Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Passwortlose Zukunft mit Passkeys

Passwortlose Zukunft mit Passkeys

Das Konzept von Passwörtern als Mittel zur Authentisierung und Sicherung von Informationen existiert seit vielen Jahrhunderten. Doch ist die Methodik, die darauf basiert, dass beide Seiten Kenntnis über die gleiche geheime Information haben, noch zeitgemäß und vor allem sicher? Die Bedrohung durch mögliche Datenleaks oder Angriffsmethoden, wie Phishing und Password-Spraying, lässt berechtigte Zweifel an der Zukunftsfähigkeit von Passwörtern aufkommen. Hier kommen Passkeys als Alternative ins Spiel, um die Nachteile klassischer Passwörter zu umgehen.

Was?

Passwortlose Authentisierung ermöglicht, die Identität von Nutzenden zu verifizieren und Zugang zu Onlinediensten zu ermöglichen, ohne dass die Kombination aus Nutzernamen und Passwort verwendet wird. Stattdessen wird die Identität ermittelt und der Nachweis darüber mithilfe einer Signatur übermittelt.

Warum?

Passwortlose Authentisierung

- verwendet asymmetrische Kryptographie,
- erfordert keine oder nur eine geringe Gedächtnisleistung und
- ist phishingresistent.

Wie?

Die **passwortlose Authentisierung** durch Passkeys auf Basis von FIDO2 kann, je nach dem gewünschten Sicherheitsniveau, mit verschiedenen Authentikatoren realisiert werden. FIDO steht dabei für **Fast Identity Online**, einen von der FIDO Alliance entwickelter Standard.

So wird Ihr Unternehmen passwortlos:

Bedarfsanalyse: Führen Sie eine umfassende Analyse der Nutzerbedürfnisse und der verwendeten Geräte durch, um passende Passkey-Modelle auszuwählen.
Pilottests: Registrierung, Authentisierung und Wiederherstellungsprozesse sollten mit Pilotgruppen getestet werden, um sicherzustellen, dass sie den Anforderungen entsprechen und die Benutzerakzeptanz gewährleistet ist.
Monitoring: Überwachen Sie Implementierung und Nutzung, um den Erfolg sicherzustellen. Berücksichtigen Sie Aspekte wie Nutzungsmetriken, Schlüsselverwaltung und Kompatibilitätssicherung.

Wieso es kein Passwort mehr braucht

Sich sicher passwortlos einzuloggen, funktioniert über sogenannte Challenges: Beim Registrierungsprozess wird im Authentikator mittels Public-Key-Verfahren ein kryptografisches Schlüsselpaar generiert. Der öffentliche Schlüssel wird anschließend bei der jeweiligen Anwendung hinterlegt, während der private Schlüssel den Authentikator nicht verlässt (Device Bound/Single Device Passkeys) oder mit der Cloud synchronisiert wird (Synced Passkeys). Die Authentisierung erfolgt durch das Senden einer Challenge an den Authentikator, die nur mithilfe des privaten Schlüssels korrekt beantwortet werden kann. Beachten Sie hierzu auch die Abbildung auf der Rückseite.

