Fact Sheet

Cogito Group

Passkeys

Passkeys

A passkey is a modern digital security tool designed to replace traditional passwords with a more secure and convenient authentication method. Instead of relying on a string of characters that you need to remember and enter manually, a passkey uses a pair of cryptographic keys: a public key stored on the server and a private key kept securely on your device.

How it works

When you log in to a website or app, your device uses the private key to generate cryptographic proof, which is then verified by the server using the public key. This process is seamless and often involves biometric authentication, such as a fingerprint or facial recognition, or a hardware security token- making it both highly secure and easy to use.

Users aren't restricted to using the passkeys only on the device where they're available. Passkeys can be used on phones when logging into a laptop, even if the passkey isn't synchronized to the laptop. This is so long as the phone is near the laptop and the user approves the sign-in on the phone. As passkeys are built on FIDO standards, all browsers can adopt them.

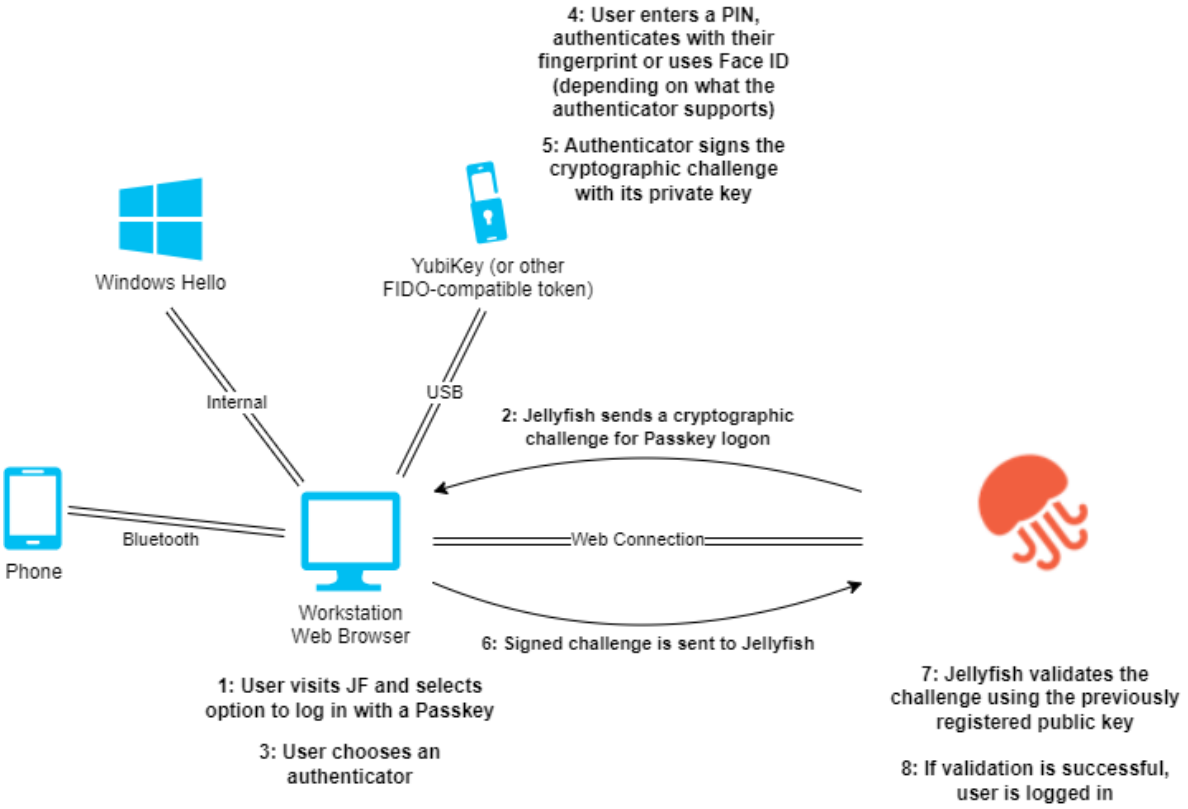
With passkeys, you don't have to worry about phishing attacks, as the private key never leaves your device, and even if hackers breach a service's database, they can't steal your login credentials.

