FIGI Security Clinic

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Part II: FIDO 2 Overview and use cases

Abbie Barbir
Amy Ulrich

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

Organized by

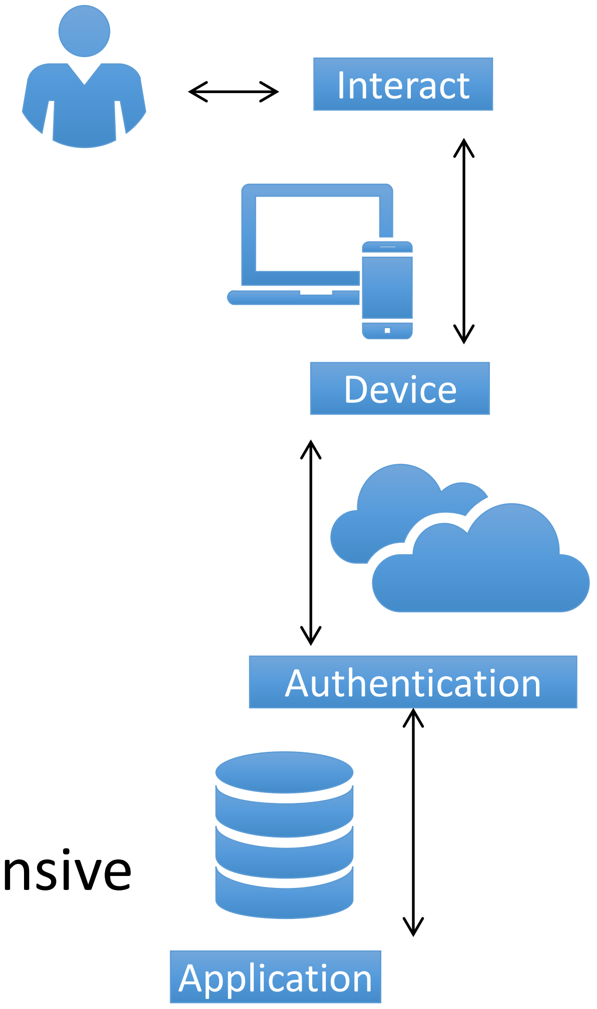
Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

Authentication: Past

- Historical Security Landscape
  - Passwords
    - Originally thought to secure access to data
    - Stronger passwords did not solve the issue
  - Short-falls
    - Users often reuse passwords
    - Many people never change passwords
    - Passwords are often shared
    - Passwords are easily cracked
    - Entering passwords is time consuming and expensive



The trouble with passwords

Most people use less than 5 passwords for all accounts

50%

of those haven't changed their password in the last 5 years

Reuse makes them easy to compromise

39%

of adults use the same password for many of their online accounts

They are very difficult to remember

25%

of adults admit to using less secure passwords, because they are easier to remember

