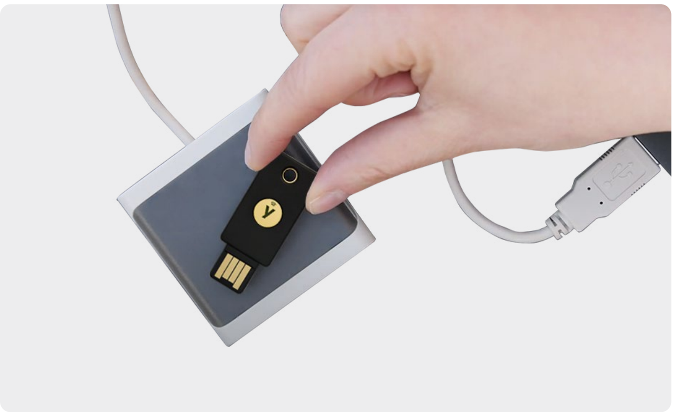
yubico



Smart Cards Simplified

Strong authentication made easy for State and Local agencies and the Private sector

The imperative for trusted smart card security that's easy to use

Access has suddenly become a high-stakes endeavor. With the rise of remote work and cloud computing due to the COVID-19 pandemic, business continuity depends on giving employees seamless access to the data and apps they require. But with cyber attacks rising in frequency, sophistication, and persistence, it's vital to ensure that only authorized users have access—and that their credentials cannot be stolen. It's time to have a conversation about authentication.

Private companies along with state and local governments need a way to authenticate users that's phishing-resistant, passwordless, user-friendly, and (most importantly) always trusted. Productivity and cybersecurity both come down to authentication, and existing solutions are often inadequate.

Smart cards are often held up as the exception. Smart cards can't be phished, like passwords, SMS or mobile authentication can, and are natively supported in the operating system. The positive implication for native support is that there is less friction for IT as leading platforms, such as Microsoft's systems (PCs and Network) support smart cards without any additional software needing to be installed. And, most on-premises applications support smart cards so no additional software needs to be installed in that case as well.

Therefore, two decades of use cases have shown smart cards to be an effective tool for strong authentication. But are they fully suited to the way we work today?

Business scenarios for YubiKeys

When trying to conduct remote provisioning.

When relying more on telework.

When instituting a BYOD policy.

When building extra security around privileged users like IT admins or high-ranking officials.

When future-proofing an agency for tomorrow's stronger security requirements

Not all smart cards are created equal

The truth is, smart cards are a powerful addition to any organization—but some options are far superior to others. The logistics of many legacy and even some modern smart card solutions are where things get tricky:

- All smart cards offer strong security, but they have historically been complex to deploy and manage at scale. More recently, starting or scaling a smart card program has become simplified thanks to solutions like YubiKeys that offer the same (or better) security but with easier implementation for IT and end users both.
- Older smart card infrastructure was not built for remote provisioning—employees had to come into the office to take a picture and get a card set up. YubiKeys on the other hand take the importance of remote work into account so that provisioning can happen from anywhere.
- A laptop, tablet, or phone needs a card reader to authenticate with a smart card, meaning more expensive hardware for IT to purchase and end users to keep track of. Variations such as the YubiKey that plugs into a standard USB port, or can do tap and go authentication using NFC, can interface directly with the vast majority of devices, including BYOD.

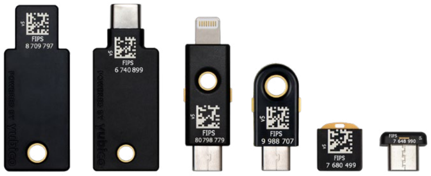
For organizations either without a smart card program, or even an organization who is considering expanding an existing program, implementing a modern, secure and flexible option should be considered. A key criterion might be to explore authentication solutions that can support both smart card/ PIV capabilities as well as modern FIDO authentication protocols, in an all-in-one solution. This provides flexibility to the organization and secures the range of legacy and modern systems as the organization evolves.

With FIDO it is important to note that it can take the security and methodology of smart cards, and make it decentralized, which offers the flexibility for remote management and ease of use at great scale. As an example, Microsoft Azure is allowing smart cards to be used to log in with a certificate-based authority (CBA). This shows that modern cloud platforms are now making it easier to use smart cards in the organizational environment to help enhance the security posture.

YubiKeys - the strong security of smart cards, only more modern and greatly simplified

YubiKeys take the core concept behind smart cards—making access contingent on having a specific possession—and update it for a new era of authentication. Replacing the traditional “card” with something more akin to a USB thumb drive sounds like a minor change, but the benefits are far-reaching.

Ultimately, smart cards are a proven solution uniquely suited to the challenges of authenticating distributed users and stopping evasive threats. And thanks to innovations engineered into the YubiKey, smart cards are as secure as before but simpler than ever.



YubiKey 5 FIPS Series

From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS

YubiKey 5 Series

YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano, YubiKey 5C Nano

Strongest security

YubiKeys enables phishing-resistant MFA with the use of Smart card/PIV or FIDO/WebAuthn authentication protocols. YubiKeys expand on traditional smart card capabilities by adding touch to sign, which validates user presence to prevent remote attacks, and by adding attestation, which verifies that a credential or authenticator can be trusted. With its strong phishing defense capabilities YubiKeys stop account takeovers, prevent ransomware attacks, and satisfy security mandates in the public and private sectors. Secure enough to handle authentication in the most sensitive industries and the highest levels of IT administration, YubiKeys are also practical enough to authenticate ALL employees.

Easy to deploy—even remotely

Issue YubiKeys to remote employees and manage their access controls from a central location. Or provision from a remote location with YubiKey secure channel provisioning. And, with YubiEnterprise Subscription and Delivery services, we even handle the logistics, making it easier than ever to buy, ship, upgrade or replace keys.

No additional hardware

YubiKeys require no additional hardware or software to be used or installed. So you can save on the cost of purchasing additional items such as smart card readers, or special laptops with readers.

Reduced software and management costs

YubiKeys work with the leading Certificate Management Servers (CMS), so organizations can continue to leverage their current CMS investment or migrate to an alternate solution.

Lower IT support burden

Reduce or remove the need for password resets, as well as the high costs associated with password support. Organizations using YubiKeys have been known to reduce support incidents by up to 92%, saving tremendously on IT helpdesk costs, not to mention less user downtime and lost productivity.

Flexible, portable and future-proofed

YubiKeys offer multi-protocol support for FIDO2/WebAuthn, U2F, OTP, and smart card, all able to be used simultaneously for different systems and applications, making them a future-proofed solution suitable for use across modern and legacy environments. Learn how Schneider Electric has secured their global supply chain with YubiKeys.

YubiKeys also support multiple forms of passwordless authentication—so users with complex environments that aren’t fully passwordless-ready today may leverage YubiKeys as a bridge to get there.

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088