



FIDO2: A WEB WITHOUT PASSWORDS

W3C TRACK AT THE WEB CONFERENCE

Andrew Shikiar
Chief Marketing Officer
FIDO Alliance

May 15, 2019



THE WORLD HAS A PASSWORD PROBLEM

CONSUMERS HAVE A PASSWORD PROBLEM

90+ ACCOUNTS

Per average user
(Oxford University)

55%

Of *IT leaders* re-use a
single password *(Sailpoint)*

<5 PASSWORDS

Per user, and 50%
haven't changed said
password in last 5
years *(Pew)*

1,300 YEARS

Collectively spent by
humans each day
entering passwords
(Microsoft)



CLUMSY | HARD TO REMEMBER | NEED TO BE CHANGED ALL THE TIME

BUSINESSES HAVE A PASSWORD PROBLEM

81%

Data breaches that involved **weak, default, or stolen passwords** (*VDBR 2016*)

36%

Rise in phishing attacks in 2018 (*Webroot*)

1,244

Breaches in 2018, with a 126% jump in exposed records containing PII (*ITRC*)

\$1M

Annual cost to a large corporation for password resets (*Forrester*)

20-50%

Of helpdesk calls are for password resets (at \$70/reset) (*Gartner/Forrester*)

49%

Password-driven cart abandonment rate (*Visa*)

ONE-TIME PASSCODES

Improve security but aren't easy enough to use



SMS
Reliability



Token
Necklace

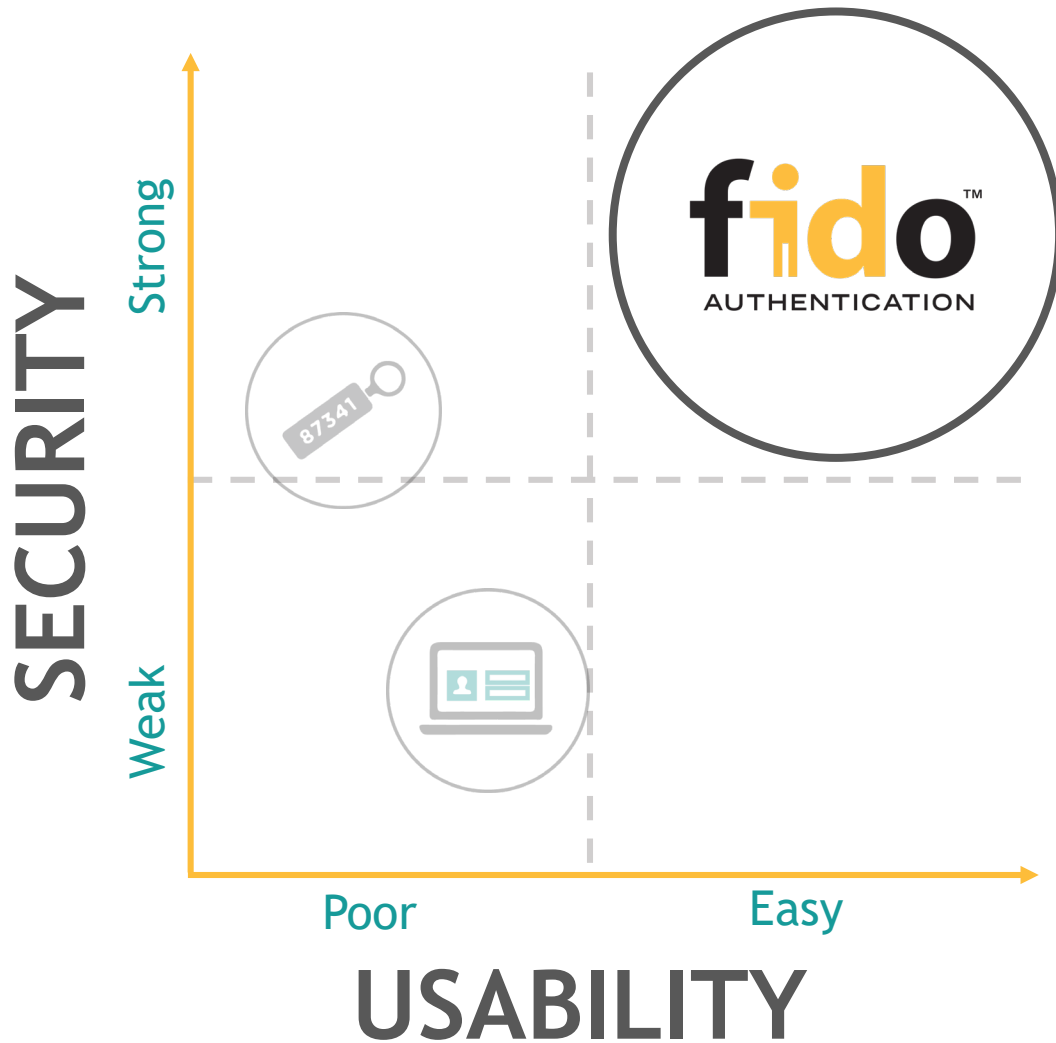


User
Confusion



Still
Phishable

INDUSTRY IMPERATIVE: SIMPLER AND STRONGER



=

Open standards for simpler, stronger authentication using **public key cryptography**

