RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: IDP-F06V

Authentication and Beyond Using FIDO and Push Notifications

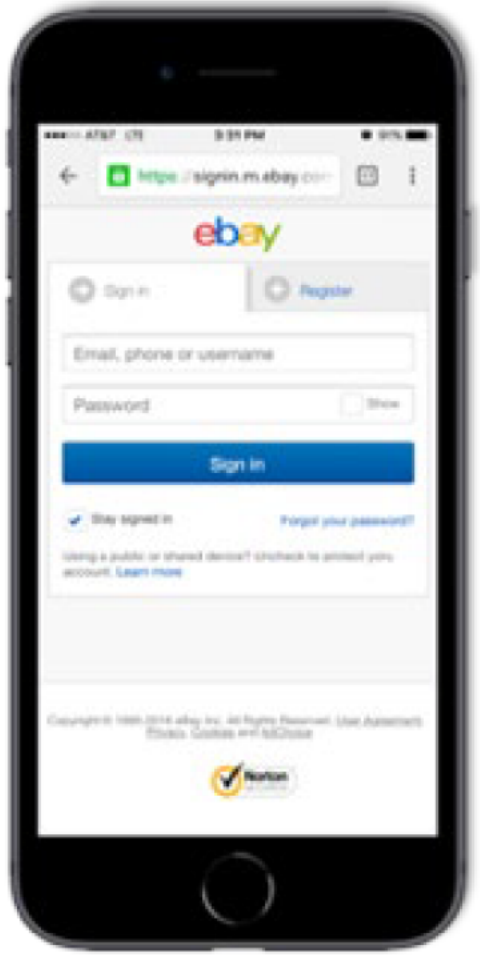
Anand Bahety

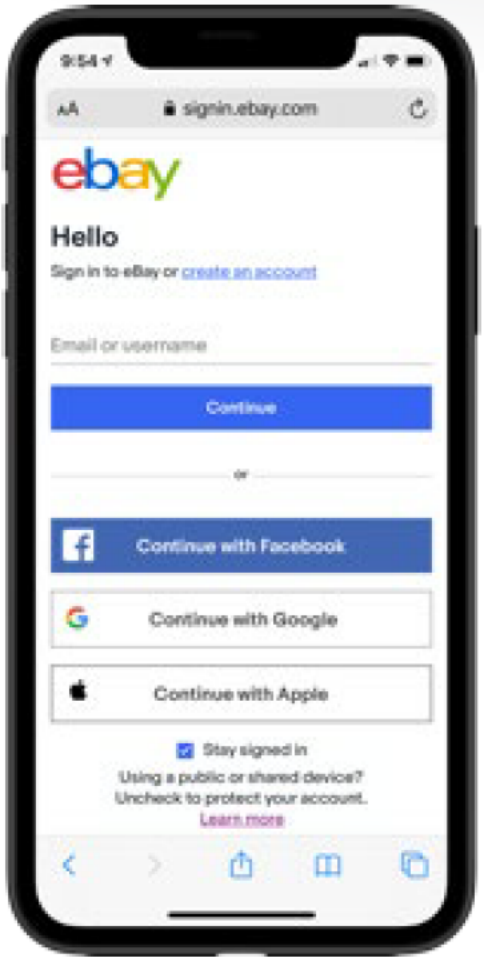
Member of Technical Staff
eBay
@anandbahety

