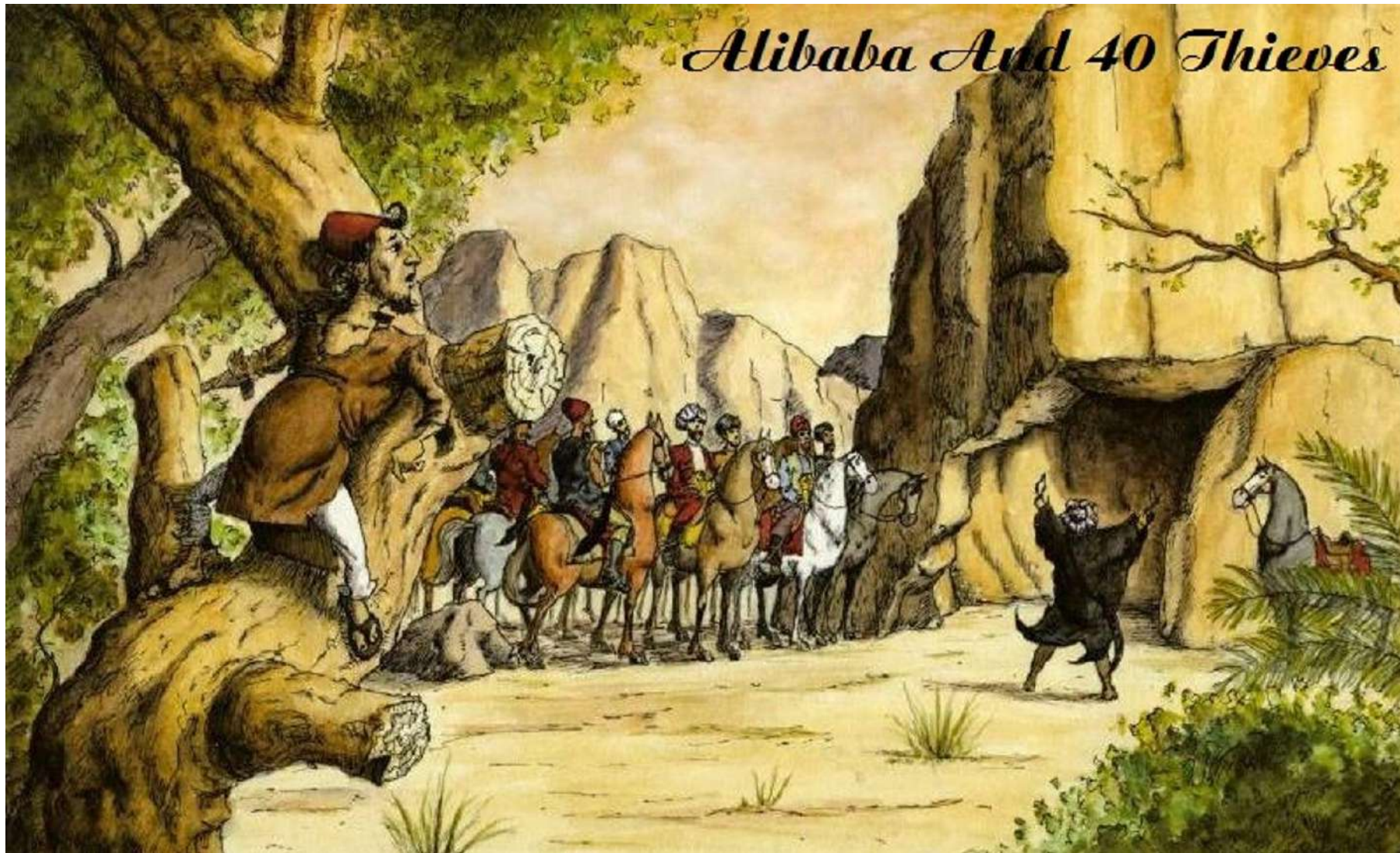


Are we entering a new era of authentication?

CHAN TZE HOONG
SENIOR TECHNICAL MANAGER
TZEHOONG.CHAN@ONESPAN.COM
6TH AUGUST 2025

What did we learn from Alibaba?



Microsoft Authenticator recent announcement:

- Passwords will no longer be supported and will no longer be saved

BUT

- They still support Passkeys

? What's Passkey ?

When are the autofill changes happening?

- Starting June 2025, you will no longer be able to **Add** or **Import** new passwords in the Authenticator App. However, you can continue saving passwords through autofill until July.
- During July 2025, you will not be able to use autofill with Authenticator.
- From August 2025, your saved passwords will no longer be accessible in Authenticator.

What happens to my saved passkeys?

Authenticator will continue to support passkeys.

Source: <https://support.microsoft.com/en-us/account-billing/changes-to-microsoft-authenticator-autofill-09fd75df-dc04-4477-9619-811510805ab6>



Passkey

A *passkey* is a FIDO authentication credential based on FIDO standards, that allows a user to sign in to apps and websites with the same process that they use to unlock their device (biometrics, PIN, or pattern). Passkeys are FIDO cryptographic credentials that are tied to a user's account on a website or application. With passkeys, users **no longer need to enter usernames and passwords** or additional factors. Instead, a user approves a sign-in with the same process they use to unlock their device (for example, biometrics, PIN, pattern).

? What's FIDO ?



Definition Extracted from: <https://fidoalliance.org/passkeys/>



Gartner's recent trends and predictions

- IAM leaders should migrate to passwordless methods with **phishing-resistant** MFA based on FIDO2 authenticators.
- By **2027**, more than **75%** of workforce authentication transactions and more than 40% of customer authentication transactions will be passwordless with accompanying security and UX benefits.
- By **2027**, more than **90%** of multifactor authentication (MFA) transactions using a token will be based on FIDO authentication protocols natively supported in AM tools.

Source: Gartner, 2024

"Migrate to Passwordless Authentication to Enhance Security and Optimize UX"
by Ant Allan, James Hoover

? What's Passwordless ?



Modern Authentication is meant to be Passwordless



Create Account

Password Requirements:

- A lowercase character
- An uppercase character
- A special character
- A numeric character
- An alphabetic character
- A minimum of 8 characters

