CS-026 · Passwords & Authentication

Passkeys

Phishing resistant credentials that replace passwords with device bound public key cryptography.

Executive Summary

A passkey is a login credential based on public key cryptography that replaces the password entirely. The secret private key stays on the user's device and never travels to the site, while the site holds only a public key. Because the credential is bound to the real site and unlocked locally with a biometric or PIN, passkeys resist phishing, credential theft, and reuse by design.

What It Is

A passkey is a modern credential built on the FIDO2 and WebAuthn standards that lets a user sign in without a password. When a user registers, their device creates a cryptographic key pair. The private key stays protected on the device or in a synced secure store, and the matching public key is sent to the site. There is no shared secret to steal, phish, or reuse. To authenticate, the user unlocks the private key locally, usually with a fingerprint, face scan, or device PIN, and the device proves possession of the key to the site. Passkeys can live on a phone, a computer, or a hardware security key, and many implementations sync an encrypted copy across a user's devices.

Why It Matters

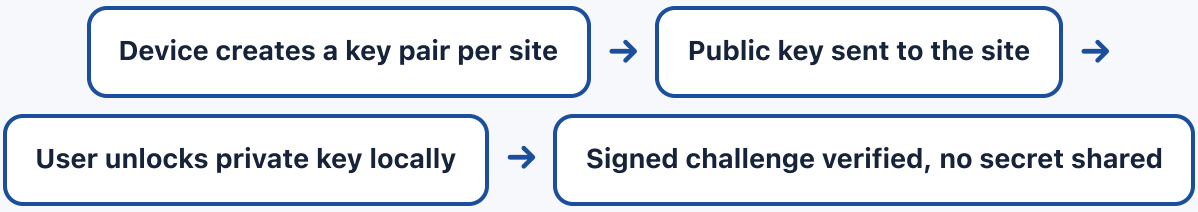
Passwords remain the weakest link in authentication, driving breaches through phishing, reuse, and credential theft. Passkeys attack the root cause by removing the shared secret altogether, which eliminates entire categories of attack at once. There is nothing for a phishing page to capture, nothing to leak in a server breach that could be replayed, and nothing to reuse across sites. Major platform and browser vendors and the FIDO Alliance have aligned behind passkeys, so adoption is accelerating. For a professional, understanding the cryptographic model and the

migration path from passwords is quickly becoming essential to identity work and to advising organizations on going passwordless.

How It Works

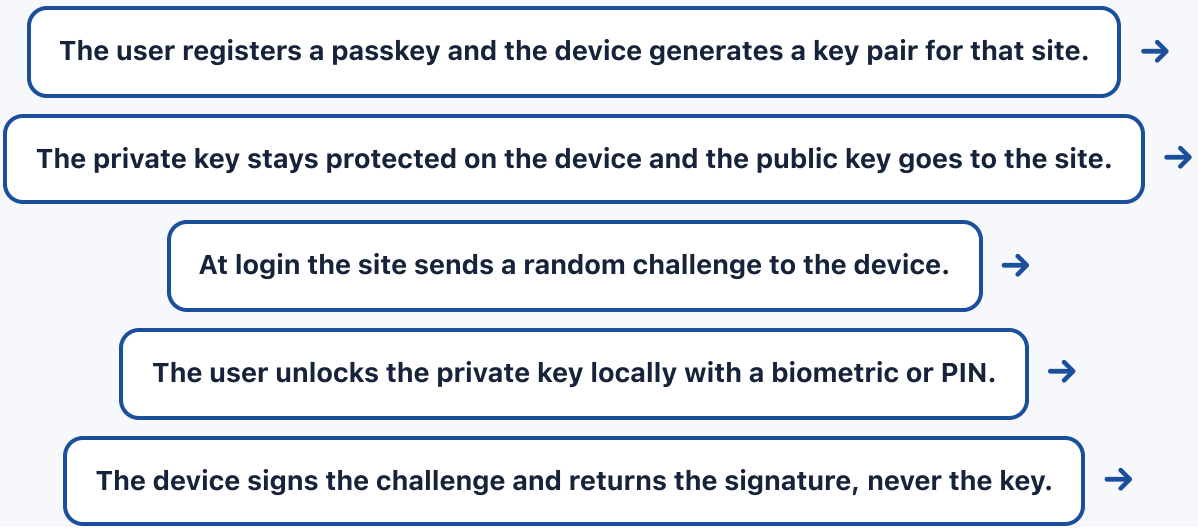
Passkeys use asymmetric cryptography. At registration the device generates a key pair for that specific site, keeps the private key protected, and shares the public key. At login the site sends a random challenge. The device asks the user to unlock the private key locally, then uses it to sign the challenge, and returns the signature. The site verifies it with the stored public key. Crucially, the credential is tied to the site's real domain, so a lookalike phishing site cannot trigger a valid signature. The private key never leaves the secure store, so a breached server exposes only useless public keys. This binding to the origin is what makes passkeys phishing resistant rather than merely convenient.

