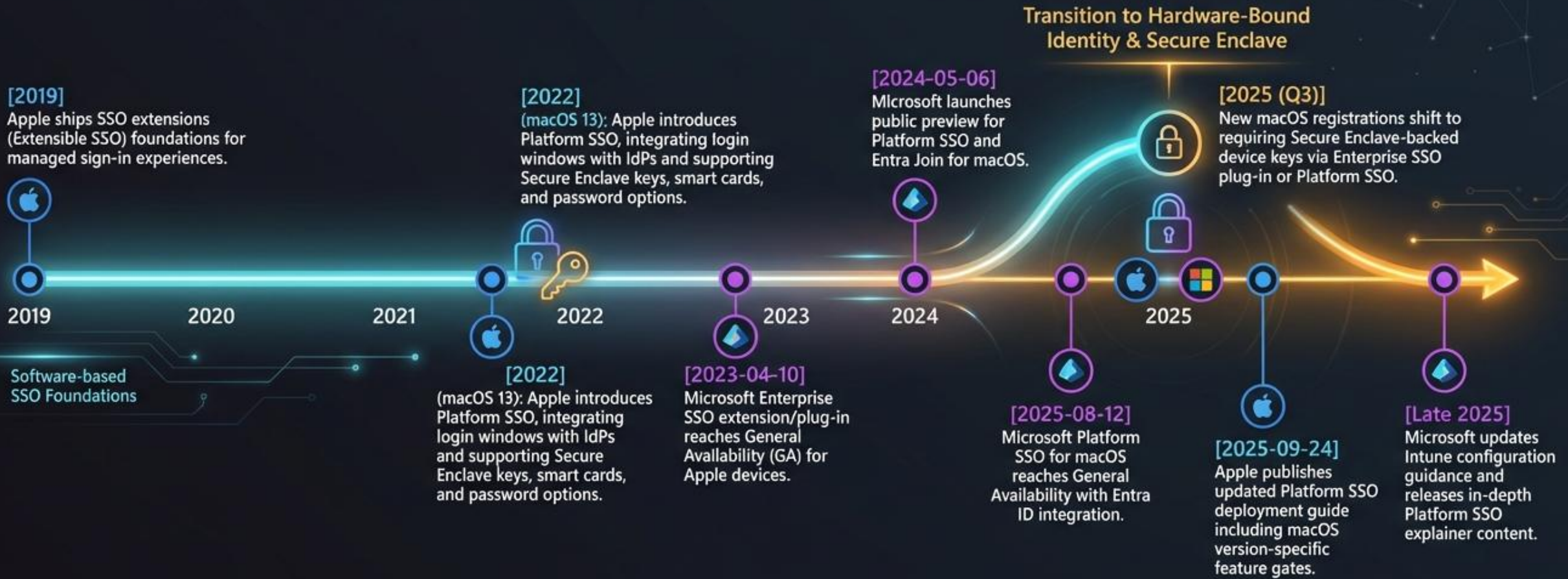


From Enterprise SSO to Platform SSO and Beyond with Microsoft Entra ID

Victor H. Vargas
Principal PM Manager
Identity, Network Access +
Artificial Intelligence
Customer Experience (CxE)

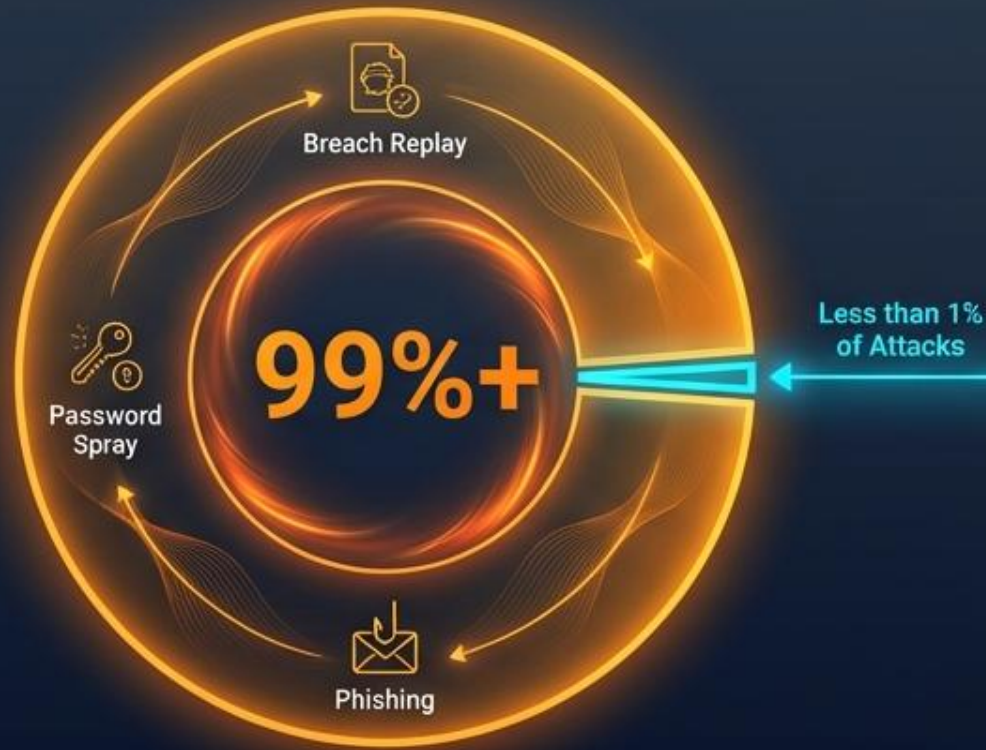
Timeline of Apple and Microsoft Platform SSO Integration (2019–2025)



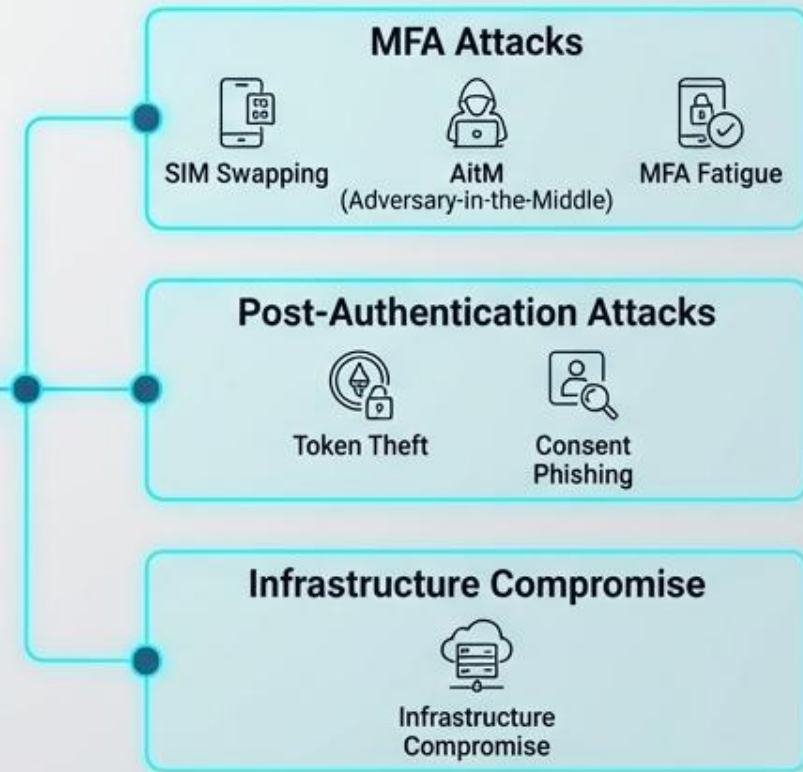
Why it matters?:

Cybersecurity Challenges

Over 99% of Identity Attacks are Password-Based



Sophisticated Attacks (Less than 1%)



Phishing: A Major Threat, Responsible for >70% of Data Breaches



Basic Security Hygiene: Implements Measures to Protect Against 98% of Attacks



Password-Based Attacks: Exploit Predictable Human Behaviors, Preventable by Strong Authentication Methods

PHISHING: TRADITIONAL CREDENTIAL VULNERABILITY



CORE DATA: Your password doesn't matter. Traditional credentials are fundamentally vulnerable to interception and deception.