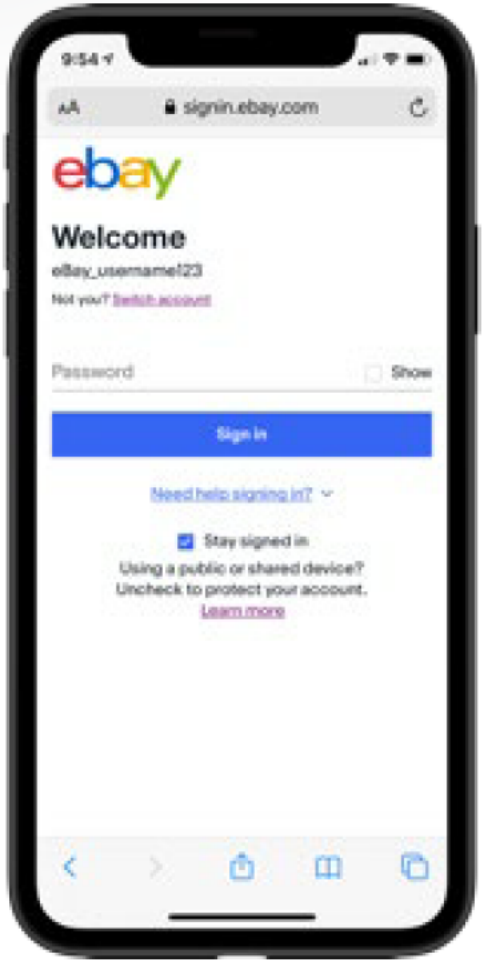
Outline

- Why consider yet another authentication framework?
- Architecture
- MFA simplified
- Challenges

Authentication @ eBay







Authentication @ eBay…

- Password
- Email / SMS verification
- KBA
- Voice auth
- Login with Google/Facebook/Apple
- Biometrics
- …

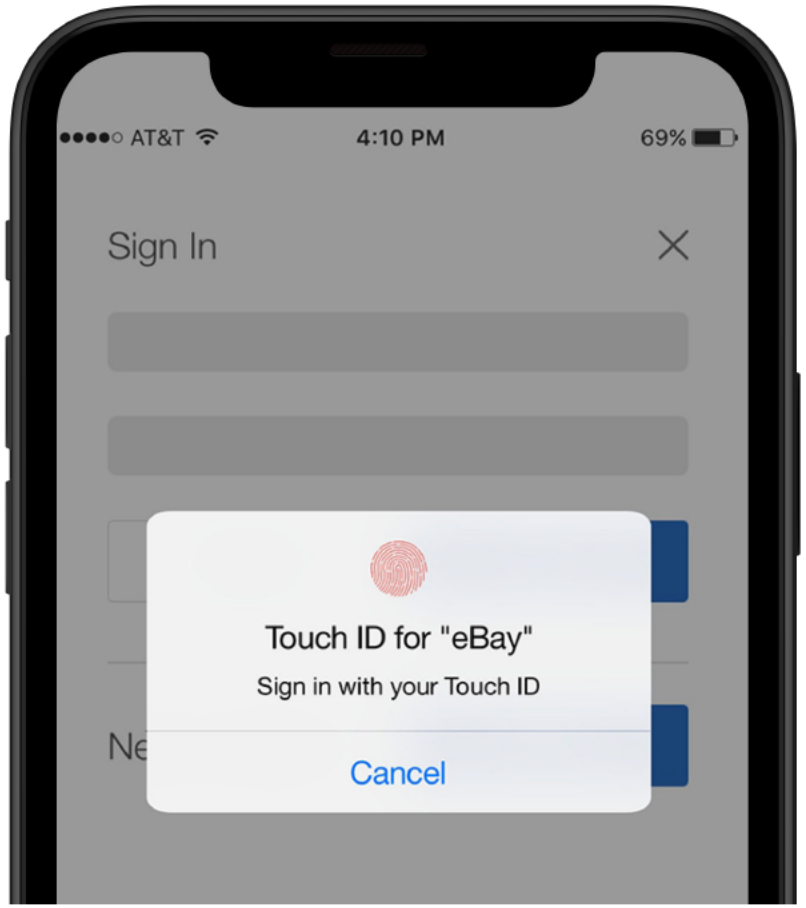
What we are aiming for?