Email Address

Password

Verify New Password



Simplify the Customer Journey

25% of people stop when asked for a new password


58% of consumers have abandoned carts due to difficulty signing in

Logged in users have a 10% higher average order value



Can Passkey Stop Attacks

Three Major Threat Categories in Digital Banking



Account Take-Over (ATO) fraud



Device Take-Over (DTO) fraud

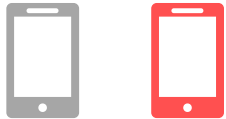


Authorized Push Payment (APP) fraud

Fraud performed by fraudster, from fraudster's device



Victim Fraudster

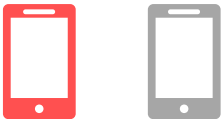


Victim's device Fraudster's device

Fraud performed by fraudster, from victim's device



Victim Fraudster

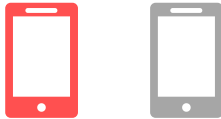


Victim's device Fraudster's device

Fraud performed by victim, from victim's device



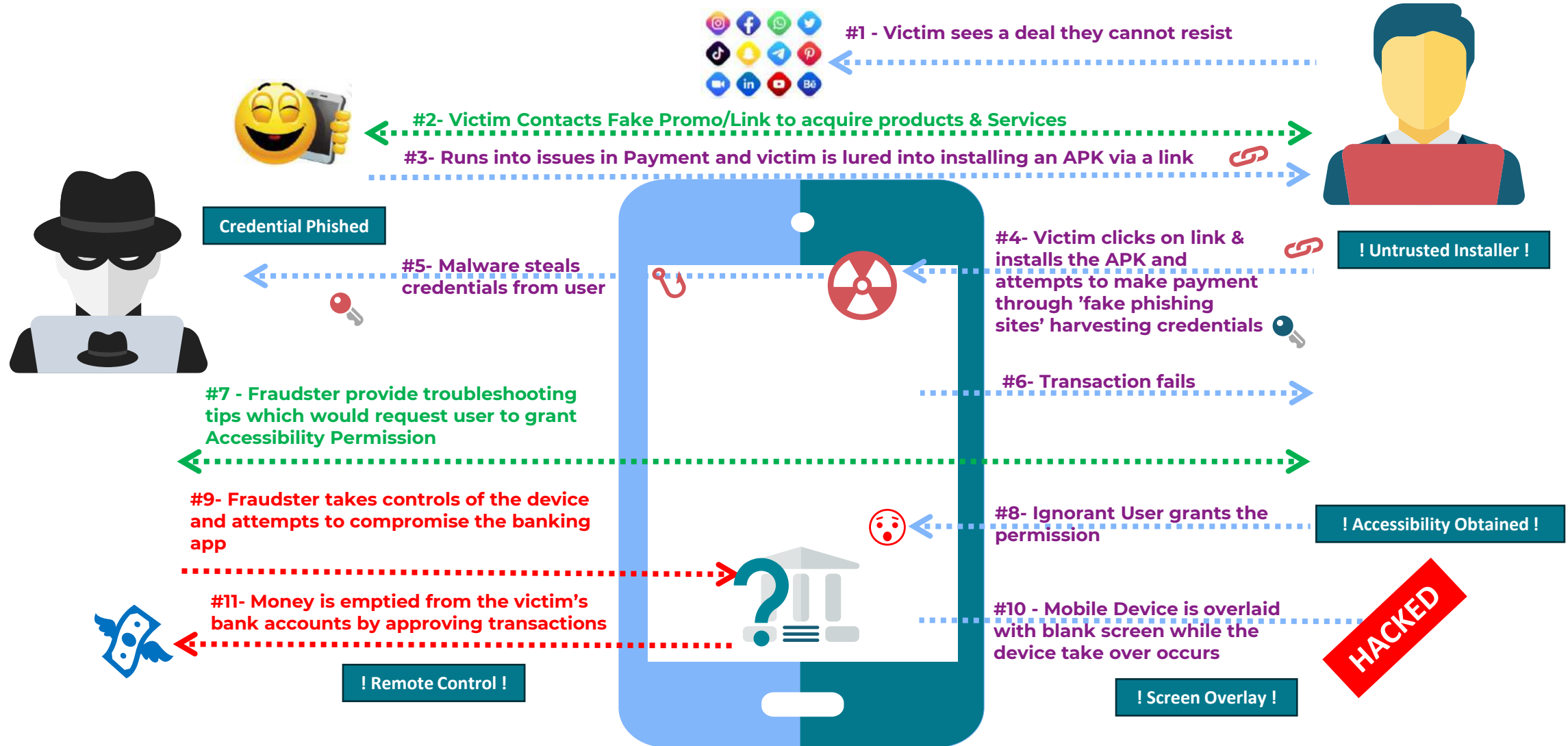
Victim Fraudster



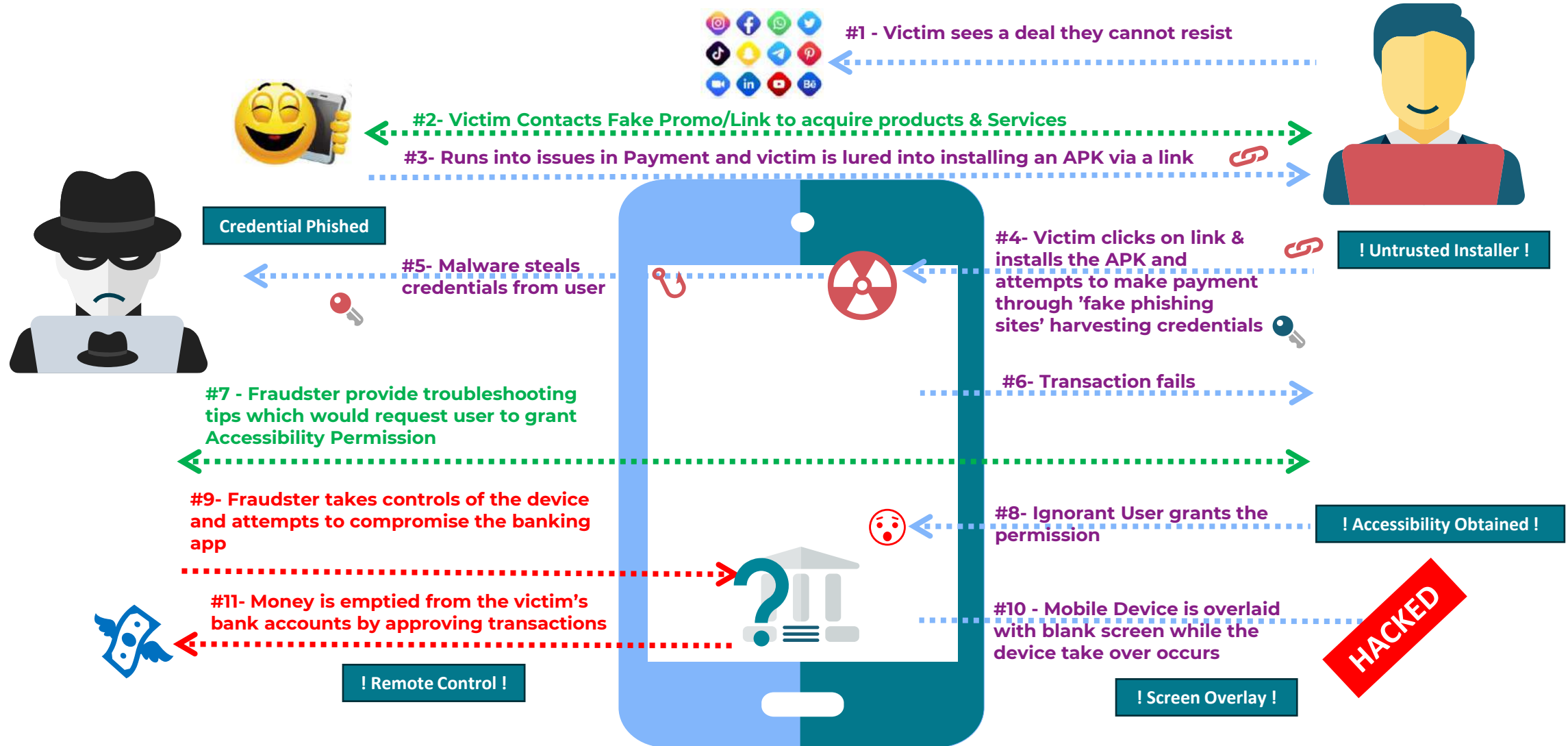
Victim's device Fraudster's device



Modus Operandi – Unauthorized Fraud using Phishing & Malware Account + Device Takeover



Modus Operandi – Unauthorized Fraud using Phishing & Malware Account + Device Takeover



The Challenges with Existing Authentication mechanisms

- Passwords
 - Easily be STOLEN / PHISHED – often without your knowledge
 - Passwords needs to be COMPLEX & Unguessable
 - Passwords needs to be Managed / RESET
- One Time Passwords (OTP)
 - Can still be STOLEN / PHISHED
 - SMS / Email OTP are usually not Encrypted and commonly intercepted
 - OTP Generated on Mobile device is subjected to Remote Access Trojan / Malware attacks that takes control of device
- Certificate/SmartCard (PKI)
 - Difficult to Manage (continuous renewal of certificate is a challenge)
 - Requires endpoint configuration (e.g. driver installation for USB based PKI devices) in some cases
 - Roaming PKI often fall back to the same weakness of being protected by Password / OTP schemes
- Biometrics
 - Often exploits False Positives and use of AI methods (e.g. DeepFake)

What are Passkeys

How do they relate to FIDO & Passwordless

FIDO Overview



- FIDO is short for **Fast Identity Online**
- Founded in 2013
- Focus on providing open and free authentication standards to help reduce reliance on passwords.
- Emphasis on **Passwordless** Authentication



FIDO standards allow secure and fast login to web sites and/or mobile apps across user's devices with a biometric or security key.