PASSWORD REUSE

SINGLE COMPLEX PASSWORD: MAJOR WEAKNESS



Using the same complex password across multiple accounts, even a complex one, introduces a major security weakness.

THE DOMINO EFFECT



A breach on one site leads to a 'domino effect' where all other reused accounts are compromised.

MODERN SOLUTION: PHISHING-RESISTANT AUTHENTICATION



~~YOUR PASSWORD~~
DOESN'T MATTER

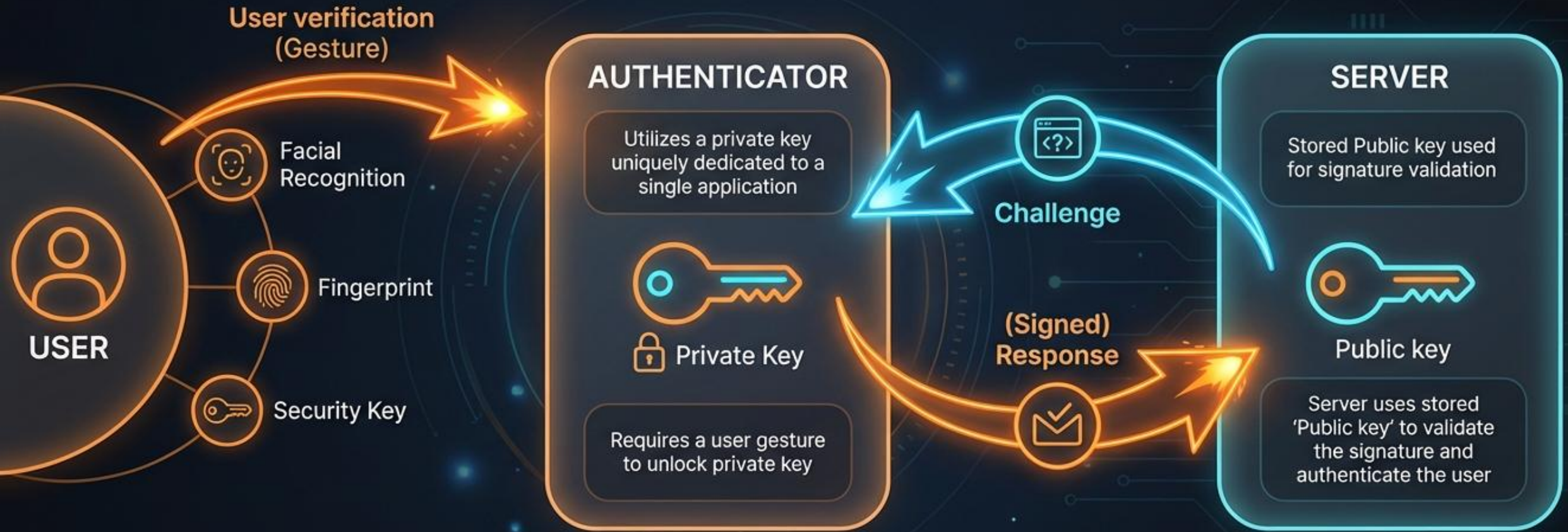
Phishing-resistant authentication renders the traditional password obsolete and significantly more secure.

Move beyond passwords for true security. Embrace phishing-resistant methods.

Phishing-Resistant Authentication Overview



FIDO Authentication: How it works



- Requires a user gesture (facial recognition, fingerprint, security key, or PIN) before the private key can be accessed.
- The Authenticator utilizes a private key that is uniquely dedicated to a single application.

- Authentication involves a challenge-response loop where the server sends a 'Challenge' to the Authenticator.
- The Authenticator returns a '(Signed) Response' to the server for verification.

- to the server for verification.
- The server uses a stored 'Public key' to validate the signature and authenticate the user.

3 Authentication Methods Support by Platform SSO



GOOD

PASSWORD

- ✓ **Local Account Sync (Entra ID)**
Supports sync with Entra ID
- ✓ **Federation Support (WS-Trust)**
Supports via WS-Trust
- ✗ **MFA for Registration**
Lacks MFA registration requirements
- ✗ **Phishing Resistant**
Lacks phishing resistance



BETTER

SMARTCARD

- ✓ **Federation Support**
Offers federation support
- ✓ **MFA for Registration**
Requires MFA for registration
- ✓ **Phishing Resistant**
Is phishing resistant
- ✓ **Local PIN/Passcode MDM**
Deferred to MDM



BEST

SECURE ENCLAVE KEY

- ✓ **Highest Security**
Provides highest security
- ✓ **Built-in Apple Hardware Phishing Resistance**
(using Windows Hello protocols)
- ✓ **Passkey Capabilities**
Passkey capabilities included

THE FIDO2 SECURITY PROMISE

Securing the future with unphishable, cryptographic credentials.



THE PERFECT ATTACK



REMOTE

Executed from anywhere with zero physical presence.



UNDETECTED

Evades security tools and surveillance for prolonged periods.



DURABLE

Maintains persistent access, resilient to countermeasures.



CHEAP

Low cost of entry, accessible to wide range of threat actors.



SCALABLE

Easily replicated across large targets with automated tools.



FIDO2 SECURE CREDENTIAL



UNGUESSABLE

Cryptographically generated keys, impossible to brute-force.



UNDISCLOSABLE

Private keys never leave the secure hardware authenticator.



MULTI-FACTOR

Requires something you have, something you are, or something you know.



SINGLE-USER

Credential is bound to a specific user identity, non-transferable.



LOCAL

Authentication occurs on the user's device, no shared secrets.



UNINTERCEPTABLE

Communication channels are encrypted, preventing man-in-the-middle.

