eBook

The Comprehensive Guide on Phishing-Resistant MFA, Passkeys and FIDO security keys.

cpl.thalesgroup.com

THALES
Building a future we can all trust

Contents

Attackers Exploit Authentication Vulnerabilities

The acceleration of digital transformation for all industries and sectors, the increased adoption of cloud-based technologies, and hybrid work norms mean that corporate and personal data are increasingly stored in dispersed cloud platforms. This data is also accessed by an expanding number of entities – apps, businesses, individuals, devices, etc.

The cyber battleground has shifted from protecting boundaries to protecting identities. An authentication system is the front door to enterprise networks, applications, and data. As such, attackers are highly focused on finding and exploiting authentication vulnerabilities.

Passwords are not viable

The Verizon 2023 Data Breach Investigations Report[1] indicates that attackers gain access to data by leveraging compromised or stolen credentials (49%) and phishing attacks. The same vectors (i.e., compromised credentials and phishing) are identified as the top two initial attack vectors in the IBM 2023 Cost of Data Breach report[2] . In fact, they are also among the top four costliest attack vectors.

Top Two Initial Attack Vectors for Data Breaches

[1] https://www.verizon.com/business/resources/reports/dbir/
[2] https://www.ibm.com/reports/data-breach

IT security professionals worldwide agree that passwords are obsolete and should be considered a relic of the past. The costs of maintaining passwords outweigh the benefits. Passwords are increasingly predictable and leave users vulnerable to credential theft and compromise. Even the most robust passwords can be phished, so motives to eliminate password-based authentication mechanisms are compelling.

In response, security agencies and national organizations strongly suggest implementing multi-factor authentication (MFA) to better protect digital identities and data. MFA is a fundamental element of a robust access management policy. MFA was created to address the shortcomings of passwords, including the fact that:

- Passwords can be shared with unauthorized users,
- Users can be tricked into giving their passwords to attackers through phishing; and
- Users often use the same or closely related passwords across multiple websites, services, and computer systems.

The US Cybersecurity and Infrastructure Security Agency (CISA) states, "MFA is one of the most important cybersecurity practices to reduce the risk of intrusions—according to industry research, users who enable MFA are up to 99 percent less likely to have an account compromised.[3]"

Costliest Initial Attack Vectors

Source: IBM 2023 Cost of a Data Breach Report

Traditional MFA is not sufficient

However, in the past few years, we have witnessed attacks known as MFA push bombing or MFA fatigue, where criminals managed to bypass MFA protection due to weaknesses in the MFA implementation. It is important to note that not all MFA solutions provide equal protection against authentication attacks, and there are critical implementation details that can impact the security and usability of an MFA deployment.

As cited in the National Institute of Science and Technology (NIST) update on MFA from February 2022 , "All MFA processes using shared secrets are vulnerable to phishing attacks." This includes authentication methods that rely on memorized secrets, SMS-based push notifications, and one-time passwords (OTP).

[3] CISA Alert (AA22-074A), https://www.cisa.gov/uscert/ncas/alerts/aa22-074a
[4] https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_%20Guidelines.pdf

The Requirement for Phishing-Resistant MFA

Considering the prevalence and success of MFA fatigue attacks, governments and security agencies suggest phishing-resistant MFA.

Phishing-resistant MFA is multi-factor authentication immune from attempts to compromise or subvert the authentication process, commonly achieved through phishing attacks such as MFA fatigue. Phishing resistance within an authentication mechanism is achieved by requiring each party to provide proof of their identity and intent through deliberate action.

In response to Presidential Executive Order 14028 for Strengthening the US Cybersecurity, the Office of Management and Budget (OMB) issued a memorandum[5] that mandates all federal agencies use phishing-resistant MFA by the end of Fiscal Year 2024. The memo states that identity is one of the five pillars of zero trust security and that "Agency staff uses enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks."

