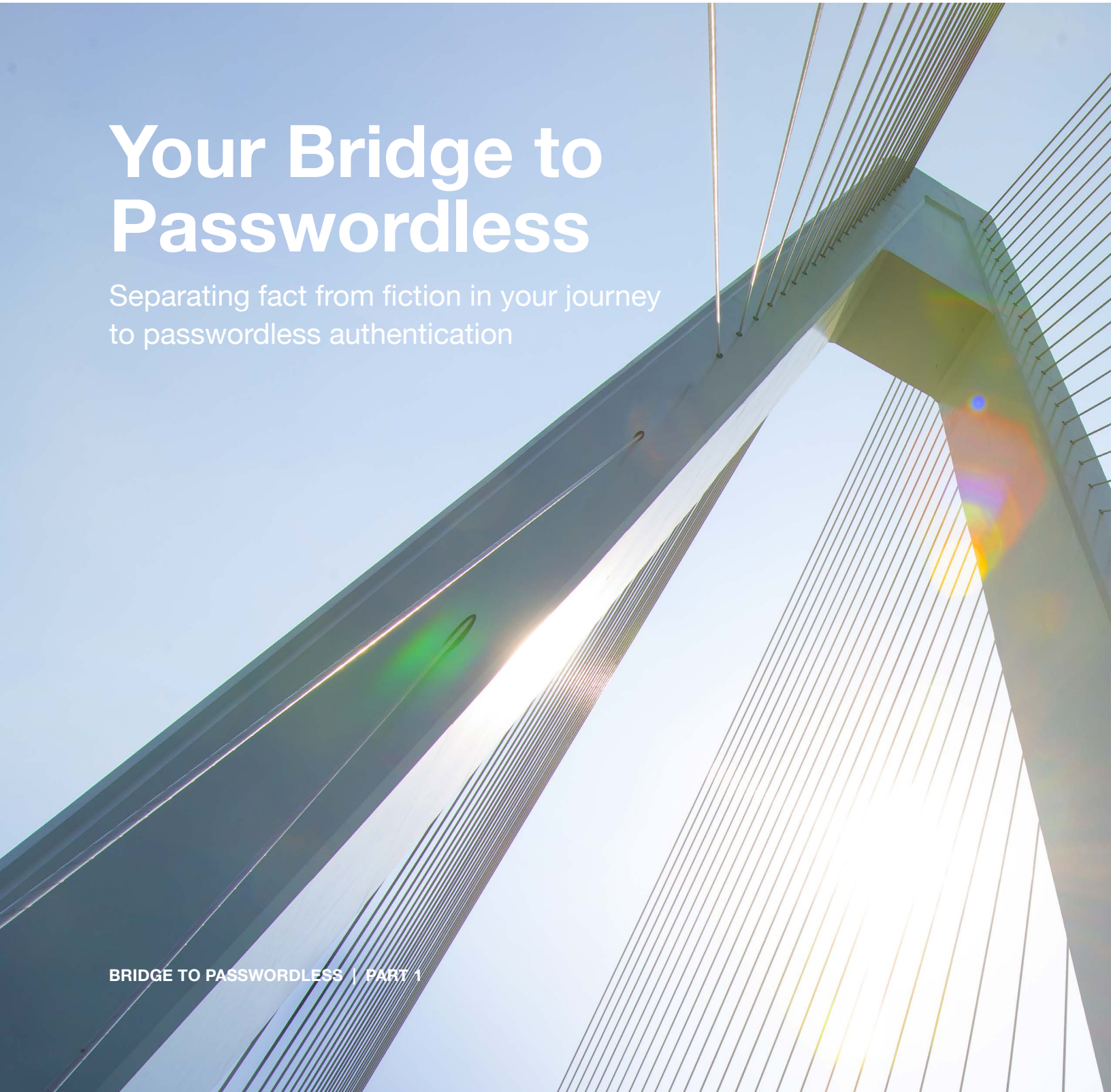
yubico



# Your Bridge to Passwordless

Separating fact from fiction in your journey to passwordless authentication

BRIDGE TO PASSWORDLESS | PART 1

# Executive Summary

Say the word “passwordless” to a room full of security professionals and you will get a range of reactions, from a wry smile to a walk-out. That’s because the information security community knows that “passwordless” is a loaded term, and the industry is filled with differing and contradictory positions on the topic.

