The Intersection of Passwordless and Zero Trust

Abrom Douglas III
InfraGard Tampa Bay
Sept 2023

Agenda

History of IAM

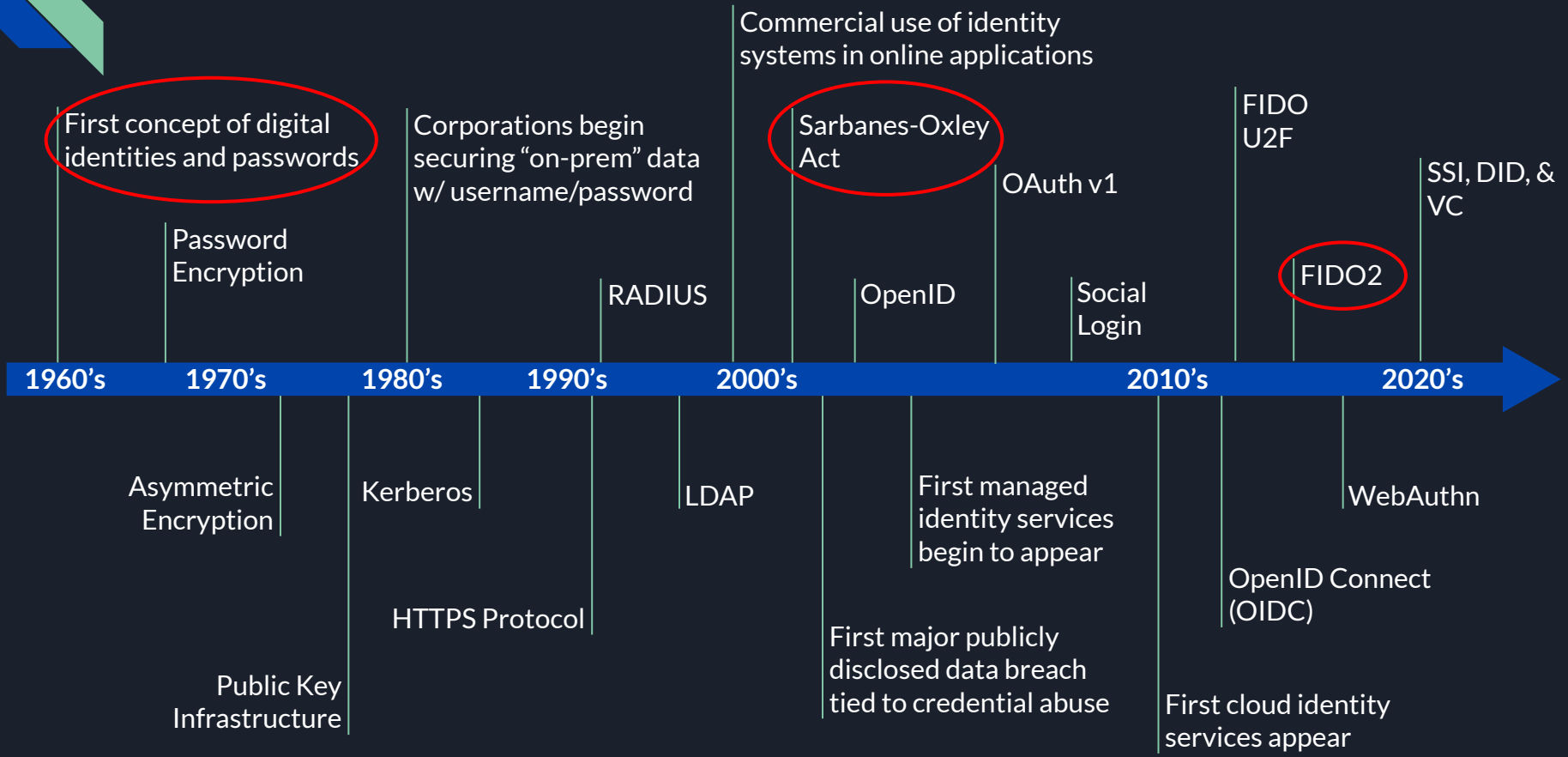
Passwordless

Zero Trust

Call to Action

Questions

History Of IAM



What is Passwordless?