- **Defined Three Specification**

- U2F – Universal Two Factor
- UAF – Universal Authentication Framework
- FIDO2

OneSpan has been a Board Member

Nok Nok Labs is also a Founder & Board Member

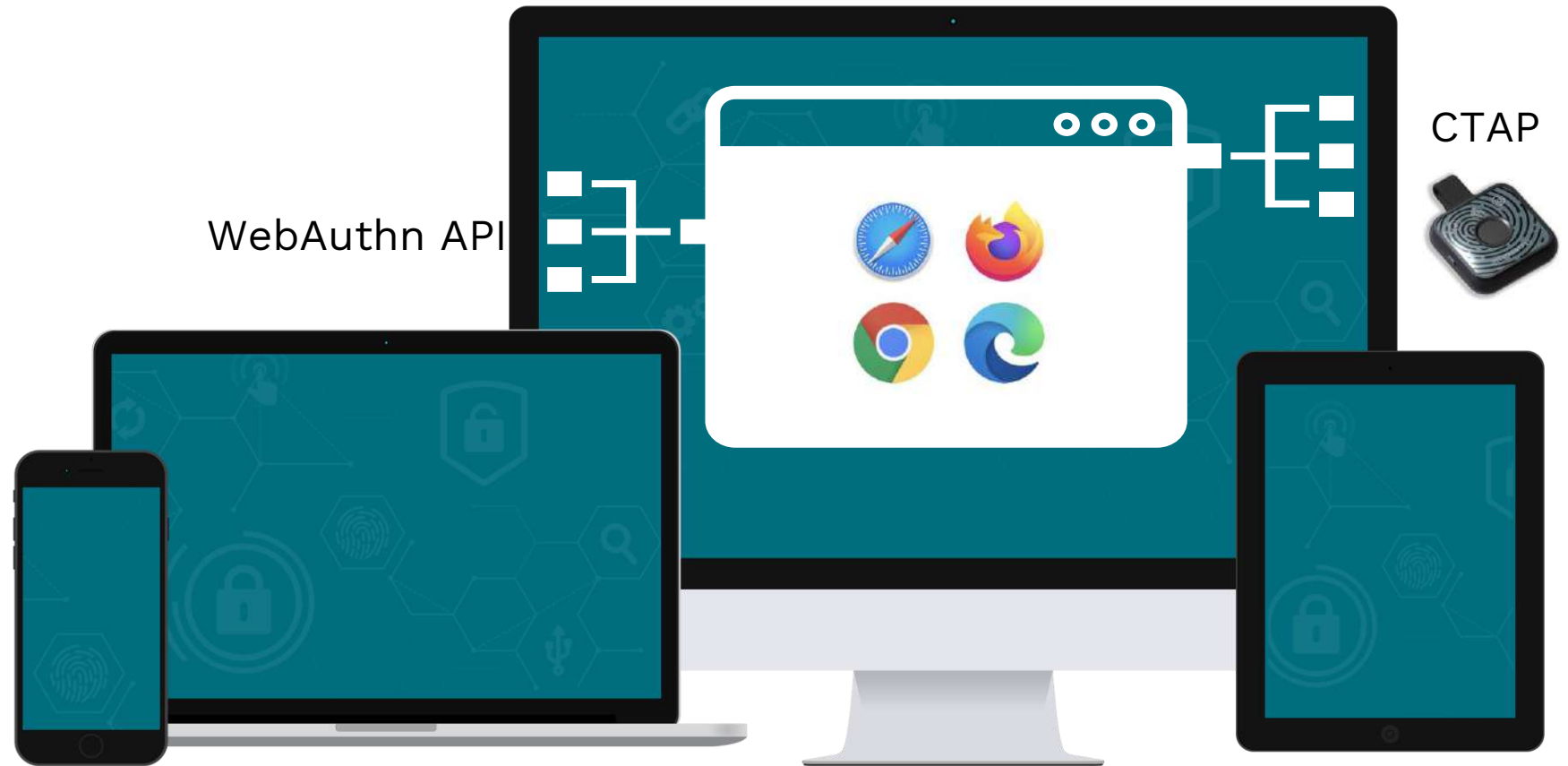
FIDO consists of Three Specifications



- **Included two more Specifications for FIDO2**

- WebAuthn – Web Authentication specifications, maintained by W3C
- CTAP – Client to Authenticator Protocol, maintained by FIDO

FIDO2 includes Two More Specifications



Benefits of the FIDO ecosystem

- Backed by global tech leaders
- Supported by major browsers & OS
- Interoperability
- Certification process
- Scalability
- Large ecosystem – including IAM vendors



Passkey awareness and adoption is increasing

Term “passkey” introduced in 2022

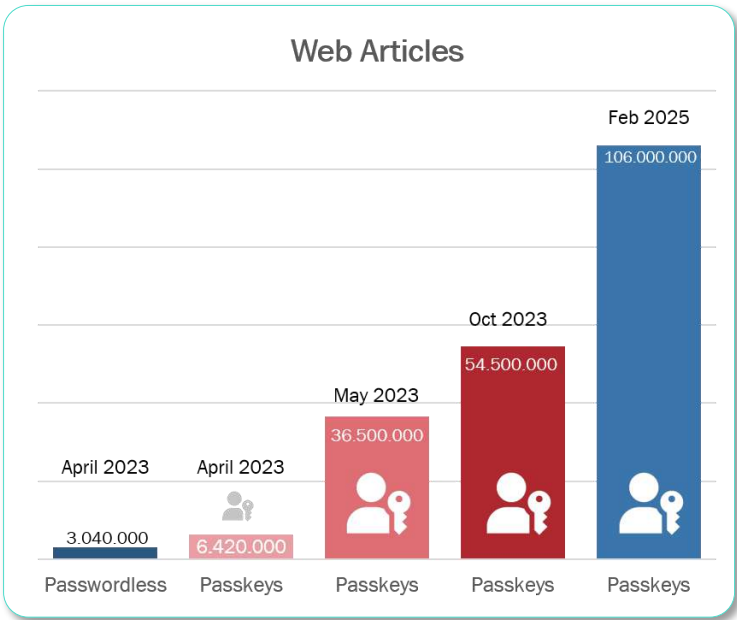
57%

of consumers
are aware of
passkeys – up from
39% in 2022



87%

of organizations
have deployed
passkeys for
workforce sign-ins

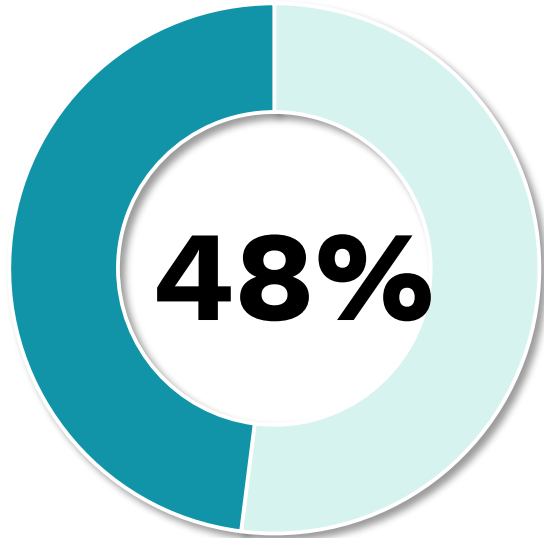


Source: Nok Nok

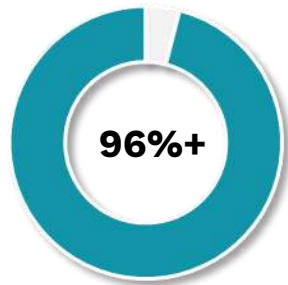
Source: FIDO Alliance



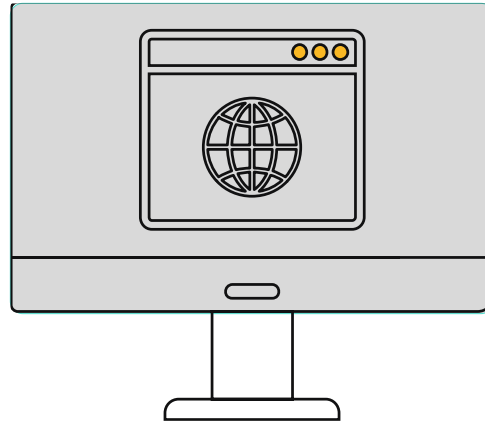
Passkey adoption by the numbers



**of the world's top
100 websites and services**

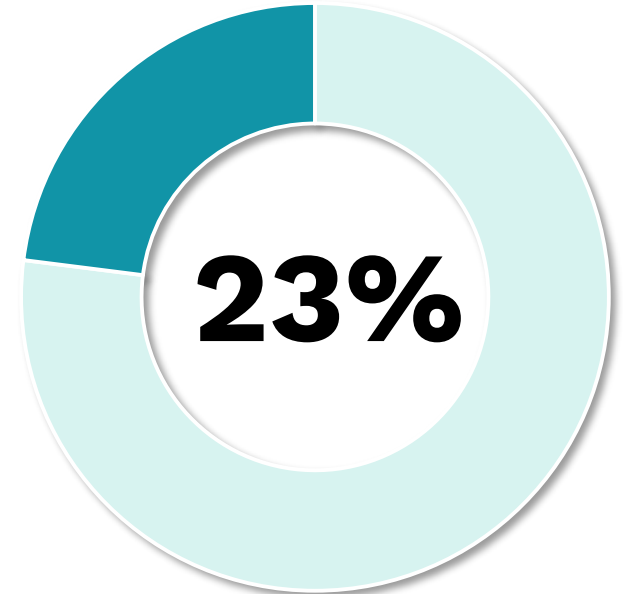


**of active
browsers**

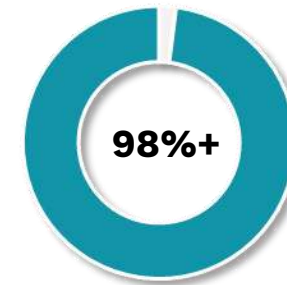


**More
than 15B**

**accounts can now leverage
passkeys for sign in**



**of the world's top
250 websites and services**



**of mobile
devices**



Goodbye Passwords/Hello Passkeys!