There are lots of places to steal them **from**

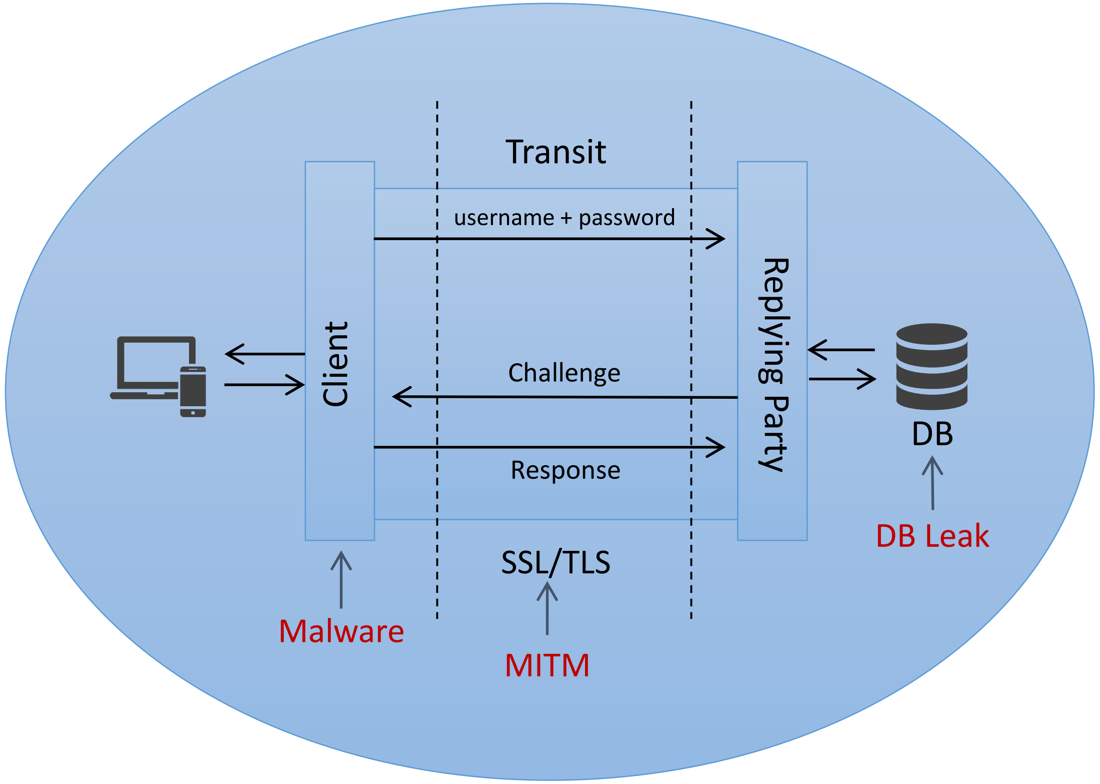
49%

of adults write their passwords down on paper

Sources: Pew research; Telesign research

Password Based Solution Short-falls

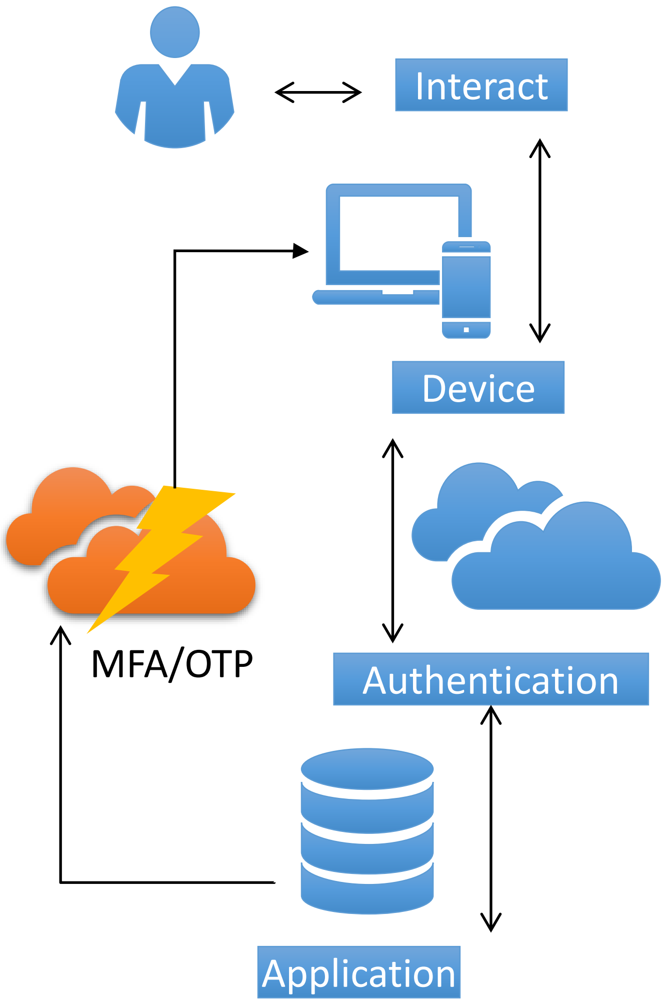
- Malware
  - File or code that can:
    - Provide remote access to infected machine
    - Send spam from the infected machine to targets
    - Investigate the infected user's local network
    - Steal sensitive data
- Man In The Middle (MITM)
  - Attacker can intercept communications to secretly eavesdrop or modify traffic between two parties
- Database Leak
  - Security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized user



FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Present Solutions

- Multi-Factor Authentication (MFA)-also known as two-factor authentication or 2FA
  - Security enhancement that asks users to authenticate with two of the following categories:
    - Something you know (such as password or PIN)
    - Something you have (such as one-time pin (OTP) to mobile phone)
    - Something you are (biometrics such as Fingerprint or FaceID)
  - Credentials must come from two different categories to provide increased security
- Browser Finger Printing (BFP)
  - Comprehensive Data Collection
    - Browser Information, Operating System, Screen Resolution, Supported Fonts, Plug-ins, Time-zone