Passkeys

Fact Sheet

Using Passkeys to securely log in to Jellyfish

Jellyfish fully supports using Passkeys. Instead of having to type in a username and password, or using other multi-factor authentication (MFA) methods, Jellyfish users can authenticate directly with a passkey. Passkeys streamline the login process, reducing the need for users to remember and manage complex passwords. This not only simplifies access but also eliminates the risk associated with weak or reused passwords.



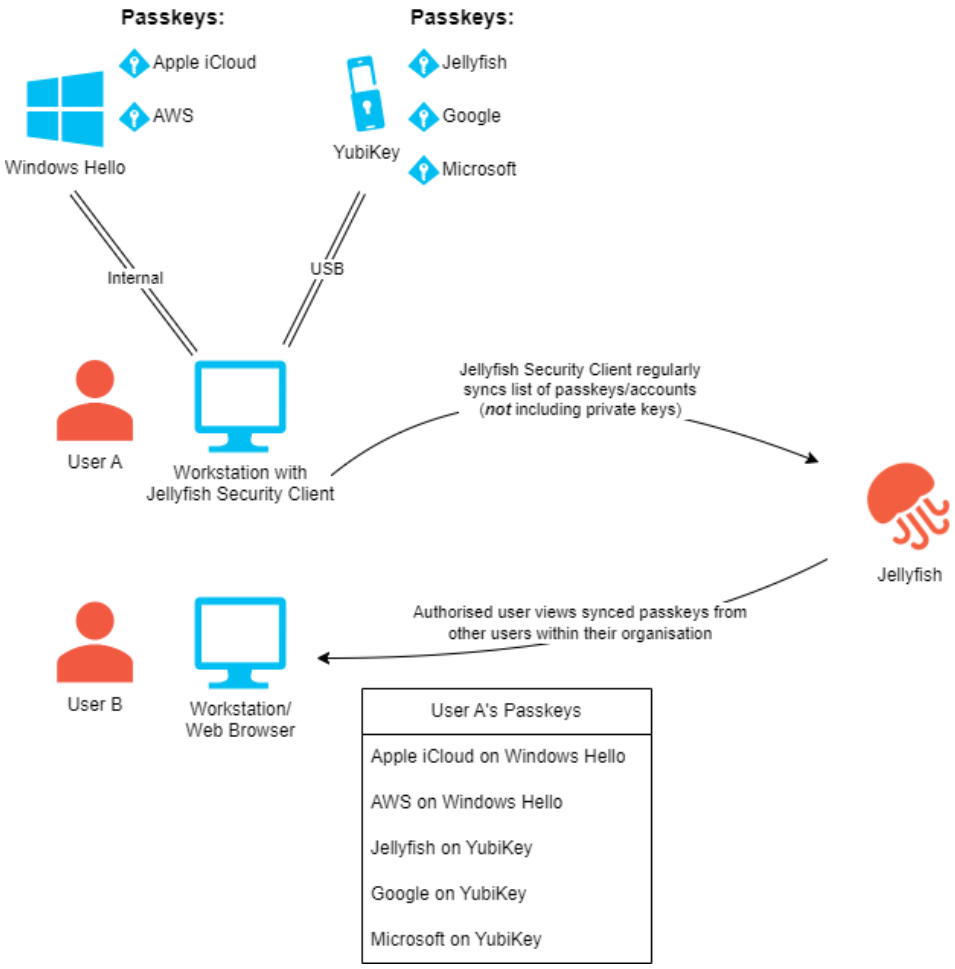
Managing Passkeys in your organisation with Jellyfish

Jellyfish allows you to centrally manage and monitor all passkeys, providing a comprehensive view of their usage and helping to detect potential security breaches. This centralised management system ensures that all passkeys are accounted for and that their usage complies with your organisation's security policies. By maintaining oversight of passkeys, Jellyfish allows you to quickly identify any unusual activity or unauthorised access attempts, thereby enhancing your organisation's overall security posture.

Passkeys

Fact Sheet

The Jellyfish platform provides a user-friendly interface that enables IT administrators to view and track passkeys on users' computers. The Jellyfish Security Client is responsible for securely uploading these passkeys to the Jellyfish platform. This visibility extends to the websites and services for which passkeys have been created, offering insights into the authentication landscape within your organisation. By leveraging the Jellyfish platform, your organisation can achieve a higher level of security, streamline passkey management, and ensure that all digital interactions are protected by the latest advancements in authentication technology.



About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.