UNIVERSITY OF OSLO

ICISSP 2025
Porto, Portugal | 20 - 22 February, 2025

Device-Bound vs. Synced Credentials: A Comparative Evaluation of Passkey Authentication

Andre Büttner **Nils Gruschka**

Department of Informatics, University of Oslo, Norway

Introduction

With passkeys, the FIDO Alliance has enabled syncing of FIDO2 credentials across a user's devices [1]. This represents a clear shift from the original single-device credentials. While this change aims to reduce the users' risk of losing their credentials, it is confronted with arguments about potential security compromises. To shed light on this controversy, we have analyzed passkeys regarding their usability, deployability, and security.

Main Contributions

1. Categorization of access levels of passkey credentials
2. Systematic comparison of passwords and different passkey types

Methodology

Comparing traditional passwords (**PW**) and passkey types regarding the occurrence of certain usability, deployability, and security benefits using the framework from "The Quest to Replace Passwords" [2].

Device-bound passkey types:

PA: Platform Authenticator (Windows Hello, Apple Touch/Face ID)
RA: Roaming Authenticator (YubiKey, Google Titan, mobile device)

Synced passkey types:

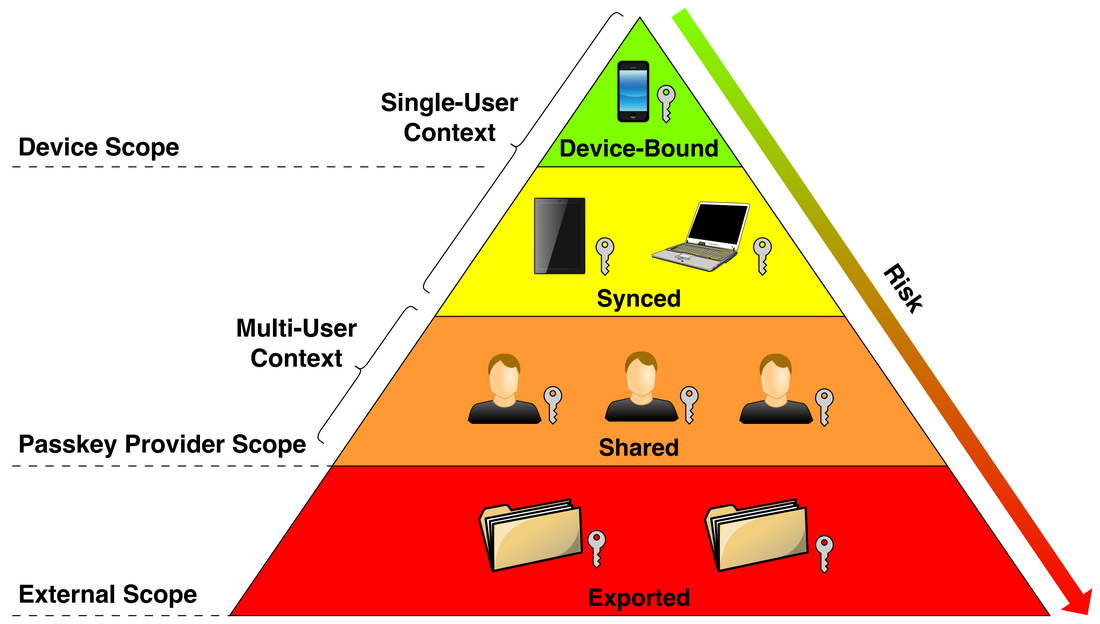
1P: First-Party Provider (Google Password Manager, Apple Passwords)
3P: Third-Party Provider (Bitwarden, Dashlane, ProtonPass)

Comparing Password and Passkeys

	Benefit	PW	PA	RA	1P	3P
Usability	Memorywise-Effortless	✗	✓	✓	✓	✓
	Scalable-for-Users	✗	✓	✓	✓	✓
	Nothing-to-Carry	✓	✓	✗	✓	✓
	Physically-Effortless	✗	✓	✗	✓	✓
	Easy-to-Learn	✓	✓	✓	~	✗
	Efficient-to-Use	✓	✓	~	✓	✓
	Infrequent-Errors	~	✓	~	✓	✓
	Easy-Recovery-from-Loss	✓	✗	✗	~	~
Deployability	Accessible	✓	✓	✓	✓	✓
	Negligible-Cost-per-User	✓	✓	~	✓	✓
	Server-Compatible	✓	~	~	~	~
	Browser-Compatible	✓	✓	✓	✓	✓
	Mature	✓	✓	✓	✓	✓
	Non-Proprietary	✓	✓	✓	✓	✓
Security	Resilient-to-Physical-Observation	✗	✓	✓	✓	✓
	Resilient-to-Targeted-Impersonation	~	✓	✓	✓	✓
	Resilient-to-Throttled-Guessing	✗	✓	✓	✓	✓
	Resilient-to-Unthrottled-Guessing	✗	✓	✓	✓	✓
	Resilient-to-Internal-Observation	✗	✓	✓	~	~
	Resilient-to-Leaks-from-Other-Verifiers	✗	✓	✓	✓	✓
	Resilient-to-Phishing	✗	✓	✓	✓	✓
	Resilient-to-Theft	✓	✓	✓	✓	✓
	No-Trusted-Third-Party	✓	✓	✓	✗	✗
	Requiring-Explicit-Consent	✓	✓	✓	✓	✓
	Unlinkable	✓	✓	✓	✓	✓

✓ offered ~ partially offered ✗ not offered

Access Levels of Passkey Credentials



Recommendations

End Users:

- Choose passkey provider based on:
  a) Device compatibility
  b) Strong authentication methods
- Use credential sharing cautiously
- Store backups offline or otherwise encrypted

Passkey Providers:

- Implement robust access control measures
- Need for more standardized user interfaces

Relying Parties:

- Require device attestation for particularly sensitive use cases
- Support the user in choosing proper recovery methods
- Do not convey wrong security guarantees

Conclusion and Outlook

Key Takeaways:

- Synced passkeys can mitigate credential loss when set up on several devices and/or backed up
- Passkeys provide more security benefits than passwords
- Security of synced passkeys depends highly on their implementation and usage

Future Work:

- Studying user perception of synced passkeys
- Evaluating the security of passkey providers

References

[1] https://www.passkeycentral.org/ (Last accessed: 2025/01/10).

[2] Joseph Bonneau et al. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes". In: *2012 IEEE Symposium on Security and Privacy*. 2012, pp. 553–567.

Digital Security Research Group

Contact
andrbut@ifi.uio.no
nilsgrus@ifi.uio.no