Architecture Diagram



The device signs the site's challenge with a private key it never shares, and the site verifies with the public key.

Visual Workflow



The site verifies the signature with the stored public key and grants access.

Common Attacks

- Phishing attempts fail because the credential is bound to the real domain
- Server breaches expose only public keys that cannot be replayed
- Malware on a fully compromised device could try to misuse an unlocked key
- Social engineering of account recovery to enroll an attacker's own passkey
- Downgrade attacks that push a user back to a weaker password fallback

Common Mistakes

- Leaving a weak password enabled as a fallback that undoes the phishing resistance
- Not planning device loss and recovery before rolling passkeys out
- Ignoring how passkeys sync, and whether that meets the organization's risk needs
- Failing to secure account recovery, which becomes the new weakest link
- Assuming every legacy application supports the standards without testing

Best Practices

- Adopt passkeys on the FIDO2 and WebAuthn standards rather than proprietary schemes
- Remove or tightly restrict weaker fallback methods once passkeys are established
- Plan device loss, recovery, and enrollment security before wide rollout
- Understand whether keys are device bound or synced and match that to your risk
- Harden account recovery so it cannot be used to plant an attacker passkey
- Offer hardware security keys as passkeys for the highest assurance accounts

Quick Checklist

- [x] Passkey support based on FIDO2 and WebAuthn confirmed
- [x] Fallback methods reviewed so they do not weaken phishing resistance

- [x] Device loss and recovery process defined and tested
- [x] Sync model understood and matched to risk requirements
- [x] Account recovery hardened against attacker enrollment
- [x] Hardware key option available for highest value accounts

Recommended Tools

Platform authenticator
Built in device biometric or PIN that unlocks a passkey

Hardware security key
Portable device that stores passkeys for high assurance login

Password manager with passkey support
Stores and syncs passkeys across a user's devices

Identity provider with WebAuthn
Enables and enforces passkey login across connected applications

Industry Standards

FIDO2
The overarching standard set enabling passwordless, phishing resistant authentication

WebAuthn
The web API that lets browsers and sites use public key credentials

NIST SP 800-63B
Recognizes cryptographic authenticators and phishing resistance at higher assurance levels

Career Relevance

Passkeys are a fast growing focus for identity and access management engineers, who design passwordless rollouts, recovery, and fallback policy. Security engineers evaluate device binding versus sync tradeoffs; GRC analysts map passkeys to assurance requirements and phishing

resistance mandates; and SOC analysts adjust monitoring as credential theft declines and recovery abuse becomes the target. Fluency in the FIDO2 and WebAuthn model is an increasingly valuable, forward looking skill for the roles AI-Governance-Jobs.com serves.

Interview Questions

- How do passkeys use public key cryptography to authenticate without a shared secret?
- Why are passkeys resistant to phishing when passwords are not?
- What is the difference between a device bound passkey and a synced passkey?
- Why does a server breach reveal little useful when a site uses passkeys?
- What becomes the weakest link once passwords are removed, and how do you protect it?

Related Certifications

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | ISC2 SSCP

Further Reading

- FIDO Alliance: Passkeys
- NIST SP 800-63B Digital Identity Guidelines
- CISA: Implementing Phishing Resistant MFA

Key Takeaways

- A passkey replaces the password with a private key that never leaves the device.
- The site holds only a public key, so a breach exposes nothing replayable.
- Passkeys are bound to the real domain, which defeats phishing by design.
- They are built on the open FIDO2 and WebAuthn standards.
- Account recovery becomes the new weakest link and must be hardened.

FAQ

▶ **Are passkeys really more secure than a password plus MFA?**

▶ **What happens if I lose the device holding my passkey?**

▶ **Do passkeys mean the end of passwords?**

Related Careers

RELATED ROLES

Iam Engineer | Security Engineer | Grc Analyst

RELATED CERTIFICATIONS

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | ISC2 SSCP

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Passkeys**
3. Go deeper: Passwords
4. Go deeper: Password Managers
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

CS-022 Passwords | CS-024 Password Managers | CS-025 Multi-Factor Authentication (MFA) | CS-032 Phishing | CS-062 Authentication