The European Union Agency for Cybersecurity (ENISA) released the guidelines "Boosting Your Organisation's Cyber Resilience[6], "which include provisions such as protecting all remotely accessible services with multi-factor authentication. Organizations should avoid using SMS and voice calls as authentication methods. Instead, they should consider "deploying phishing-resistant tokens such as smart cards and FIDO2 security keys."

Joint guidance on Identity and Access Management[7] by CISA and the National Security Agency (NSA) mentions, "Some, but not all, MFA solutions also mitigate phishing attacks. Given the prevalence of phishing as an attack vector, phishing resistance should be a key consideration in choosing an MFA solution." Finally, CISA, in two distinct security advisories, "strongly urges system administrators and other high-value targets to implement or plan their migration to phishing-resistant MFA" and that businesses should "enforce phishing-resistant MFA to the greatest extent possible" to harden their environment[8].

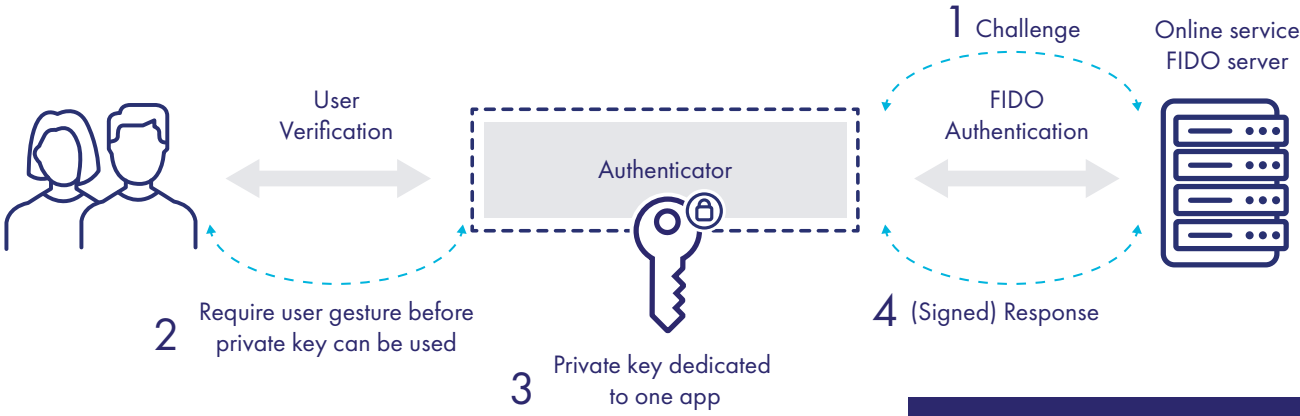
All the above documents indicate FIDO as the golden solution for phishing-resistant MFA.

[5] OMB memorandum M-22-09
[6] ENISA guidelines : "Boosting your Organisation's cyber resilience"
[7] CISA/NSA "Recommended best practices for administrators: identity and access management"
[8] These advisories can be found at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a and https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

What is FIDO2?

The primary purpose of the FIDO2 standard is to address multiple user authentication scenarios and provide a passwordless, multi-factor authentication workflow through cryptographic tokens. A FIDO2 authenticator, or a FIDO security key, embeds one or more private keys, each dedicated to one online account.

The FIDO protocol requires a "user gesture" — a PIN, biometric method, or authentication token — before the private key can be used to sign a response to an authentication challenge.



The steps followed for authenticating a user are shown in the image above and are the following:

1. The online service sends an authentication challenge for users to log in using a previously registered device.
2. The user unlocks the FIDO authenticator using the "gesture" registered previously (Touch, PIN or Biometry).
3. The device uses the user's account identifier to select the correct private key and sign the service's authentication challenge.
4. The device sends the signed challenge back to the online service, which verifies it with the stored public key and logs in the user.

FIDO2 Benefits

Security:

- Unique login credentials across every website, which are never stored on a server, eliminating the risks of phishing, all forms of password theft, and replay attacks

User experience:

- Users login with simple built-in methods on their devices or by leveraging easy-to-use FIDO2 security keys.

