FIDO: Open Standards for Digital Identity and Authentication

FIGI Symposium 2021

1 June 2021

Jeremy Grant
Advisor
FIDO Alliance
jeremy.grant@venable.com

fido™ ALLIANCE

(Not) breaking news: Password problems

53%

of those who fell for a phishing attack were repeat victims
(Verizon)

49%

password-driven cart abandonment rate
(Visa)

55%

of IT leaders re-use a single password
(Sailpoint)

51%

of passwords are reused across services
(University of Oxford)

20-50%

of helpdesk calls are for password resets
(Forrester)

80-90%

e-commerce sites' attempted log-ins are compromised by stuffing
(Shape Security)

$5 billion

cost to U.S. businesses each year
(Shape Security)

30 billion

stuffing attempts in 2018
(Akamai)

1,300 years

collectively spent by humans each day entering passwords
(Microsoft)

36% rise

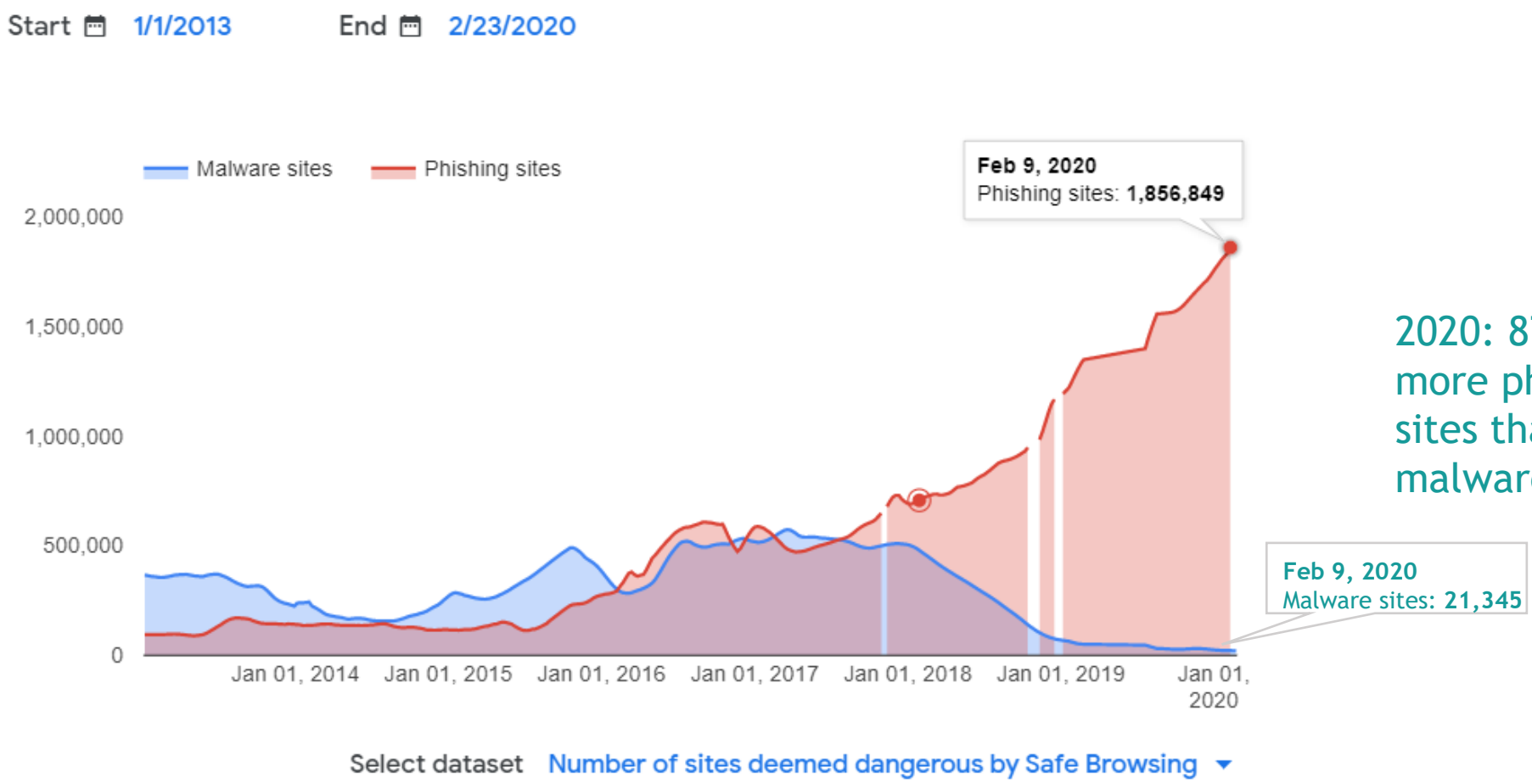
in phishing attacks in 2018
(Webroot)