The purpose of this whitepaper is to take an objective approach to understanding the challenges that passwords present, what “passwordless” means, and what enterprises can expect moving forward as passwordless authentication matures. However, you can’t have a conversation about passwordless until you first have a conversation about passwords.

## The password paradox

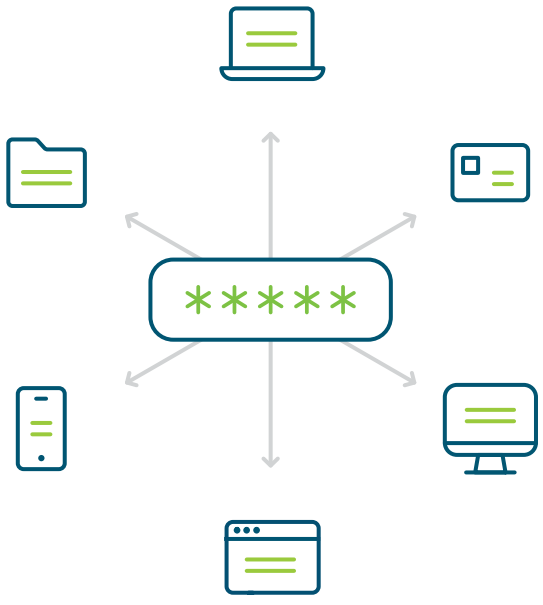
Passwords are the most common form of user authentication, and they should be taken with a grain of salt because, while easy to create, they offer weak security and a poor user experience.

By definition, a password is a shared secret. The secret is known by the user and the validation service, is often stored across various computing devices, and may even be shared in messages or on a sticky note. Each service, device, or user with knowledge of that secret can be the target of a cyber attack.

To improve security, best practice commonly dictates that passwords be **unique** and **complex.** However, these practices are increasingly ineffective against modern phishing attacks and make passwords more difficult to use. To avoid "forgot password" flows, it becomes tempting to share passwords across services (which, again, increases security risks).

Security and usability are at odds with passwords. Better security leads to a worse user experience, and vice versa.

So time to say goodbye to passwords, right? Not so fast.




There is a lot to like about passwords. Let's not throw the baby out with the bath water. While passwords may offer poor security and usability, they are still widely used for several reasons:

- **Portability:**
  A password or shared secret can be applied to almost anything — access to devices, documents, accounts, services, or even your kid's treehouse. It doesn't require a lot of infrastructure or dependencies to implement this form of authentication, making it really easy to gate access to something.
- **Compatibility:**
  With very few exceptions, every app and service that you use has a password. Sure, it may require an additional second factor to authenticate, but the password is foundational and universal. You never really have to think about whether or not a service is compatible with the concept of a password. Entering passwords is the default activity you do everyday.
- **Interoperability:**
  Whether you're authenticating on a computer, smartphone, Nintendo, or Apple TV, you can easily input a password. Passwords are universally supported, and you don't need to upgrade to the latest mobile device or install client software to use a password. They just work.

Why is this important? If the goal is to retire password authentication, any alternative needs to offer significant improvements in both **security** and **usability** without compromising our needs for **portability**, **compatibility**, and **interoperability**. To put these concepts in perspective, let's define the term "passwordless."

## What is passwordless authentication?

Over the past few years, the term "passwordless" has gained momentum and now it is used by many security, authentication, and identity solution providers — each with their own unique nuance.

For clarity, I think it is best to use a broader definition. At Yubico, we have adopted the following:

**"Passwordless authentication is any form of authentication that doesn't require the user to provide a password at login."**

It may seem simple, but there is a bit to unpack here. There are a lot of different implementations of passwordless authentication and they all have tradeoffs.

Some implementations of passwordless are specifically designed to address usability issues:

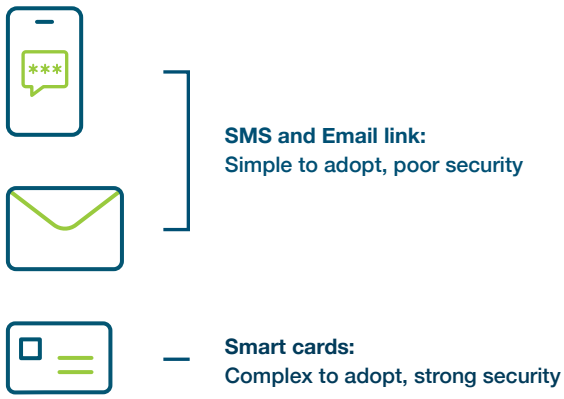
**SMS** – Many refer to SMS verification as passwordless because you don't need to remember a password. Usually you're sent an OTP code that is valid for a short period of time that the user can use to authenticate themselves. (And the irony is that "OTP" stands for "one-time password" — that is the common usage of the term.)

