thalesgroup.com

THALES

Building a future we can all trust

FIDO PASSKEYS

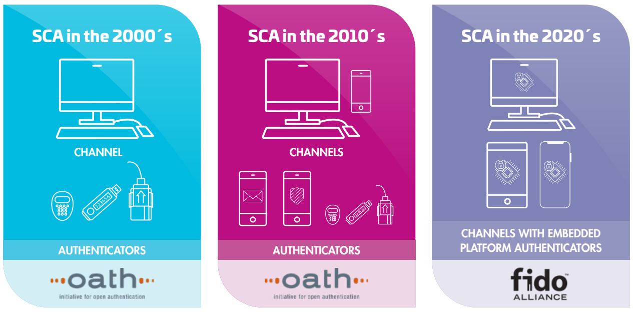
for financial institutions

WHAT DO FIDO PASSKEYS MEAN FOR **FINANCIAL INSTITUTIONS?**

SAY GOODBYE TO PASSWORDS…AND HELLO TO PASSKEYS

Over the past 30 years, authentication for digital banking services has evolved, from basic user ID plus passwords to various multi-factor authentication methods using hardware tokens, SMS OTP, dedicated authenticator apps and embedding authenticators in mobile banking apps. The goal has always been to achieve the best balance between security and user experience. But despite all the progress, one thing remains unchanged: everyone continues to depend on passwords, no matter how much end users and financial institutions dislike them. Until now.

Evolution of Strong Customer Authentication (SCA)



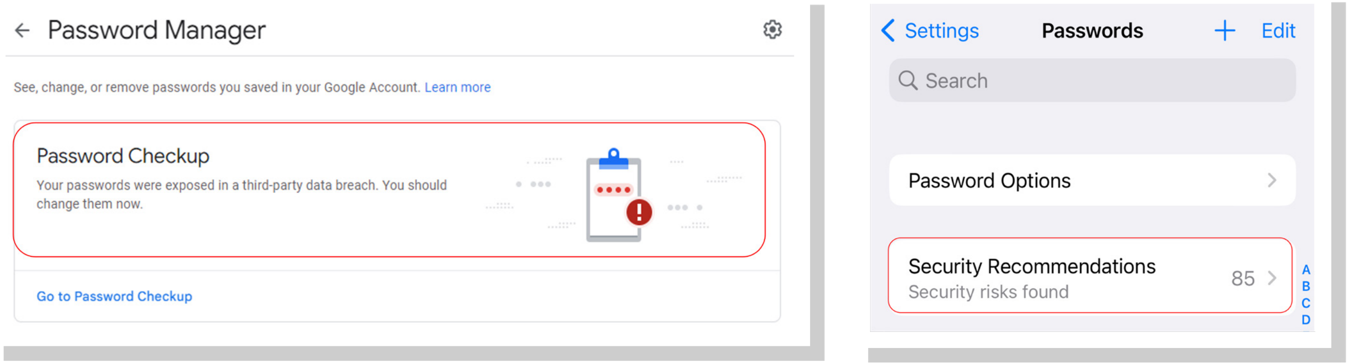
Passkeys have now arrived, on a mission to end with passwords for good and to completely rock the digital world. In this leaflet we will explain what they are, what impact they will have, and what financial institutions (FIs) should consider before implementing them.

THE ISSUE WITH PASSWORDS

Passwords have been around since the dawn of internet, but using them is problematic. The average user has more than 100 passwords to keep track of[1]. Meaning we tend to make them too easy to guess, we reuse them multiple times, and yet we forget them. Or we simply write them down somewhere. It's no wonder that they are an open door for fraud attacks and that password reset is the number one customer care incident.

Password phishing - where a user is socially engineered into revealing their password to a fraudster – is behind most Account Takeover attacks. But there is also a constant flood of data breaches, in which stolen user credentials are sold on the dark web, making passwords highly vulnerable. Thales' Digital Trust Index shows that one in three consumers globally has already been a victim of a data breach[2].

In short, passwords are not user friendly, they are unsafe and very costly!



Password Manager

See, change, or remove passwords you saved in your Google Account. Learn more

Password Checkup

Your passwords were exposed in a third-party data breach. You should change them now.