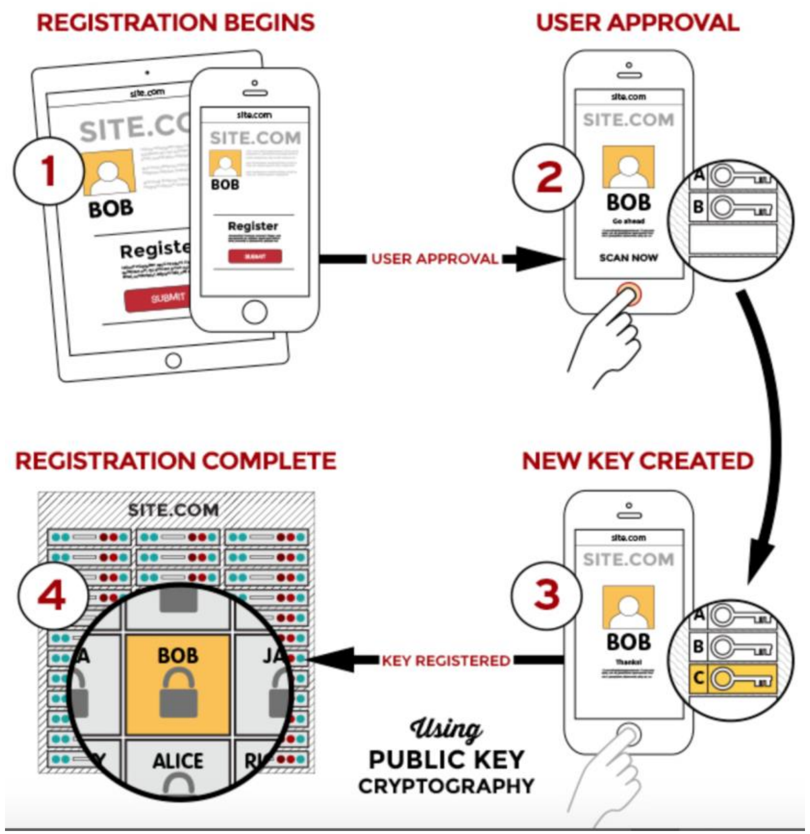


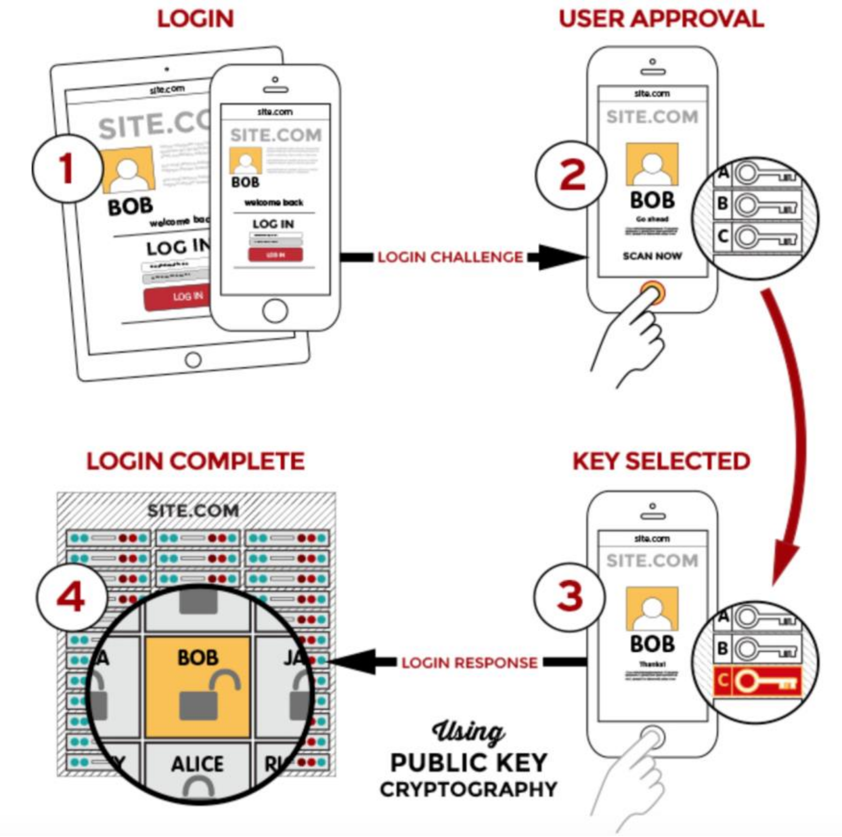
FIDO: Moving beyond Passwords

FIDO Defined

- What is FIDO?
  - “Fast IDentity Online”
  - FIDO authentication is the answer to the world's password problem and lack of interoperability between strong authentication devices
  - FIDO authentication is based on free and open standards
  - Addresses many authentication use cases
    - Security key, multi-factor, fingerprint, facial recognition, etc.
  - FIDO allows for open standards for simpler, stronger authentication using public key cryptography
    - Single Gesture Phishing-resistant MFA
    - Keys and biometrics stay on device
    - No server-side secrets
    - No 3rd Party protocol

