IDENTITY DAYS

La (R)évolution des Passkeys

Pedro Martinez - THALES

IDENTITY DAYS

AGENDA DE LA CONFÉRENCE

Pedro MARTINEZ

THALES
Building a future we can all trust

Business Owner CIAM B2C
Thales DIS

- 25 years working on Identity Management and Authentication, across functions, regions and verticals

- Member of the Board of the FIDO Alliance

- Intro

- Passkeys

- La clé de leur success

- UX

- Types de Passkeys

- Offre Thales

- Conclusion

IDENTITY DAYS

Intro: 1 Observation ...

40 ans d´évolution technologique

1980's

2020's

THALES
Building a future we can all trust

40 ans d´évolution technologique

1980's

2020's

40 ans d´évolution technologique

1980's

2020's

IDENTITY DAYS

Intro: ... et 1 petit histoire

FIDO Alliance

Mission: Replace passwords with something better

FIDO HW tokens and FIDO on Mobile Apps

1

2

HW
tokens

Mobile
apps

May 5th 2022: Google /Apple / Microsoft join forces to kill Passwords

Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins

Microsoft   Google   Apple

Faster, easier and more secure sign-ins will be available to consumers across leading devices and platforms

Mountain View, California, MAY 5, 2022 – In a joint effort to make the web more secure and usable for all, Apple, Google and Microsoft today announced plans to expand support for a common passwordless sign-in standard created by the FIDO Alliance and the World Wide Web Consortium. The new capability will allow websites and apps to offer consistent, secure, and easy passwordless sign-ins to consumers across devices and platforms.

Read the full PR

Where can we store passkeys?

1

HW tokens

2

My Bank's App

fido SDK

Mobile apps

3

16 android

Windows Hello | macOS

OS platforms

THALES
Building a future we can all trust

Passkey adoption by the numbers

15 billion *accounts already set for passkeys"* – **Andrew Shikiar, FIDO Alliance Executive Director, Oct 2024**

Passkeys are now available for sign-in on

48%

of the world's top 100 consumer websites

3 billion *accounts already using passkeys* – **Andrew Shikiar, FIDO Alliance Executive Director, Oct 2025**

Passkeys are being deployed by the largest relying parties

Passkeys are being adopted by more and more services every day

Adopted even by highly regulated markets, like Finance

Passkeys

What are passkeys?

Passkeys are cryptographic credentials for authentication of users to digital services, following specifications of the FIDO Alliance

THALES
Building a future we can all trust

FIDO protocol: Authentication in 2 steps

User Experience

Under the Hood Security

STEP 1: User – Device

User authenticates locally using device biometrics (or PIN)

User

User´s Authenticator Device

STEP 2: Device – Backend

Cryptographic exchange following FIDO protocol

Service Provider's Authentication server
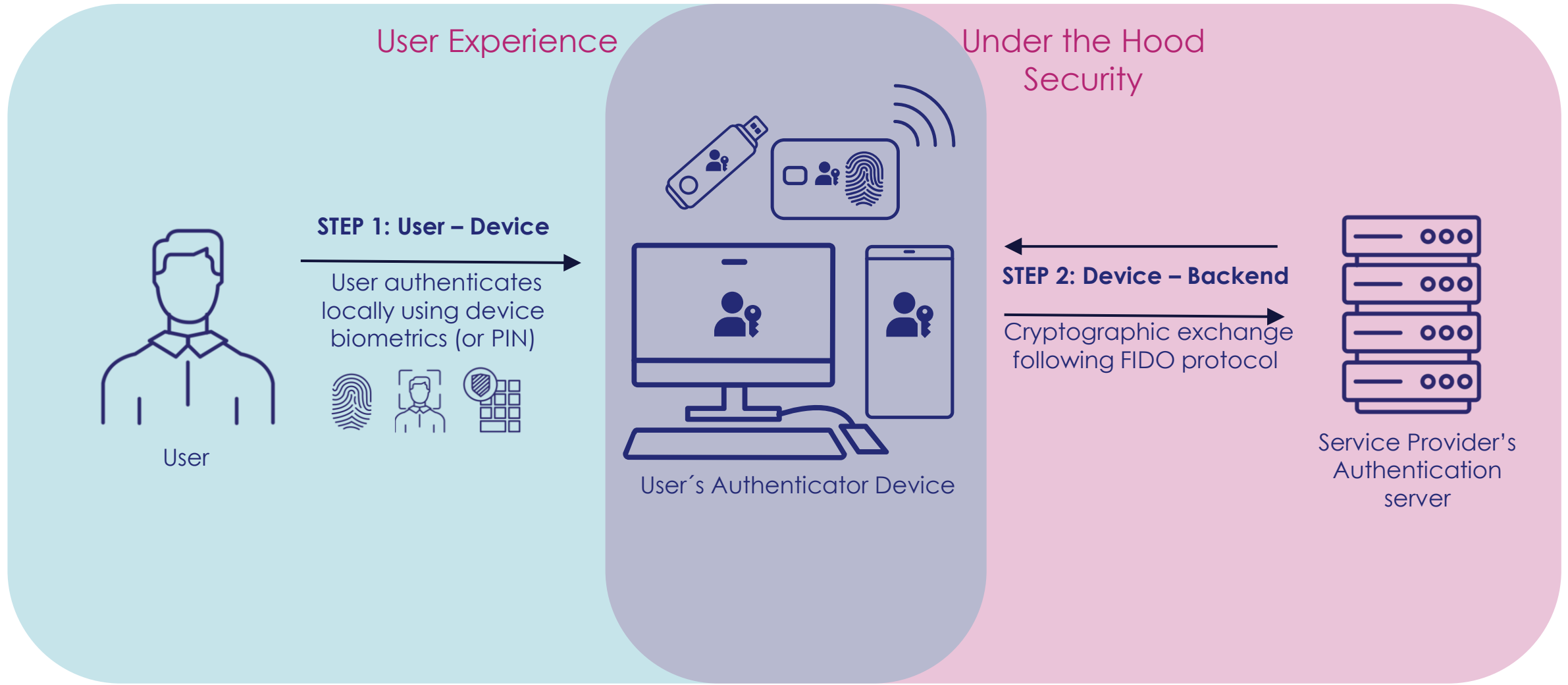
FIDO protocol: Creation of a passkey