1,244

breaches in 2018, a 126% jump in exposed records containing PII
(Identity Theft Resource Center 2018 Breach Report)

With authentication, Phishing is the threat

Phishing sites grew by 557% (2016-2020)



2020: 87x more phishing sites than malware

Source: https://transparencyreport.google.com/safe-browsing/overview?hl=en

The Credential Theft Cycle

7,098 data breaches last year

15.1 billion exposed records in 2019

Data Breach leads to credentials for sale on Dark Web

Credential loss grew by 284% in 2019

Criminals purchase credentials, use botnets to prep attacks

Credentials cost $0.70 - $2.30

Credential stuffing attacks on e-commerce, enterprise, etc

80-90% of login attempts to e-commerce sties are spoofs

Up to 2% of stuffing attempts are successful

Annual cost to US Businesses: $5 billion

Server-side Authentication Credentials

Sources: ITRC, Verizon, Shape Security, Akamai

And this past year, everything got worse

(#thanksCOVID) ☹

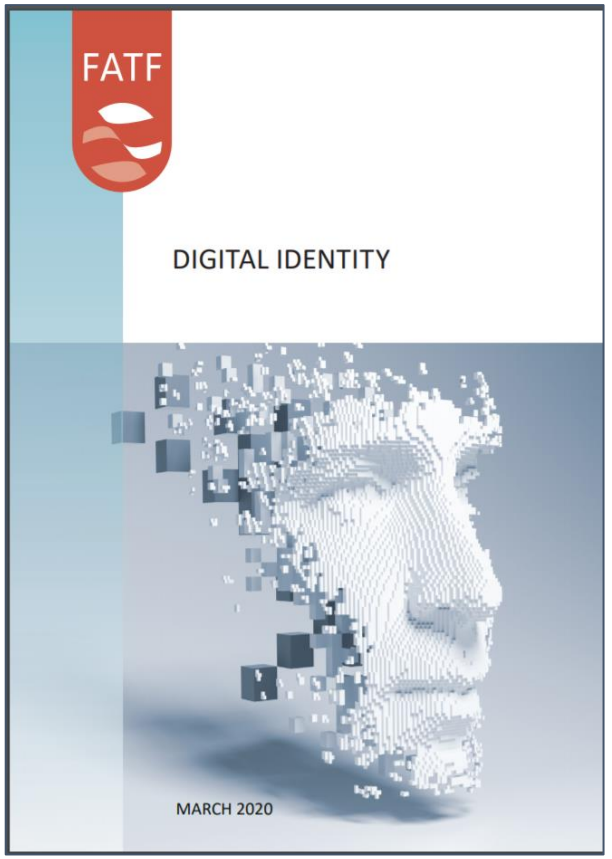
How to deliver security of Digital Financial Services?

How to guard against account takeovers?

FATF recommendations to combat phishing

"Multi-factor authentication (MFA) solutions, such as SMS one-time codes texted to the subscriber's phone, add another layer of security to passwords/passcodes but they can also be vulnerable to phishing and other attacks.

