KOBALT.IO

Going Passwordless: The Future of Cybersecurity

Nov 8, 2022

About Michael Argast

- >20 years in Information Security
- Career spans operations, security sales, leadership, consulting
- Roles at Sophos, TELUS, **Kobalt.io**
- Well connected to local and international community - member of Vancouver ISACA, Provincial Security Advisory Committee, SecSig and more
- Presented/press internationally - Moscow InfoSec, Oxford University, New York Times, Associated Press.
- Father of three girls, into camping, snowboarding, travel

Agenda

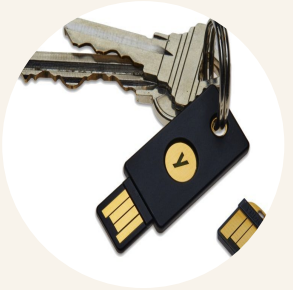
1. Passwords in a cloud centric world
2. Passwords are under frequent attack
3. Traditional passwords
4. Password managers and Identity brokers
5. Moving to passwordless authentication
6. How does passwordless work?
7. Advantages and disadvantages
8. The key role of devices
9. Implications for end-users, developers, IT/security

Passwords in a cloud centric world

- The single largest risk to most businesses cloud services are account compromises
- Hundreds of services, websites, passwords
- Leads us to password managers (1Password), SSO and MFA.

';--have i been pwned?