FIDO Alliance is the global industry collaboration dedicated to solving the password problem

...with no dependency on “shared secrets”

LEADING THE EFFORT



CONSUMER ELECTRONICS



SECURITY & BIOMETRICS



HIGH-ASSURANCE SERVICES

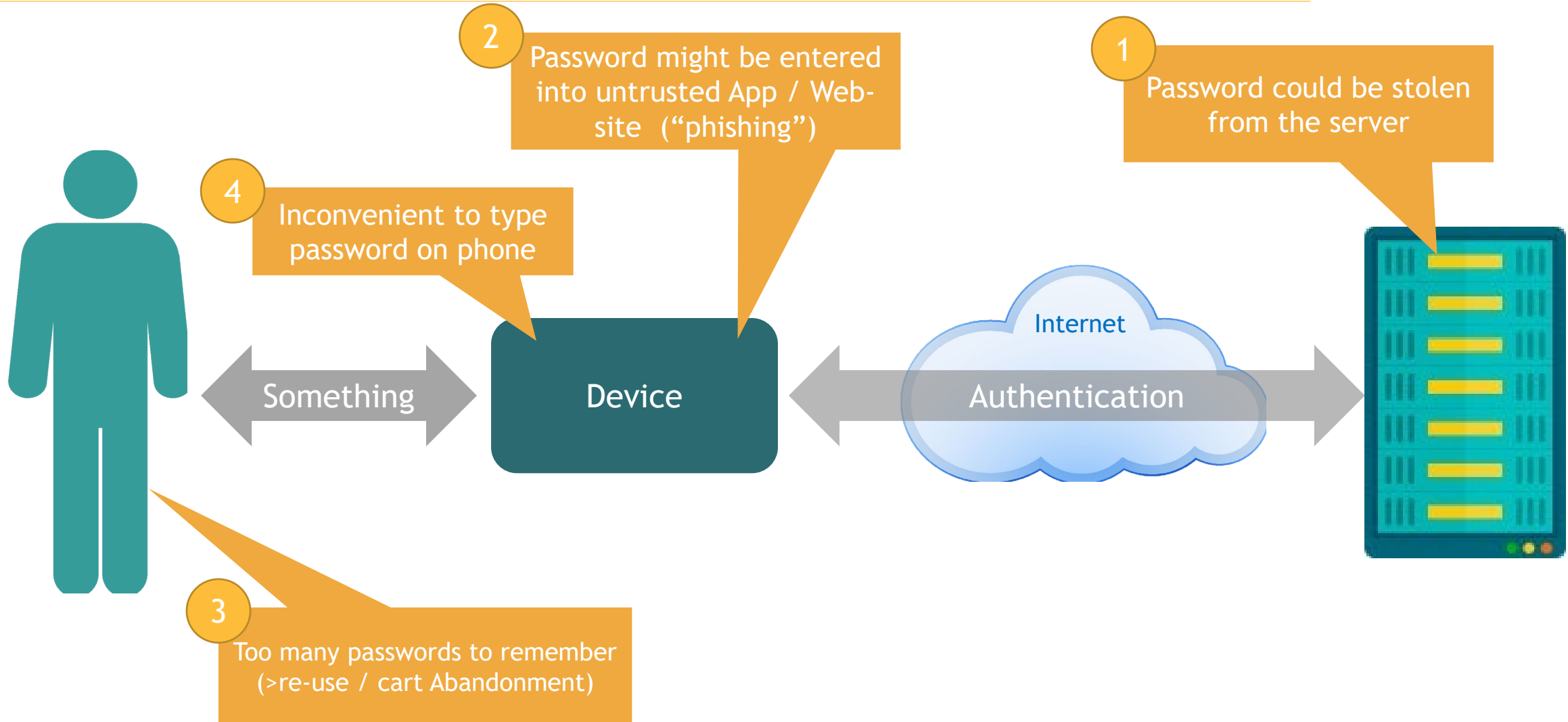
INDUSTRY PARTNERSHIPS



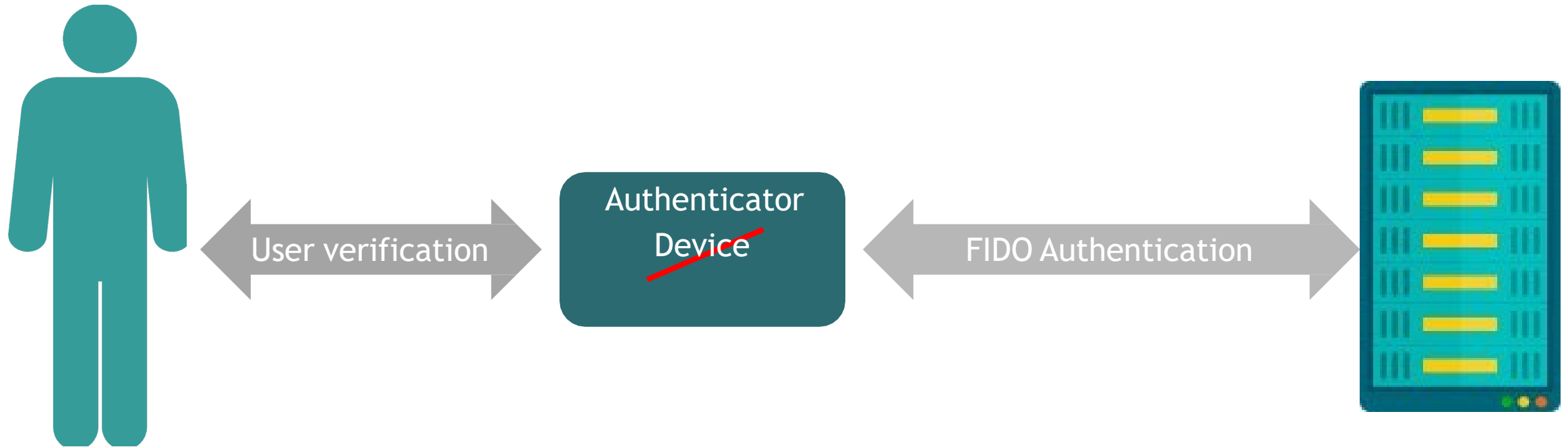


HOW FIDO WORKS

OLD AUTHENTICATION WITH PASSWORDS



HOW DOES FIDO WORK?



FIDO AUTHENTICATORS

We see “Bound” or “Platform” Authenticators, (authenticators that are an integral part of a smartphone or laptop)



We see “Roaming” Authenticators, (authenticators that can be connected to different smartphones/laptops using CTAP)