Passkey creation:
After successful biometric verification, the passkey is created on the device
A Passkey is a cryptographic credential that binds a user with a service. It consists of 2 keys: public and private.
The private key remains on the device, whereas the public key is sent to be stored on the FIDO Authentication Server

User´s device

Authentication server

Private Key

Public Key
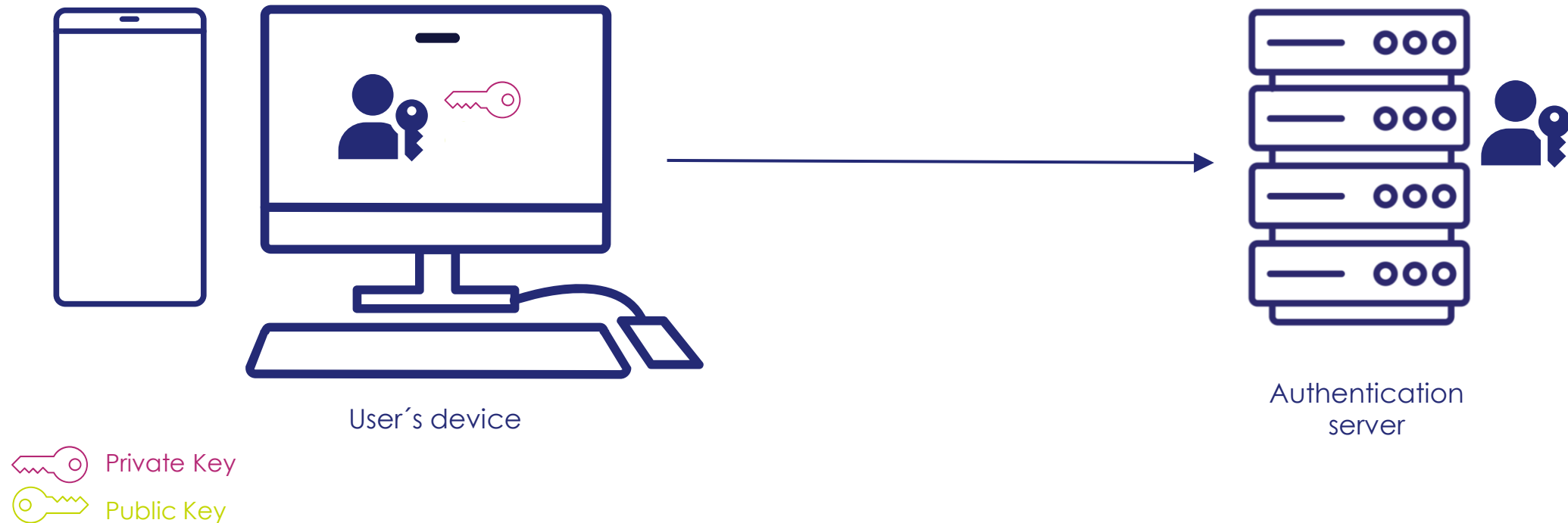
FIDO protocol: Authentication with a passkey

Passkey Authentication:

After successful biometric verification, the authentication server sends a random challenge to the device.
The device generates a cryptographic signature to the challenge with the private key of the passkey
and sends it back to the authentication server.
The Authentication server verifies the response from the device using the public key, and delivers an OK/NOK response
to the authentication attempt

Challenge

Response (Challenge, 🔑)