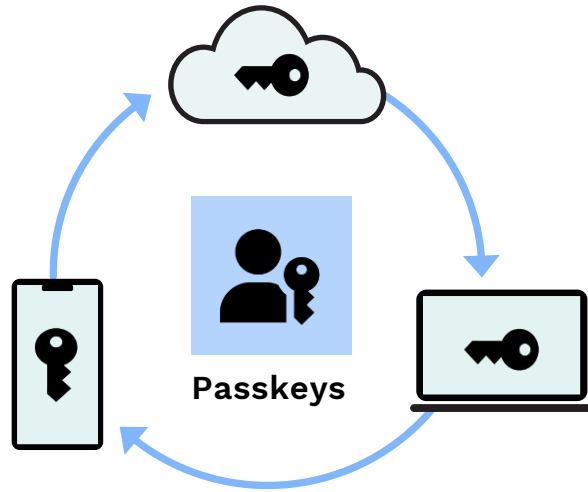
Google



Microsoft



iCloud



fido[™] simpler
ALLIANCE stronger
authentication

Simple User Experience

Protection from #1 cause of breaches

- ✓ Increase onboarding conversion
- ✓ Improve sign-in speed and success
- ✓ Reduce password resets
- ✓ Protect users from account takeover

Supported by the Ecosystem



Features of FIDO2 Standards

User experience



Passwordless experience



Gesture log on



Support most devices



One device to All application/accounts



Fast and convenient

Security



Public key cryptography



Private key never leave the device



Biometrics never leave the device



Server never store secrets

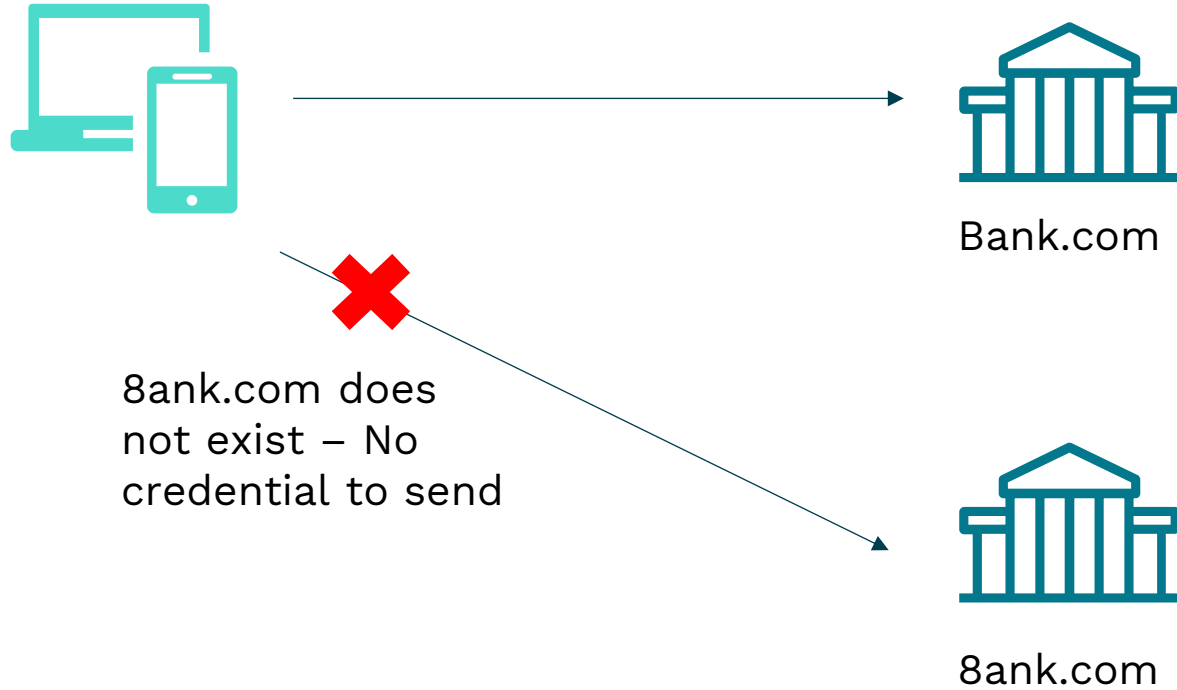