In both categories you find support for different modalities

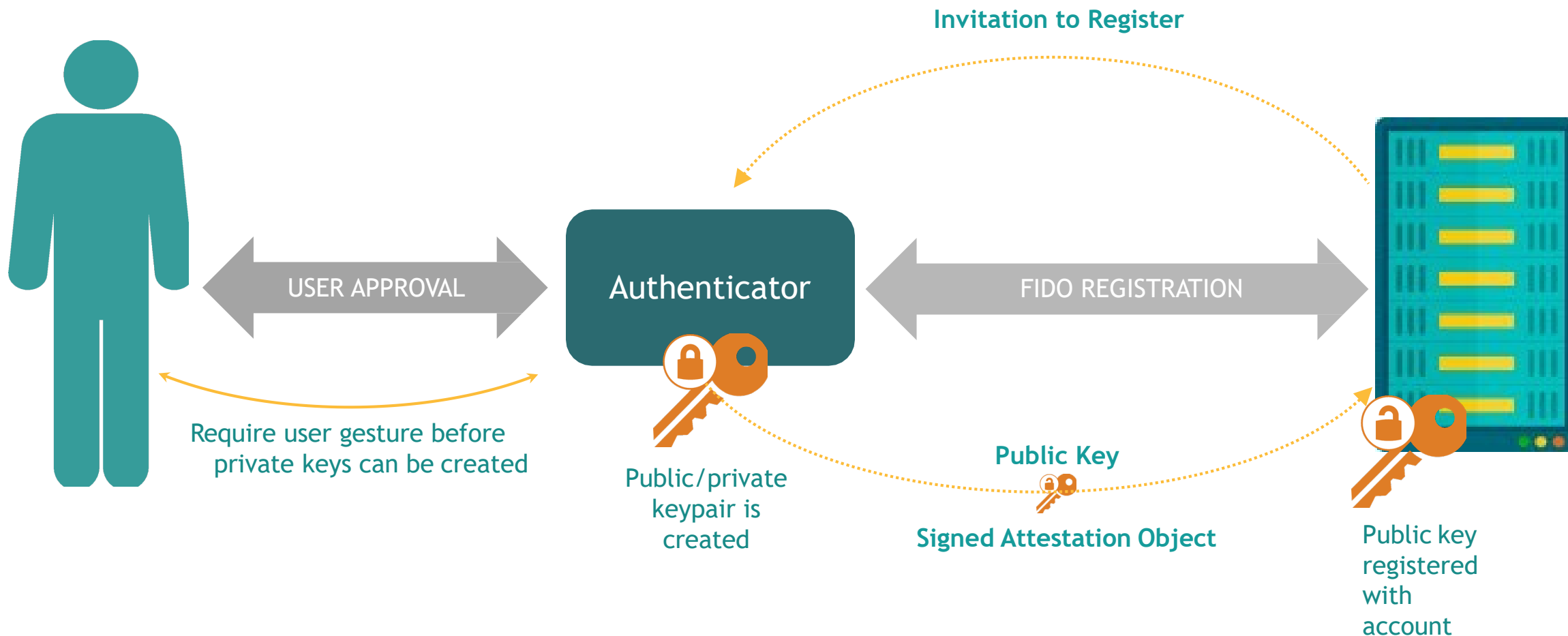


User Presence Challenge
 (“A” user)

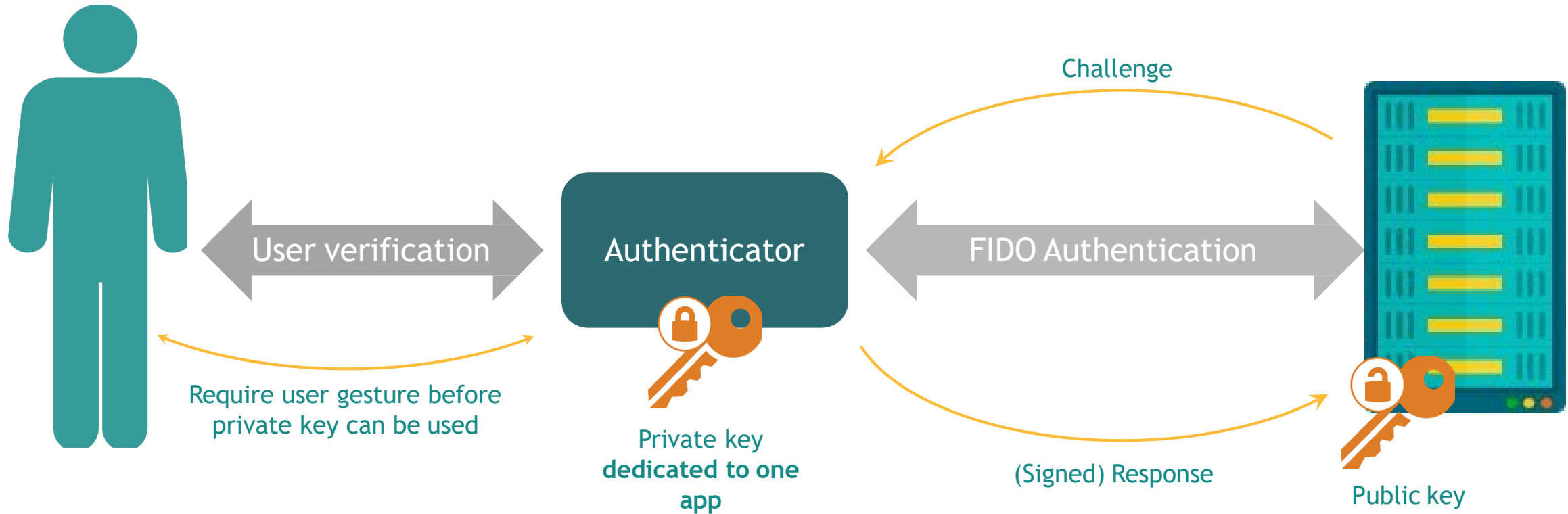


User Verification Methods
 (“THE” user)