Auth OK / NOK

User´s device

Service Provider's
Authentication
server

🔑 Private Key

🔑 Public Key
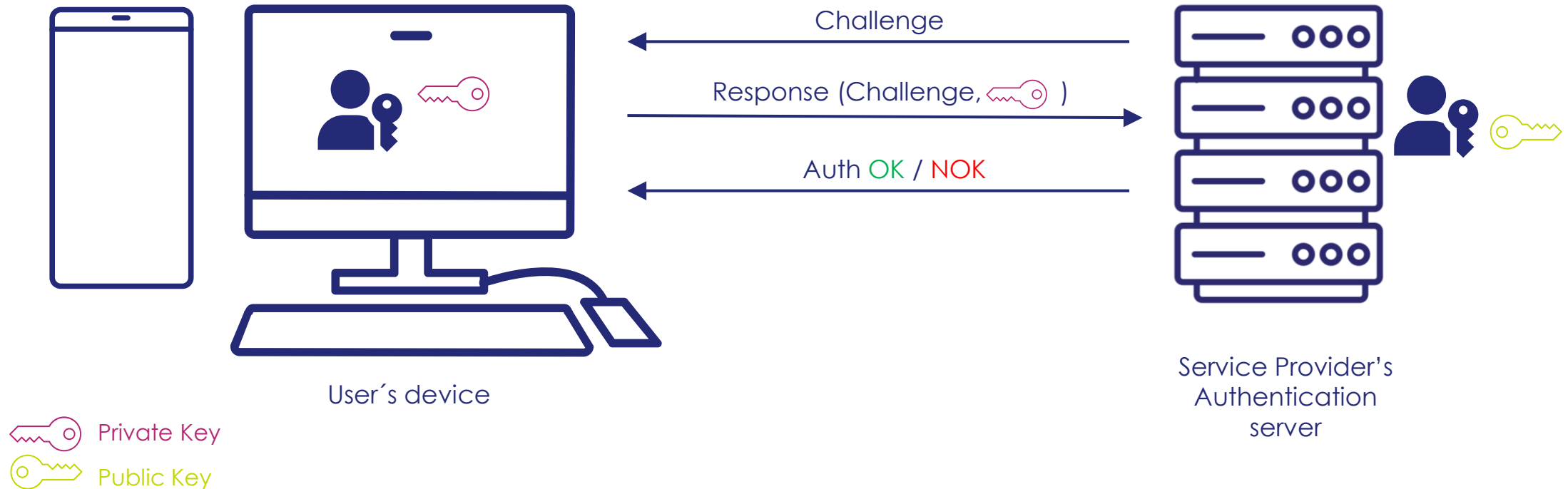
The many benefits of passkeys

UX

> **Biometrics** vs typing

> **Nothing to remember**, renew, reset, re-enrol

Security

> Passkeys are **immune to**:

Phishing

Data leaks

ROI

> **More user engagement**
  - Faster logins, Higher success rate, less abandonment

> **Less Costs**
  - **20-50%** of all helpdesk calls are for password reset*
  - **$70** is the average cost of a password reset helpdesk call**

*Source: Gartner
**Source: Forrester

THALES
Building a future we can all trust

All main mobile and computer platforms and browsers already support passkeys natively

ON EVERY PLATFORM

98%+

of mobile devices

16

android

Windows Hello

macOS

THROUGH EVERY MAJOR WEB BROWSER

96%+

of active browsers

All trademarks, logos and brand names are the property of their respective owners.

THALES
Building a future we can all trust

No one looks back after switching to Passkeys

Microsoft

- 99% completion rate for passkey enrollment
- 98% sign-in success rate
- 3x faster sign-ins over passwords
- 9x faster sign-ins over password + MFA

Microsoft

PlayStation

- 24% reduction in sign-in time on web
- 29% of password resets resulted in passkey conversion, removing passwords completely
- 88% of users engaging with passkey content completed the transition and eliminated their passwords

PlayStation®

Mercari

- Sign-in success rate grew from 67.7% (SMS 2FA) to 82.5% – over a 21% improvement
- Authentication time decreased from 17s (SMS 2FA) to 4.4s – nearly 4x faster
- ZERO phishing incidents

mercari

Air New Zealand

- 30% opt-in in first 24 hours
- 4.7x improvement time to complete & improvement in success rate
- 50% reduction in abandonment rates
- Reduced account recovery calls and call center attacks