No link-ability between accounts



Channel Binding – the key anti-Phishing Property of FIDO

Check if
Bank.com is
same as
previously
registered within
device

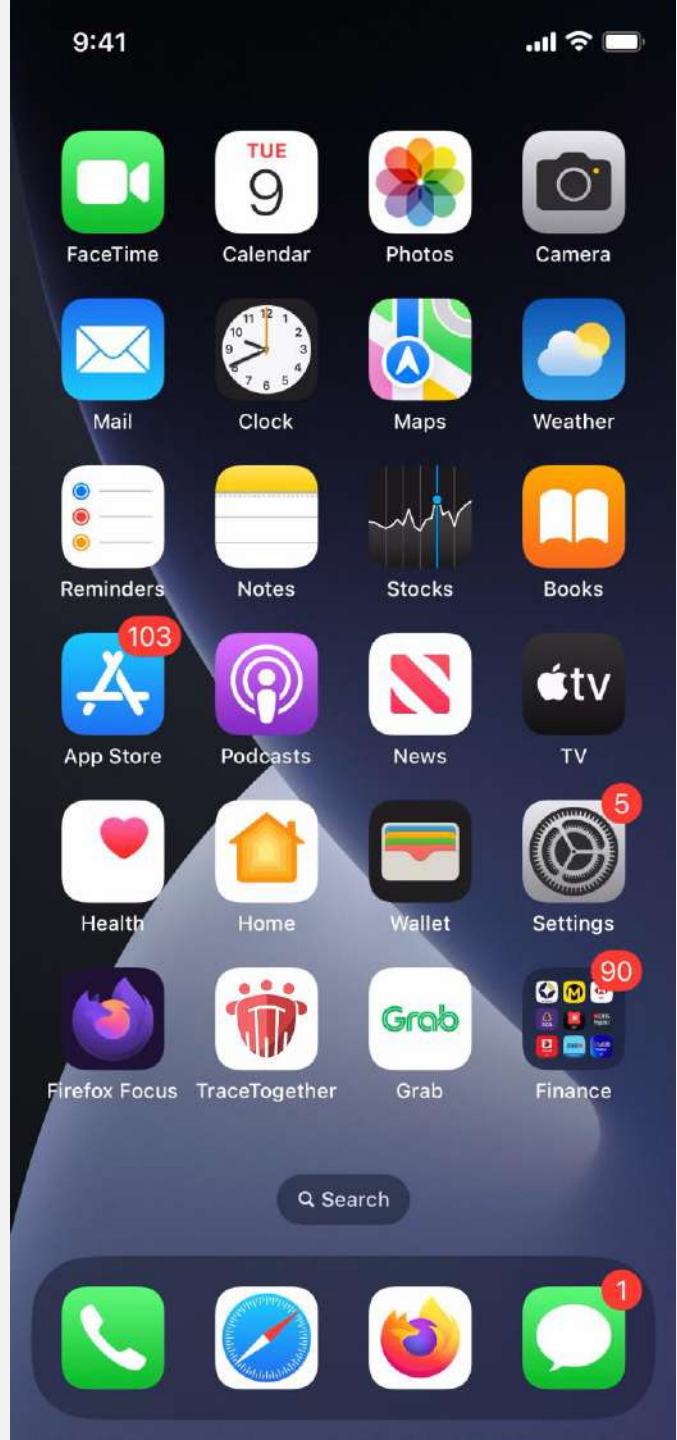


Registering Passkey



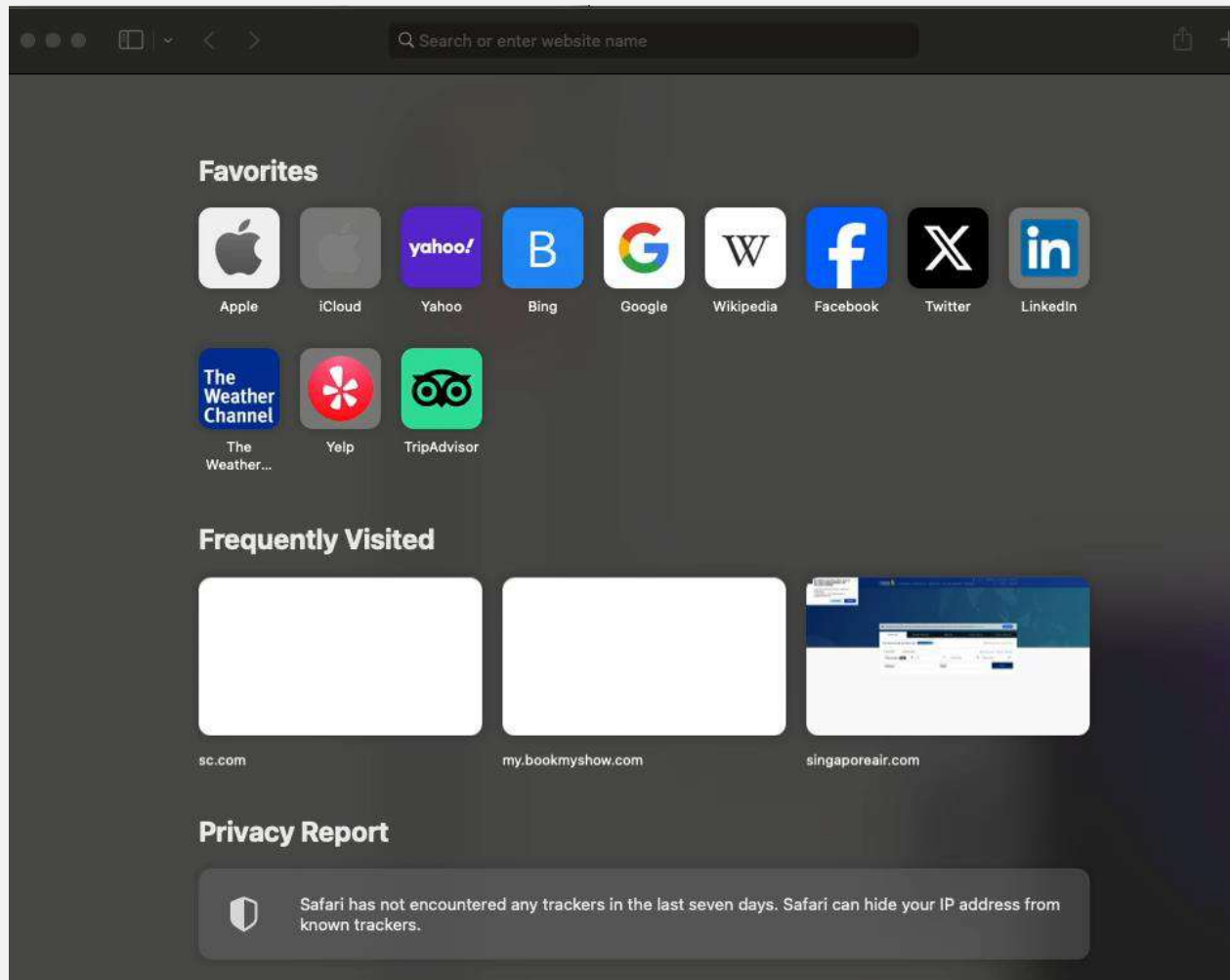
Use Cases

Passkey is now on the platform
- Usable by different browsers

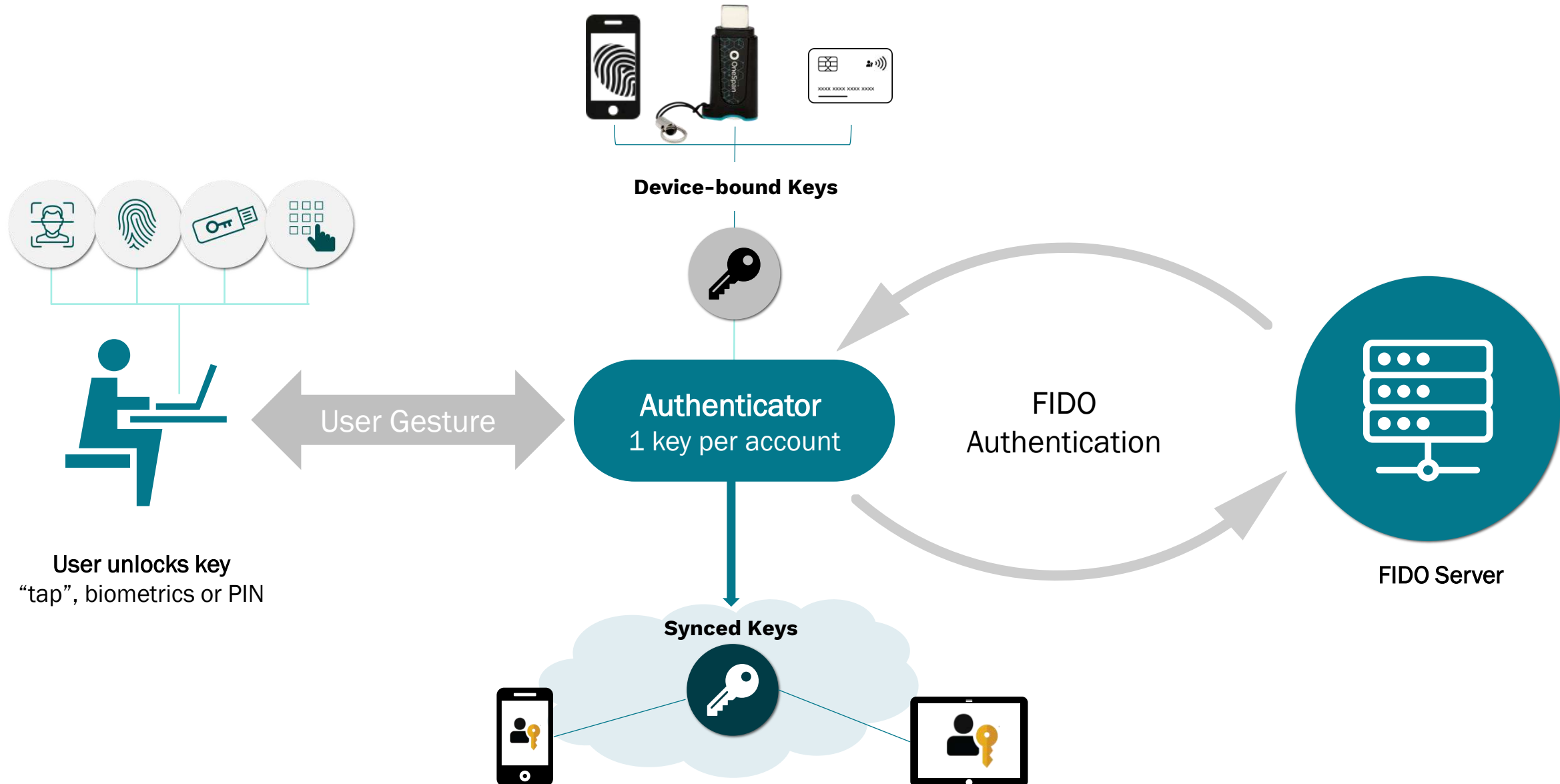


Use Cases

Passkey is also synced to other devices
- Usable by another Synced device



FIDO Authentication Ecosystem at a glance

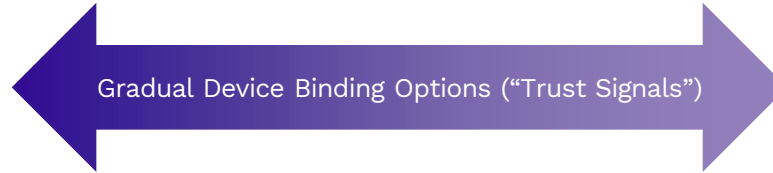


Two Types of Passkeys



Device Bound

- Can be used through native apps, without UX changes
- **For high security, require a device bound key to detect known devices**