Passwordless authentication refers to a system that does not require the use of passwords at all

Considerations of Passwordless

- Public key infrastructure (PKI)
- Multi-factor Authentication (MFA)
  - Biometric
  - Token-based
  - Device-based
- Secure channels of communication
- User experience
- Account recovery

How to achieve Passwordless?

Fast **ID**entity **O**nline (FIDO): FIDO authentication is the answer to the password problem!

Secure

User Ex

Privacy

Scalable

FIDO2: Latest spec from The FIDO Alliance

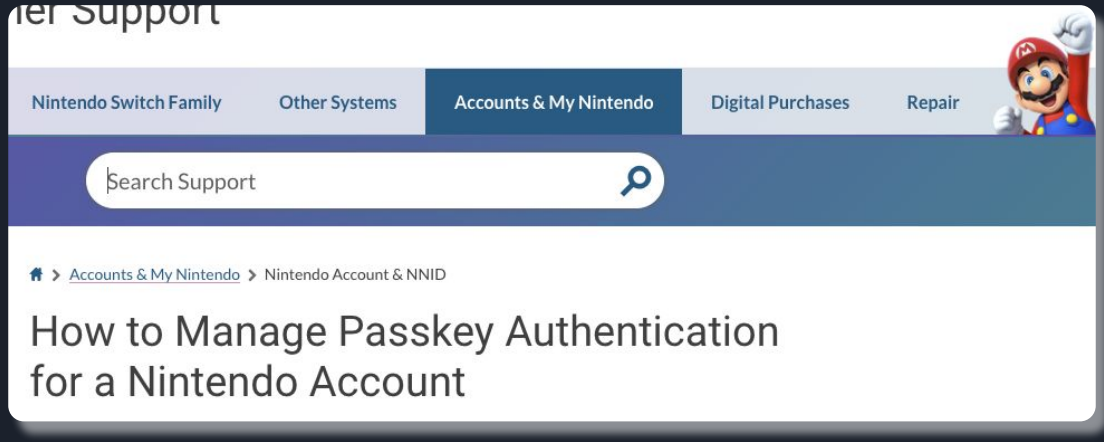
WebAuthn: Standard for browser-based authentication