- Security
- Usability
- Maintainability

Then comes FIDO

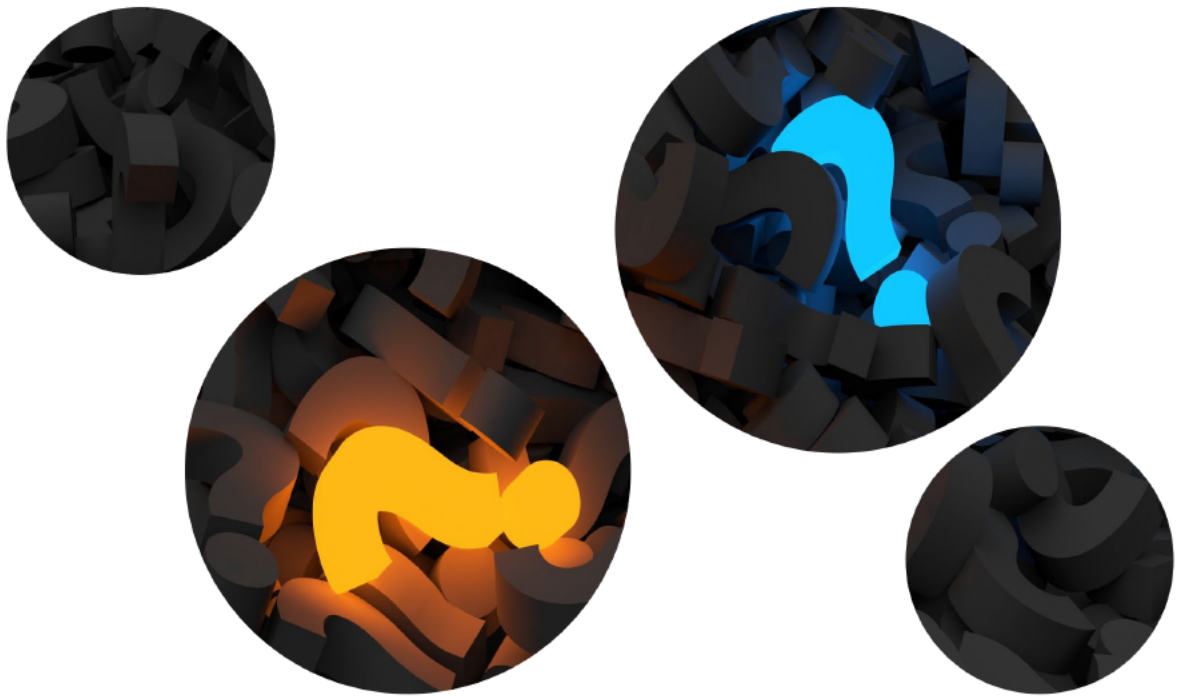
- Latest industry standard for authentication
- Bridge gaps between security and usability
- Problems avoided all together
  - Shared secrets
  - MITM

eBay + FIDO



FIDO UAF to implement biometric based primary authentication

Options for other platforms?



FIDO UAF

+

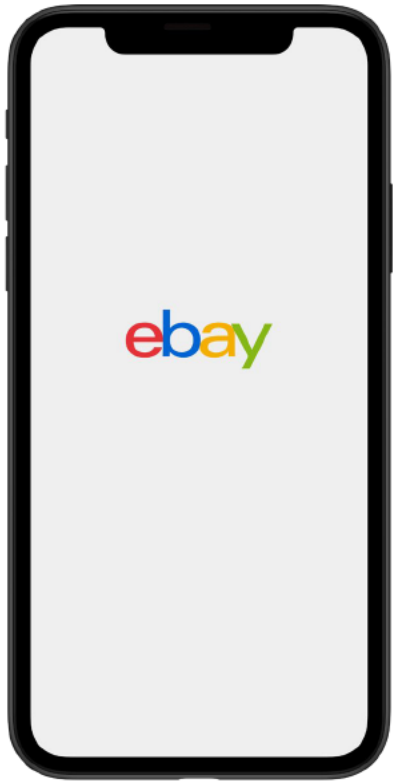
Push Notifications

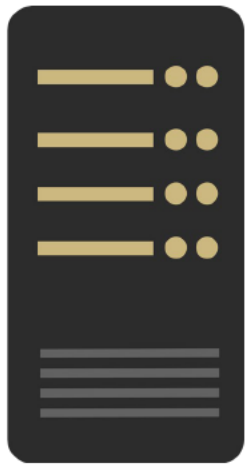
Why Push Notifications?