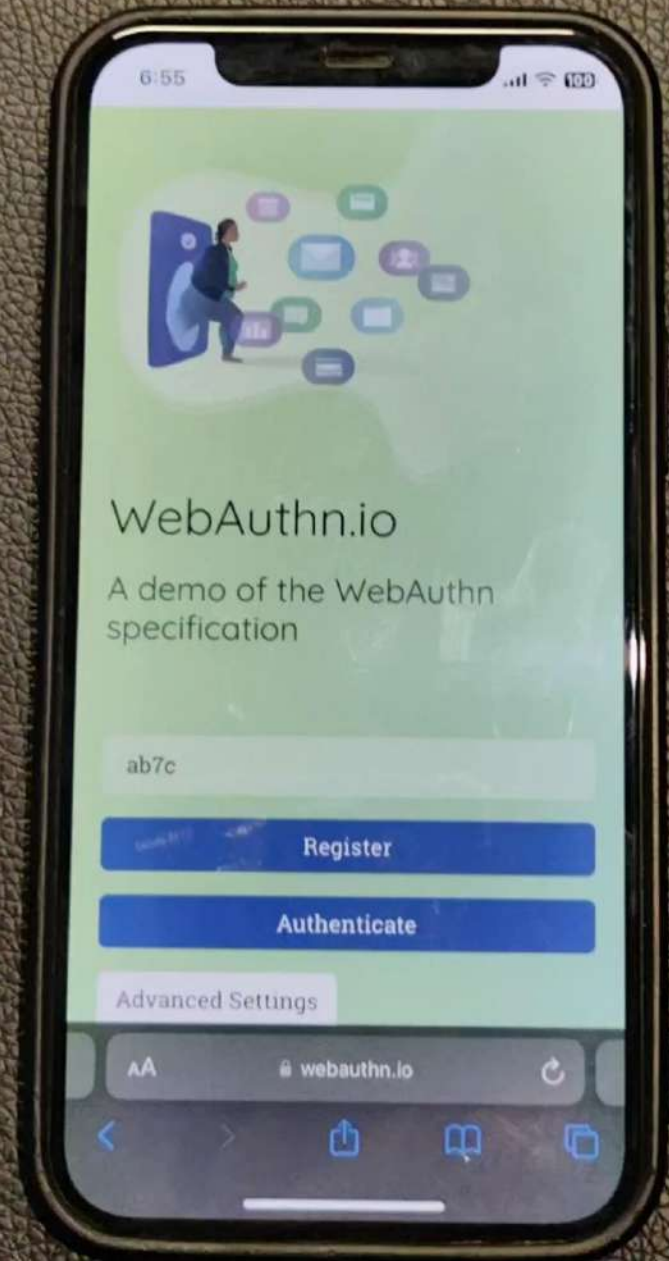
Synchronized

- Introduced in 2022
- Synced across all your devices
- **Synced passkeys can practically replace passwords**

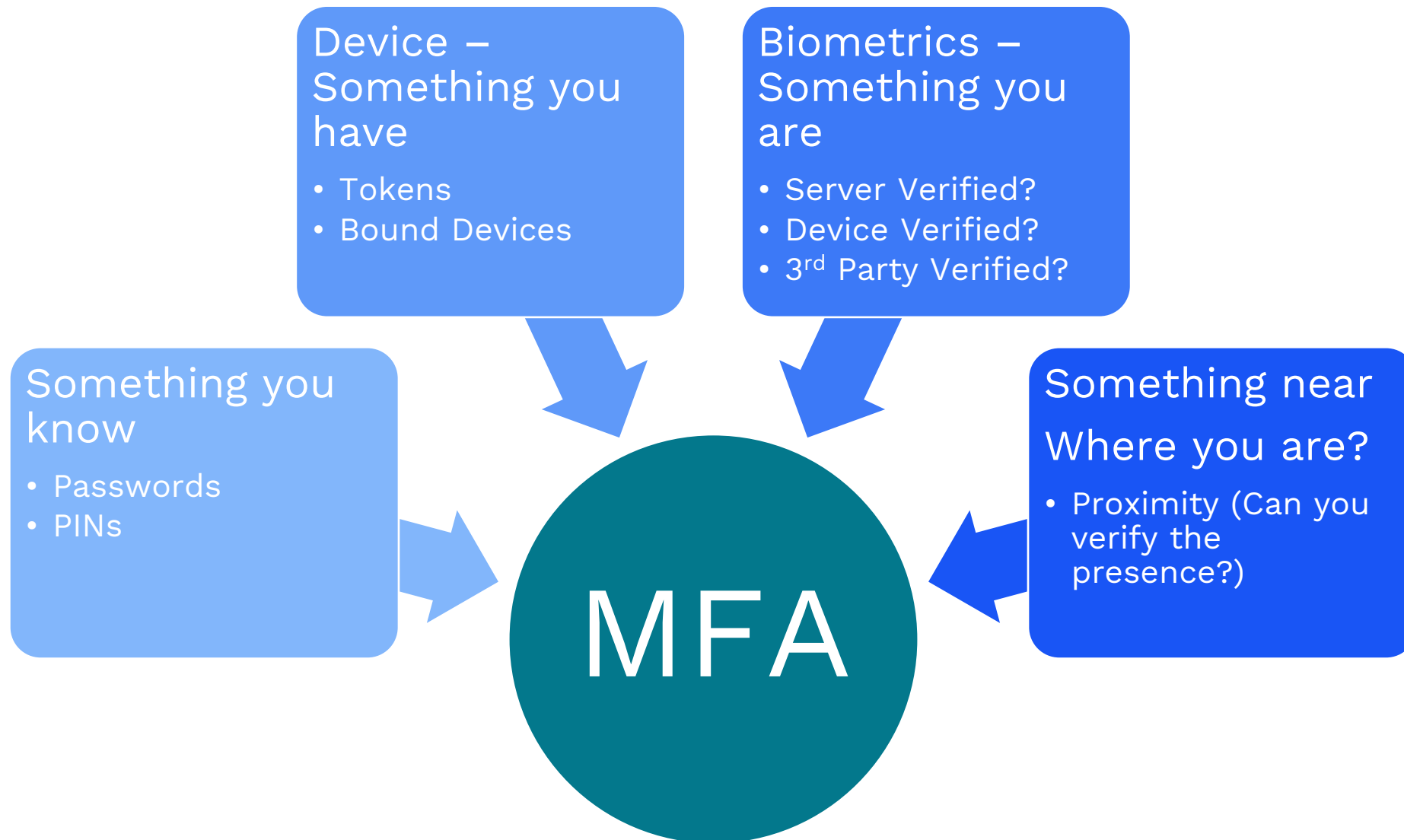


Use Case

Authenticating using
External Device Authenticator



Does your MFA Authentication combine 2+ of factors below? What is the best MFA?



Solving ~~The Challenges with Existing~~ FIDO2 Authentication mechanisms

- Passwords

- Easily be STOLEN / PHISHED – often without your knowledge
- Passwords needs to be COMPLEX & Unguessable
- Passwords needs to be Managed / RESET

FIDO is Passwordless – Nothing to Steal / Phish

- One Time Passwords (OTP)

- Can still be STOLEN / PHISHED
- SMS / Email OTP are usually not Encrypted and commonly intercepted
- OTP Generated on Mobile device is subjected to Remote Access Trojan / Malware attacks that takes control of device

Dedicated, tamper resistant, secure element protected device

- Certificate/SmartCard (PKI)

- Difficult to Manage (renewal of certificate is a challenge)
- Requires endpoint configuration (e.g. driver installation for USB based PKI devices) in some cases
- Roaming PKI often fall back to the same weakness of being protected by Password / OTP schemes

Zero Setup Effort – broad support via WebAuthn / CTAP

- Biometrics

- Often exploits False Positives and use of AI methods (e.g. DeepFake)

External authenticator needs to be obtained first with on device secure biometrics

Our FIDO Offering



DIGIPASS® FX1 BIO



fido™
CERTIFIED



Phishing-resistant

- Public key cryptography – legitimate site



Biometric protected

- Protect your secret key with on-board fingerprint scanner



Ease of use

- Single key provides secure access to + 1,000 services and apps



Physical security

- Reduce attack surface with dedicated hardware key



Zero footprint

- No drivers or software installation required



Multi-platform support

- Plug and authenticate on desktop, laptop, tablet, or mobile
- Connectivity options: USB-C, Bluetooth, NFC

