Passkey Mythbusters: Short Takes on Common Misunderstandings

Tim Cappalli
Nishant Kaushik
Matthew Miller

authenticate 2025
THE FIDO CONFERENCE

Agenda

- Overview of the passkey ecosystem
- Misconceptions
- Q&A

The Passkey Ecosystem

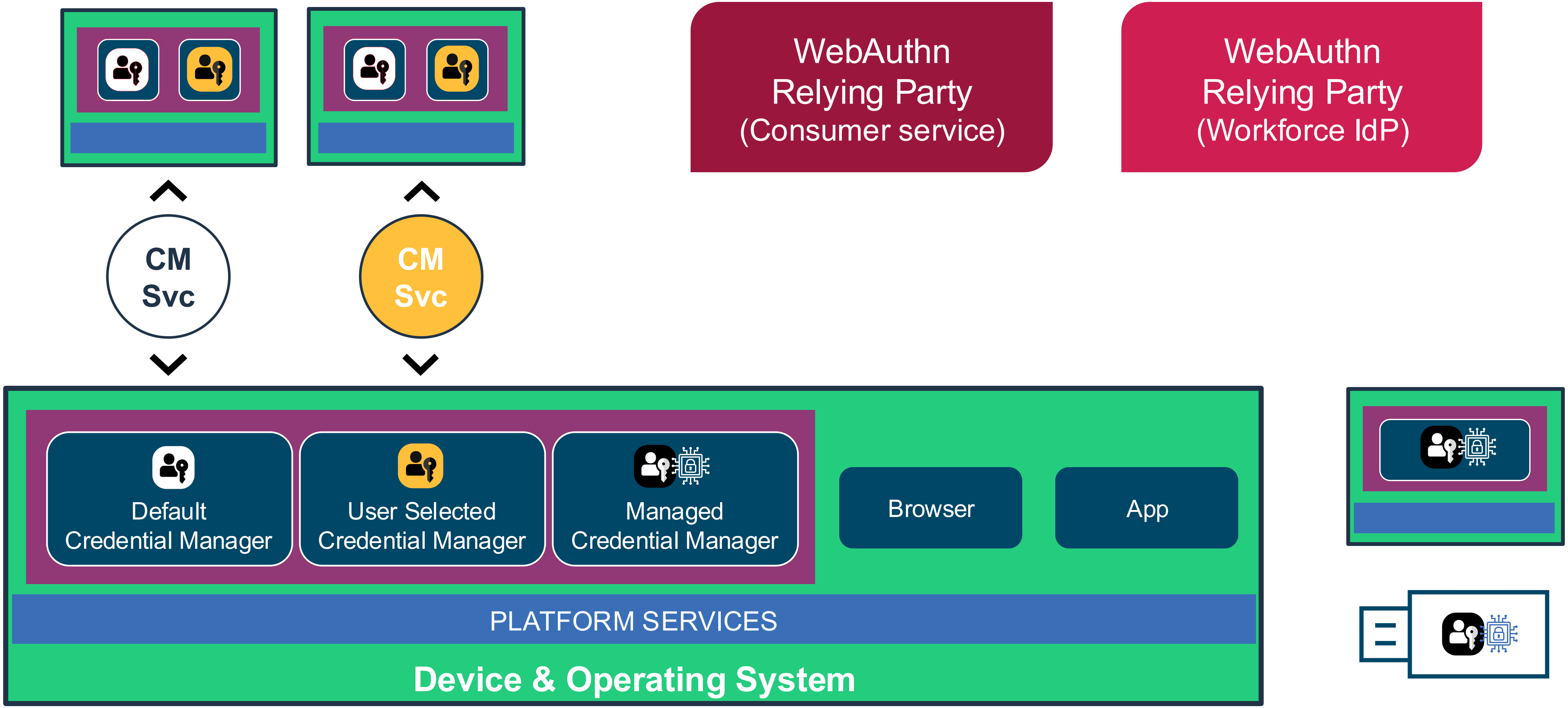
Users

Browsers & Apps

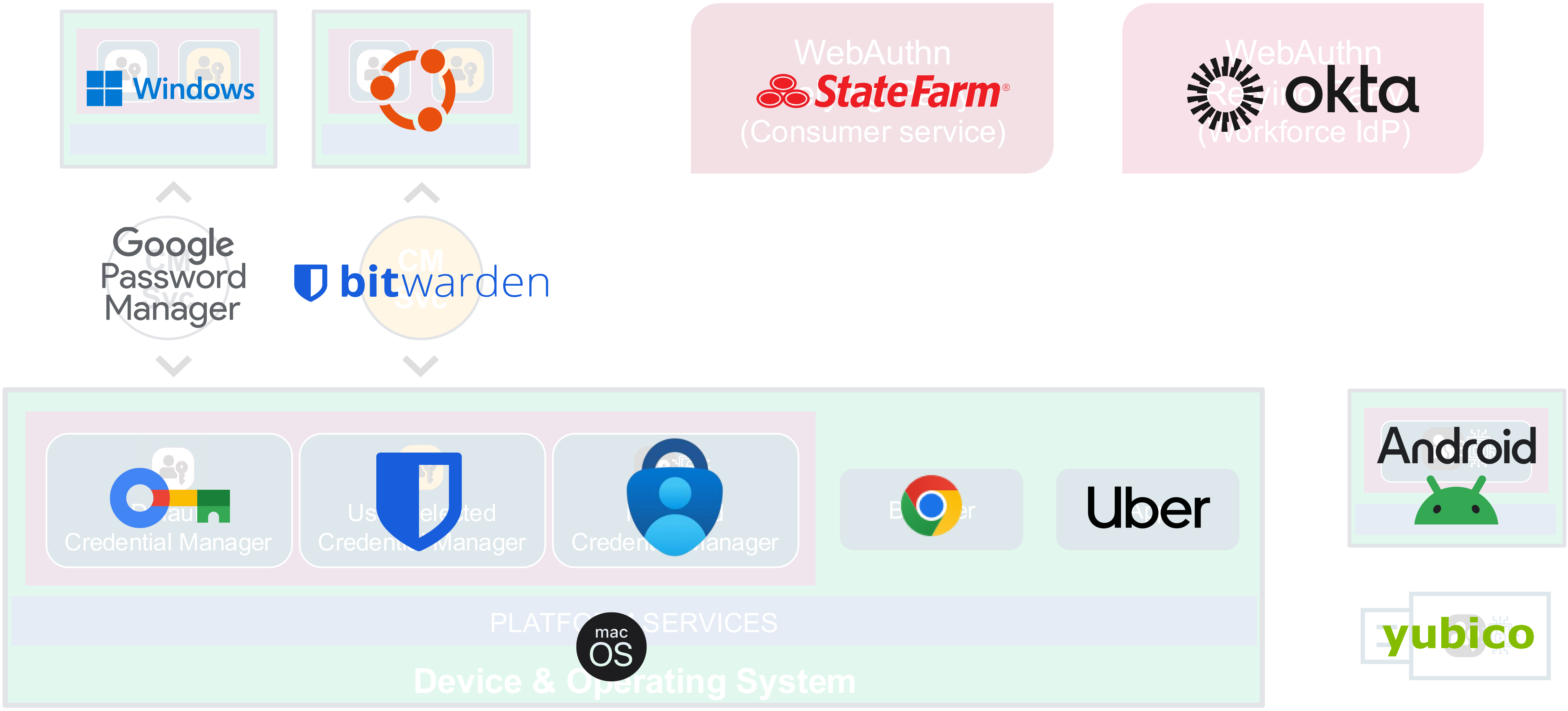
Device & OS

Credential Managers (Authenticators)