AIR NEW ZEALAND

THALES
Building a future we can all trust

Create a passkey
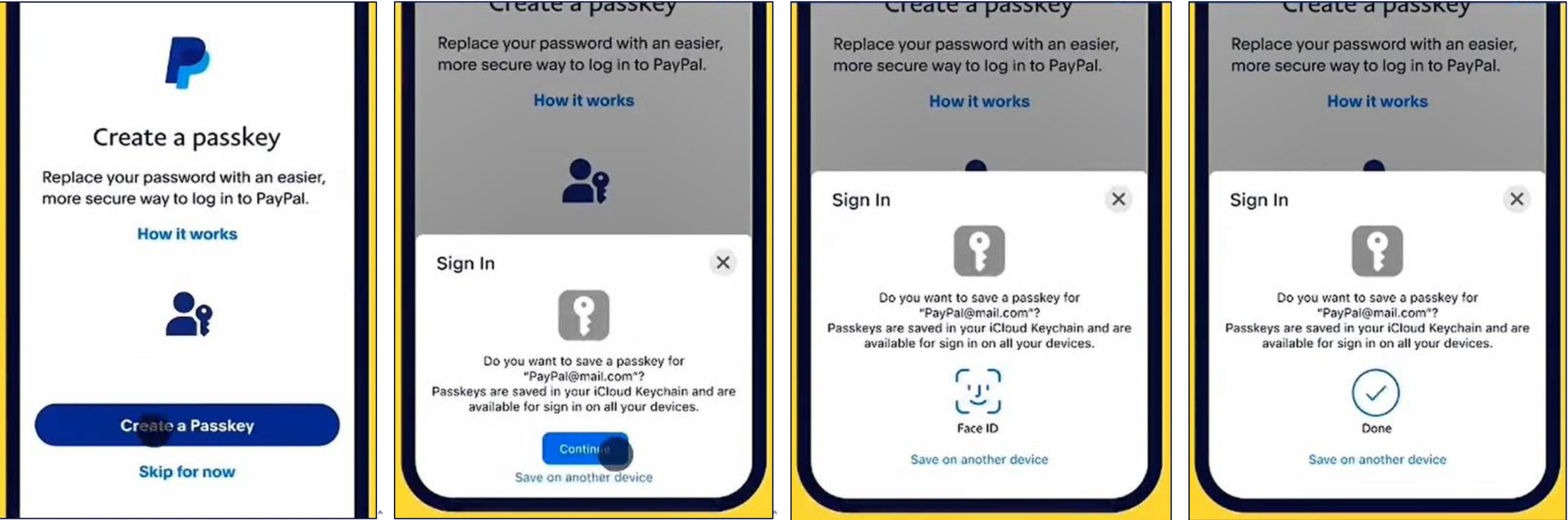
Login with a passkey (iOS)
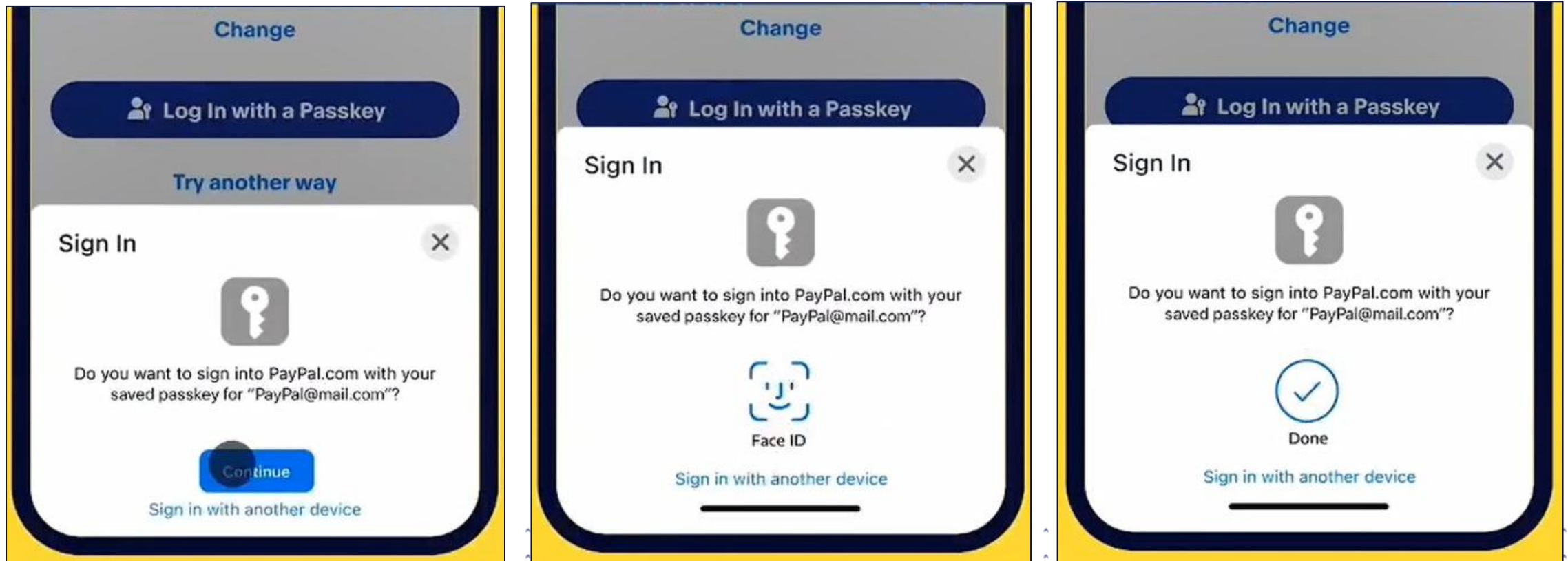
Login with a passkey (Android)