DIGIPASS[®] FX7



fido[™]
CERTIFIED



Phishing-resistant

- Public key cryptography – legitimate site



Tap to authenticate

- Verify user presence with a simple click



Ease of use

- Single key provides secure access to + 1,000 services and apps



Physical security

- Reduce attack surface with dedicated hardware key



Zero footprint

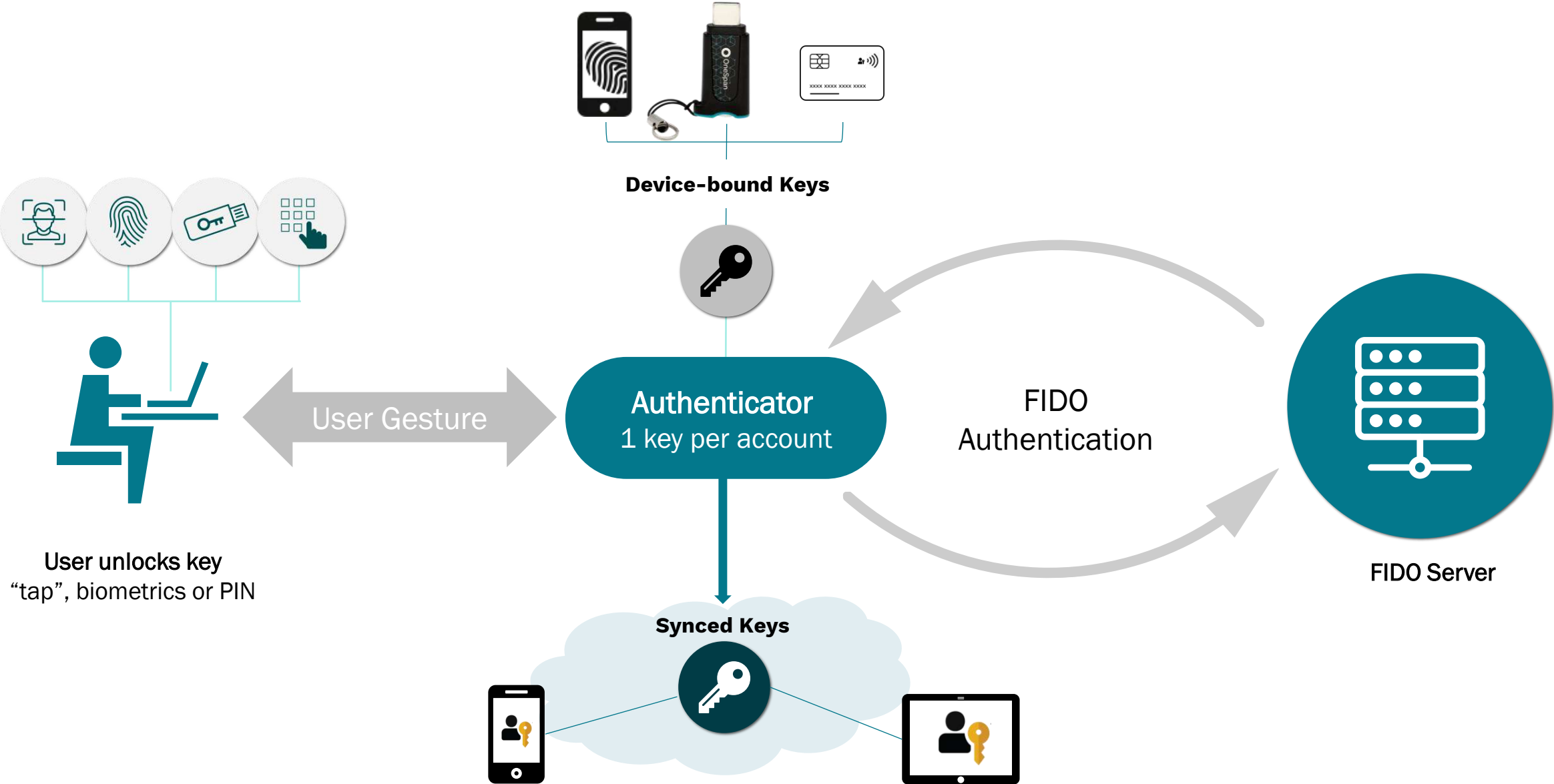
- No drivers or software installation required



Multi-platform support

- Plug and authenticate on desktop, laptop, tablet, or mobile with USB-C

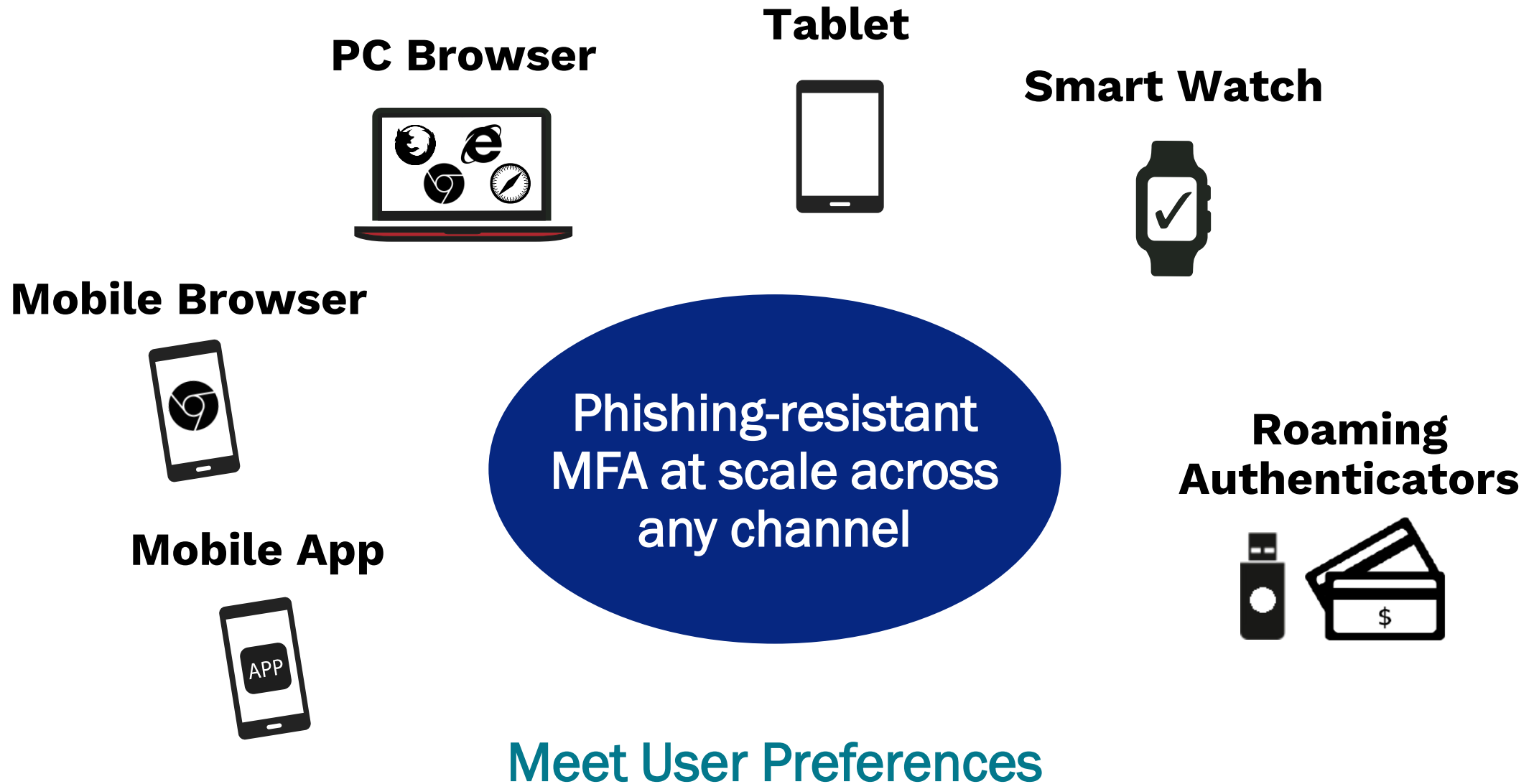
FIDO Authentication



***But
Modern Authentication
needs to be
Operationalized
and
Scale***



Leader in Passwordless Transformation



FIDO is open standard, why OneSpan?

- **FIDO considered strategic** – need thought-leader partner with deep domain expertise
- **Complex backend** – need open APIs, easy integration, flexibility
- **Many use cases** – need comprehensive capabilities across any platform
- **Complex workflows** – need adaptive policies
- **Large user base** – need scale



Looking into the Future for Authentication

Market Drivers for FIDO2 Authentication – Are these in your checklist?