CTAP2: Spec for OS communication w/ local authenticators

source: https://fidoalliance.org/

Passkey Frenzy

A compliant authenticator that uses public-key cryptography to authenticate



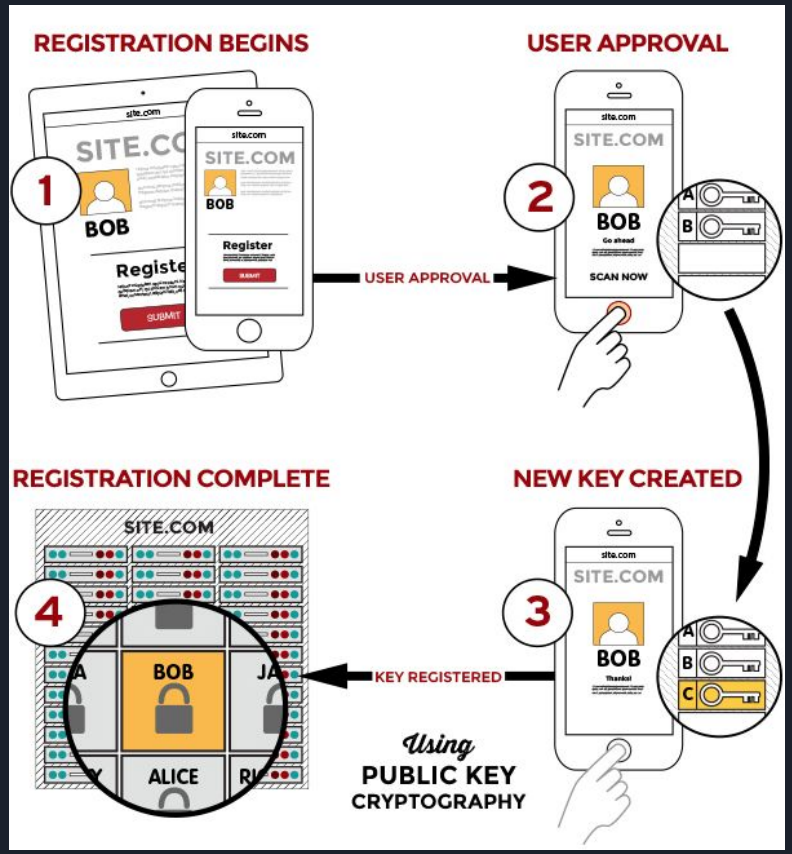
https://www.nintendo.com/

Passkeys optimize access and usability for FIDO Authentication

Passkeys 101

- Intuitive
- Automatically unique per-service
- Breach-resistant
- Phishing-resistant
- Stored in a hardware authenticator, by the platform, or third-party provider

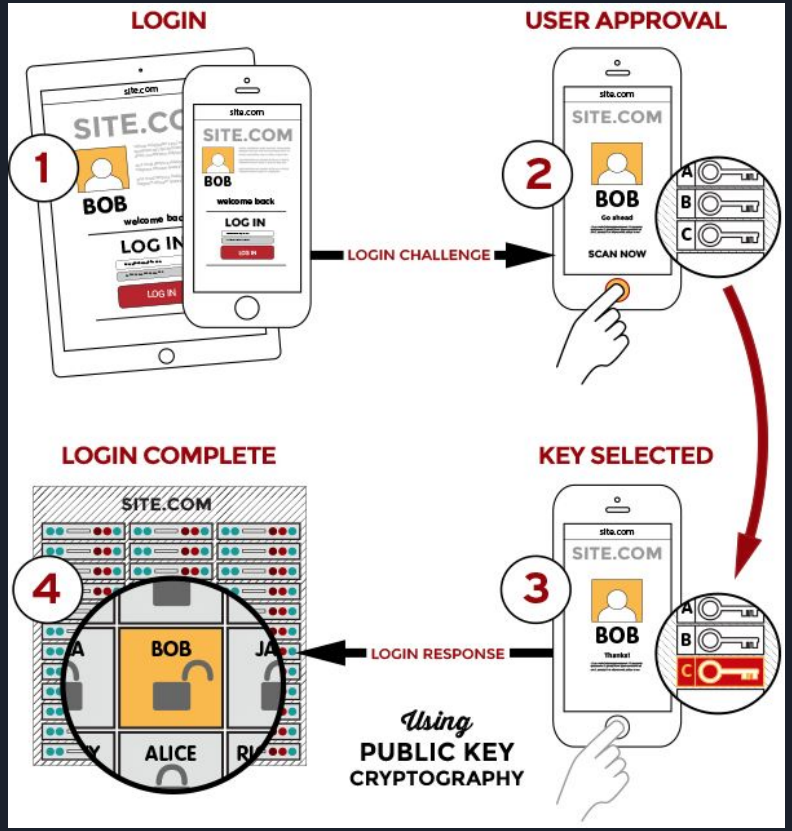
How do Passkeys Work- Registration



1. Choose FIDO Authenticator
2. User unlocks FIDO authenticator
3. New unique public/private keypair per local device, online service, and user's account
4. Public key sent to online service and associated w/user account

source: https://fidoalliance.org/

How do Passkeys Work- Login



1. Service will challenge user w/ previously registered device
2. User unlocks authenticator with same method as registration
3. Device uses account identifier to select correct key and sign challenge
4. Signed challenge sent to service and verified against stored public key

source: https://fidoalliance.org/

What is Zero Trust Architecture (ZTA)?