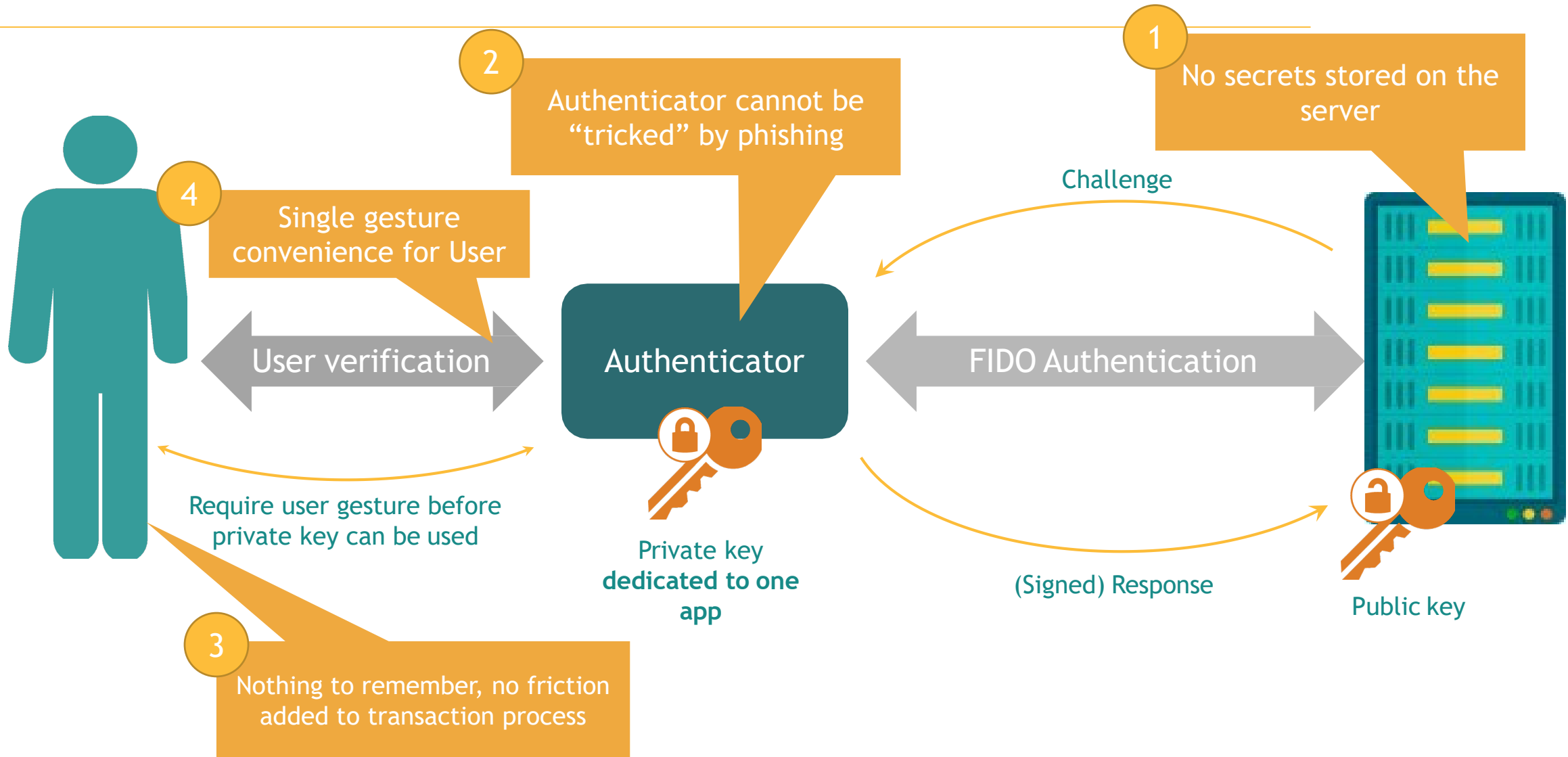
HOW DOES FIDO WORK? - REGISTRATION



HOW DOES FIDO WORK? - AUTHENTICATION

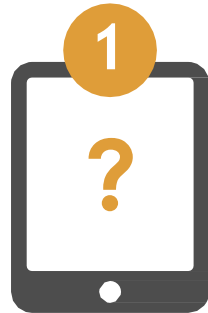


FIDO AUTHENTICATION VS. PASSWORDS



FIDO USER EXPERIENCES

Passwordless Experience



Authentication Challenge



Biometric User Verification*



Authenticated Online

Second Factor Experience



Second Factor Challenge



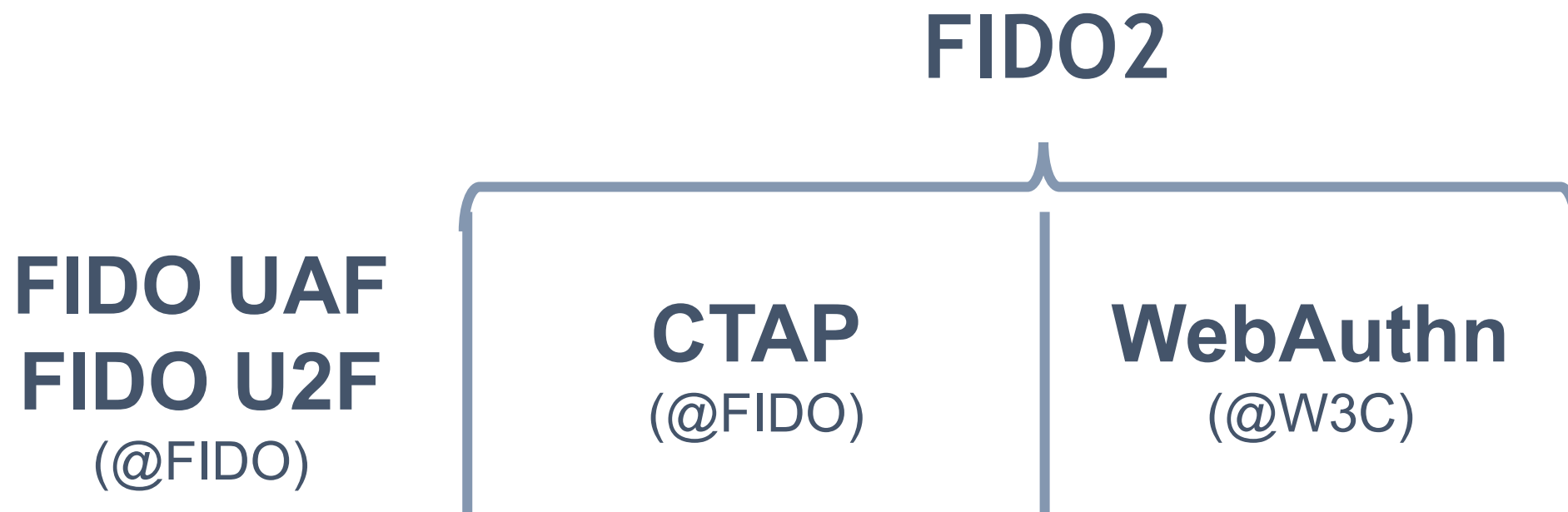
Insert Security Key* /
Press Button



Authenticated Online

*There are other types of authenticators