- Leverage widespread adoption of eBay apps
- User friendly
- Seamless access
- Alerting – a bonus

Architecture

FIDO UAF
Client libraries
(iOS & Android)

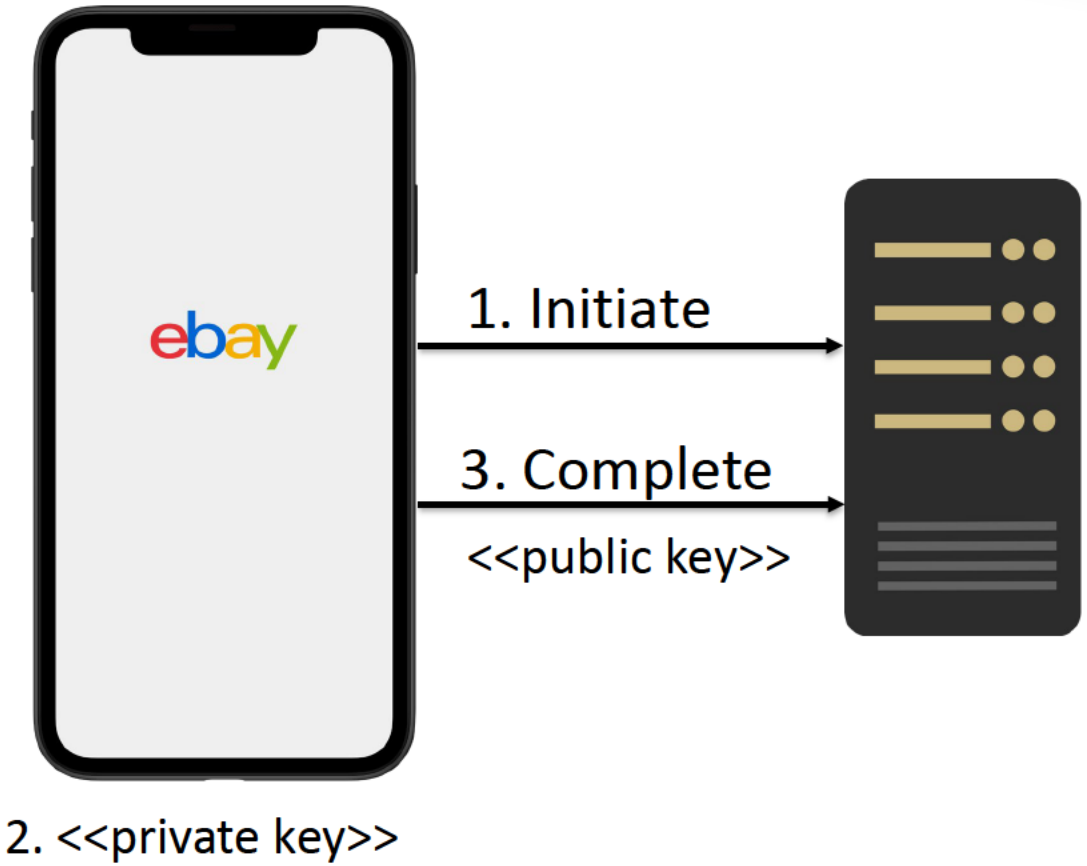




FIDO UAF Server
(Java)