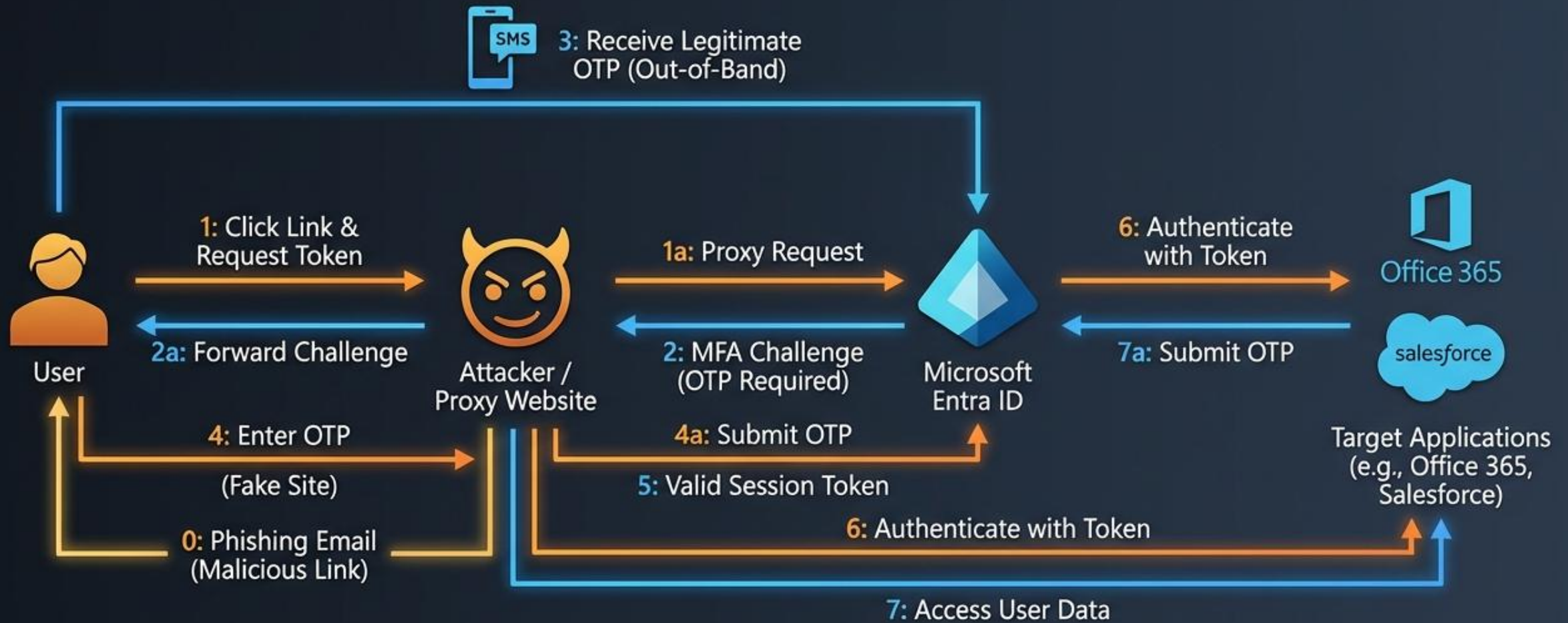


UNPHISHABLE

Origin-bound credentials only work on the legitimate website.

fido²
FACTUALLY ACCURATE SECURITY

MITM: How Machine-in-the-Middle defeats OTP





SECURE

- Unique credentials & asymmetric keypairs
- Inherently phish-resistant
- Global standard part



fid02 FIDO2: Best by Design



EASY TO USE

- Eliminates passwords (no need to remember, lose, or change)
- Eliminates one-time passcodes
- Simple gestures: taps, fingerprints, or facial scanning



INTEROPERABLE

- Works across all major browsers: Chrome, Firefox, Safari, Edge
- Platforms: Windows, Android, iOS, macOS
- Various form factors supported



TRUSTWORTHY

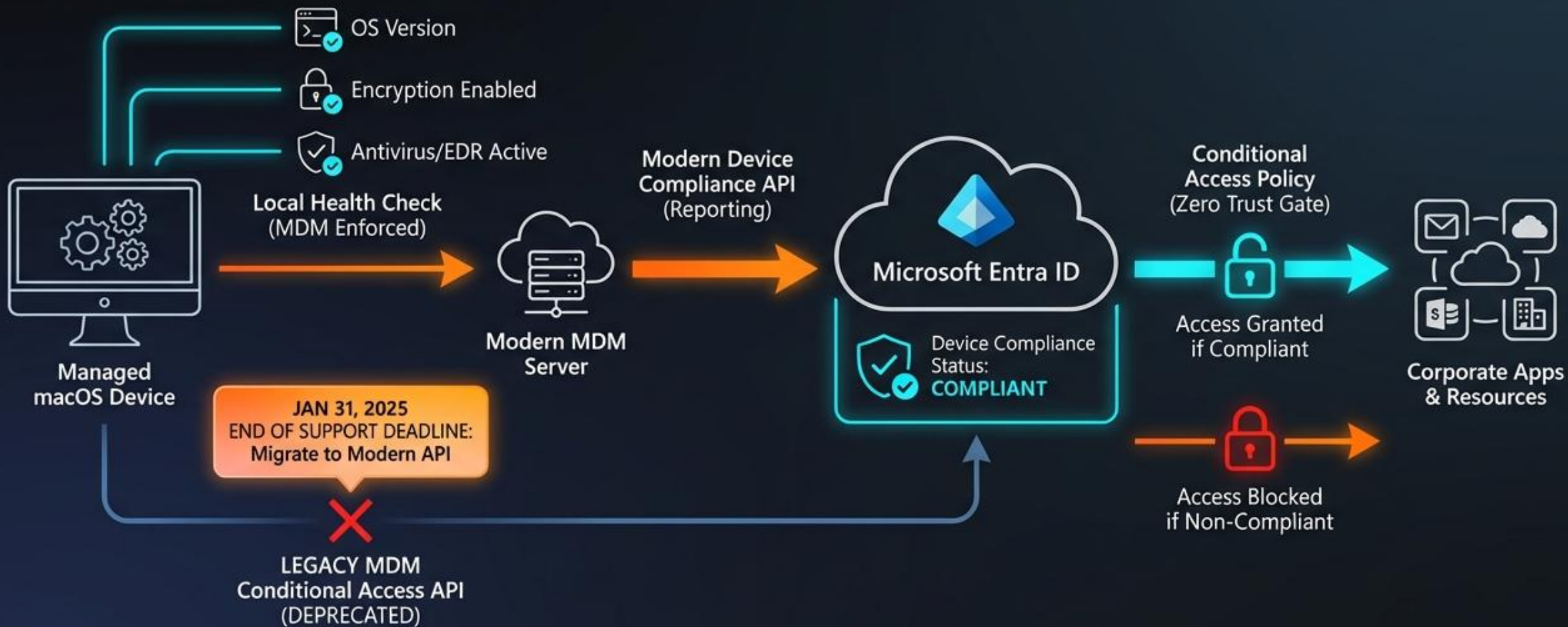
- Built on standards: WebAuthn & CTAP
- Biometrics never leave the device
- No sharing of personal info like email or phone numbers