THALES
Building a future we can all trust
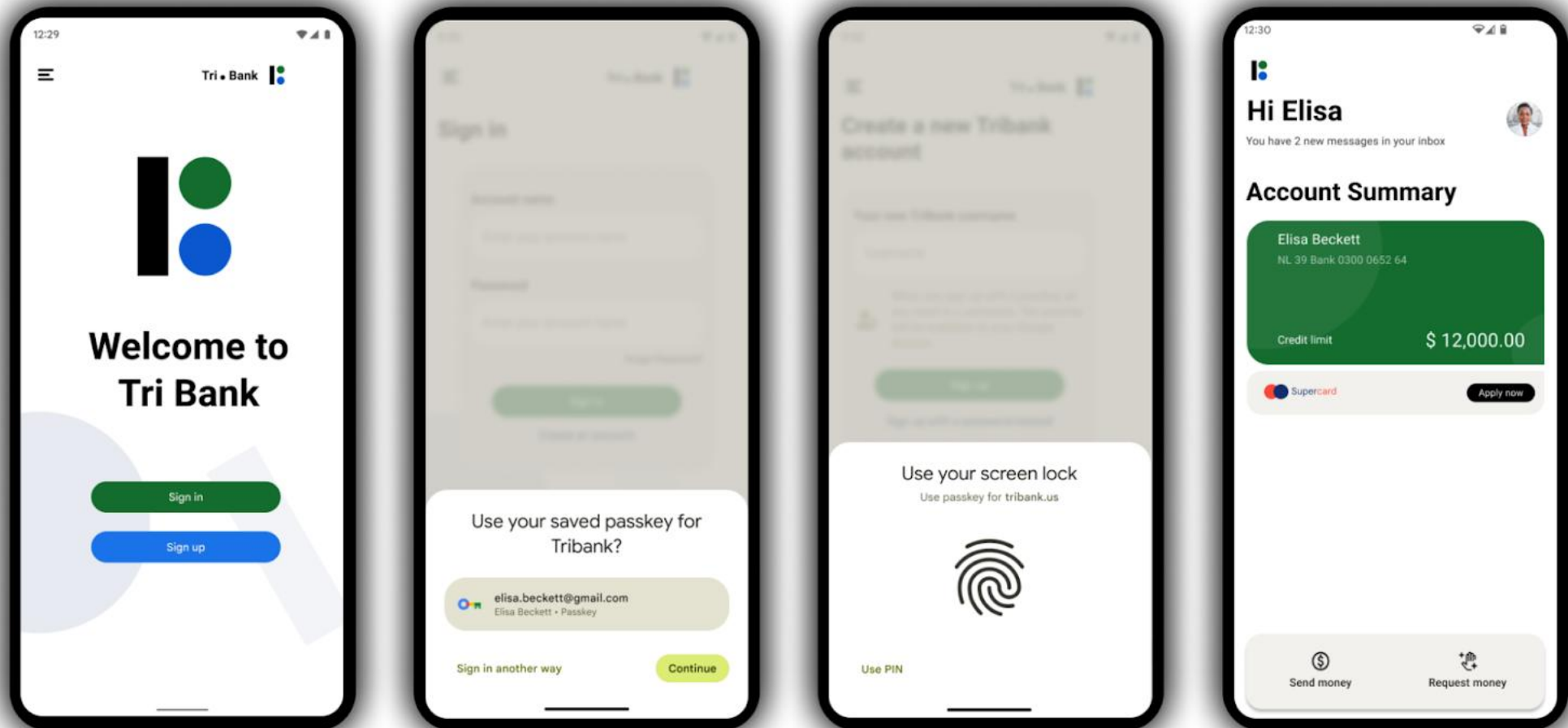
Login with a passkey on a PC or a MacBook