FIDO Explained

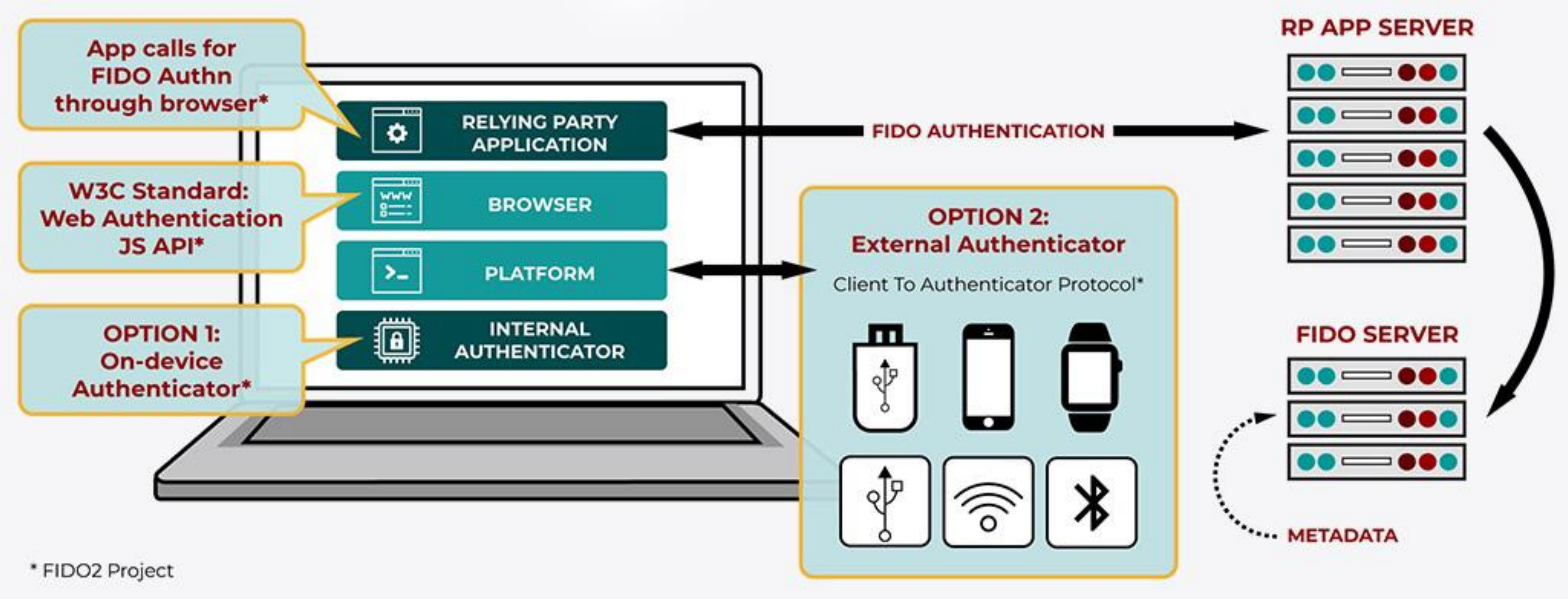




Along Comes FIDO 2

- What is FIDO 2?
  - An updated set of FIDO standards
    - Provides extended set of functionality to cover more use cases
    - FIDO2 supports existing password less FIDO UAF and FIDO U2F use cases
  - Web Authentication (WebAuthn)
    - Enables FIDO Authentication though standard web API which can be built into browsers/web platforms
    - Currently supported in Win 10, Android, Google Chrome, Firefox, MS Edge, Safari
    - Provides users an easier log in experience when accessing internet accounts on their preferred device
  - Client to Authenticator Protocol (CTAP)
    - Expands use cases over previous FIDO standards
    - Enables external devices or FIDO security keys to work with browsers supporting WebAuthn
      - Can also be used as authenticators for desktop applications and services

WebAuthn + CTAP Flow

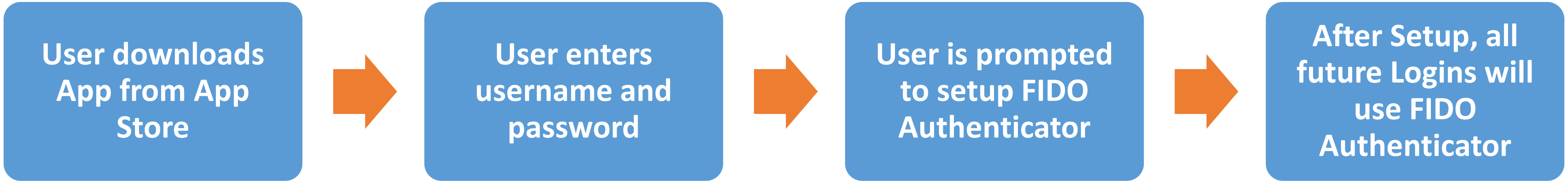


App calls for FIDO Authn through browser*
W3C Standard: Web Authentication JS API*
OPTION 1: On-device Authenticator*
RELYING PARTY APPLICATION
BROWSER
PLATFORM
INTERNAL AUTHENTICATOR
FIDO AUTHENTICATION
OPTION 2: External Authenticator
Client To Authenticator Protocol*
RP APP SERVER
FIDO SERVER
METADATA