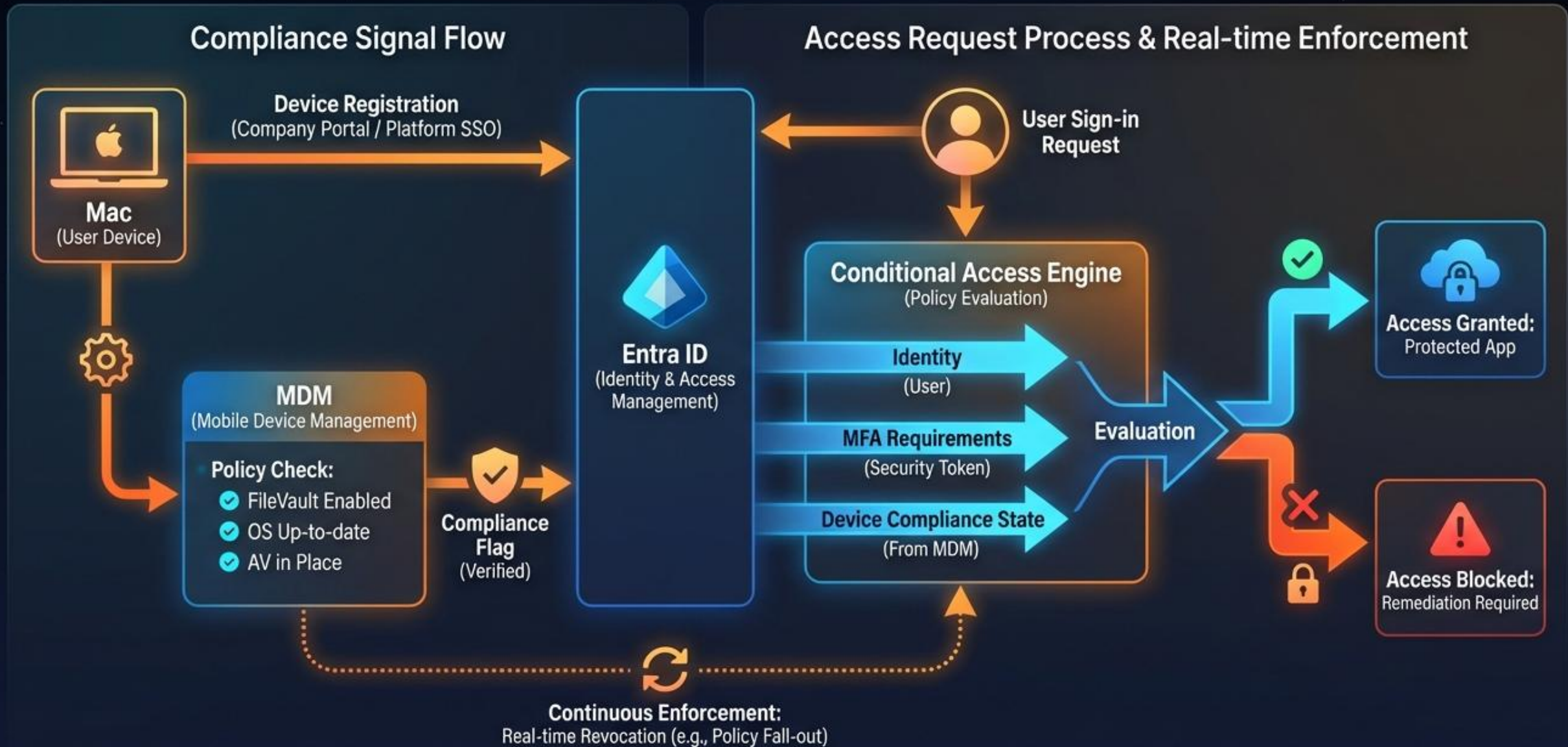
Modern Identity for macOS with Microsoft Entra

Microsoft Entra Device Compliance

Evaluates security requirements (OS, encryption, AV), MDM integrates via Entra's modern Device Compliance API, **Required for Conditional Access** → Zero Trust on macOS, Legacy MDMs Conditional Access deprecated.

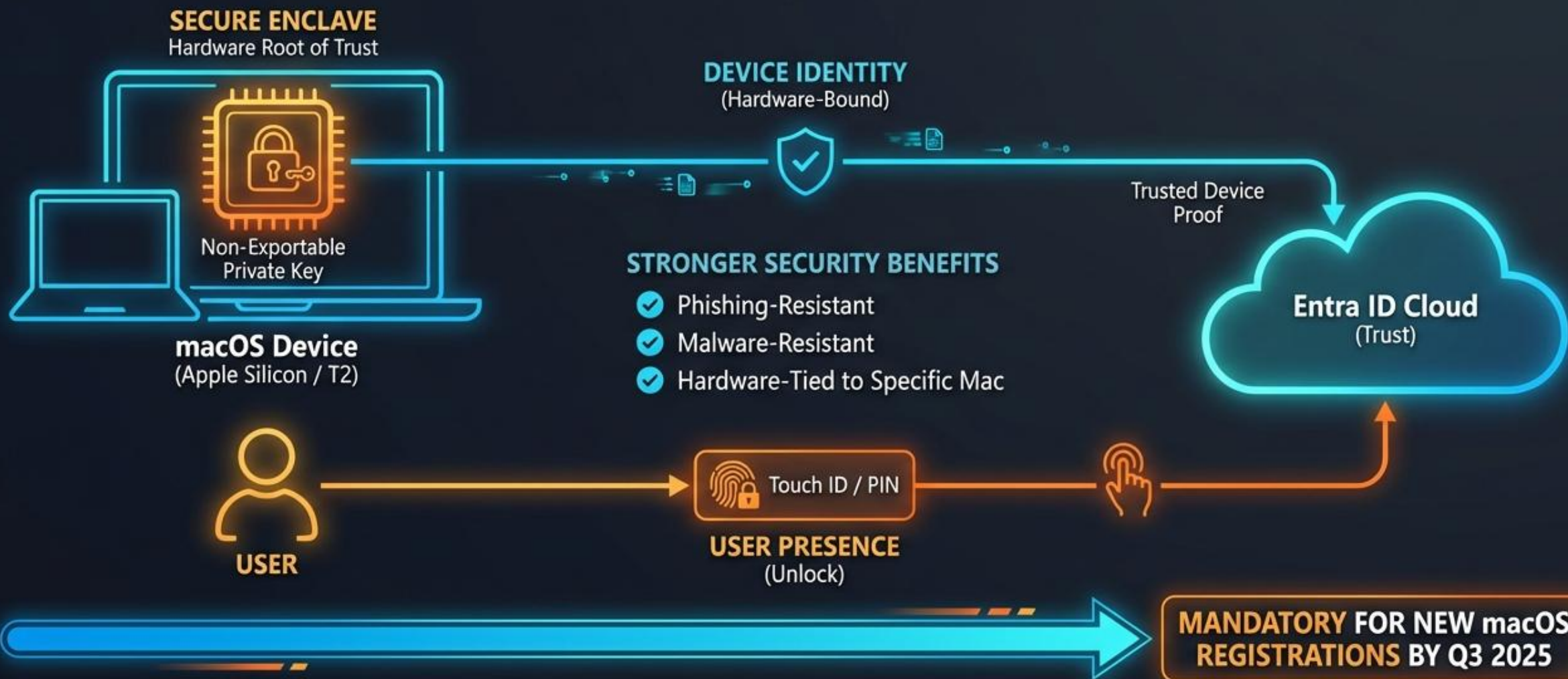


How Entra ID Calculates Compliance & Grants Access



SECURE ENCLAVE – DIFFERENTIATING USER VS. DEVICE IDENTITY

Hardware-Bound Keys, Separate Credentials, Stronger Security for macOS Platform SSO



Why are PINs better than Passwords?

1. Tied to Device (Useless Without It)



Secure Enclave Communication via Protected API. Device-Specific Binding.



