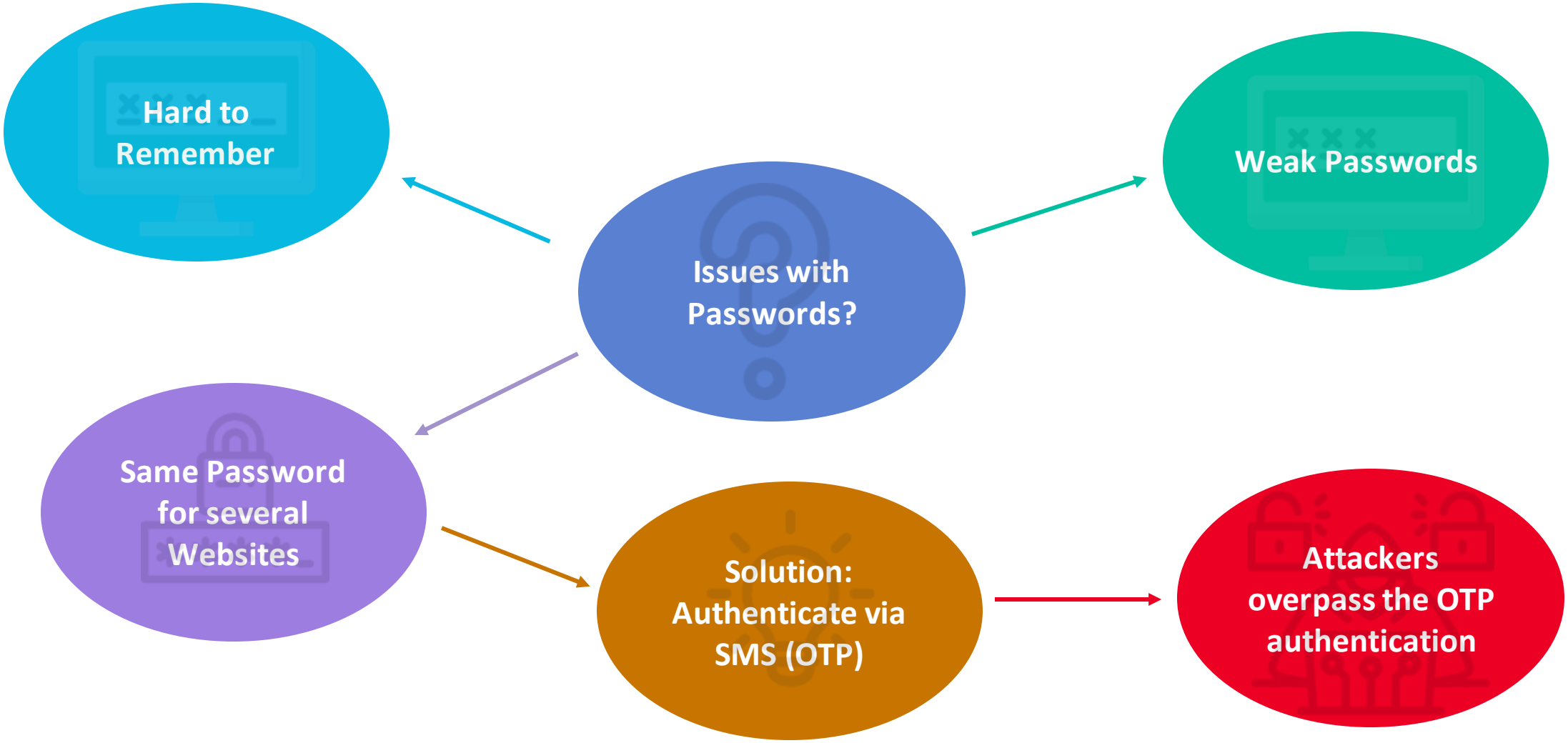
Flash Memory Summit

Phishing Resistant Multi Factor Web Authentication using Roaming Authenticator

Vishwas Saxena

Senior Technologist, Western Digital

Passwords are not fit for the Authentication purposes?



Why FIDO?