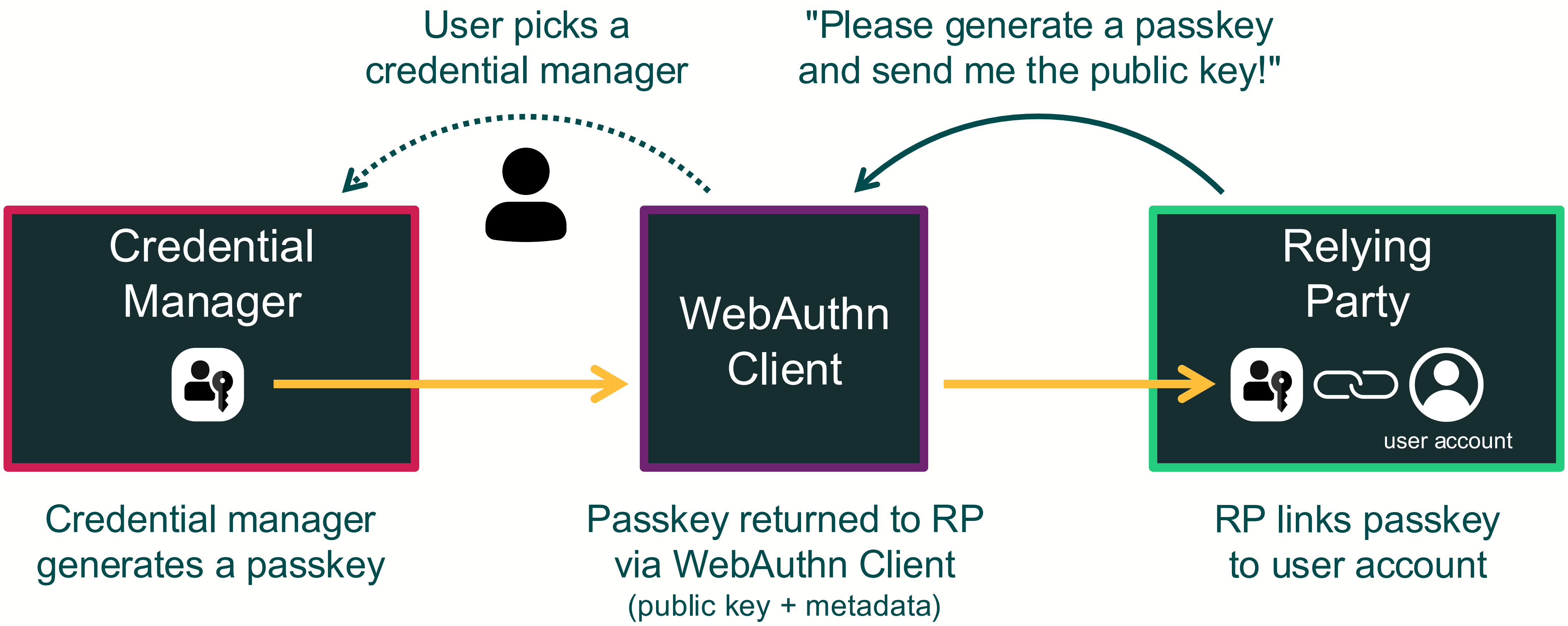
Relying Parties


WebAuthn
Relying Party
(Consumer service)
WebAuthn
Relying Party
(Workforce IdP)
CM
Svc
CM
Svc
Default
Credential Manager
User Selected
Credential Manager
Managed
Credential Manager
Browser
App
PLATFORM SERVICES
Device & Operating System

EXAMPLES


Windows
WebAuthn
Relying Party
StateFarm
(Consumer service)
WebAuthn
Relying Party
okta
(Workforce IdP)
Google Password Manager
CM Svc
bitwarden
CM Svc
Default
Credential Manager
User-selected
Credential Manager
Credential Manager
Browser
Uber
App
Android
yubico
PLATFORM SERVICES
mac OS
Device & Operating System

Bring Your Own Key



User picks a credential manager

"Please generate a passkey and send me the public key!"

Credential manager generates a passkey

Passkey returned to RP via WebAuthn Client (public key + metadata)

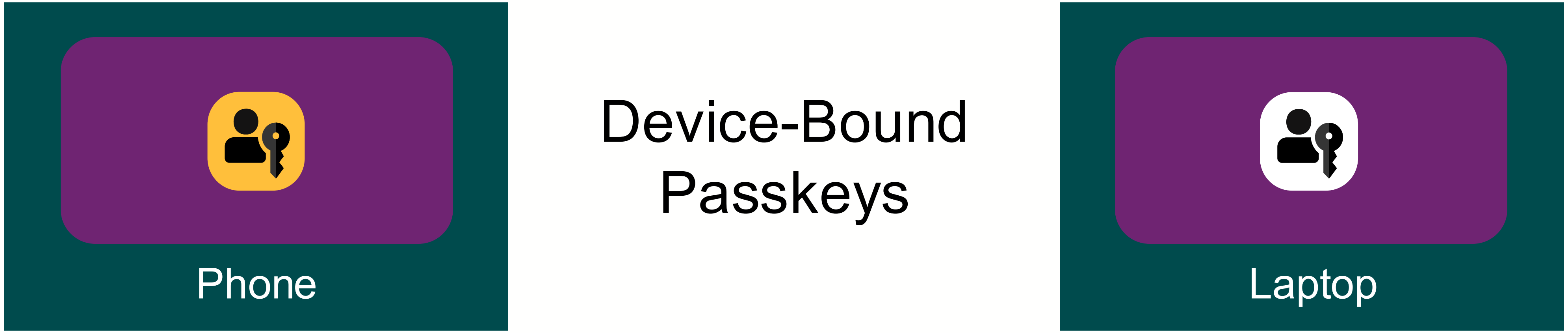
RP links passkey to user account

Misconceptions

Are passkeys stored in the cloud in the clear?

"Are passkeys stored in the cloud in the clear?"

