, prefer traditional passwords, or be unfamiliar with new technology. This is why fallback options are crucial in any passkey adoption strategy.

Fallback options might include:

- **Password login:** Retain for users who opt out or face technical barriers.
- **Multi-factor authentication (MFA):** SMS codes, authenticator apps, or email verification for step-up security.
- **Account recovery flows:** Well-designed processes that do not solely rely on passkeys.

This respectful approach aligns with industry best practices observed by companies like Arena Plus, aiming for broad inclusivity rather than forced compliance.

Opt-In Rollout: Measuring Passkey Adoption Without Force

Rather than flipping a switch for everyone at once, a phased, opt-in rollout carefully introduces passkeys to subsets of users. This allows teams to monitor adoption metrics, identify pain points, and iterate accordingly.

How can you measure meaningful adoption during such rollouts? Consider these approaches:

1. **Instrument registration and login flows:** Track how many users enroll in passkeys after prompts.
2. **Analyze authentication method usage:** Percentage of logins via passkeys versus passwords or other factors.

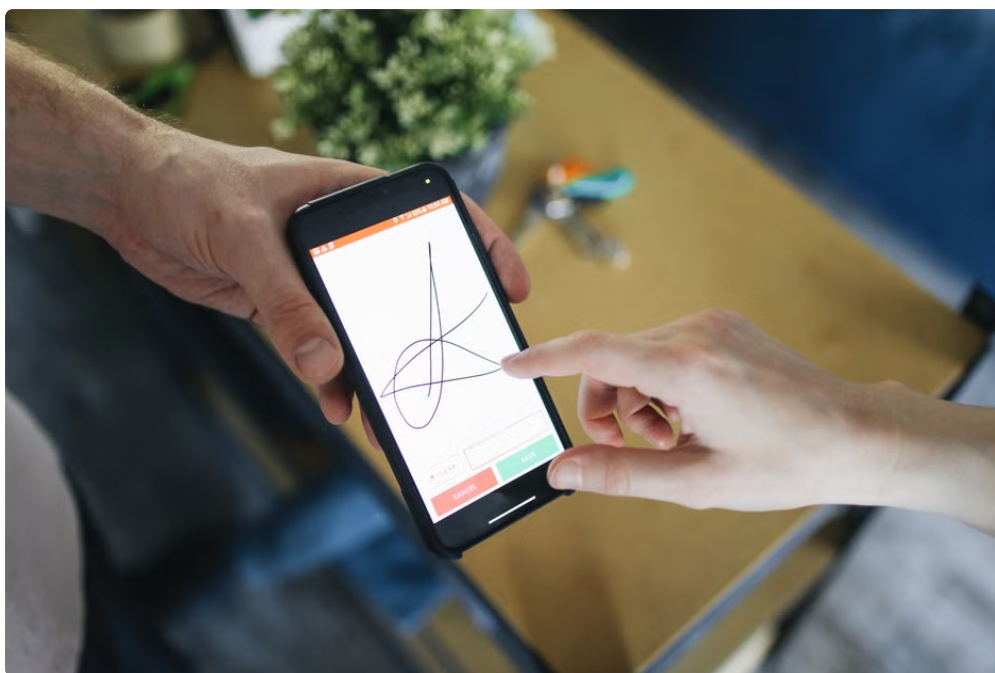
3. **Monitor fallback triggers:** When and why users revert to password login or recovery options.

4. **Collect user feedback:** Direct surveys or in-app feedback mechanisms to understand user sentiment.

This data-driven approach helps teams at Houzz and similar platforms understand real-world adoption without alienating users who prefer to stick with older methods for now.

Handling Risk-Based Authentication and Step-Up Checks

Not all interactions carry the same security requirements. Risk-based authentication lets you adapt security challenges based on contextual signals like device reputation, location, or transaction value.



During opt-in rollout phases for passkey adoption, risk-based step-up checks can be carefully calibrated:

- **Low-risk actions:** Allow passwordless login and quick access via passkeys or fingerprint authentication.
- **Higher-risk actions:** Trigger additional verification, such as email confirmations, SMS codes, or biometric prompts.

By incorporating these adaptive measures, companies like Arena Plus balance security with usability, encouraging users to adopt passkeys over time without feeling blocked by rigid policies.

Common Mistakes to Avoid

When measuring passkey adoption, there are pitfalls worth watching out for:

- **Inventing pricing or fees related to adoption:** Avoid assumptions about the costs users might incur—if pricing is unclear or unknown, disclose nothing rather than guessing.
- **Inconsistent terminology:** Use harmonized language across registration, login, and recovery flows to reduce user confusion.
- **Surprise hidden requirements:** Display password or passkey criteria upfront rather than after errors.
- **Unreadable device lists:** Present device and browser info clearly in account security dashboards to help users make informed decisions.

Conclusion

Measuring passkey adoption is a crucial step toward a safer, more user-friendly authentication ecosystem. By embracing opt-in rollouts, respecting fallback options, and integrating passkeys thoughtfully within the digital identity lifecycle—as seen with Arena Plus, Houzz, and Houzz Pro—companies can move deliberately and inclusively.

Remember these core takeaways:

- Keep registration fields minimal and clear.
- Educate users gracefully on benefits of passwordless authentication.
- Offer fallback options and never force passkey adoption prematurely.
- Use risk-based step-up authentication to protect sensitive actions.
- Collect meaningful adoption data before scaling.

By following these principles, your team can confidently measure and accelerate passkey adoption, creating an accessible and secure user experience for all.