Client & Server open sourced

Registration



1. Initiate Registration protocol

2. User Enrolls and Device generates keypair

3. eBay server stores only the public key

Private key securely stored on user's device

Authentication

2. User approves

1. Initiate Authentication protocol

2. User Approves and App signs the payload using private key

3. eBay verifies signature using public key. Attempt approved (or denied)

Private key never leaves user's device

Deep dive

- Transaction identifier, the only important notification payload
  - Short-lived, on-time use, by itself of no use
  - Nothing sensitive over the wire
  - Avoids the need for end to end TLS to secure notification payload
- Re-use existing FIDO deployment
- Flexible integration into existing apps

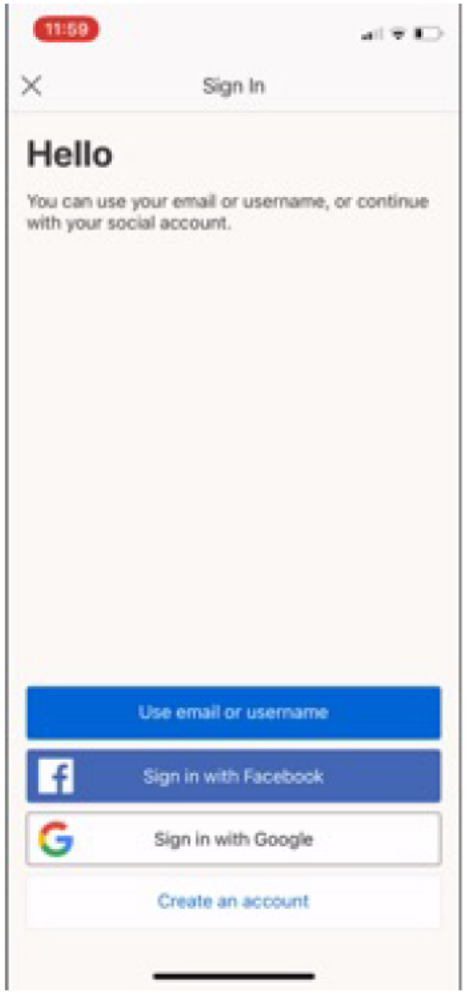
MFA simplified

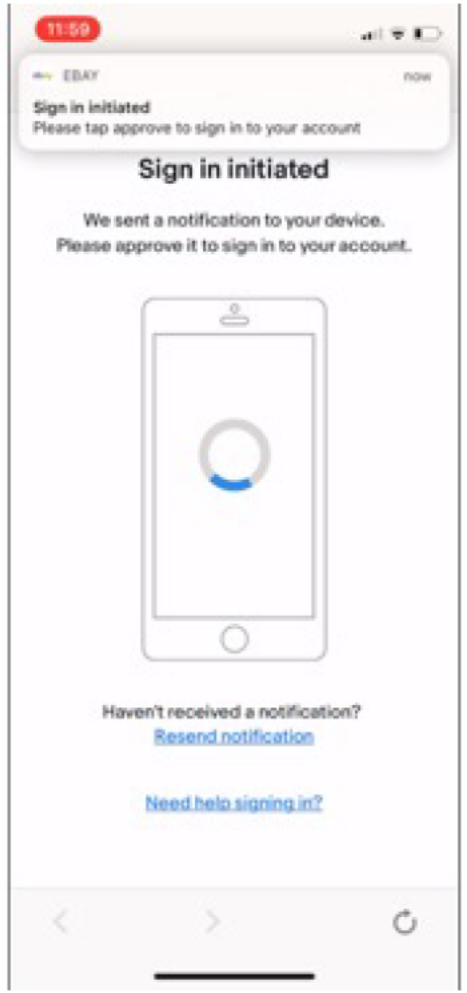
- Primary
- Secondary (2FA)
- Password less (across all platforms)