**Email Magic Link** – A unique link with a token is created for a user and delivered to an email. Clicking the link verifies the user for that particular service.

There are variants of using SMS to deliver the magic link but in general these two authentication flows may offer better usability than passwords, but both are highly susceptible to phishing. If the user is tricked into typing in the OTP code or clicking on the magic link, neither of these passwordless solutions offer much security.

Other implementations of passwordless are specifically designed to address security issues:

**Smart Cards (PIV/CAC)** – Smart cards are one of the most effective ways to protect against phishing. The user must insert their smart card into a reader, and validate the smart card with a unique PIN. This is a surefire way to stop remote phishing attacks in their tracks. But traditional smart cards may be somewhat complex for administrators to implement and manage, and involve having a good strategy in place to implement at scale. While the administrative usability leaves room for improvement, the end user usability and security are both top notch and similar to FIDO2, thus may be considered as a component of an enterprise passwordless solution as infrastructure and environments evolve to support newer standards.




Let's take a quick sidebar and talk about passwords and PINs.

## Password vs. PIN

From a usability standpoint, they may seem very similar — something else to remember. But from a security perspective, they are very different. A password is transmitted and validated on a server, which means it can be intercepted or stolen. A PIN is local to the device. For example, when you use your debit card at an ATM, the PIN only unlocks the debit card. It is never transmitted or stored elsewhere. That's why when you have a debit card stolen and are issued a new card, you are required to select a new PIN.

There are a few reasons why this distinction is important.

**A PIN is way more secure than a password. It is local to the device, instead of a password that resides on a server that can be easily breached.**

**Most strong forms of passwordless authentication require a PIN, so you still have to remember something. However, we all use PINs to protect one of our most prized possessions — our money!**

**PINS are short, non-complex, and hardly, if ever, change. Compare that to a password that is not only highly vulnerable, but has to also be changed constantly and to ever more complex forms and longer lengths in order to mitigate risks that continue to evolve and become more sophisticated.**

**Most biometric authenticators use your face or fingerprint to "release" the PIN to perform the operation, and will default to PIN when biometric isn't available (like when you restart your iPhone or try to unlock it if your face isn't properly visible). In other words, the biometric authenticator doesn't actually replace the PIN.**