1Password



Passwords are under frequent attack

Phishing
Trick you into entering your username and password

Malware
Steals your password while you're working

Data Breaches
Your email and password(s) are available for sale

Brute Force Attacks
Uses common passwords and variations to force in

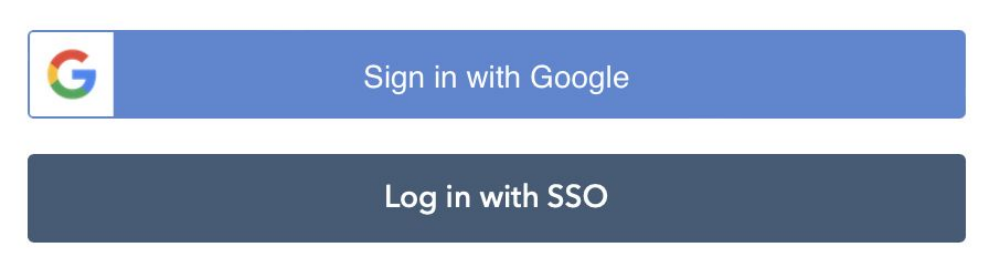
Traditional passwords

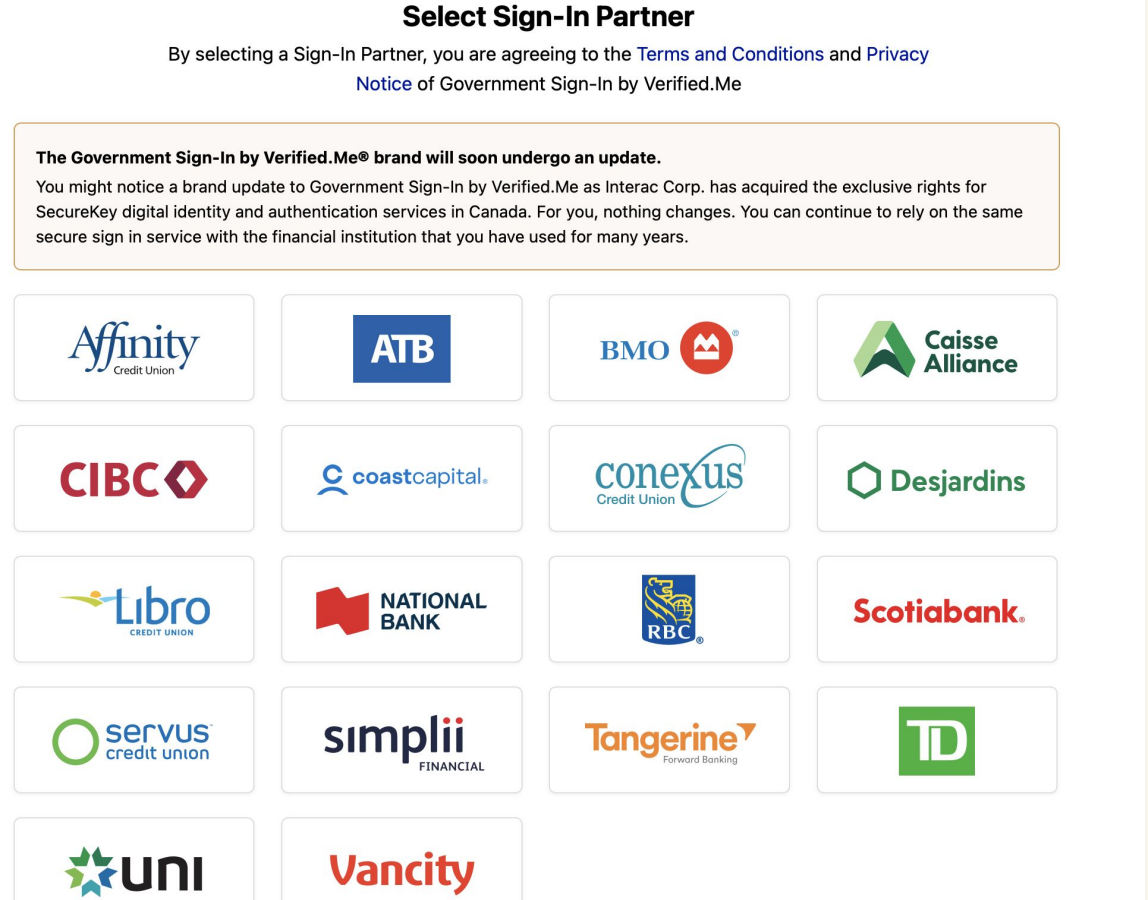
- A shared secret between service and user
- Stored in multiple locations (user system, server)
- Subject to phishing and compromise