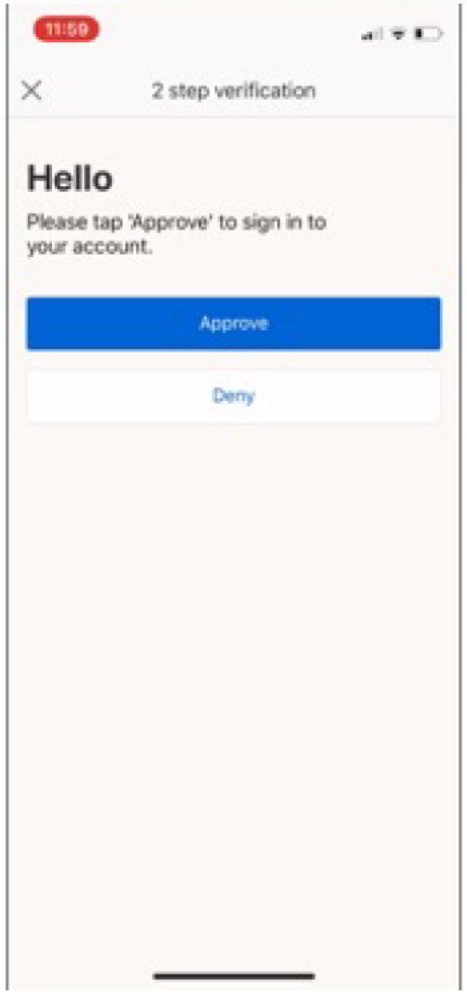
Challenges

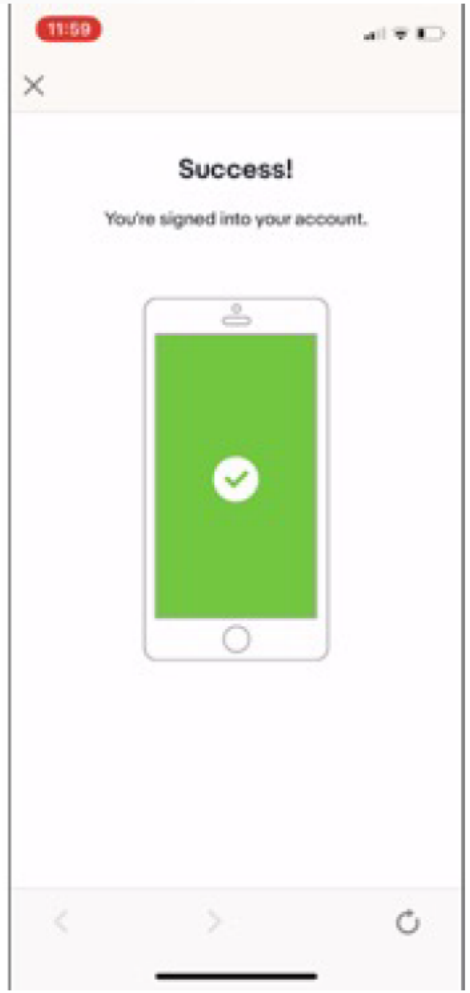
- Different devices have different capabilities
- Back up factor
- Key rotation