Passwords can be replayed anywhere.

2. Local to Device (Not Transmitted)



Local Authentication Prevents Interception. Resistant to Phishing.



Passwords are often transmitted.

3. Backed by Hardware (Physical Foundation)



Security Foundation Built into Physical Hardware. Private Keys Locked in Chip.

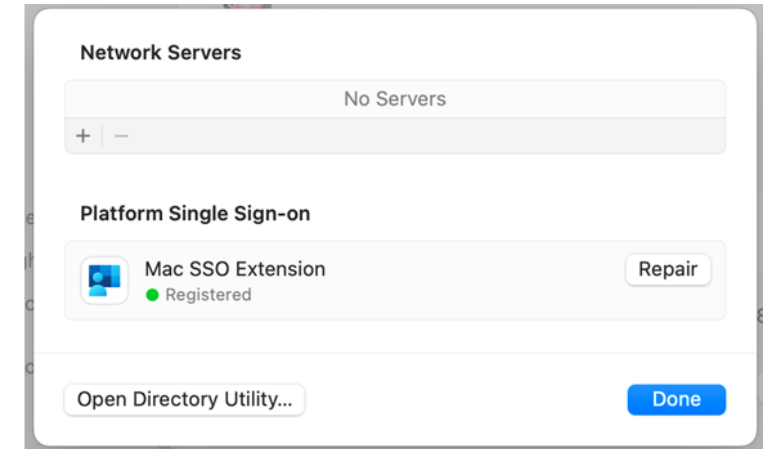
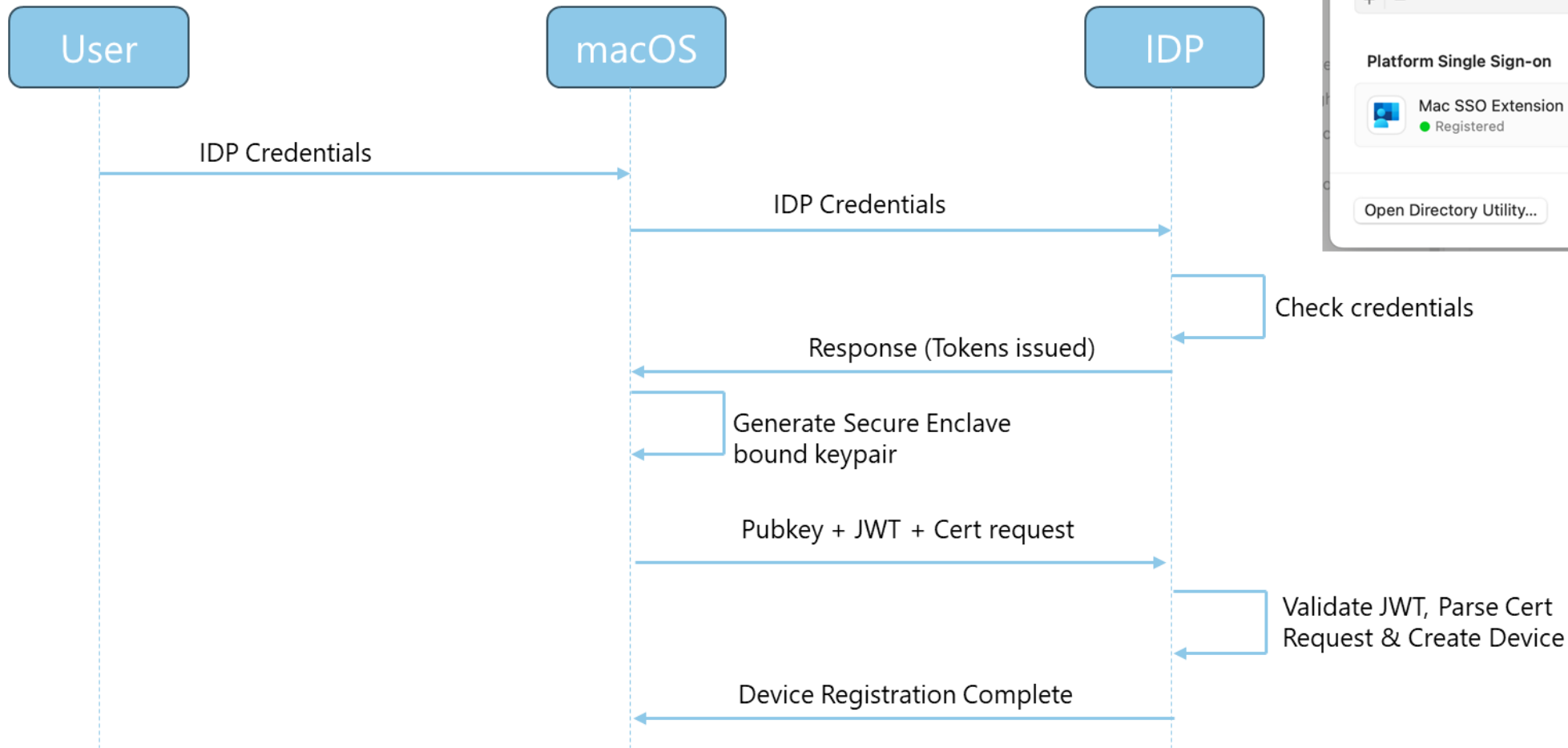


Software-only solutions are vulnerable.