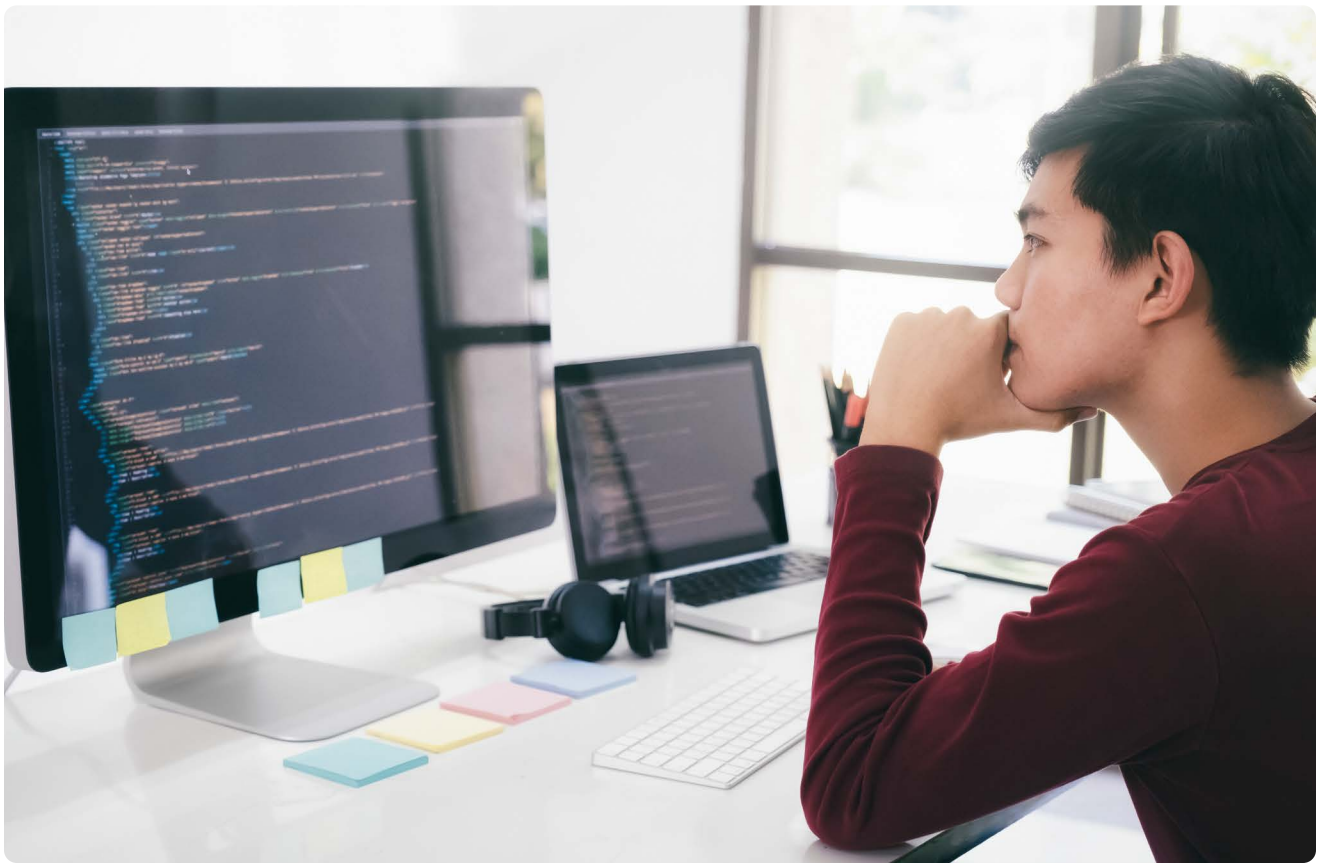
## The role of open standards and identity platforms

Want to have your passwordless cake and eat it too? That's what open standards bring to the party.

It takes a rich open standards ecosystem built to achieve security and usability, while also satisfying the need for portability, compatibility, and interoperability to scale to the masses. Since our inception, Yubico has advocated for open security standards to achieve these goals. Yubico paved the way by pioneering the WebAuthn and FIDO open standards, and worked with tech giants like Google, Microsoft, and Apple to integrate these standards into the operating systems, and browsers we use every day. These standards, paired with a YubiKey, allow for strong authentication across devices, apps, and services without any additional proprietary software. It just works.

Identity and access management (IAM) solutions (e.g. Azure Active Directory, Okta, Duo, Ping) have also embraced open standards by layering on top of the platform giants to deliver the functionality and scale that enterprises need to adopt strong passwordless authentication for business critical applications and services.

If you're already invested in an IAM platform, explore what passwordless options they offer. Most will have a mobile authentication app to augment some of the user experiences on various legacy systems providing an alternative non-WebAuthn/FIDO passwordless experience. While mobile authentication is stronger than a password, mobile authentication apps are phishable, which is why all leading IAM platforms have native support for hardware security keys like the YubiKey.




## The bridge to passwordless

Passwordless is a journey, not an overnight transition. And Yubico is on this journey with you.

This transitory period is what the YubiKey was designed for — to be able to meet you right where you are and evolve with your security infrastructure. YubiKeys don't require client software or peripherals, like a card reader. And we designed the YubiKey to support the broadest set of security protocols, enabling a single device to work across a side range of applications and services, regardless of where those providers are in their passwordless journey.

You can put an end to account takeovers now using the phishing-resistant YubiKey as a second factor on top of a password. And that same YubiKey can be deployed in passwordless environments with our IAM partners as a smart card or a FIDO2 security key. The YubiKey truly is your bridge to passwordless.

Together with the open standards ecosystem and IAM partners, Yubico is excited to deliver security and usability at any scale, without compromise.

www.yubico.com

yubico

## About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.