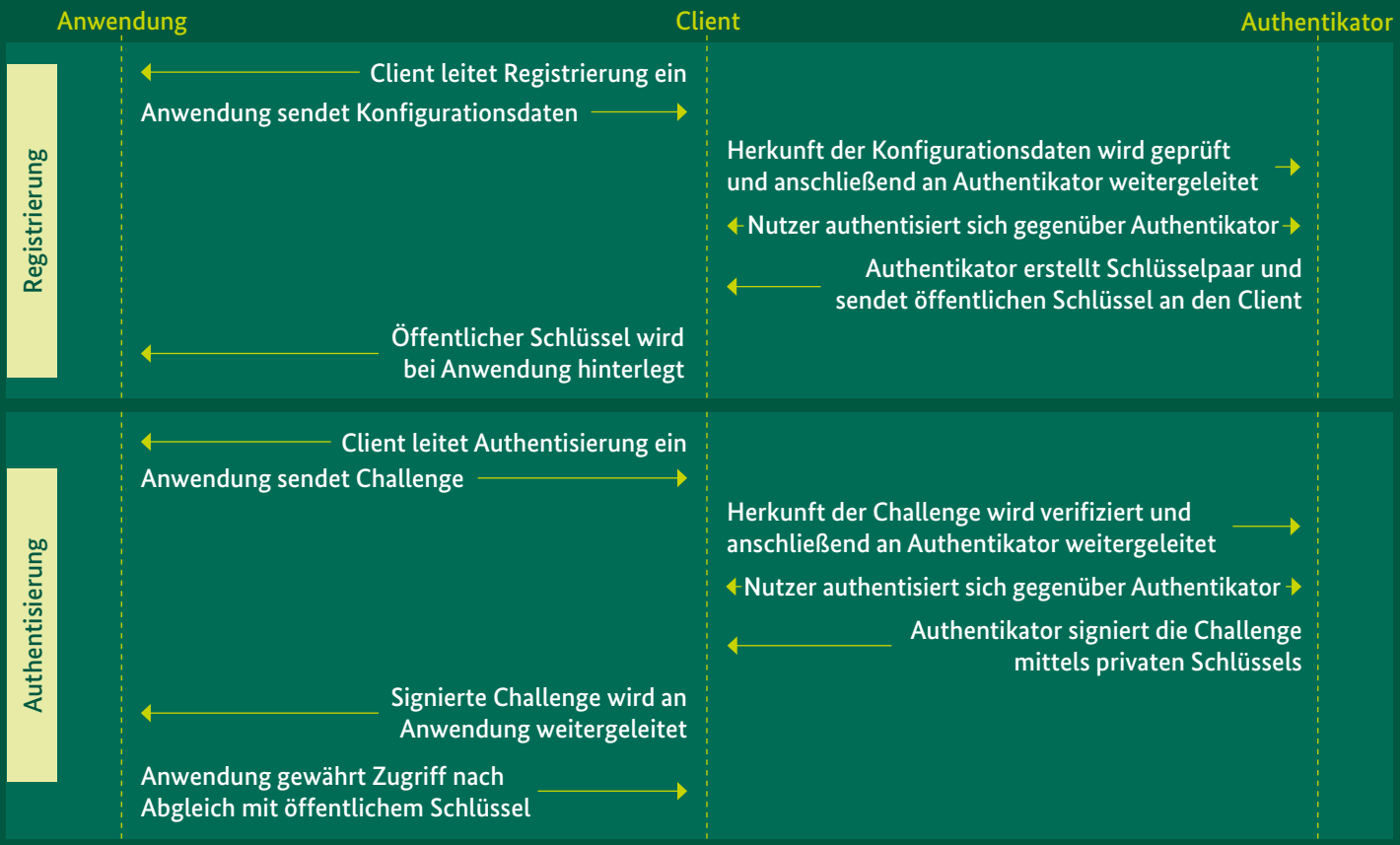
Als Authentikator sieht der FIDO2-Standard verschiedene Optionen mit unterschiedlichen Sicherheitsniveaus vor. Der Schlüssel kann als Softwarezertifikat gespeichert werden, sicherer ist aber die separate Speicherung in Hardware auf einer Chipkarte oder einem speziellen USB-Stick/NFC-Token. Auch moderne Smartphones und Notebooks mit einem Trusted Platform Module bieten einen sicheren Schlüsselspeicher. Die Wahl geeigneter Authentikatoren hängt immer vom jeweiligen Use-Case ab. Softwarelösungen sind zwar benutzerfreundlich und bieten bis zu einem gewissen Grad Sicherheit, jedoch sollten Unternehmen mit hohen Sicherheitsanforderungen dennoch die Verwendung dedizierter Authentikatoren in Betracht ziehen.

Neben der Wahl geeigneter Authentikatoren sind bei der Umstellung auf Passkeys Faktoren wie Benutzerschulungen, die Entwicklung einer Account-Recovery-Strategie oder Probleme beim Rollout der Authentikatoren zu berücksichtigen. Der Aufwand lohnt sich, bedeutet er doch letztendlich mehr Cybersicherheit!

Die **FIDO-Allianz** ist eine offene Industrievereinigung mit dem klaren Ziel, die weltweite Abhängigkeit von Passwörtern zu reduzieren. Sie fördert die Entwicklung, Nutzung und Einhaltung von Standards für Authentisierung von Benutzenden und Geräten. So bietet sie z. B. Zertifizierungs- und Partnerprogramme an, um in einem ständigen Austausch mit der Industrie die Verwendung der FIDO-Standards global zu fördern.

Weitere Informationen unter:
www.fidoalliance.org

Registrierungs- und Authentisierungssequenz



Weitere Informationen auf der BSI-Webseite

Impressum

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

Tel.: 0800 274 1000

E-Mail: bsi@bsi.bund.de

www.bsi.bund.de

Bildnachweis

Adobe Stock/Martin

Stand

März 2024