*Phishing-resistant authenticators where at least one factor relies on public key encryption (e.g., authenticators built off PKI certificates or the **FIDO standards**) can help combat these vulnerabilities."*



ONE-TIME PASSCODES?

They are still “shared secrets”

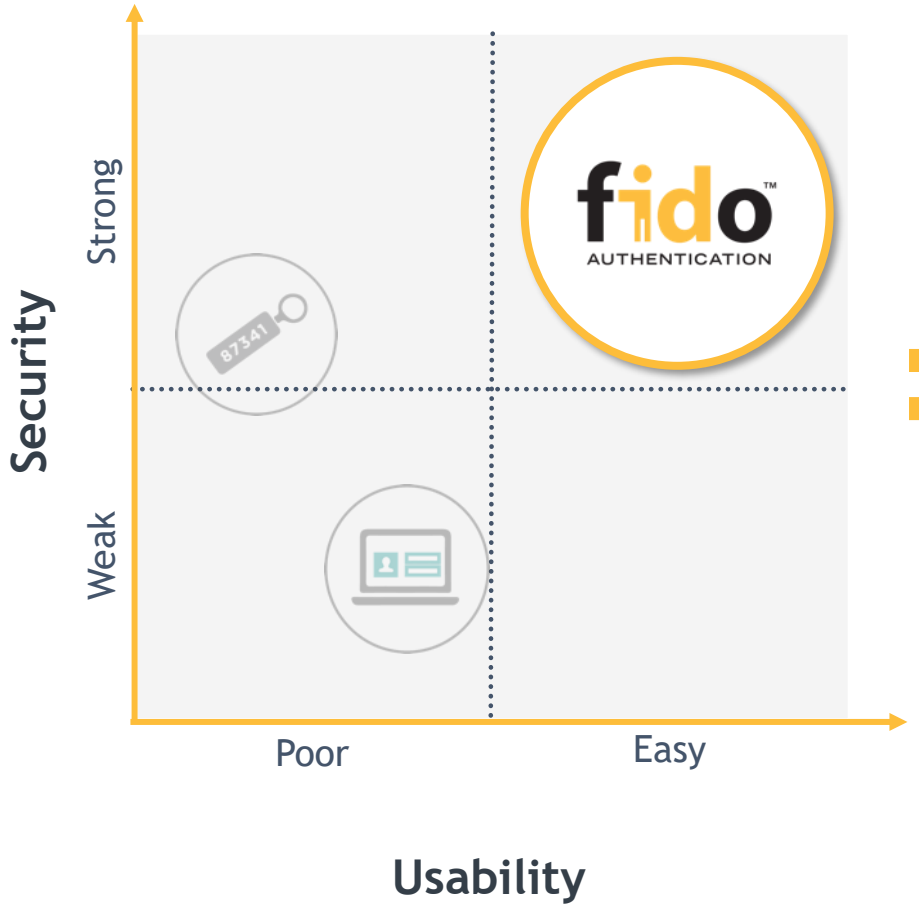
SMS
Vulnerability

Token
Necklace

User Experience
Friction

Still
Phishable

Industry imperative: Simpler and stronger



=

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

Single Gesture
Possession-based Authentication

What's FIDO?

The FIDO Alliance is an open industry association with a focused mission:

Develop authentication standards, certification and market adoption programs to help reduce the world's over-reliance on passwords.

An industry movement

+ Sponsor members

+ Associate members

+ Liaison members

Track record of successful collaboration

- **3 Sets of Specs Released**

- **Growing Platform Support**




- **Increasing Market Adoption**

Standardization across other organizations

WebAuthn meets W3C Final Recommendation

FIDO CTAP and FIDO UAF are ITU standards (X.1277 and X.1278)