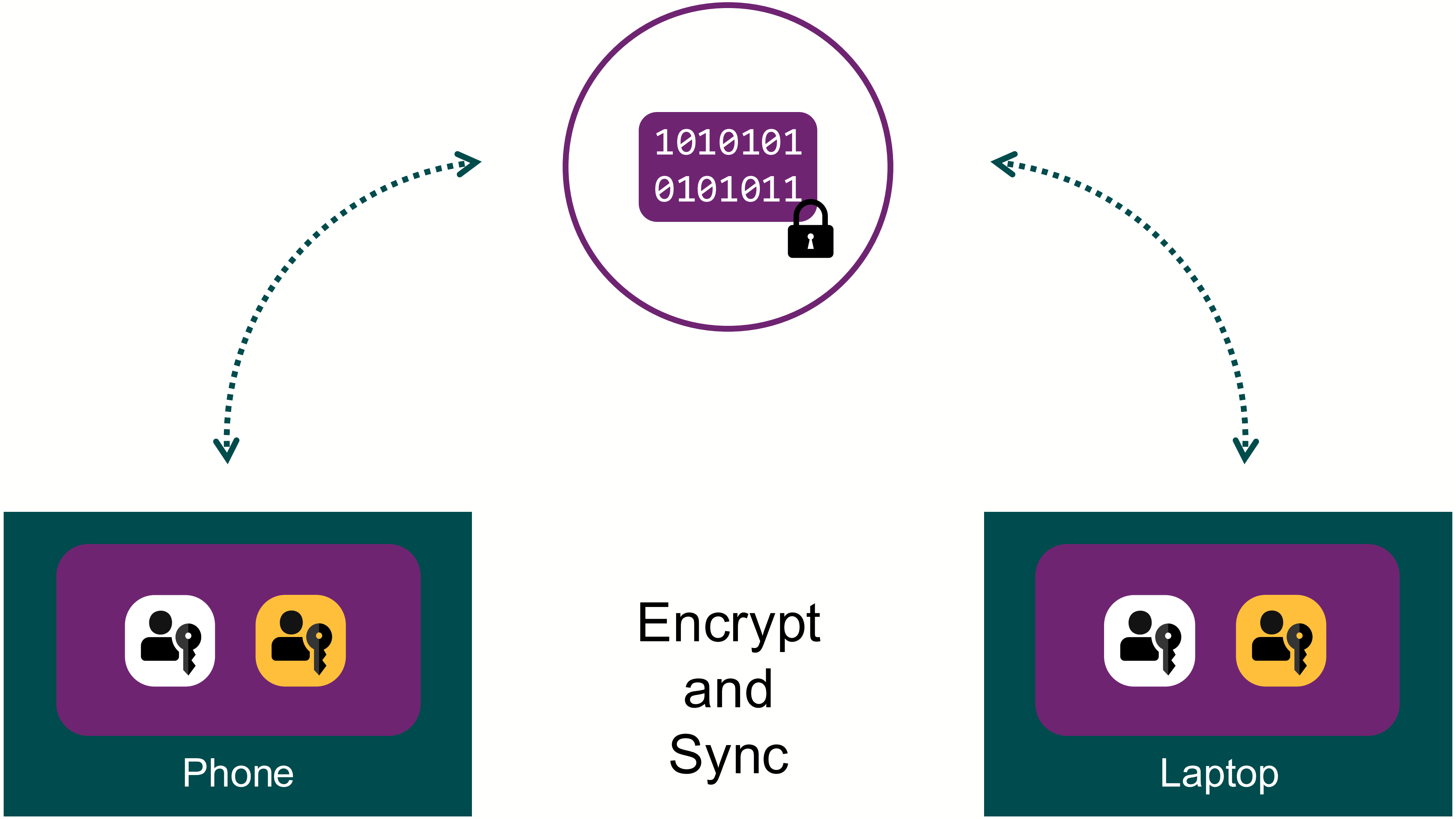
- *"Synced passkeys are not stored in the providers systems (the cloud), and only leverage the cloud as transport to sync from one device to another"*
- *"Synced passkeys are stored in the providers systems (the cloud) in end-to-end encrypted, and therefore non-operational, form"*
- *"Synced passkeys are stored in the providers systems (the cloud) in the clear, and therefore operational, form"*