- Added additional features (biometrics, secret questions, MFA) to overcome design flaw but fundamentally anchored in same design

Password managers and identity brokers

We now have hundreds of passwords...

1. We are told have unique, long, complex passwords
2. Password managers like 1Password fill this gap for users
3. Identity brokers also streamline user experience





Moving to passwordless authentication

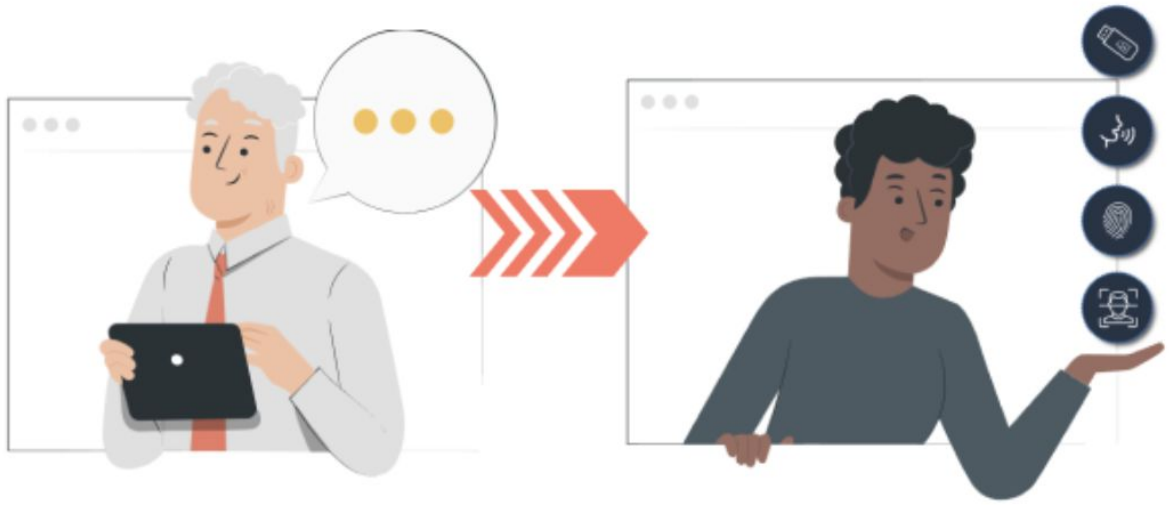
Initial implementations of Fido2 have already started