THALES
Building a future we can all trust

IDENTITY DAYS
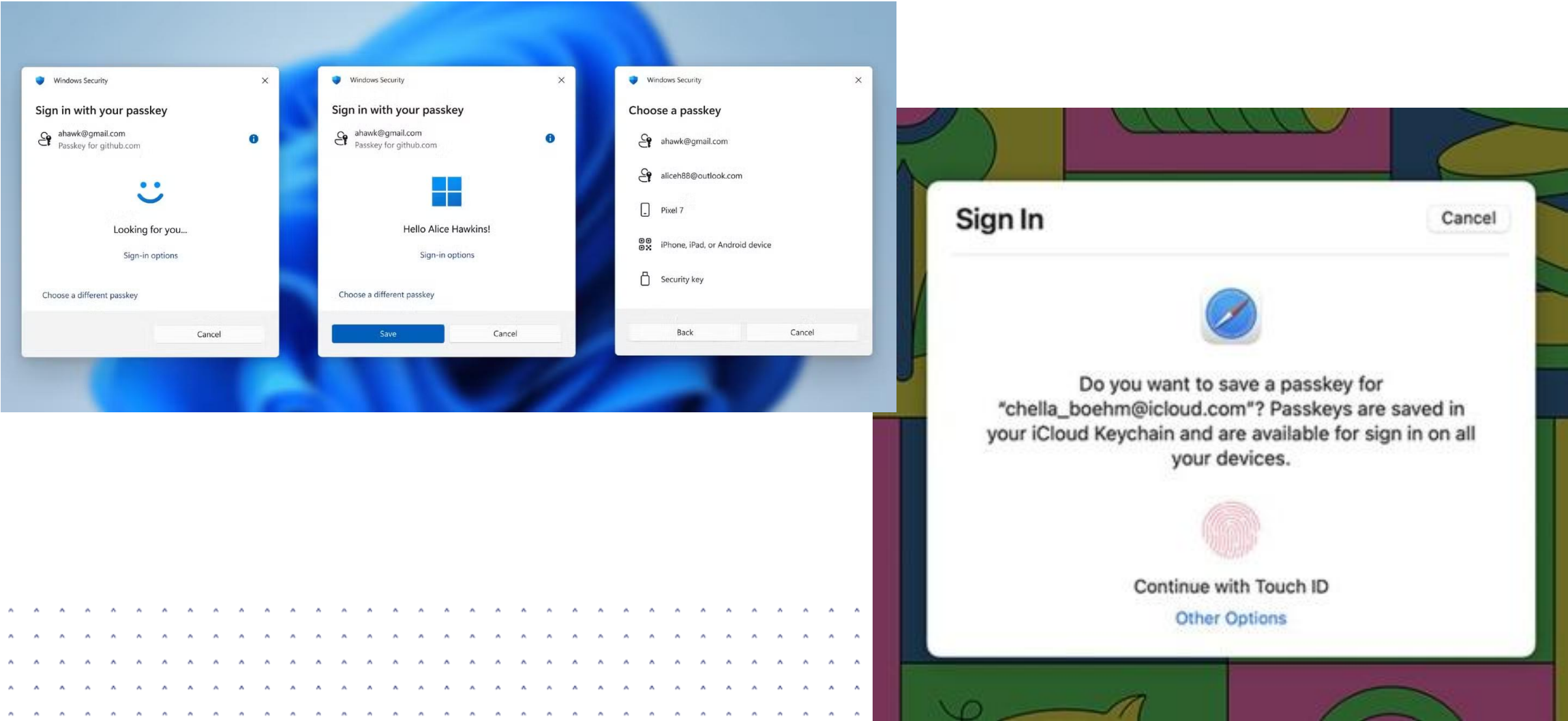
Types de Passkeys

On the client side, passkeys can be managed by:

1
HW tokens

2
Mobile apps

My Bank's App
SDK

3
OS platforms

THALES
Building a future we can all trust
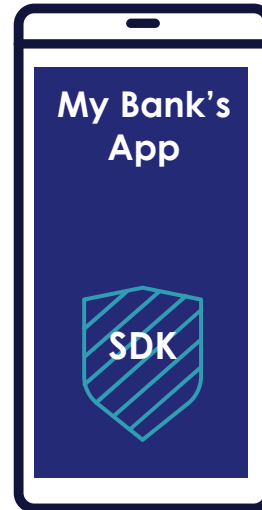
Platform passkeys may "sync" to the platform's cloud
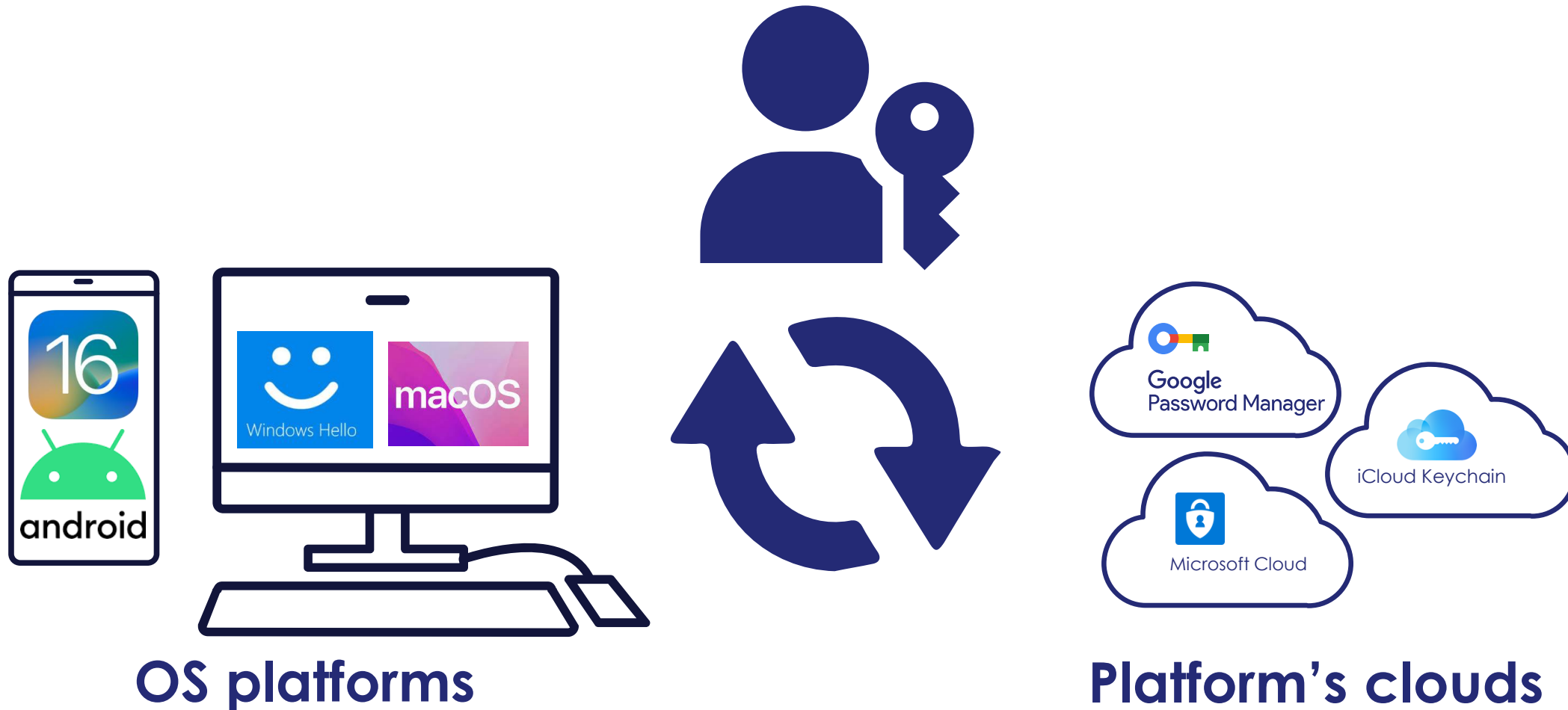
OS platforms