Set of cybersecurity paradigms that move from implicit trust to explicit trust

Special Publication (NIST SP) - 800-207

What is Zero Trust? Architecture (ZTA)?

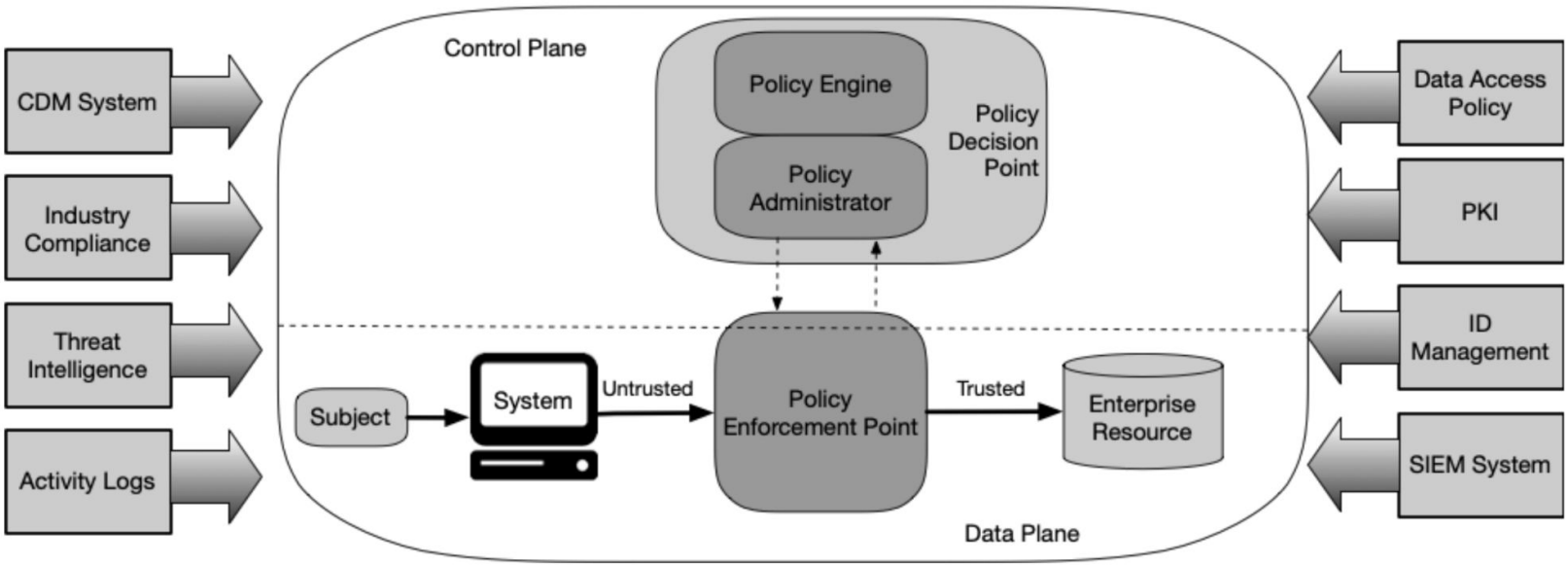


Figure 2: Core Zero Trust Logical Components

Special Publication (NIST SP) - 800-207

Principles of Zero Trust

- Never Trust, Always Verify ✓
- Identity & Access Management (IAM) ✓
- Network Segmentation
- Least Privilege Access ✓
- Continuous Authentication & Authorization ✓
- Micro-perimeters
- Enhanced Visibility & Monitoring ✓
- Device Security ✓
- API Security ✓

Call To Action

Passwordless

1. Establish baselines
2. Buy-in and communication
3. Start with less passwords
4. Collaborate with vendors and experts

Zero Trust

1. Define what ZTA means
2. Assess current state
3. Develop strategy
4. Implement controls
5. ZTA is a marathon

Questions?

Thank you!

All icons in presentation from Flaticon

Thank you!

Abrom Douglas III


linkedin.com/in/abrom


@iamAbrom


@iamAbrom@infosec.exchange