Phone

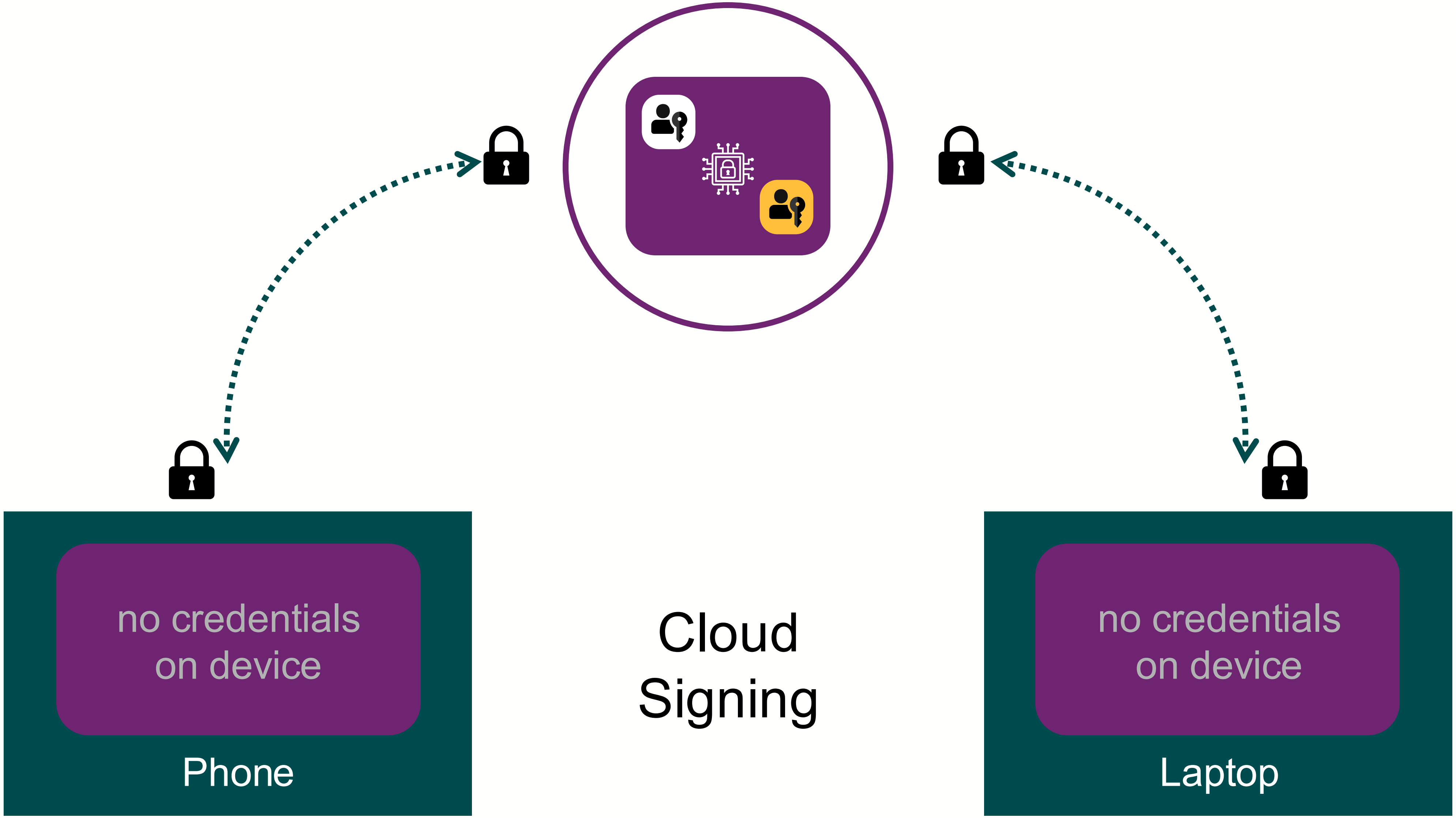
Device-Bound Passkeys

Laptop



Encrypt
and
Sync

Cloud Signing



no credentials on device

Phone

no credentials on device

Laptop

> *RP IDs are the primary defense against phishing attacks.*

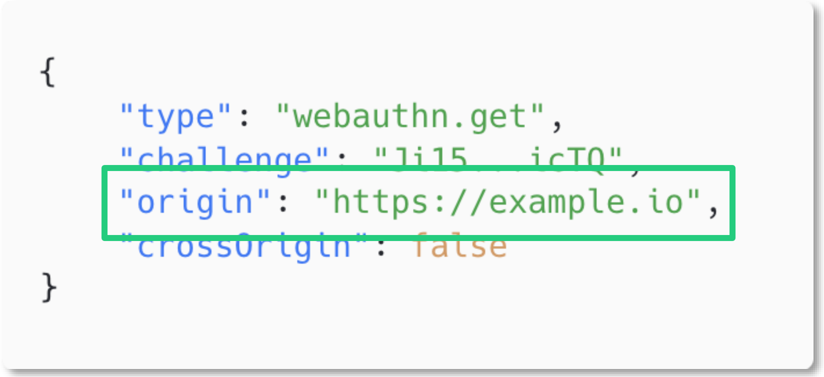
Misconception:

"RP IDs are the primary defense against phishing attacks."

Reality:

Authenticators **sign over the origin** where the WebAuthn call occurred, as reported by the **browser**. RPs can **explicitly verify** that a response came from an expected origin.

clientDataJSON



```
{
    "type": "webauthn.get",
    "challenge": "Ji15...icTQ",
    "origin": "https://example.io",
    "crossOrigin": false
}
```

Valid Origins:

https://example.com
https://example.co.jp
https://example.io

Welcome In!

RP ID plays a role, but more for user agent pre-selection

matthew@example.com
`login.example.com`

Usable on...?

- ✅ `https://login.example.com`
- ❌ `https://login.example.xyz`
- ❌ `https://fidoalliance.org`
- ❌ `https://Iogin.example.com`

Passkeys don't defend against remote attacks.

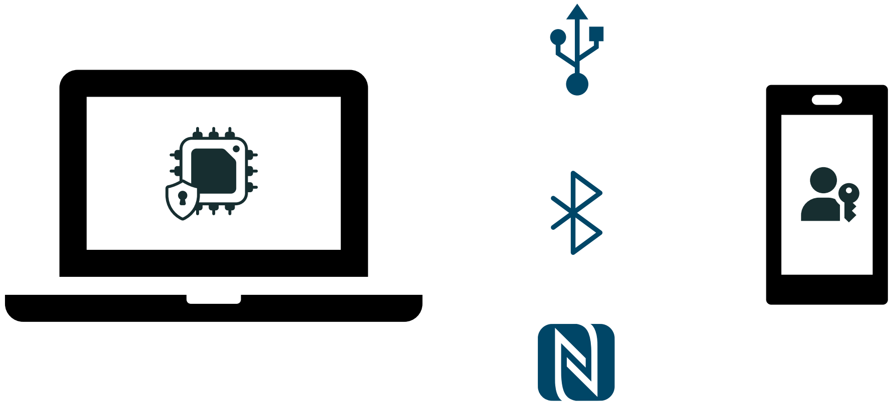
Misconception:

"Passkeys don't defend against remote attacks."