Platform's clouds

THALES
Building a future we can all trust

Synced passkeys (a.k.a. multidevice passkeys)

3. Passkey behaviour
Microsoft/Apple/Google cloud provisions the private key to the other devices of the same user. All devices share the same passkey.

1. Enrolment on first device
Key pair created on device, public key exported to FIDO server

2. Export to cloud
OS exports the private key to the device´s OS cloud

Service provider's
Authentication Server

Google
Password Manager

iCloud Keychain

Microsoft Cloud

Platform's Cloud

Private Key

Public Key

THALES
Building a future we can all trust

2 types of passkeys for 2 different uses

Synced passkeys

Phone — **Managed by the device OS**

Tablet

Desktop

Synced passkeys are exported to the cloud and propagate to other devices

Great for Password Replacement

Device-bound passkeys

Hardware FIDO security keys

Managed by the Mobile App

The private key never leaves the device

Great for MFA/SCA

THALES
Building a future we can all trust

IDENTITY DAYS

Offre Passkeys de Thales

Thales offer for Passkeys

SECURITY

CONSUMER | WORKFORCE

SCA MFA

Device-bound passkeys

FIDO HW Tokens

IDPrime Fido · fido ALLIANCE · NFC))) · THALES

Thales FIDO2 SDK for Mobile Apps

My Bank's App · fido SDK

Password replacement

Synced passkeys

Native FIDO on PC & Mobile OS Platforms

android · Windows Hello · Ventura

Authentication server

fido CERTIFIED FIDO2

THALES
Building a future we can all trust
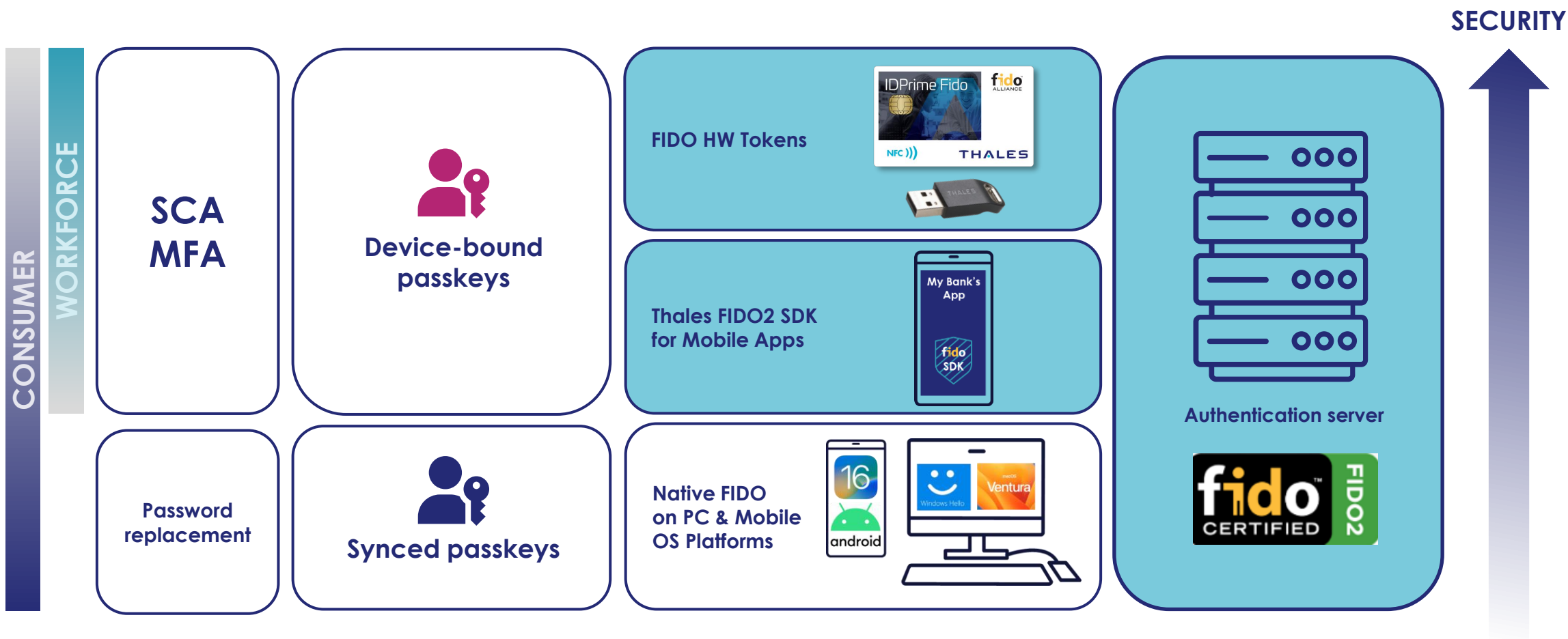
Introducing Device-Bound Platform Passkeys