Go to Password Checkup

Settings Passwords + Edit

Search

Password Options

Security Recommendations 85
Security risks found

Passwords are frequently exposed in data leaks, which is a huge security risk.

PASSKEYS WILL CHANGE EVERYTHING

Passkeys are cryptographic credentials for authentication, designed using FIDO Alliance specifications. The FIDO Alliance cross-industry coalition was set up in 2013 with one clear objective: to define and deploy a simpler and more secure alternative to passwords for user authentication. It has gathered influential companies worldwide to develop open, interoperable authentication standards and implement the technology in their respective products.

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

fido ALLIANCE

Passkeys will put an end to the use of passwords. This is inevitable, for three main reasons:

#1 – THEY ARE GREAT

UX

- Use biometrics instead of typing
- Nothing to remember, reset, renew or re-enroll

Security

- Immune to phishing and data leaks

Cost savings

- Helpdesk
  - Up to 50% of all helpdesk calls are for password reset[3]
  - €65 is the average cost of a password reset helpdesk call[4]
- No HSM required

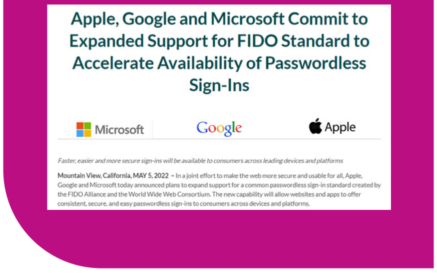
#2 – INDUSTRY IS COMMITTED

FIDO Alliance

- 40+ board member companies
- 300+ companies in total
- Global coverage

The giants are onboard

- Apple, Google, Microsoft
- VISA, Mastercard, Amex
- Facebook, Amazon,
- Intel, Qualcomm, AMD, Samsung,
- Entidades fiancieras



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.

#3 – THEY ARE AVAILABLE EVERYWHERE

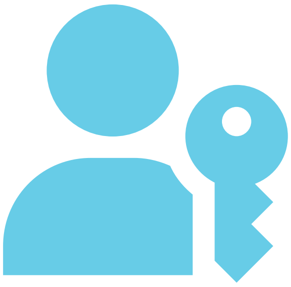
On every platform

16
android
Hello
macOS
Ventura

Through every major web browser

The industry has created a passkey icon aimed at ensuring end users will instantly recognise the technology regardless of the platform or operating system.

Passkey authentication is now being introduced for digital services across multiple industries by a fast-growing list of companies, including Google, PayPal, eBay, Kayak, Best Buy (US) and Boursorama Banque (Fr). Passkeys have been designed with user experience in mind, and it's clear that they will make daily life easier for everyone. This means that **a future without passwords is finally within sight!**



The official passkeys icon

WILL PASSKEYS MEET THE NEEDS OF FINANCIAL INSTITUTIONS?

Passkeys are undoubtedly more secure than traditional passwords. But do they meet the needs of the banking world and are they compliant with strict financial regulations, such as PSD2 in Europe?

SECURITY?

- Relies on cloud security of Apple / Google / Microsoft

! Not under FI's control

COMPLIANCE WITH REGULATIONS?

- Combine 2 authentication factors (biometrics + possession) ✓
- No unique device binding (only ecosystem) ✗

! Not PSD2 compliant

To answer these questions, we must first examine passkey synchronisation. One of the reasons why passkeys will succeed is their ubiquity: Apple, Google and Microsoft have already implemented passkey support in their operating systems, so there is native support for them on (almost) all smartphones and computers. These passkeys have one key feature: they synchronise with their respective clouds and from there they propagate to all other devices associated with the same cloud user account.

As soon as they are created they are uploaded by the device OS to its corresponding cloud (e.g. iCloud keychain or Google credential manager), and from there they propagate to any other device associate to the same user's cloud account. For this reason, we refer to them as **"synced passkeys"**.

Synced passkeys have two main benefits:

1) Users only have to enrol once to get a passkey on all their devices.

2) If their device is lost or stolen, they can easily recover their passkey.