Reality:

FIDO2 mandates user control of the authentication device. Typically, this is the **same as the access device**. FIDO **Cross-Device Authentication** allows a second device to be used for authentication but **still enforces proximity.**

Proximity



> *Cross-device authentication is phishable QR code auth.*

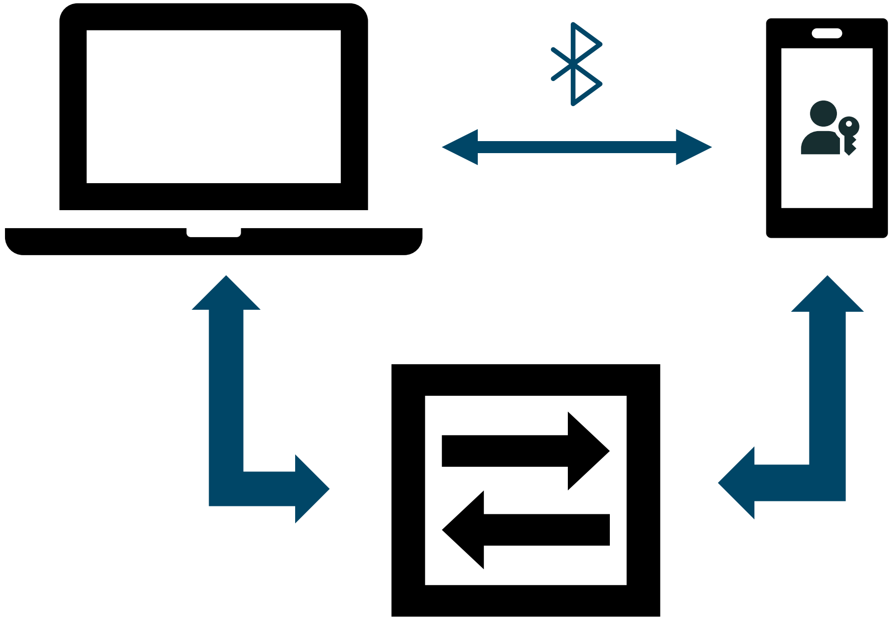
Misconception:

"Cross-device authentication Is phishable QR code auth."

Reality:

Scanning the QR code triggers the use of **BLE** to establish proximity. A WebAuthn response is then returned **from the mobile device** over an end-to-end encrypted connection through a WebSocket.

Proximity via BLE



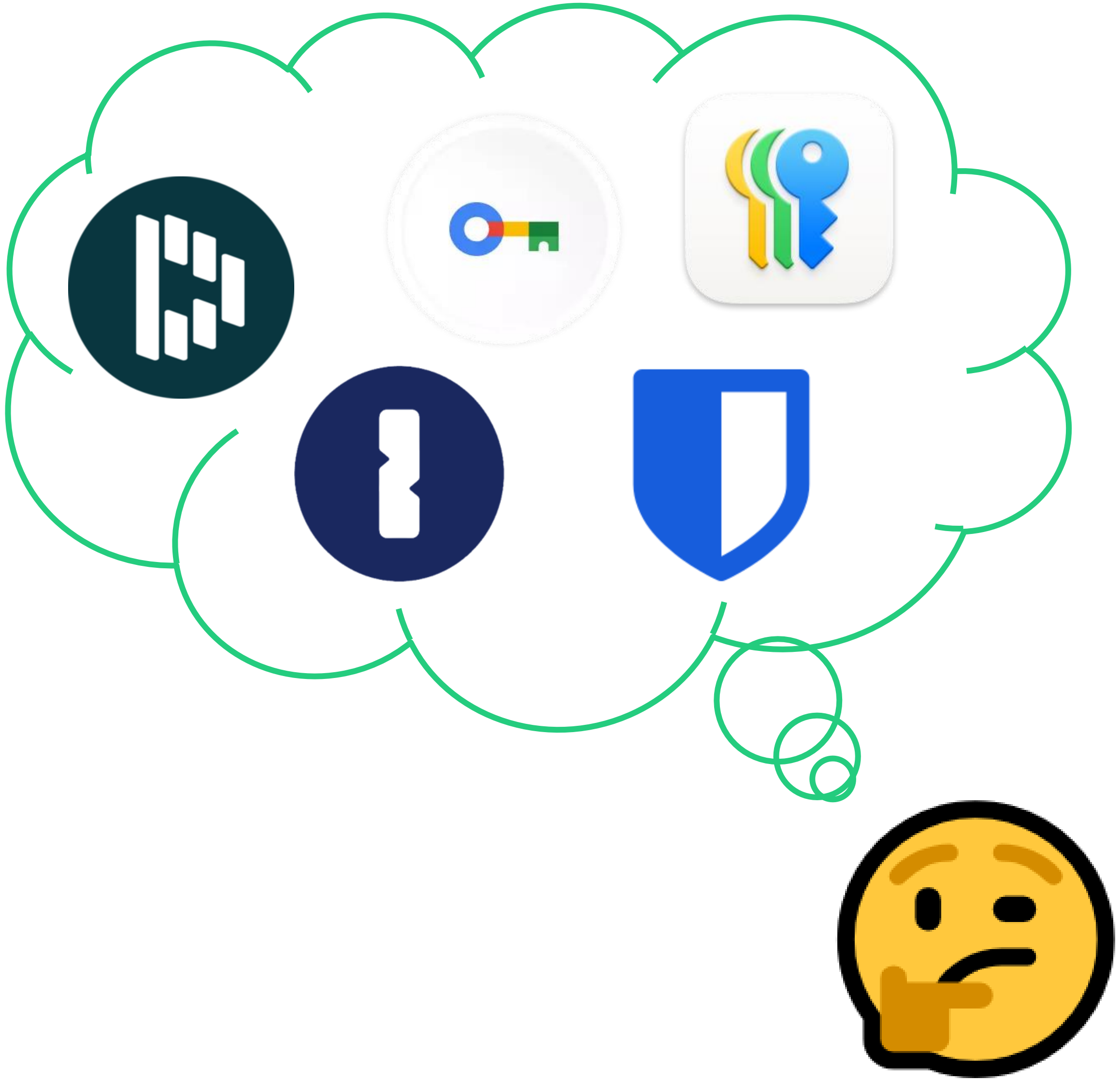
> *Passkeys are a way for Big Tech to lock users into their ecosystem.*