ISO 27553, 29115 engagement

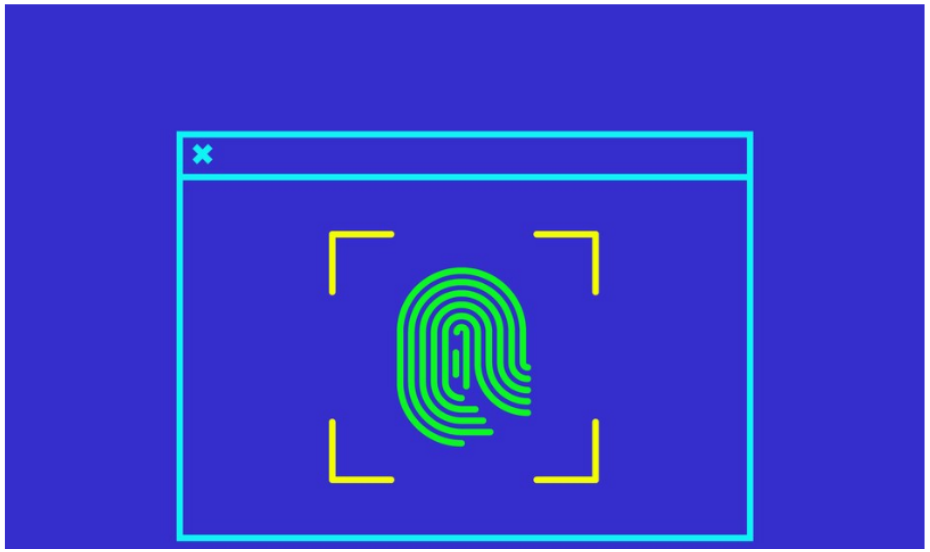

Over 2.5 Billion Devices can
support FIDO Authentication

1B+ Android Devices Have FIDO “Built In”

WIRED GIVE A GI

LILY HAY NEWMAN SECURITY 02.25.19 06:00 AM

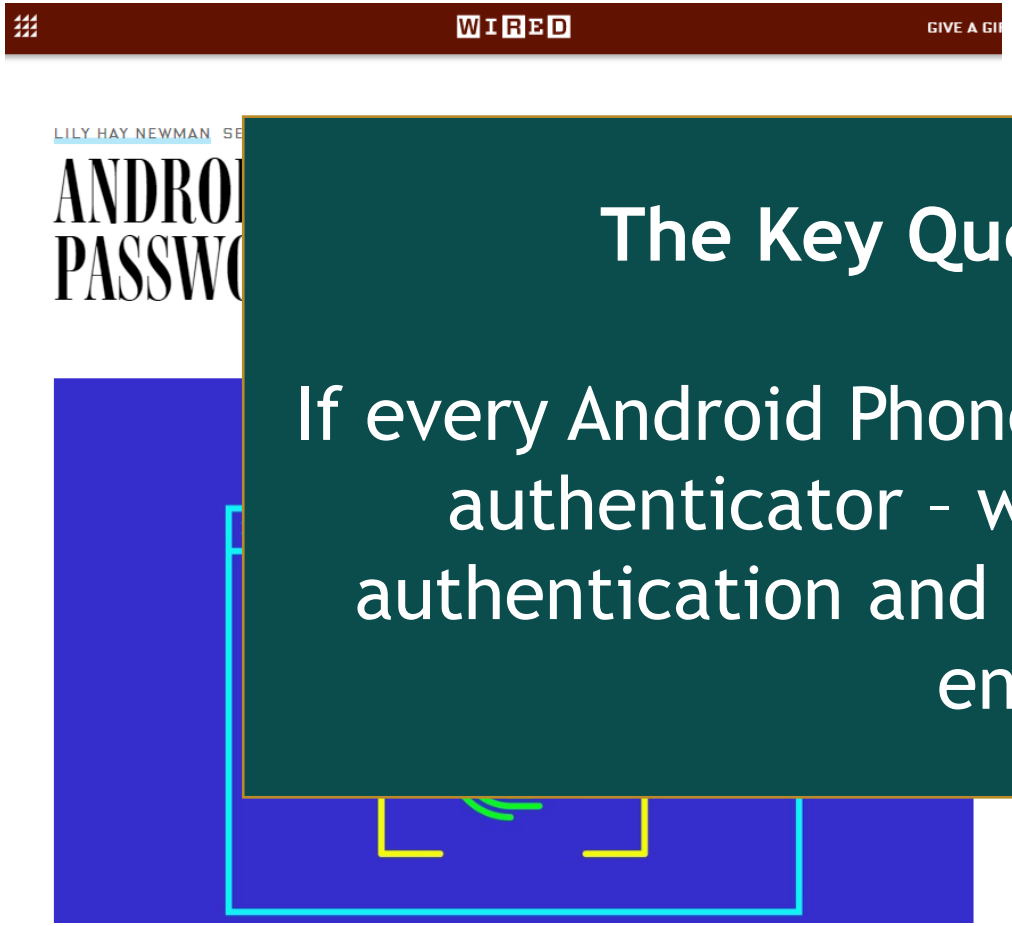
ANDROID IS HELPING KILL PASSWORDS ON A BILLION DEVICES