IDENTITY DAYS
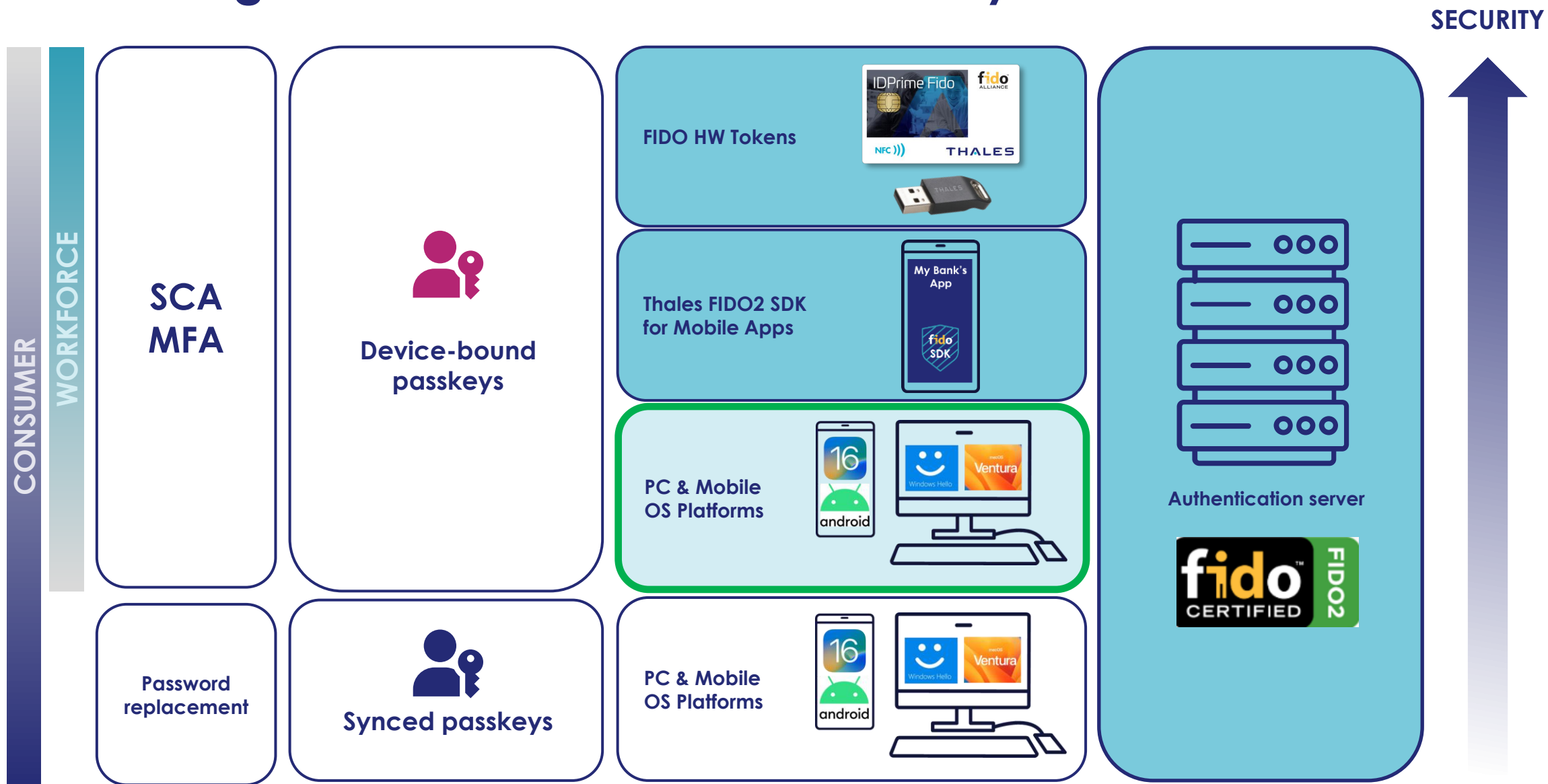
Conclusion

Takeaway

1

PASSWORDS → PASSKEYS

> **Passkeys are inevitable.**
  They will replace passwords for B2C, at last. And Fast.

2

You need FIDO Authentication in your back-end

> Thaales offers FIDO Authentication onprem or as a cloud service

> For low assurance (login) and for Strong Customer Authentication (SCA)

3

We can help you

> To manage transition from passwords to passkeys for consumer log in

> To manage transition from your legacy SCA to FIDO/passkeys based SCA

42

IDENTITY DAYS

@IdentityDays
#identitydays2025