- Microsoft platforms including AD support started in 2021
- Apple has deployed multi device support via “passkeys” in iOS 16, macOS Ventura
- Android is also expected in Fall 2022 (currently in beta)

Enabling a fundamental shift to phishing-resistant authentication

From legacy, knowledge-based credentialing

To modern, possession-based credentialing

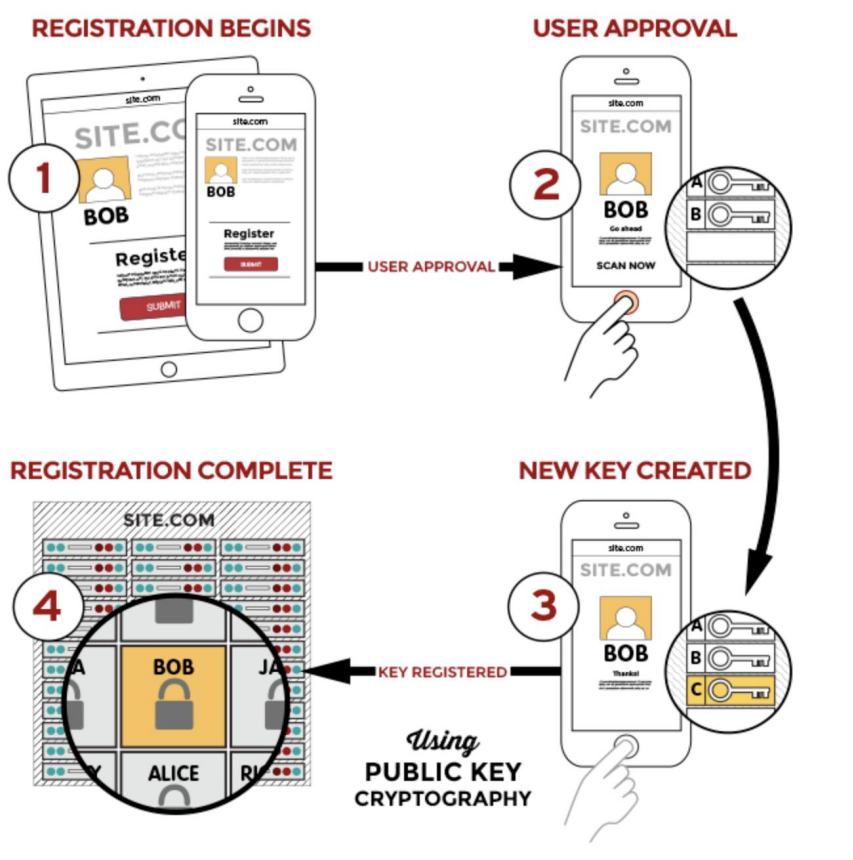


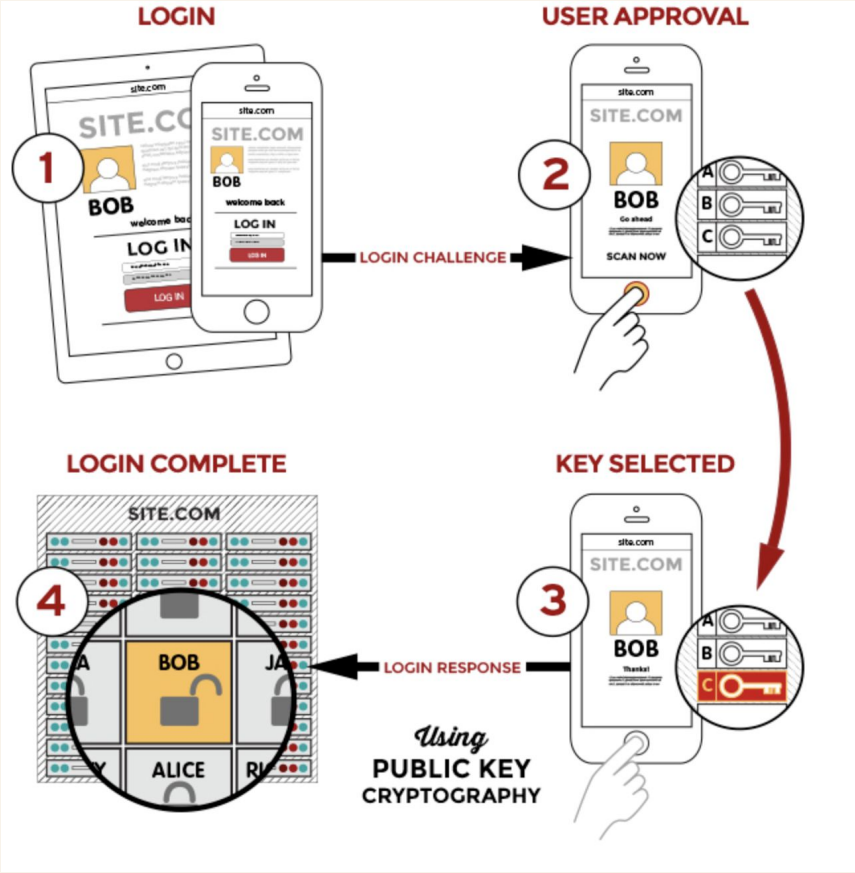
- Stored on a server
- SMS OTP
- KBA
- Passwords

- On-device (never on a server)
- Local Biometric / PIN
- DocAuth
- Multi-device FIDO credentials

How does passwordless work?

Remember Alice and Bob and PGP?





Advantages and disadvantages

Advantages

- Leverages devices users own and strong biometrics
- Much harder to phish/steal credentials
- Easier user onboarding and authentication
- Degree of familiarity from “sign on with” approaches

Disadvantages

- Implementation effort
- Not backward compatible with legacy technologies
- New user workflows
- User device still a potential point of weakness