IT'S MORE IMPORTANT than ever to manage your passwords online, and also harder to keep up with them. That's a bad combination. So the FIDO Alliance—a consortium that develops open source authentication standards—has pushed to expand its secure login protocols to make seamless logins a reality. Now Android's on board, which means 1 billion devices can say goodbye to passwords in more digital services than seen before.

On Monday, Google and the FIDO Alliance announced that Android has added certified support for the FIDO2 standard, meaning the vast majority of devices running Android 7 or later will now be able to handle password-less logins in mobile browsers like Chrome. Android already offered secure FIDO login options for mobile apps, where you authenticate using a phone's fingerprint scanner or with a hardware dongle like a YubiKey. But FIDO2 support will make it possible to use these easy authentication steps for web services in a mobile browser, instead of having the tedious task of typing in your password every time you want to log in to an account. Web developers can now design their sites to interact with Android's FIDO2 management infrastructure.

1B+ Android Devices Have FIDO “Built In”



The Key Question for FIGI:

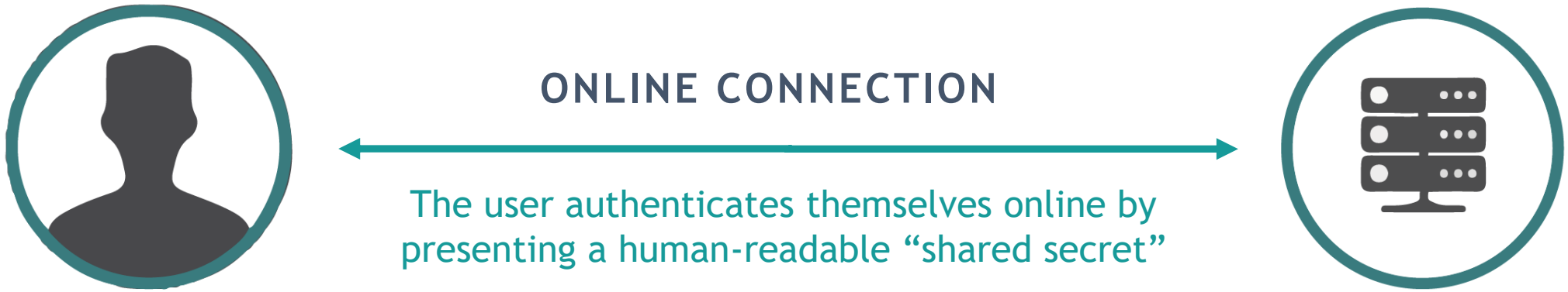
If every Android Phone is now a certified FIDO authenticator – what new models for authentication and credentialing does this enable?