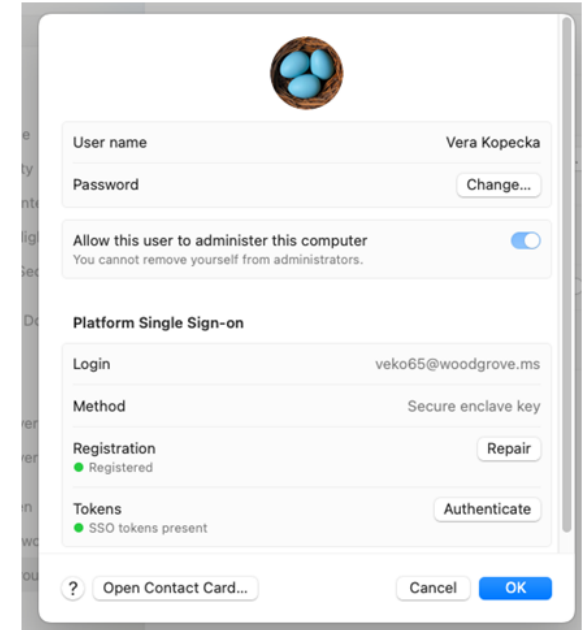
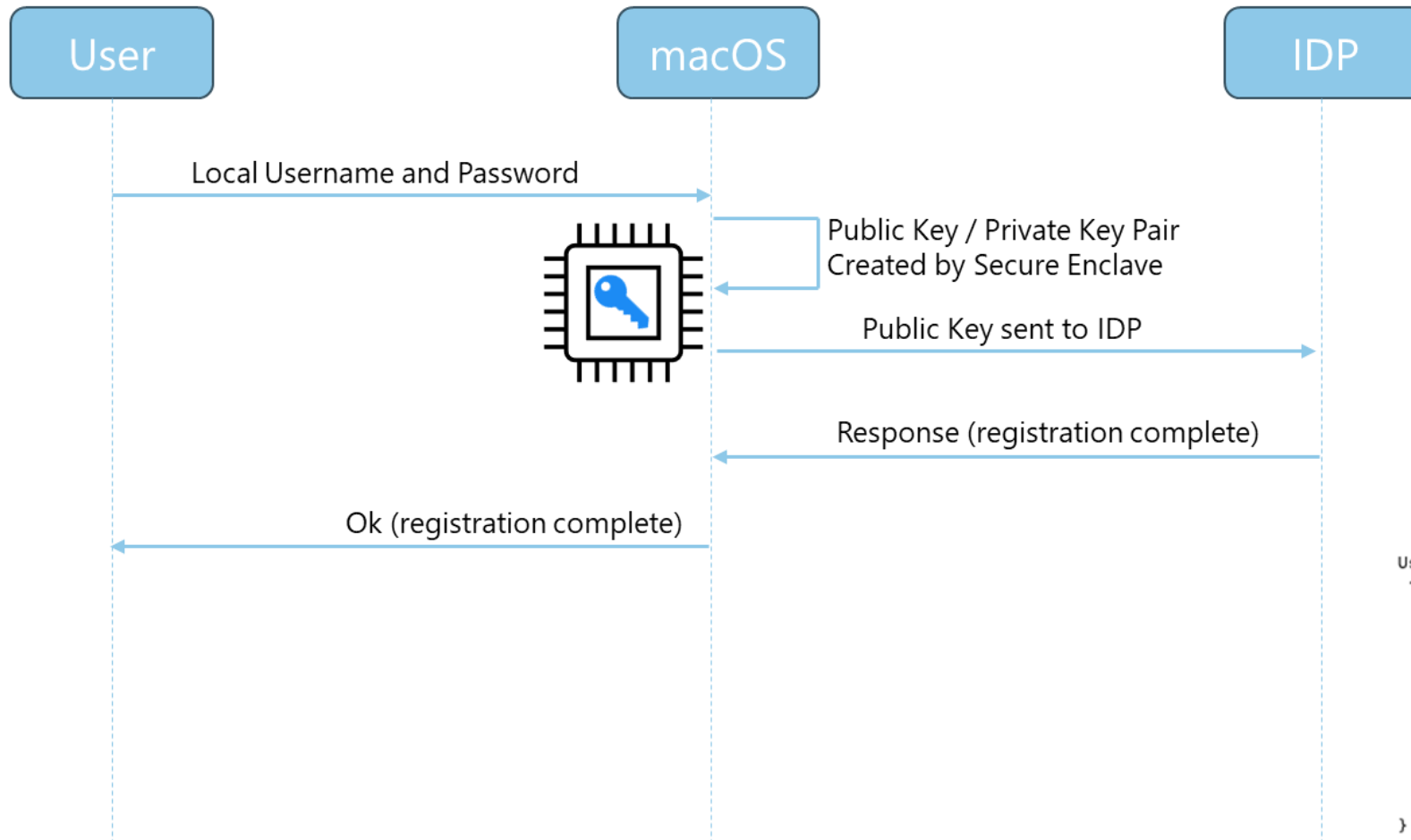
Modern Authentication: Moving to Hardware-Backed PINs & Touch ID for True Phishing Resistance.

Deep Dive:

Step 1: Device Registration



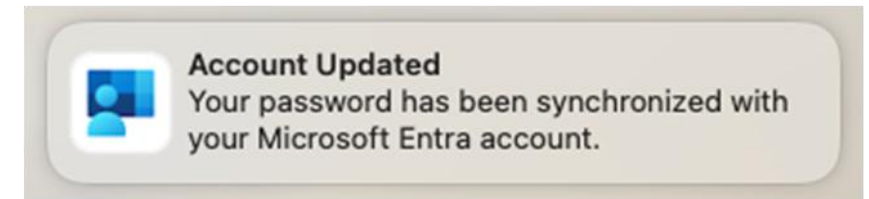
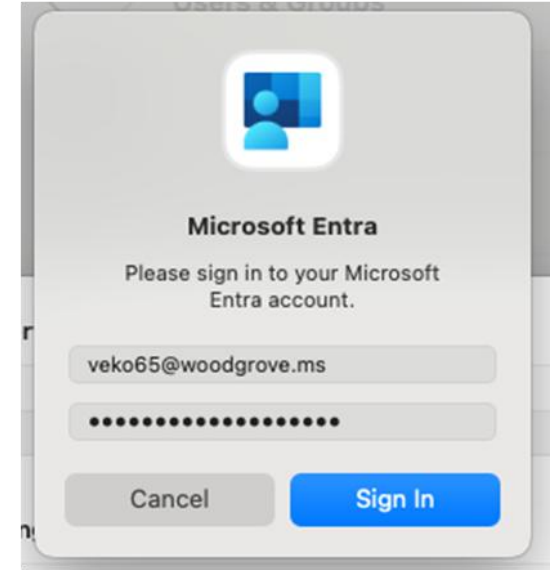
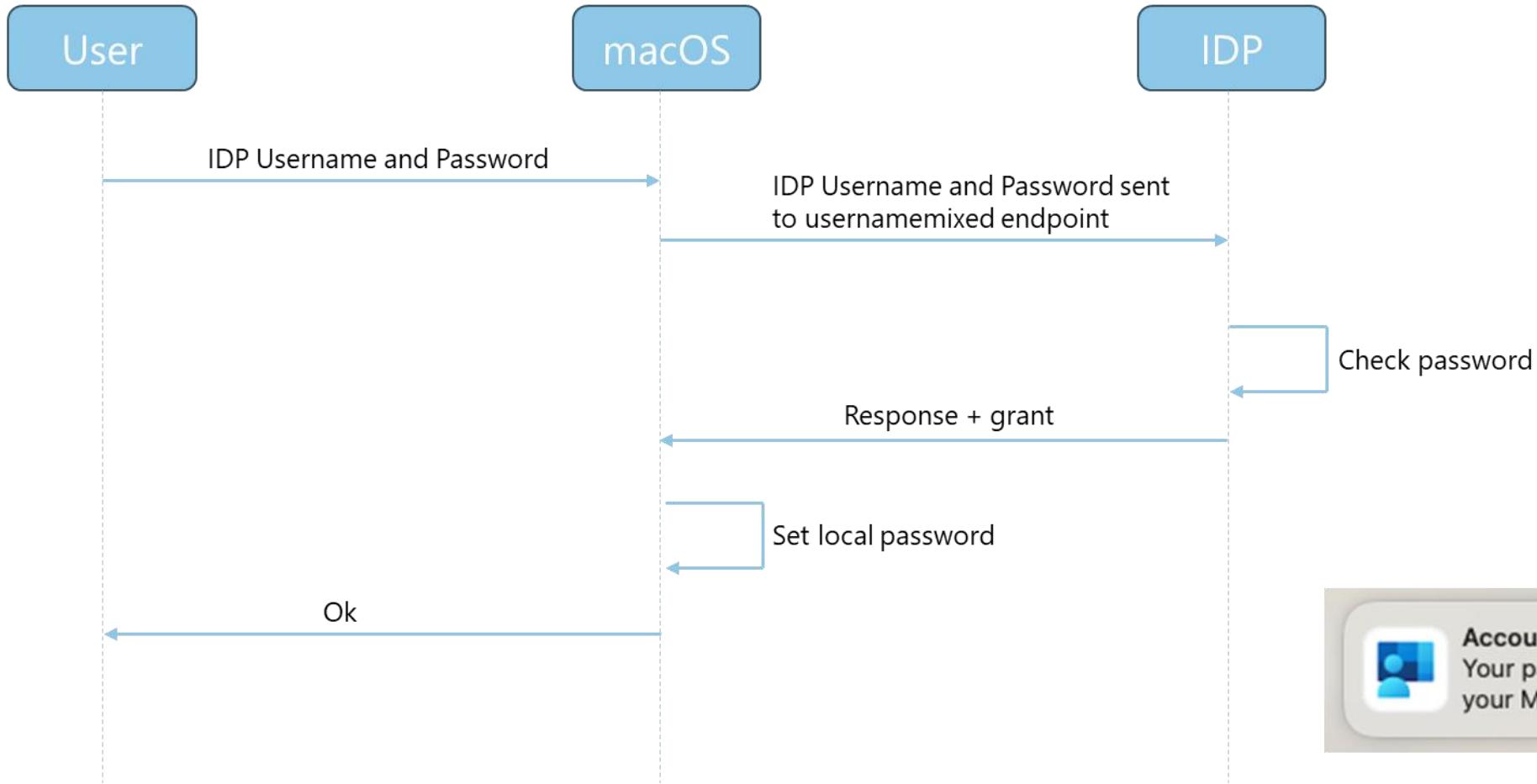
Step 2: User Registration - Secure Enclave Key Flow