But this puts in question whether synced passkeys – while certainly much more secure than passwords – reach the bar set by most regulations to comply with Strong Customer Authentication (SCA) rules. SCA requires the combination of two independent authentication factors; in the case of passkeys, biometrics and possession of a recognised device. But proof of possession is questionable for synced passkeys, because you can use the passkey you create on one device to access a service from another device. There is no unique user-device binding with synced passkeys, a requirement that certain financial regulations – such as PSD2 in Europe – demand for a solution to be SCA compliant.

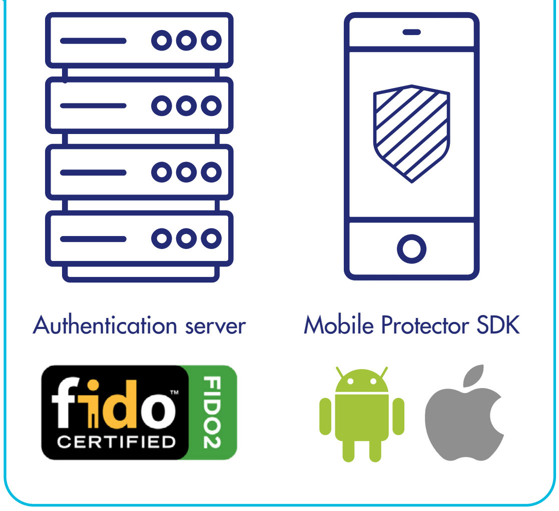
This means that while synced passkeys – the ones managed natively by smartphones, tablets and computers – are a good way of getting rid of passwords, FIs may need something else to comply with SCA. That something else is another type of passkey: a passkey that does not sync to the cloud, but instead remains on the device where it is created, uniquely bound to that single device. This is called a **device-bound passkey**. Besides SCA compliancy, device-bound passkeys have another benefit for financial institutions: they are not managed by the device OS, but by the FI's own mobile app, hence the FI retains full control of the passkey and no third parties are involved.

	Synced passkeys	**Device-bound passkeys**
GREAT FOR	**Password replacement**	**SCA**
MANAGED BY	Device OS	Mobile app
PRIVATE KEY	Uploaded to cloud	Never leaves device
DEVICE BINDING	No	Yes
PSD2 COMPLIANCE	No	Yes

HOW TO TRANSITION TO PASSKEYS

End users are already being exposed to passkeys from various digital services and they will expect the same frictionless experience when they want to access digital banking. They will have the added peace of mind of knowing that their passkey cannot be guessed, phished or compromised by a massive data leak. FIs will want to adopt passkeys as well, not only to please users but also to reduce customer care costs and fraud risks. However, authentication is a critical functionality used by the entire user base, and FIs will need to be assured of a smooth transition from their current authentication solution, with no disruption for their end users.

Gemalto IdCloud for FIDO passkeys



Our Gemalto IdCloud platform supports authentication based on OATH OTP (today's mainstream SCA technology) and FIDO for passkeys. We support synced passkeys for password replacement, as well as device-bound passkeys for SCA, thanks to our FIDO SDK that you can embed into your mobile apps. Furthermore, at Thales we have extensive experience helping FIs to transition from legacy authentication solutions while ensuring compliance with standards and regulations and enabling them to achieve high level service security.

We recommend introducing passkeys in two steps.

First, connect to Gemalto IdCloud's FIDO authentication server to enable login to digital banking services with synced passkeys as replacement for passwords. This can coexist with your current SCA solution.

Second, let Gemalto IdCloud handle SCA as well, upgrading your mobile app with FIDO mobile SDK and enabling you to discontinue your legacy authentication solution to optimise costs. This migration can be done without any friction for end users. We know how to do it.

WANT TO KNOW MORE?

Book a meeting and let us show you the best way to implement passkeys.

FIDO® is a trademark (registered in numerous countries) of FIDO Alliance, Inc. The passkey icon is a trademark of FIDO Alliance, Inc.

Sources:
[1] nordpass.com [2] Thales Consumer Digital Trust Index [3] Gartner [4] Forrester

THALES

Building a future we can all trust

> Thalesgroup.com <