IT'S MORE IMPORTANT than ever to manage your passwords online, and also harder to keep up with them. That's a bad combination. So the FIDO Alliance—a

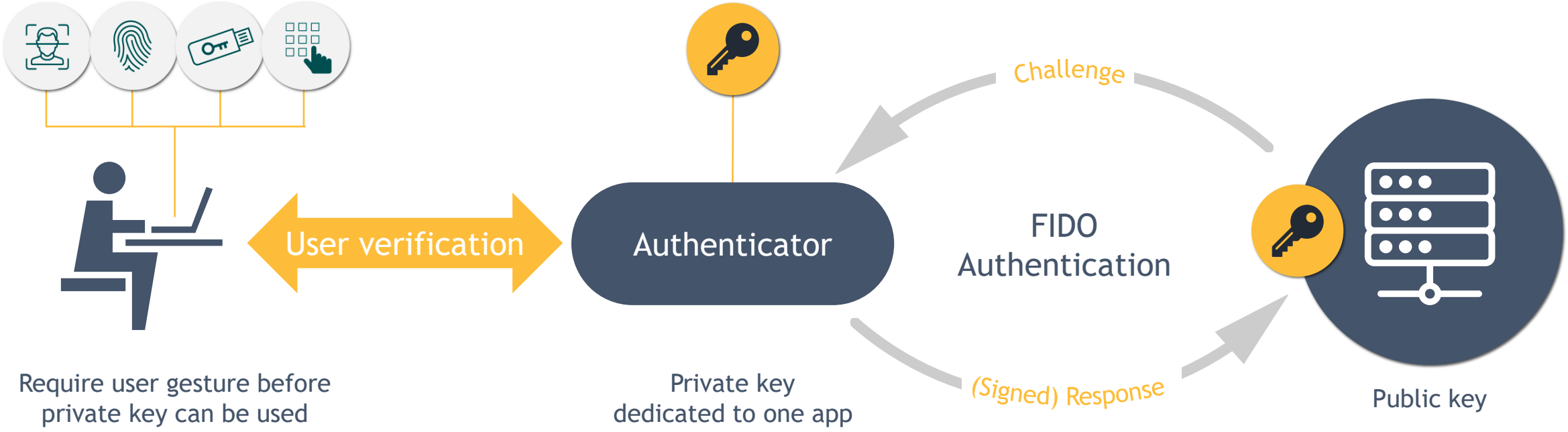
mobile browser, instead of having the tedious task of typing in your password every time you want to log in to an account. Web developers can now design their sites to interact with Android's FIDO2 management infrastructure.

HOW DOES FIDO WORK?

How old authentication works



How FIDO authentication works



FIDO authenticators

We see “Bound” Authenticators

(authenticators that are an integral part of a smartphone or laptop)

We see “Roaming” Authenticators

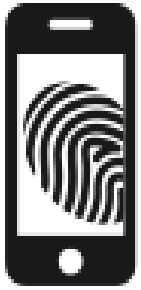
(authenticators that can be connected to different smartphones/laptops using CTAP)