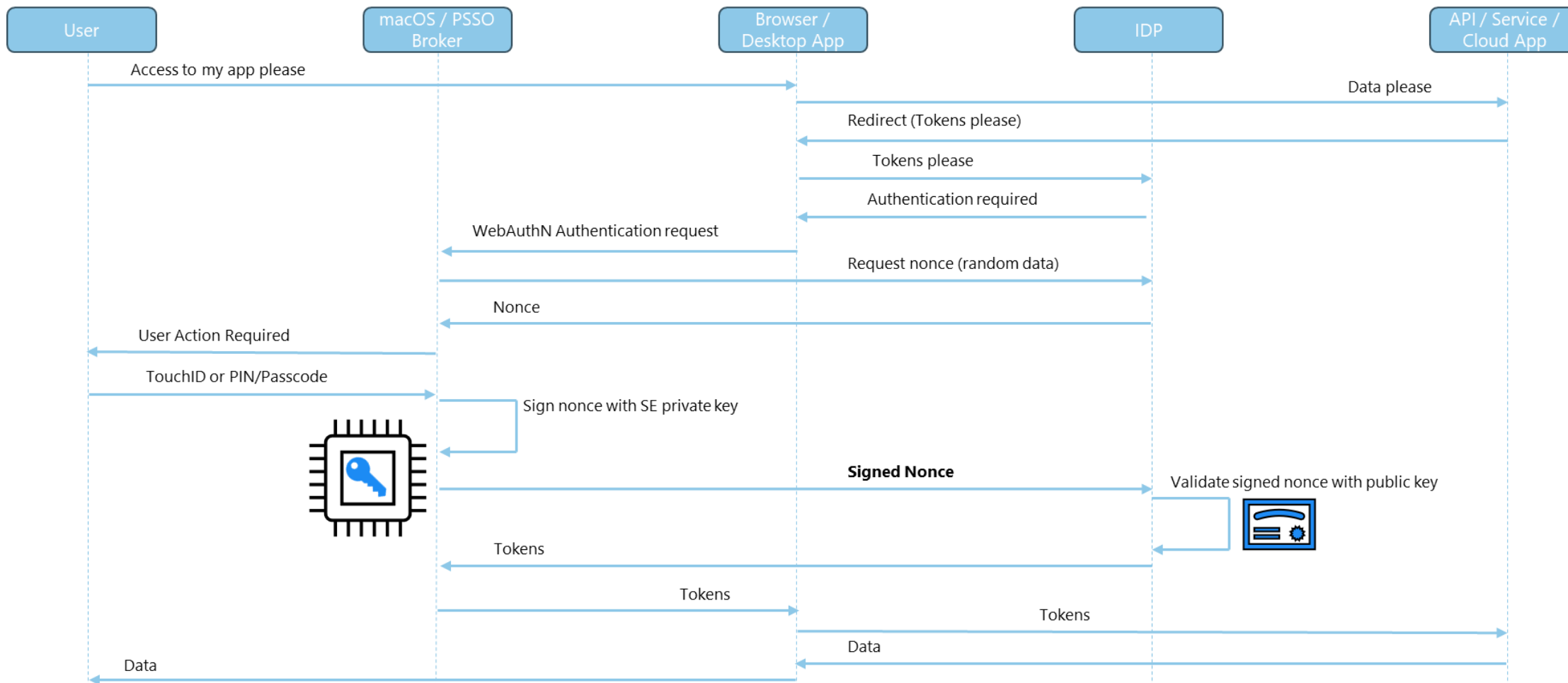
User Configuration:

```
{
  "_sepKeyData" : "cpRyk+90gI1JMO6zFpYVUqbx+3R85P+Bdwi91ERTKZE=",
  "created" : "2024-07-03T21:30:42Z",
  "lastLoginDate" : "2024-07-03T21:29:49Z",
  "loginType" : "POLoginTypeUserSecureEnclaveKey (2)",
  "state" : "POUserStateNormal (0)",
  "uniqueIdentifier" : "4251CE01-07A2-40B5-A267-BCC3667A96A6",
  "userLoginConfiguration" : {
    "created" : "2024-07-03T21:30:42Z",
    "loginUserName" : "v***@woodgrove.ms"
  },
  "version" : 1
}
```