FIDO Specifications



BACKED BY CERTIFICATION (>500)

- Functional Certification (End-to-End):

- Conformance Testing
- Interoperability Testing



- Authenticator Security Certification Levels

- How well do you protect the private key?
- 3rd-party laboratory verification
- Complemented by Biometric Component certification



- Universal Server:

- Ensures compatibility with all FIDO Certified Authenticators



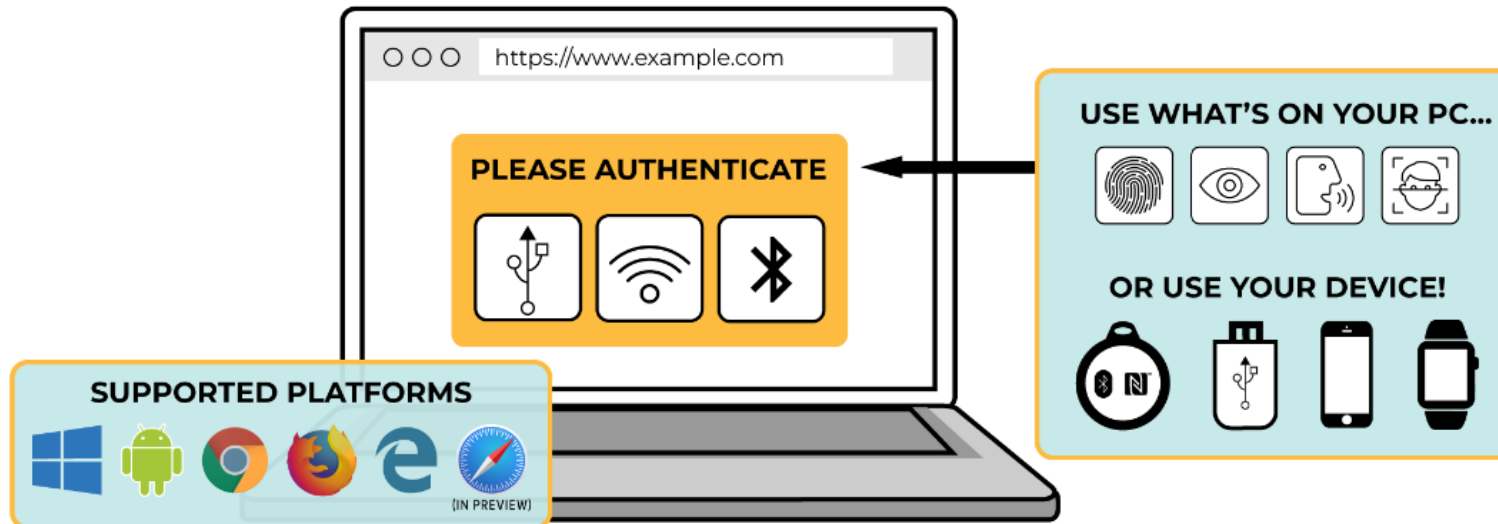


FIDO IN THE MARKET

FIDO NOW A W3C WEB STANDARD

FIDO2 (CTAP & W3C Web Authentication)