* FIDO2 Project

Use Cases

Use Case 1 – Native Mobile App FIDO Authentication



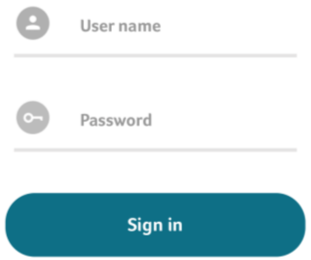
User downloads App from App Store

User enters username and password

User is prompted to setup FIDO Authenticator

After Setup, all future Logins will use FIDO Authenticator

Google Play



Touch ID Face ID

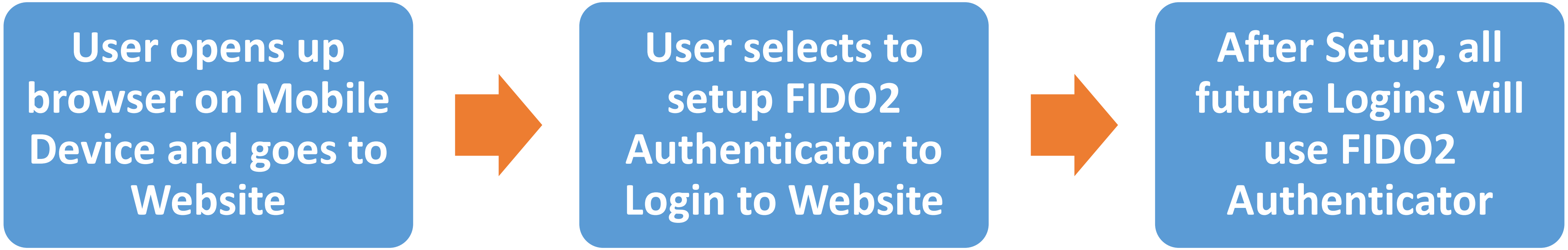
fido™

Touch ID Face ID

Use Case 1- FIDO Mobile Enrollment & Authentication

Play Video

Use Case 2 – Mobile Web FIDO2 Enrollment & Authentication



User opens up browser on Mobile Device and goes to Website

User selects to setup FIDO2 Authenticator to Login to Website

After Setup, all future Logins will use FIDO2 Authenticator

WebAuthn

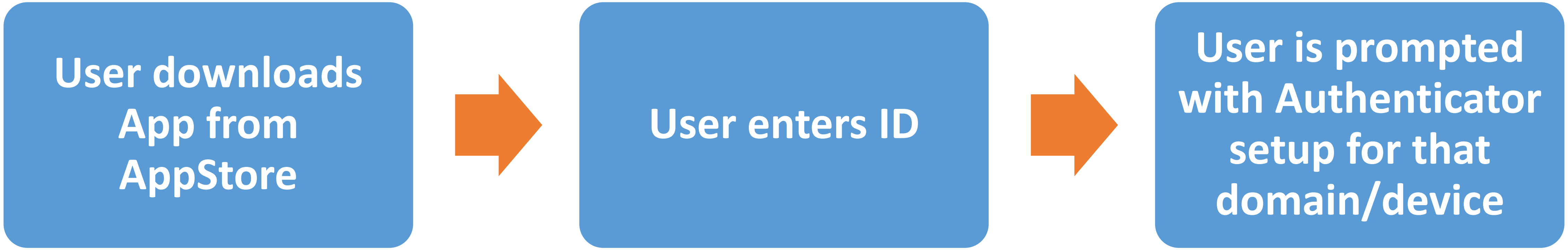
Touch ID

Face ID

Use Case 2 – FIDO2 Mobile Web Enrollment & Authentication

Play Video