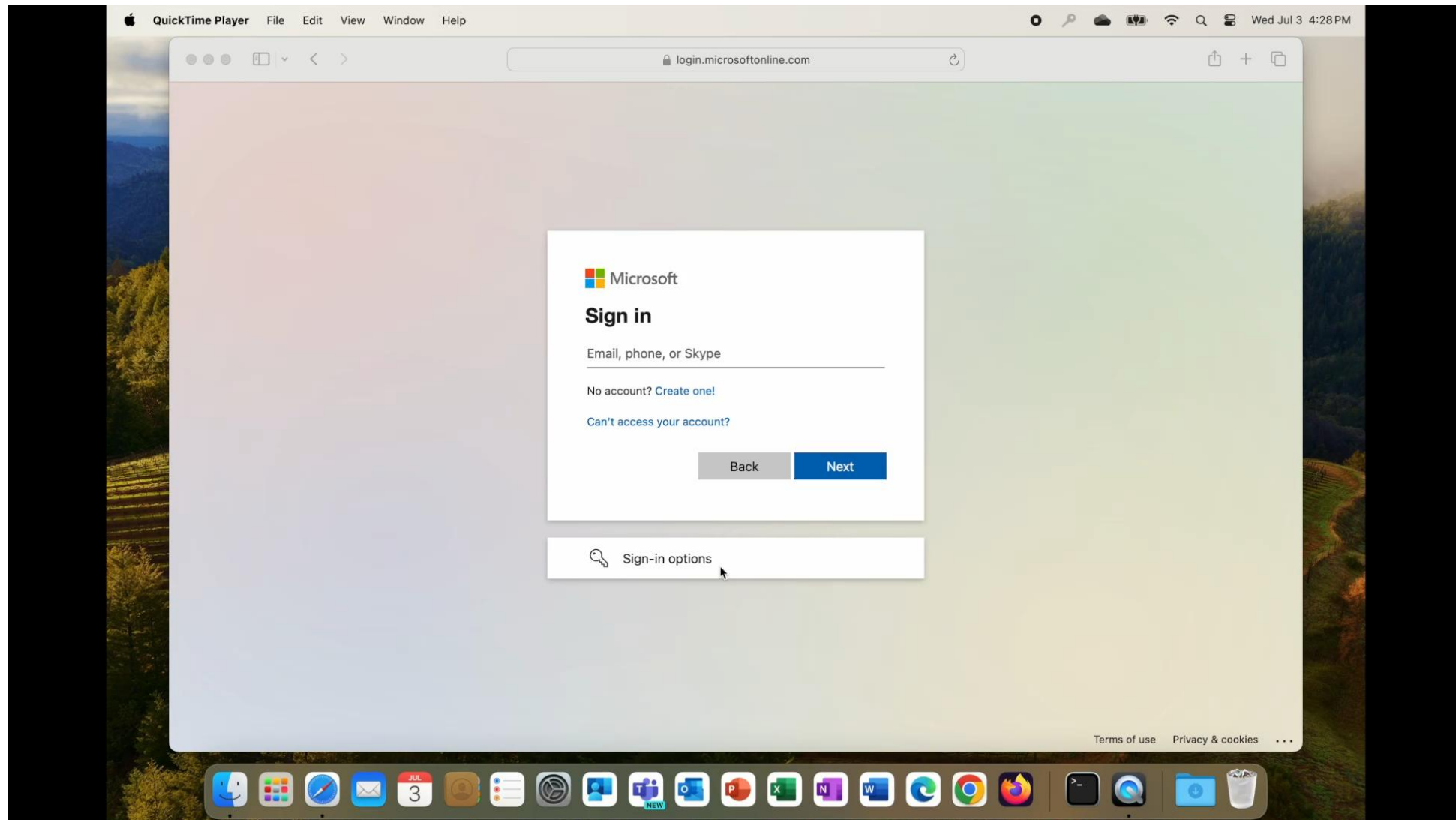
Step 2: User Registration - Password Sync Flow



Secure Enclave Key Interactive Authentication Flow



Secure Enclave Key Registration Experience



What PSSO Means for IT Admins

Platform SSO: macOS Login with Entra ID for True SSO

Benefits

- Fewer Prompts & Login Fatigue
- Passwordless Sign-in
- Synced Accounts
- Automatic Device Join into Entra

Business Applications



macOS Login Screen



Phishing-Resistant Verification (Secure Enclave Keys)



Challenges

- Deployment Complexity (New MDM Profiles)
- User Training (New Login Experience)
- Shared Mac Scenarios (Extra Config)

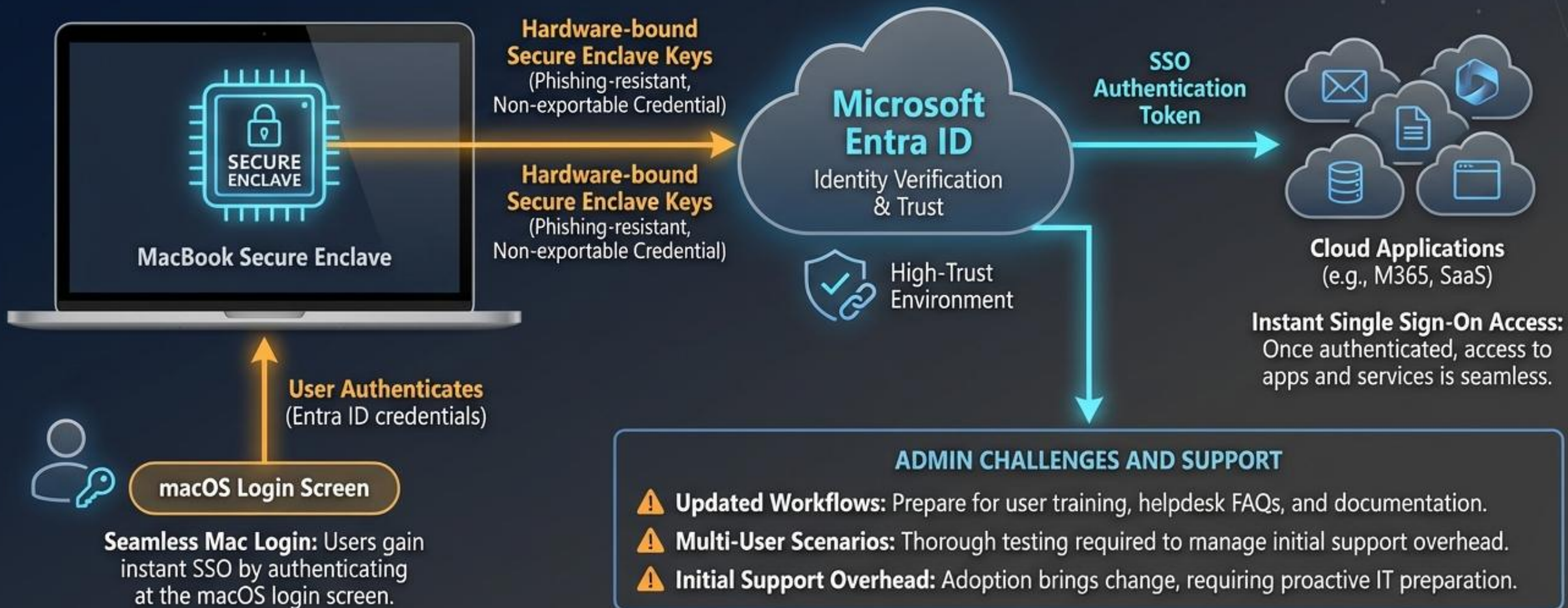
GA: Aug 2025



Closing:

Platform SSO: Key Benefits and Implementation Considerations

Seamless Mac Login, Stronger Authentication, and Admin Realities




What's Next for Platform SSO on macOS


Apple & Microsoft Entra Roadmap (High-Level) - Evolving from "SSO for apps" to "identity-native macOS"



WHAT THIS MEANS

 **For users:** Fewer prompts, faster sign-in, and a Windows-Hello-like experience on Mac.

 **For security teams:** Hardware-bound identity, phishing resistance, and consistent Conditional Access enforcement.

 **For IT:** Simplified onboarding, fewer helpdesk tickets, and cloud-first macOS identity without directory binding.

Bottom line: Platform SSO is becoming the foundation for passwordless, cloud-native macOS identity.

Resources:

[Configure Platform SSO for macOS devices - Microsoft Intune | Microsoft Learn](#)

[Troubleshooting the Microsoft Enterprise SSO Extension plugin on Apple devices - Microsoft Entra ID | Microsoft Learn](#)

[Get started with a phishing-resistant passwordless authentication deployment in Microsoft Entra ID - Microsoft Entra ID | Microsoft Learn](#)