FIDO2 BRINGS STRONGER, SIMPLER AUTHENTICATION TO INTERNET USERS WORLDWIDE



FIDO IS AN ITU STANDARD



x.1277 -- ITU ratification of FIDO UAF

x.1278 -- ITU ratification of FIDO2 CTAP (includes CTAP1/U2F)

BIOMETRIC CERTIFICATION



SAMSUNG

and program to empirically
Galaxy S10 and S10+
through **Third-Party Labs**

they **Correctly Identify Users**

Biometric Modality

Implementation Types

FIRST TO ACHIEVE FIDO BIOMETRIC CERTIFICATION



VERSION 1.1

ANDROID IS NOW FIDO2 CERTIFIED

Mobile apps and websites can now leverage FIDO standards to provide a simpler and secure biometric login for users *on over a billion devices supporting Android 7.0 or later*



WINDOWS HELLO IS NOW FIDO2 CERTIFIED



Over **800 million** users with Microsoft accounts can now leverage built-in biometrics or local PINs to access their desktops and related Microsoft services



CROSS PLATFORM SUPPORT



MOZILLA:

PASSWORDLESS WEB AUTHENTICATION SUPPORT VIA WINDOWS HELLO



“Firefox 66 supports using the Windows Hello feature for Web Authentication on Windows 10, enabling a passwordless experience on the web that is hassle-free and more secure.

“Firefox has supported Web Authentication for all desktop platforms since version 60, but Windows 10 marks our first platform to support the new FIDO2 “passwordless” capabilities for Web Authentication.”

U2F API			WebAuthn API			
	Chrome/Windows					
U2F			CTAP2			
USB	NFC	BLE	USB	NFC	BLE	Hello

U2F API			WebAuthn API			
	Firefox/Windows					
U2F			CTAP2			
USB	NFC	BLE	USB	NFC	BLE	Hello

U2F API			WebAuthn API			
	Edge/Windows					
U2F			CTAP2			
USB	NFC	BLE	USB	NFC	BLE	Hello

U2F API			WebAuthn API			
	Chrome/Android					
U2F			CTAP2			
USB	NFC	BLE	USB	NFC	BLE	Plat

U2F API			WebAuthn API			
	Firefox/Android					
U2F			CTAP2			
USB	NFC	BLE	USB	NFC	BLE	Plat

U2F API			WebAuthn API			
	Safari/iOS					
U2F			CTAP2			
USB	NFC	BLE	USB	NFC	BLE	Plat

U2F API			WebAuthn API			
	Chrome/MacOS					
U2F			CTAP2			
USB	NFC	BLE	USB	NFC	BLE	Plat

U2F API			WebAuthn API			
	Firefox/MacOS					
U2F			CTAP2			
USB	NFC	BLE	USB	NFC	BLE	Plat

U2F API			WebAuthn API			
	Safari/MacOS					
U2F			CTAP2			
USB	NFC	BLE	USB	NFC	BLE	Plat

Special Thanks to Adam Powers & Akshay Kumar

Supported	In Development	Status Unknown
-----------	----------------	----------------

Note: “Android” means “via Google Play Services”

FIDO CERTIFIED ECOSYSTEM (SAMPLE)



SONY



yubico



Google



FUJITSU



RSA



SHARP

FEITIAN
WE BUILD SECURITY

RAON
SECURE

nok
nok

Lenovo



LINE



ANDROID



SECURITY KEYS (and more)