The key role of devices…

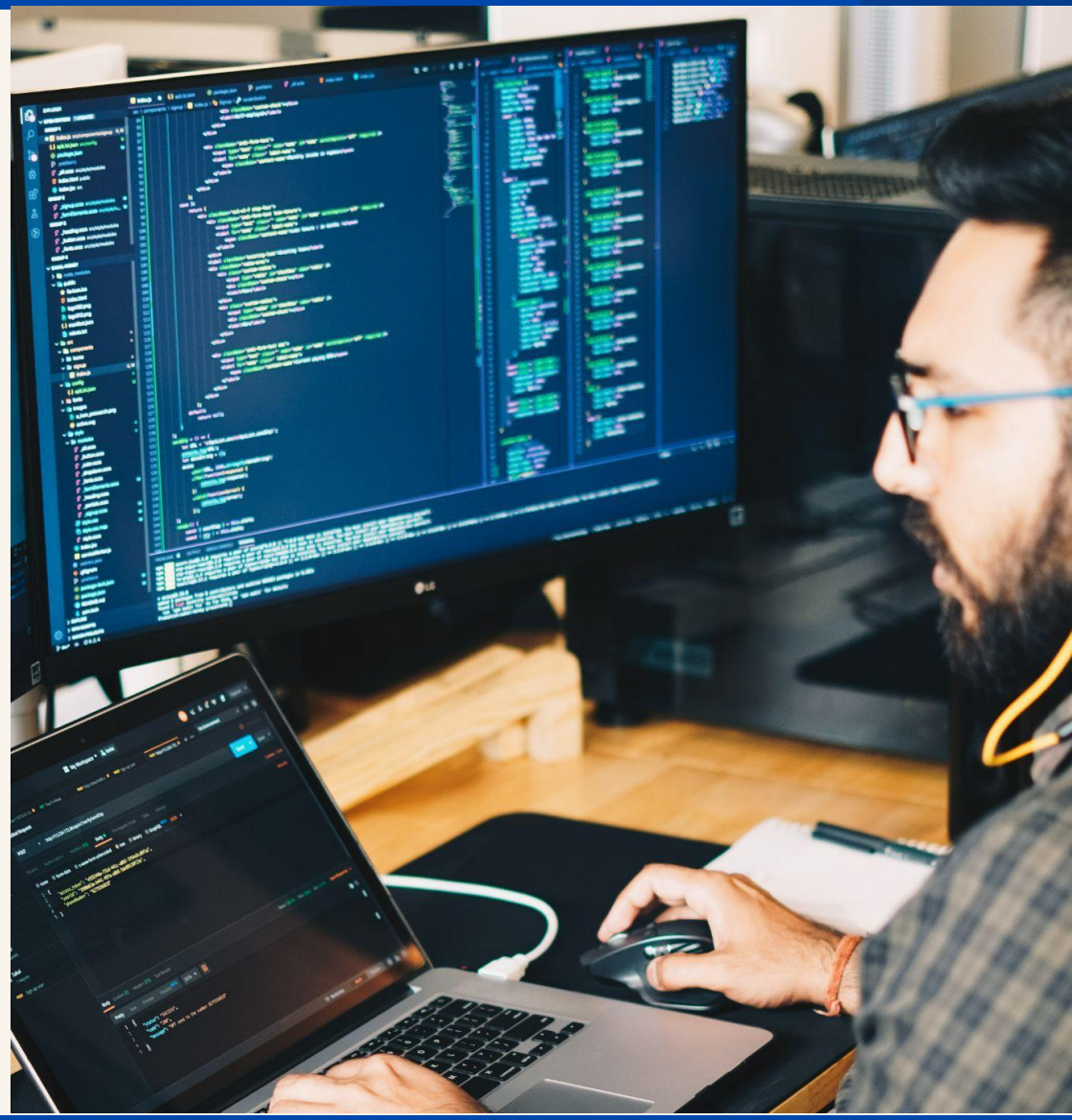
- The user’s device is where keys are stored
- But users use a mix of operating systems, device types and personal and work devices…
- Similar to the “device lost with all my MFA tokens” issue
- Enter “passkeys” which are industry standard and have support from Microsoft, Apple, Google

Implications for End-users

1. You will need devices that support Fido2/passwordless
2. When you set up accounts at new websites, your workflow will change (register, authenticate)
3. Use strong security on your devices
4. Enjoy the new passwordless world!

Implications for Developers

1. You will need to implement the new user registration and authentication workflows in your web applications (simple Javascript API call)
2. Not all users will be able to migrate right away, so you may have to maintain a legacy workflow
3. Apps/websites that do this early will have higher user adoption rates and grow faster
4. You will likely see inclusion of passwordless requests from business clients (similar to SSO)



Implications for IT/Security

1. Your users will need to be educated on the new workflows
2. Password resets will go down as will credential based attacks
3. Device loss/theft and recovery will become more critical
4. Strong end-device security postures and policies will be critical
5. We will live in a hybrid world until you can migrate your users and applications
6. You should consider passwordless support an indicator of stronger security stance amongst vendors

Questions?

KOBALT.IO

info@kobalt.io

www.kobalt.io

/kobaltio

@kobaltio