Misconception:

"Passkeys are a way for Big Tech to lock users into their ecosystem."

Reality:

OS-provided credential managers are many people's first. But the passkey ecosystem offers myriad third-party choices for users and enterprises alike. BYOCM is the prevailing implementation model.



decisions, decisions...

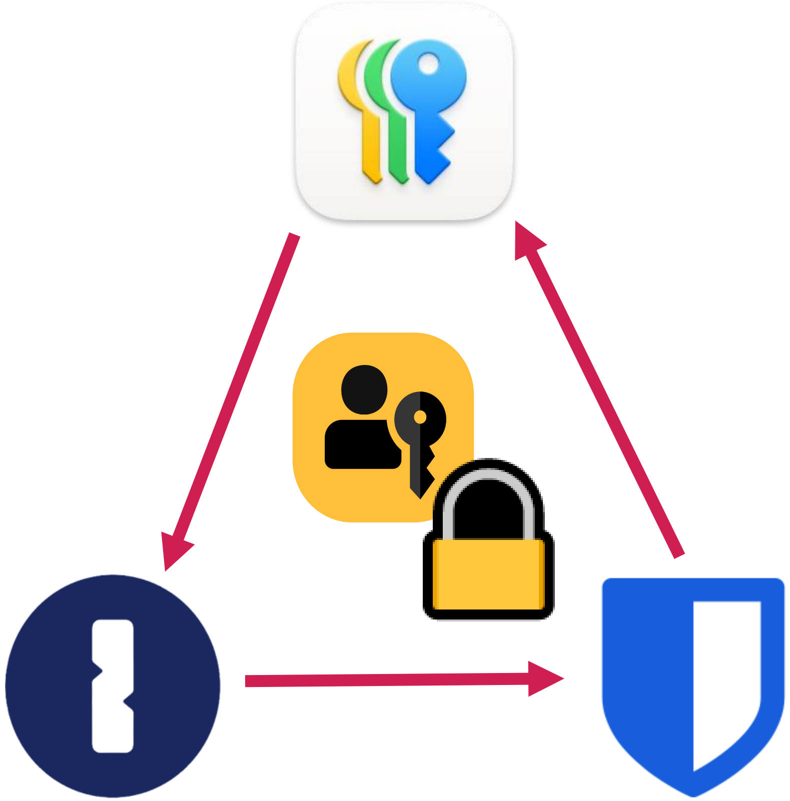
> *My passkeys will get stuck on my iPhone if I switch to Android!*

Misconception:

"My passkeys will get stuck on my iPhone if I switch to Android!

Reality:

FIDO CXP realizes the long-term vision of offering user choice while avoiding the same risks that plagued password migration. It enables provider-to-provider migrations without putting passkeys at risk.



© FIDO Alliance 2025

> *Passkeys are not suitable for workforce use cases.*

"Passkeys are not suitable for workforce use cases."

- ➢ *"I can only use passkeys if I am managing all the devices."*
- ➢ *"My workforce will be able to sync their work passkeys to their personal devices."*
- ➢ *"Only device-bound passkeys are suitable for workforce use cases."*

Misconception:

"I can only use passkeys if I am managing all devices."

Reality:

Synced passkeys are available by default on consumer devices, no management or special configuration required.

Managed credential managers do not require device management (but can be enhanced using DM)

Misconception:

"My workforce will be able to sync their work passkeys to their personal devices."

Reality:

If users are not provided a credential manager / authenticator that meets your business requirements, this is true!

The default credential managers on unmanaged, user owned devices are designed for consumer scenarios and user control.