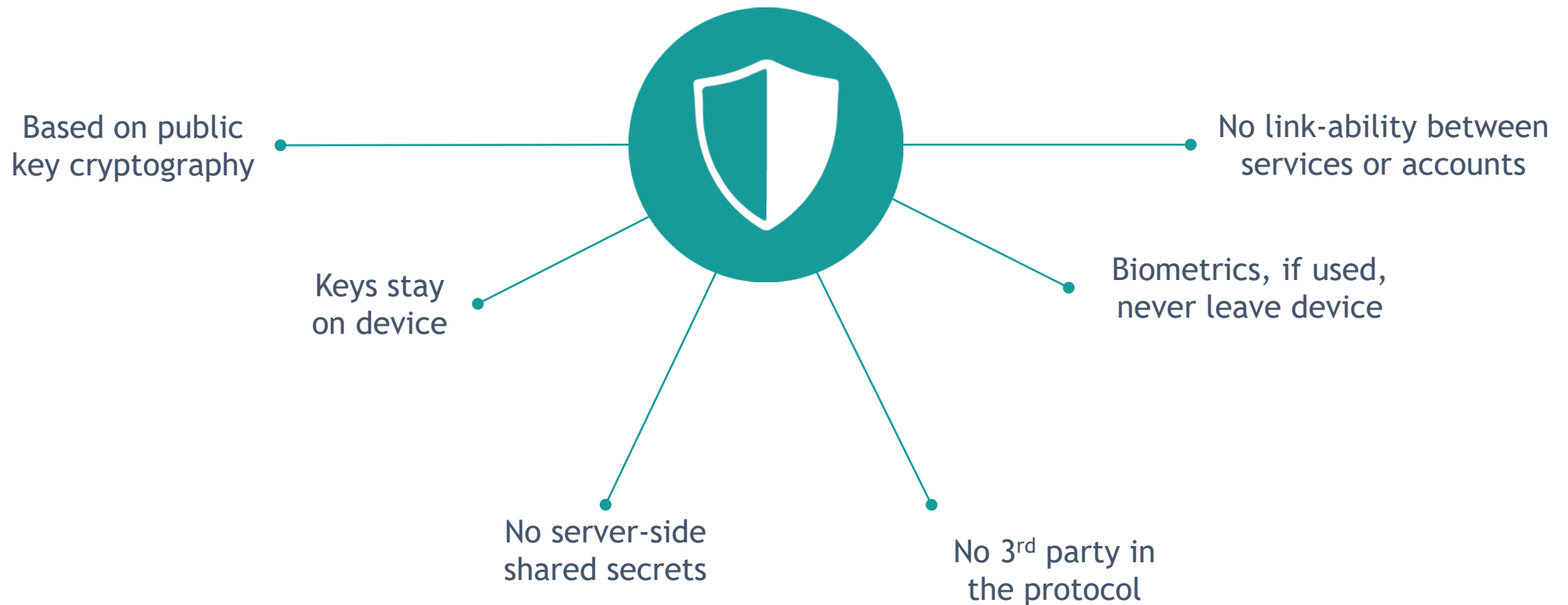
CLOUD/SERVER SOLUTIONS

HANDSETS + PCS

FIDO IS BEING USED AROUND THE WORLD (Sample of deployments in production)



SECURE BY DESIGN



SECURE IN PRACTICE

85,000 employees
over 18 months



23 Google: Security Keys Neutralized Employee Phishing

Google has not had any of its 85,000+ employees successfully phished on their work-related accounts since early 2017, when it began requiring all employees to use physical Security Keys in place of passwords and one-time codes, the company told KrebsOnSecurity.

Security Keys are inexpensive USB-based devices that offer an alternative approach to two-factor authentication (2FA), which requires the user to log in to a Web site using something they know (the password) and something they have (e.g., a mobile device).

A Google spokesperson said Security Keys now form the basis of all account access at Google.

“We have had no reported or confirmed account takeovers since implementing security keys at Google,” the spokesperson said. “Users might be



A YubiKey Security Key made by Yubico. The basic model featured here retails for \$20.

ADVERTISING/SP

Mailing
Subscr

dis
with
the
Find
with

No ATO's from phishing since using FIDO

WHAT'S NEXT...

KNOW YOUR CUSTOMER (eKYC/ID&V)



IoT Device ID/AuthN



FIDO: THE FUTURE OF USER AUTHENTICATION



FIDO Authentication is the industry's response to the password problem

- **INDUSTRY SUPPORT** - FIDO represents the efforts of some of the world's largest companies whose very businesses rely upon better user authentication
- **THOUSANDS OF SPEC DEVELOPMENT HOURS** - Now being realized in products being used every day
- **ONGOING INNOVATION** - Specifications, certification programs, and deployment working groups establishing best implementation practices
- **ENABLEMENT** - Leading service providers representing billions of user identities are already FIDO-enabling their authentication processes

Take Part in the FIDO Ecosystem

Build FIDO Certified Solutions

Deploy FIDO Authentication

Join the Alliance

Attend FIDO Events

Email: info@fidoalliance.org

Twitter: [@fidoalliance](https://twitter.com/fidoalliance)

www.fidoalliance.org