In both categories you find support for different modalities

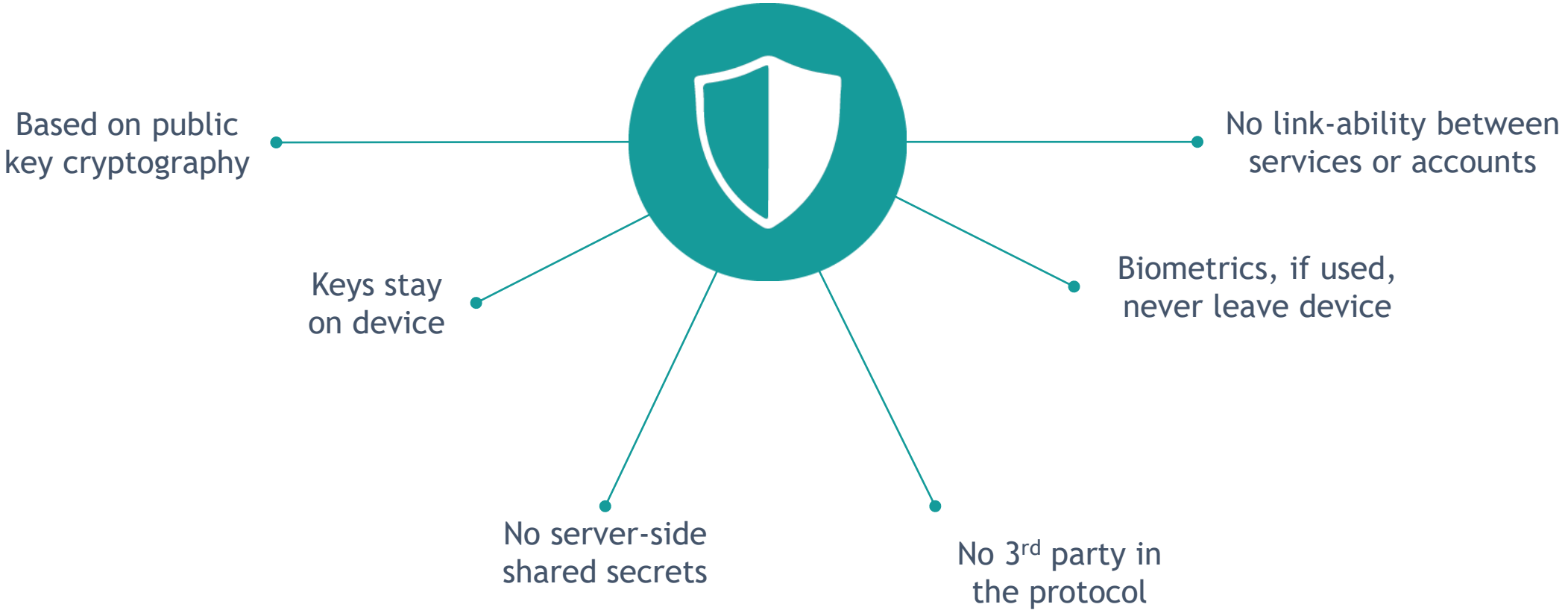
User Presence Challenge
(“A” user)

User Verification Methods
(“THE” user)

A smartphone can be <u>both</u> a “bound” authenticator and a “roaming” authenticator



Privacy By Design



Security in Practice

Google

85,000+ employees
over 18 months

No ATO's from phishing
since using FIDO Authentication

KrebsonSecurity
In-depth security news and investigation

ADVERTISING/SP

23 JUL 18 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 YubiKey Security Key made by Yubico. The

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

Mailing
Subscr

dig
with
the
Find
with

How old authentication works: User experience

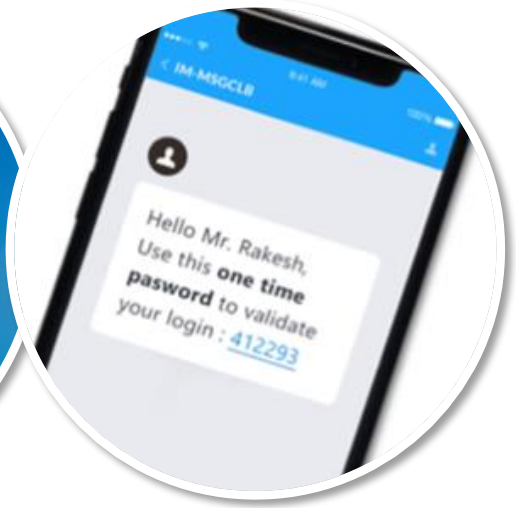
PASSWORDS

Frustrating to type on tiny screens…

… and easy to forget

TRADITIONAL MFA

Extra hardware for every app…



…or more codes to type

How FIDO Authentication works: User experience

FIDO Authentication

Use what's on your device…

…or something you carry with you…

…for an overall better user experience

The Future of User Authentication

FIDO Authentication is the industry's answer 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

Thank you!

@FIDOALLIANCE
WWW.FIDOALLIANCE.ORG

Jeremy Grant
jeremy.grant@venable.com