Misconception:

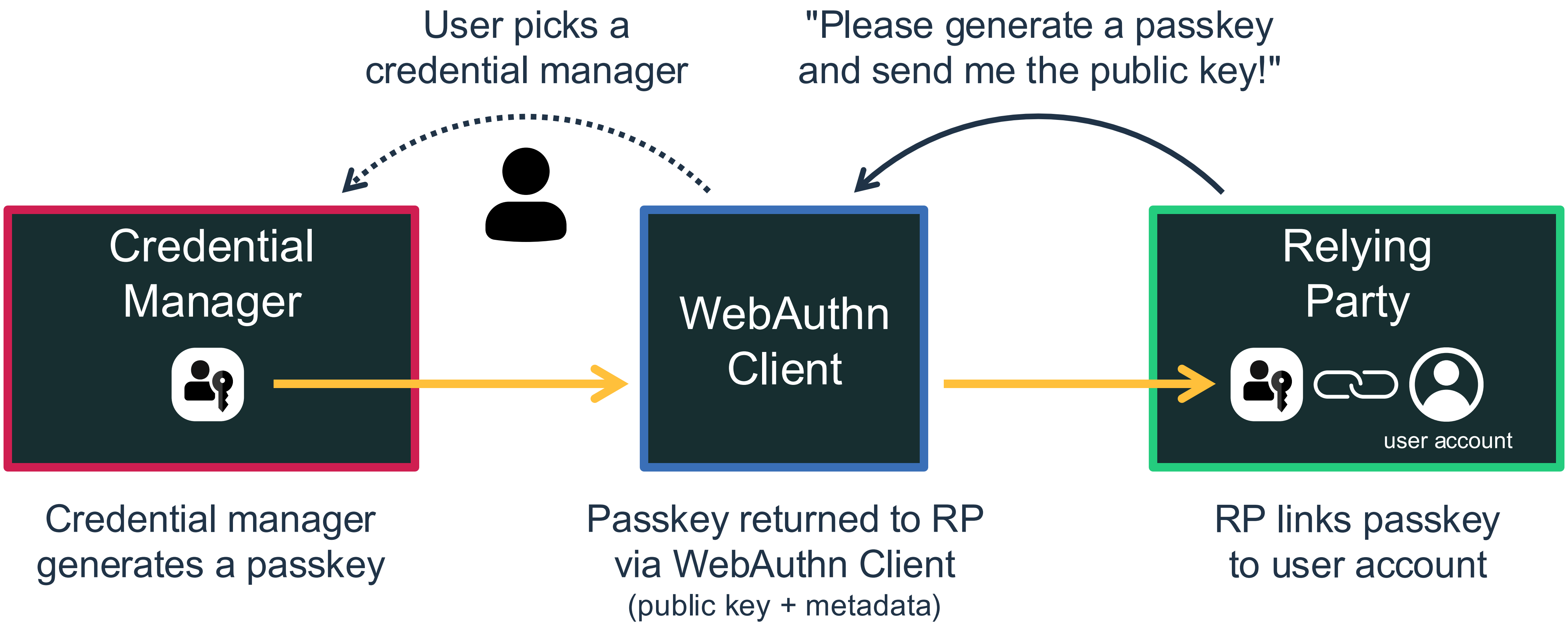
"Only device-bound passkeys are suitable for workforce use cases."

Reality:

Nearly every organization has groups of users for which synced passkeys are more than adequate (typically people who only have access to their own data).

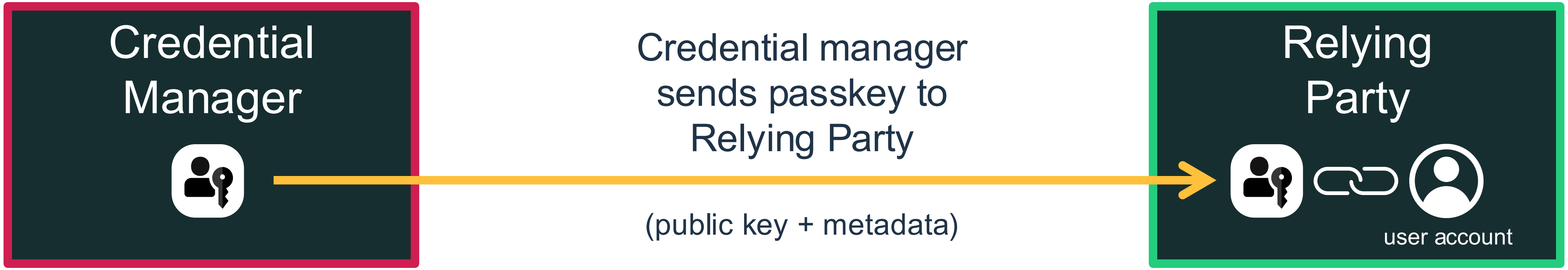
In cases where more control is desired, managed credential managers can provide policy and controls for synced or device-bound passkeys.

Provide ~~Bring~~ Your ~~Own~~ Key



Provide ~~Bring~~ Your ~~Own~~ Key

Credential manager
generates a passkey
(user or admin initiated)



Credential Manager

Credential manager
sends passkey to
Relying Party

(public key + metadata)

Relying Party

user account

RP links passkey
to user account

Q&A