Prevent social engineering
with phishing-resistant
authentication



Safeguard corporate data/apps
against attacks



Drive better user
experience with frictionless
authentication



Maintain cost efficient and
standardize solution



Single authentication option
(convergence of authentication token)



Simplify system deployment
without rip-and-replace

Key Properties of Future Authentication

Phishing Resistance

- Prevent user from providing credentials that can be phished by fraudsters or malicious sites.
- Implementation: direct submission of OTP from mobile to server (no displaying of OTP) or use FIDO authentication protocol

Passwordless Authentication

- Remove password from authentication. Password has a long list of issues that can be exploited easily by fraudster.
- Implementation: replace password (what you know) with biometric (who you are).

Proximity Check

- Ensure authenticator (and therefore user) is in front of application that needs authentication.
- Implementation: design authentication protocol that requires “connection” between authentication and application.

Transaction Signature

- Protect integrity and authenticity of high-risk (financial) transactions, after user has logged in.
- Implementation: signature generated on transaction data (e.g. beneficiary account, transfer amount).

WYSIWYS Signature

- Allow user to see and understand the meaning of the transaction being authorized
- Implementation: display transaction data on **trustworthy** display of authenticator

Application Protection

- Protect mobile authenticator against runtime app attacks or compromised operating environment.
- Implementation: protect mobile authentication with app shielding.



OneSpan Authentication Family

	SMS OTP	Hardware OTP & TDS	Software OTP & TDS	Push OTP & TDS	Hardware CRONTO	Software CRONTO	Software FIDO (UAF)	Hardware FIDO2	Hardware VISION
Use Case	OTP sent via SMS or Email	OTP displayed on Hard Token	OTP displayed on Soft Token	OTP triggered via Push Notification and sent <u>transparently</u> to bank	OTP displayed via scanning of CRONTO code	OTP displayed via scanning of CRONTO and sent to bank <u>transparently</u>	Credential generated via signing of challenge using UAF protocol	Credential generated via signing of challenge using FIDO2 protocol	Combine benefits of Hardware FIDO2 and Hardware CRONTO
Product Name	Virtual Digipass	Digipass 260/270/275	Mobile Security Suite	Mobile Security Suite	Digipass 770/772	Mobile Security Suite	Mobile Security Suite	Digipass FX1/FX7	Digipass FX2
Crypto Algo	Symmetric Key	Symmetric Key	Symmetric Key	Symmetric Key	Symmetric Key	Symmetric Key	Asymmetric Key	Asymmetric Key	Asymmetric + Symmetric Key
Phishing Resistant?	No	No	No	Yes (Phishing Resistant)	Yes (Phishing Resistant)	Yes (Phishing Resistant)	Yes (Phishing Resistant)	Yes (Phishing Resistant)	Yes (Phishing Resistant)
Malware Resistant?	No	Industry is moving towards CRONTO or FIDO solutions						Yes	Yes
Transaction Protection?	No	Yes (Transaction Signing)	No	Yes (Transaction Signing)	Yes (via WYSIWYS)	Yes (via WYSIWYS)	No	No	Yes (via WYSIWYS)
Proximity Based?	No	No	No	No	No (via quishing)	No (via quishing)	No	Yes	Yes (via FIDO2)
Remarks	1. Weakest solution 2. Most regulators already advised banks to move away from SMS OTP years ago.	1. Include both OTP and TDS 2. Mostly used in Corporate banking today	1. Widely adapted in Retail banking today 2. Require app shielding 3. Singapore banks will not display OTP on app	1. Widely adapted in Retail banking today 2. Require app shielding	1. Widely used in European Banks to reduce OTP phishing	1. Widely used in European Banks to reduce OTP phishing	1. Early Banks adopting FIDO will probably continue using UAF	1. Singapore Banks will deploy such phishing resistant token toward end 2025	1. Include best benefits from FIDO2 and CRONTO

OneSpan Mobile Authentication + Security Solution

Mobile Authentication

Multi Factor Authentication

Transaction Data Signing

Credential Provisioning

Mobile Threat Detection

Network (VPN, Proxy) Detection*

RAT Detection*

Malware Detection*

Device Identification & Reputation

Device Identification

Device Binding

Device Data Collector

Mobile App/SDK Protection

App Shielding

Code Obfuscation

SDK Protection

Mobile Channel Protection

Secure Channel

API Protection

Mobile Data Protection

Asset Protection

White Box Cryptography

Secure Storage

OneSpan Shielding Portal

OneSpan Threat View Portal *

** Roadmap features to be released in H2 2025*



Thank You! Q&A

Chan Tze Hoong
tzehoong.chan@onespan.com

Company Overview

World leading provider of strong authentication, transaction signature, electronic signature for digital banking security

NASDAQ: OSPN



OneSpan

EXPERIENCE

30+ years of experience in strong authentication, transaction signing, and mobile security

30+

4000+

PROTECT

4000+ customers worldwide secure every login using our hardware/software authenticators .

TRUST

60%+ of the world's largest banks partner with OneSpan to protect digital banking

60%+

100+

GLOBAL

1,000+ banks across 100+ countries work with OneSpan to secure customer journeys

SECURE

300M+ authenticators issued to protect digital identities and online transactions

300M+

Company Overview

World leading provider of strong authentication, transaction signature, electronic signature for digital banking security

NASDAQ: OSPN



OneSpan

EXPERIENCE

30+ years of experience in strong authentication, transaction signing, and mobile security

30+

60%

TRUST

60% of the world's largest banks trust OneSpan to protect their digital and internet banking

GLOBAL

1,000+ banks across 100+ countries work with OneSpan to secure customer journeys

100+

\$B+

PROTECT

Authenticate and Protect transaction worth billion of dollars everyday across the world

SECURE

300M+/400M+ hardware/software authenticators issued to protect digital identities and online transactions

300/400M+

About MCMC & BlackBerry Cybersecurity Center of Excellence (CCoE)



Located in **Cyberjaya**, the CCoE is a regional hub dedicated to strengthening cybersecurity talent and leadership. The center delivers **hands-on training**, runs initiatives to help everyone enter the cybersecurity industry, and supports the **development of future cybersecurity leaders** through targeted programs and strategic collaborations.

It aims to **strengthen national cyber capabilities** through capacity building programs and strategic partnerships tailored for both public and private sectors.

Complimentary class for eligible civil servants

Courses range:

Beginner (i.e. Cybersecurity awareness, Intro to Cybersecurity, etc.)

Intermediate (i.e. Mobile Security Intermediate, IAM Intermediate, etc.)

Advanced (i.e. Role-based training - SOC Analyst, Incident Responder, Penetration Tester, etc.)

Executive (i.e. Certification course – ISC2 CISSP, EC-Council CCISO, etc.)

Training method – Classroom, Online Instructor-led, Self-learning



Upcoming Mobile & IAM Course



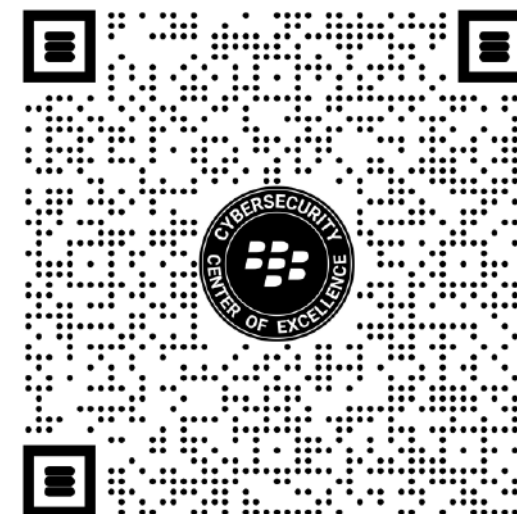
AUGUST 2025

Introduction to Mobile Security	6 th Aug (Classroom) 19 th Aug (Online)
Mobile Security Intermediate	7 th – 8 th Aug (Classroom)
Introduction to Identity & Access Management (IAM)	12 th Aug (Classroom) 20 th Aug (Online)
IAM Intermediate	13 th – 14 th Aug (Classroom)

SEPTEMBER 2025

Introduction to Mobile Security	9 th Sep (Classroom) 30 th Sep (Online)
Mobile Security Intermediate	10 th – 11 th Sep (Classroom)
Introduction to Identity & Access Management (IAM)	4 th Sep (Online) 22 nd Sep (Classroom)
IAM Intermediate	23 rd – 24 th Sep (Classroom)

Scan QR code to register now



Thank You! Q&A

Chan Tze Hoong
tzehoong.chan@onespan.com