Use Case 3 – Native Mobile App FIDO2 Authentication



User downloads App from AppStore

User enters ID

User is prompted with Authenticator setup for that domain/device

Google Play

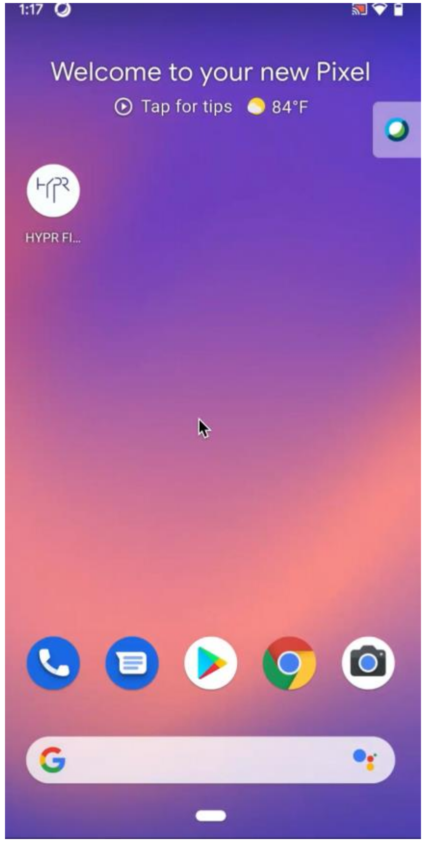
WebAuthn

Touch ID

Face ID

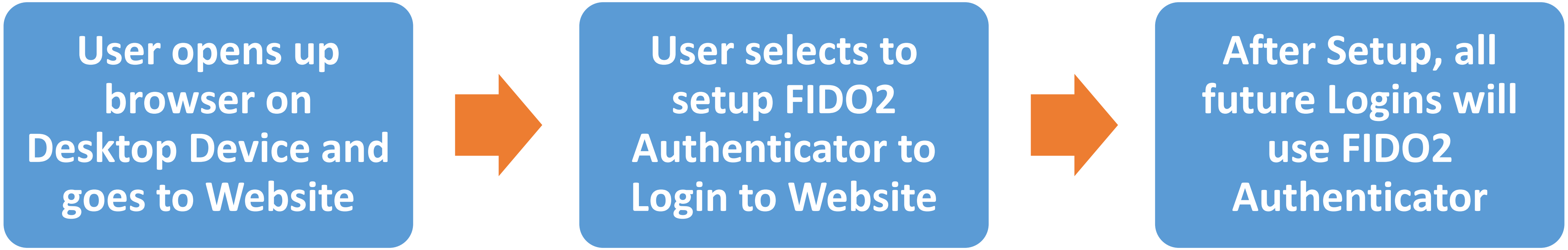
* * *

Use Case 3 – FIDO2 Mobile Authentication



Play Video

Use Case 4 – Desktop Web FIDO2 Enrollment & Authentication

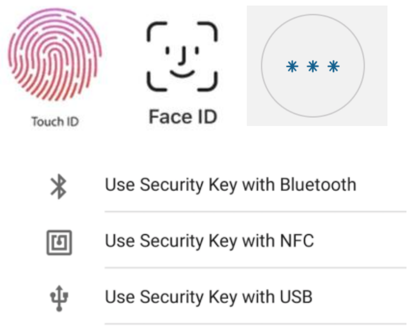


User opens up browser on Desktop Device and goes to Website

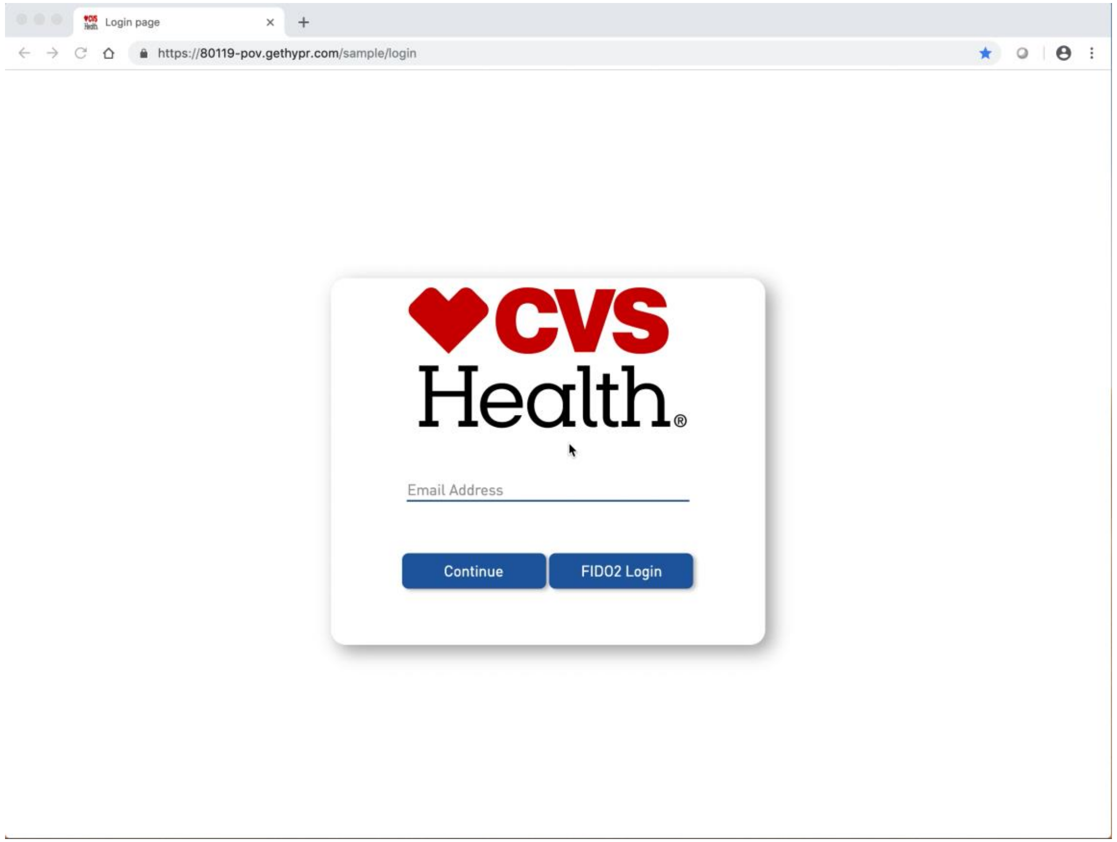
User selects to setup FIDO2 Authenticator to Login to Website

After Setup, all future Logins will use FIDO2 Authenticator

WebAuthn

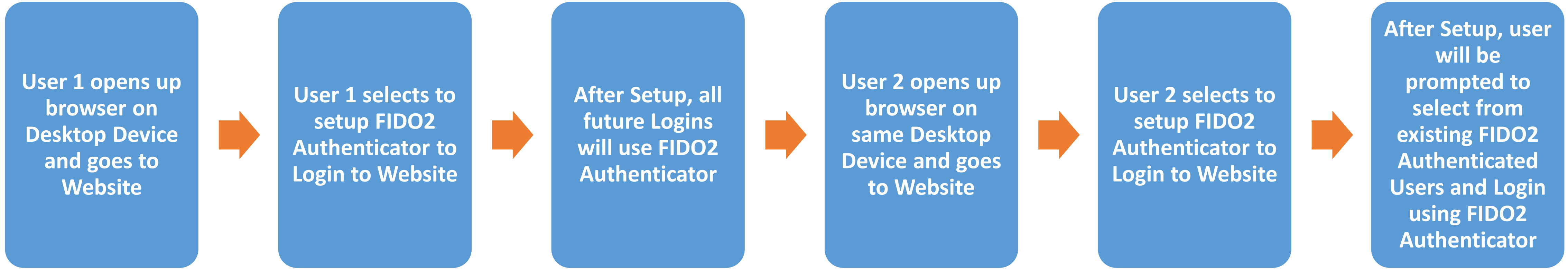

Touch ID
Face ID
* * *
Use Security Key with Bluetooth
Use Security Key with NFC
Use Security Key with USB