Framework in action





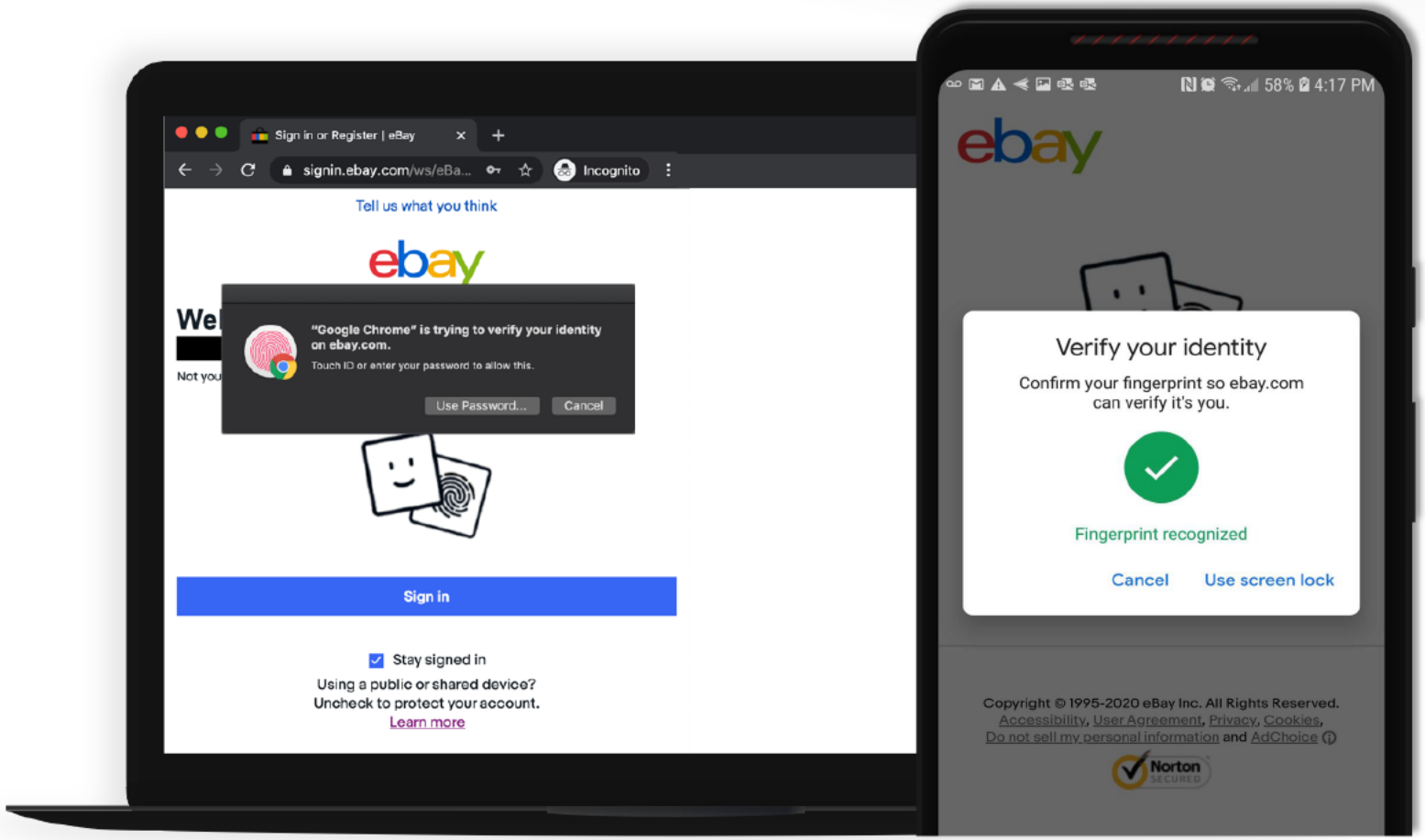




Beyond Just Authentication

- Account recovery
- Trusted device management
- Step-up authentication
- Continuous authentication

Wait, but what about WebAuthn?



Approach

- Build vs. buy?
- Integrate into existing FIDO deployment
- Experimented with different client platforms
- For now, alternate primary auth

Challenges again!

- Support for multiple TLD
- Back up factor
- Inconsistent experience
- Common logo / content

Let's summarize

- Secure, easy-to-use and robust authentication framework using FIDO + Push notifications
- MFA simplified
- Use cases beyond just authentication
- Truly password less? Not yet!

What can you do next?

- Evaluate your authentication portfolio, aim for truly password less
- Experience FIDO + Push notification in action
  Enable push notification based 2FA on your eBay account
- Get hands on, eBay open sourced libraries
  https://github.com/eBay/UAF
- Read further
  eBay Makes web login easier
  Push Notifications based 2-step verification

Thank you