Strong

Authentication is ideally backed by a Hardware Security Module, which can safely store private keys and perform the cryptographic operations needed for WebAuthn.

Scoped

A keypair is only useful for a specific origin, like browser cookies. A keypair registered at 'webauthn.guide' cannot be used at 'evil-webauthn.guide', mitigating the threat of phishing.

Attested

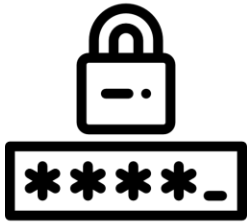
Authenticators can provide a certificate that helps servers verify that the public key did in fact come from an authenticator they trust, and not a fraudulent source.

FIDO (Fast IDentity Online)

- More secure and user-friendly authentication framework.
- FIDO leverages public key cryptography and multi-factor authentication to provide strong authentication process.
- Eliminates the vulnerabilities associated with passwords, reducing the risk of unauthorized access.
- Multi-factor authentication in FIDO combines something the user possesses (e.g., a physical token) with something they are (e.g., biometric data) or something they know (e.g., a PIN).

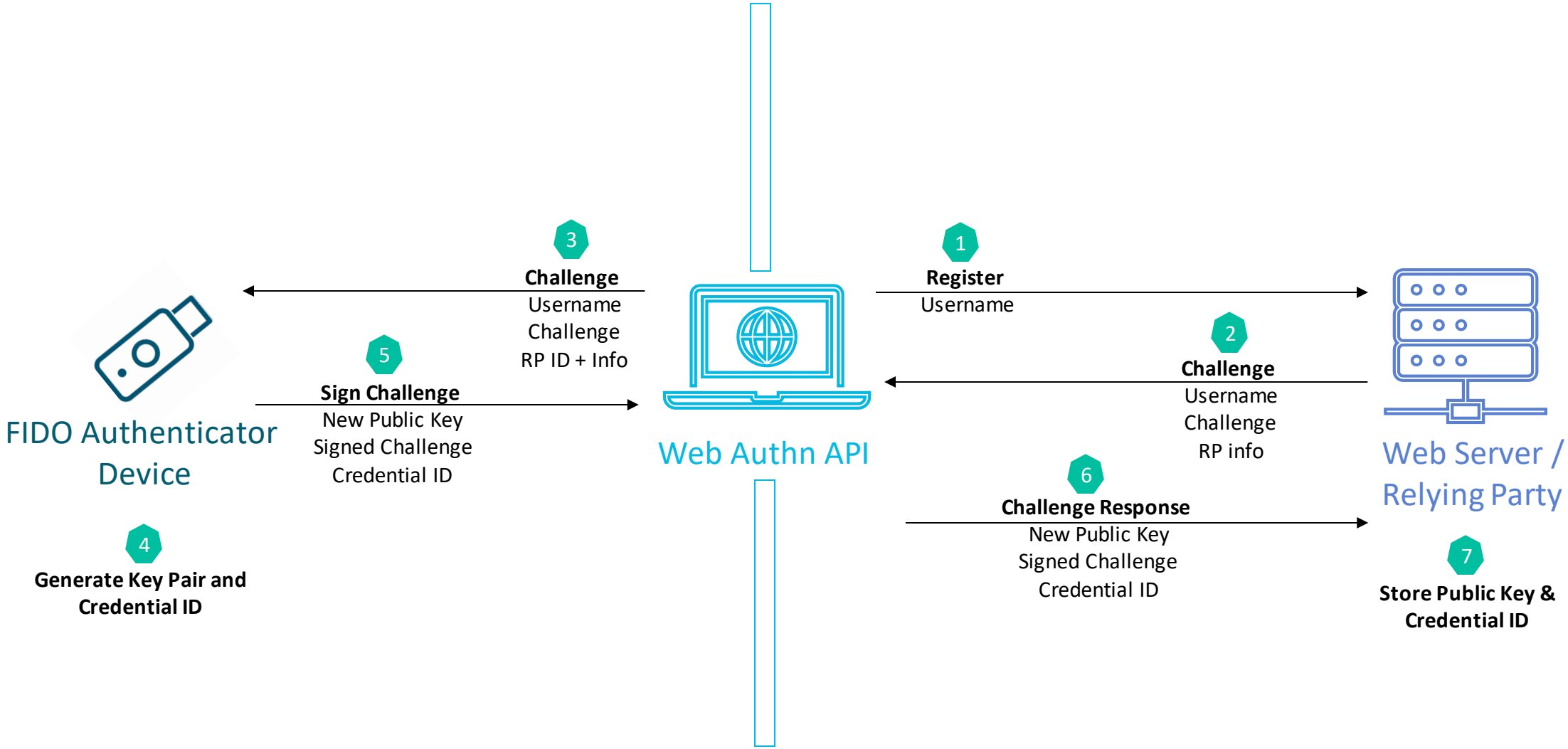
Something you have

Something you are

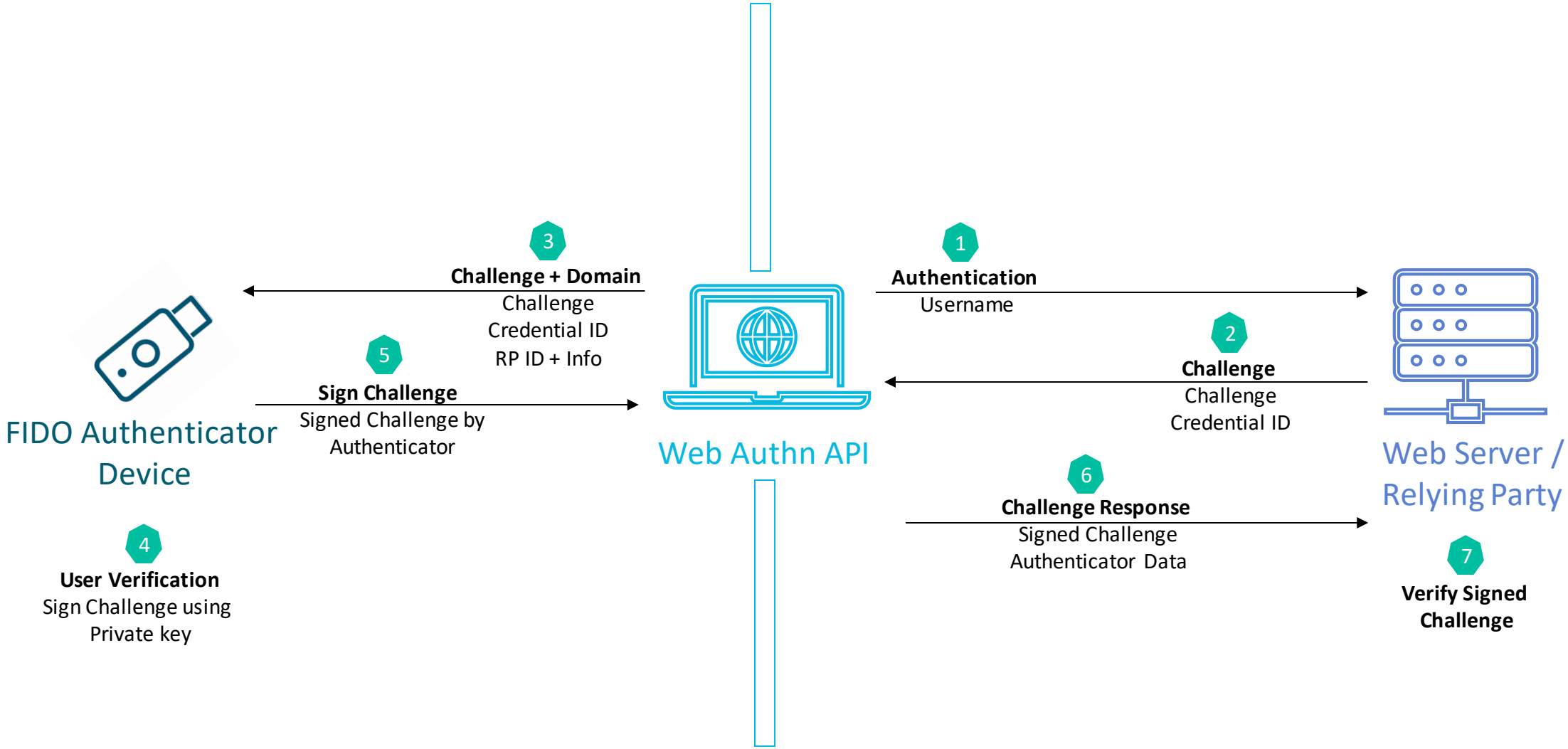


Something you Know

FIDO Registration: How it works?



FIDO Authentication:



Summary

Flash Memory Summit

Simpler & Stronger

Reduce Reliance on Complex Passwords

Remote Authenticator

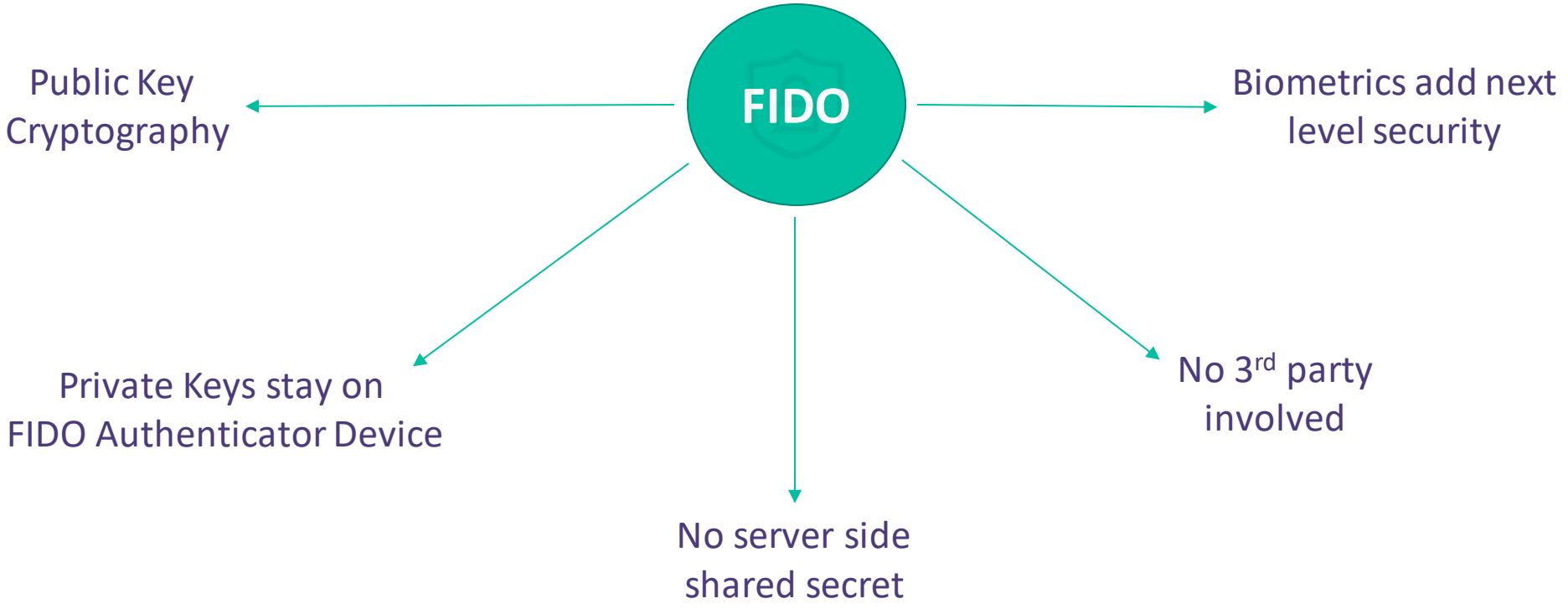
Fast and Convenient

Secure

Summary

Flash Memory Summit

Simpler & Stronger



Thank You