Use Case 4 - FIDO2 Web Authentication



Play Video

Use Case 5 – Multiple Users on Same Device (Resident Key) - FIDO2 Enrollment & Authentication



User 1 opens up browser on Desktop Device and goes to Website

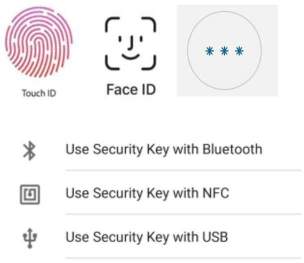
User 1 selects to setup FIDO2 Authenticator to Login to Website

After Setup, all future Logins will use FIDO2 Authenticator

User 2 opens up browser on same Desktop Device and goes to Website

User 2 selects to setup FIDO2 Authenticator to Login to Website

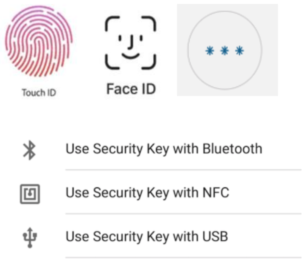
After Setup, user will be prompted to select from existing FIDO2 Authenticated Users and Login using FIDO2 Authenticator



Use Security Key with Bluetooth

Use Security Key with NFC

Use Security Key with USB

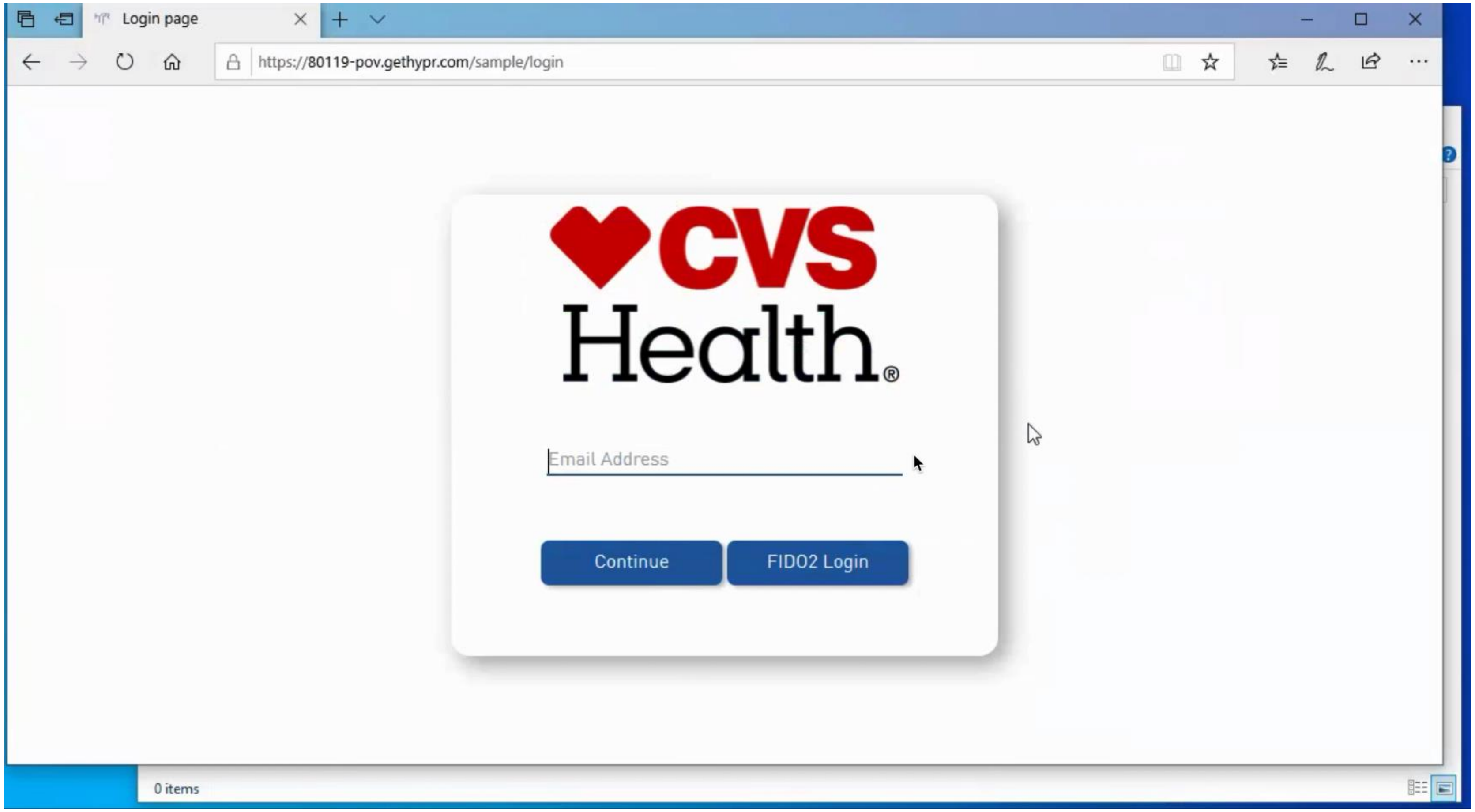


Use Security Key with Bluetooth

Use Security Key with NFC

Use Security Key with USB

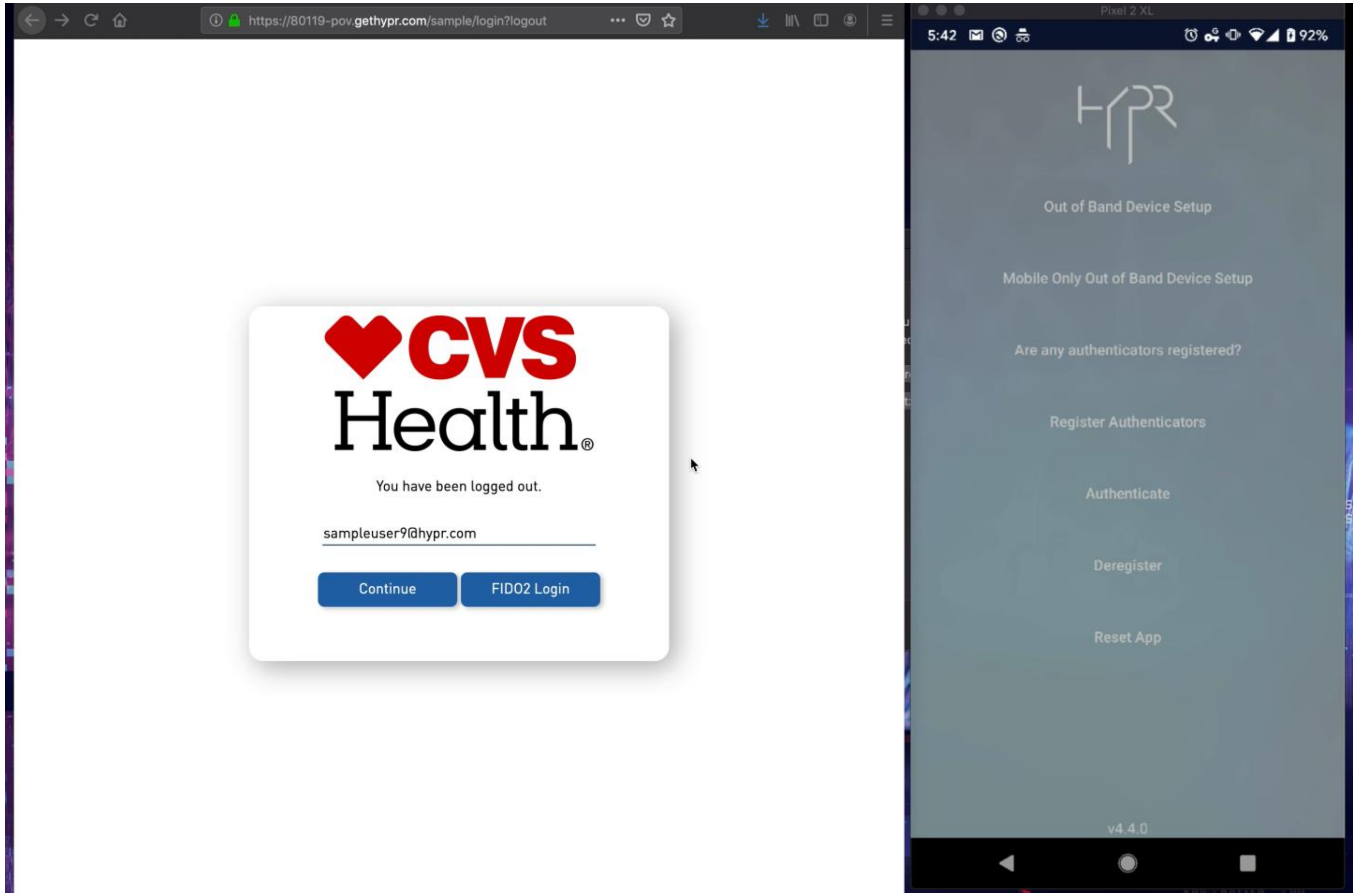
Use Case 5 – FIDO2 Multiple Users Same Device (Resident Key)



Play Video

Appendix – Other Use Cases

Web – Password-less Authentication (Push to Mobile)



https://80119-pov.gethypr.com/sample/login?logout

You have been logged out.

sampleuser9@hypr.com

Play Video