Privacy:

- Unique keys for each internet site that cannot be used to track users across sites. Biometric data, when used, never leaves the user's device.

Scalability:

- Enable FIDO2 through simple API calls supported across all leading browsers and platforms.

What are passkeys?

FIDO passkeys were introduced in April 2022. Passkeys are password replacements that provide faster, more accessible, and more secure sign-ins to websites and apps. Unlike passwords, passkeys are resistant to phishing and credential stuffing and are designed so that there are no shared secrets.

From a consumer or end-user perspective, passkeys are a replacement for passwords. From a technical standpoint, passkeys are FIDO credentials discovered by browsers or housed within native applications that enable passwordless authentication. Passkeys replace passwords with cryptographic key pairs for phishing-resistant sign-in security and an improved user experience. The cryptographic keys are used from end-user devices (computers, phones, or FIDO security keys) for user authentication.

There are two types of passkeys:

1. Synced passkeys are managed by phone or computer operating systems and automatically sync between the user's devices via a cloud service. The cloud service also stores an encrypted copy of the FIDO credential.
2. Device-bound or single-device passkeys are available only from a single device from which they cannot be copied. In this case, the cryptographic private key never leaves the device.

Synced Passkeys and MFA

Passkeys are kept on a user's device (something the user "has"). If the online service requests a user verification, passkeys can be exercised by the user with a gesture, such as a biometric or PIN (something the user "is" or "knows"). Thus, authentication with passkeys embodies the core principle of multi-factor security – using two or more distinct authentication factors.

However, many organizations have not recognized synced passkeys as an official MFA method. For example, NIST, under the process of revising SP 800-63-4, Digital Identity Guidelines, is evaluating the implications of two passkey features, syncing across devices belonging to the same user and sharing between users[9].

[9] For more insight, see https://www.nccoe.nist.gov/sites/default/files/2023-01/digital-identity-guidelines-kickoff-revision-4-presentation.pdf

FIDO2 and Regulatory Compliance

Businesses are governed by an increasingly complex network of regulations, jurisdictions, and standards that dictate security and privacy requirements. One common denominator in all laws is the need for strong authentication. Besides meeting the requirements of the US administration and the EU security agency, FIDO2 is a proven solution for complying with various security and privacy regulations.

Global privacy laws (GDPR and CCPA)

Almost 75% of global countries have privacy regulations[10], most of which reflect the core principles of GDPR. Data subjects, citizens, enjoy the rights of access, rectification, erasure, and portability of their personal data. A key component of delivering these capabilities securely is ensuring the authenticity and validity of the identity of individuals exercising these data rights.

The FIDO2 standard and supported devices embrace the protection of personal data and enable simplified yet efficient authentication. FIDO2 is based on public key cryptography, while the keys are generated and stored locally on the FIDO security key without any shared secrets. The authentication response is encrypted, protecting from phishing and credential stuffing attacks, while the biometrics are only stored and processed on the user's device.

Financial regulations and standards (PSD2)

The financial sector is heavily regulated, and for good reason, since attackers often target it.

The European Union Payment Services Directive (PSD2) aims to create an integrated European payments market, making payments safer and more secure to protect consumers. One of the critical requirements of PSD2 is the need for Strong Customer Authentication (SCA) using multiple authentication factors where "the breach of one of the elements does not compromise the reliability of the other elements."

In addition, PCI DSS 4.0 focuses on applying more robust authentication standards to payment and control process access log-ins. The new requirements include multi-factor authentication for all accounts with access to the cardholder data, not just administrators accessing the cardholder data environment.

Banks and payment service providers can leverage the FIDO2-accredited devices to meet the compliance requirements of the European Banking Authority and the PCI Security Council. The use of asymmetric cryptography helps to mitigate all known attacks that target "shared" credentials like passwords. Biometrics and security keys prove the "who you are" and "what you have" authentication factors while offering enhanced user convenience.

[10] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

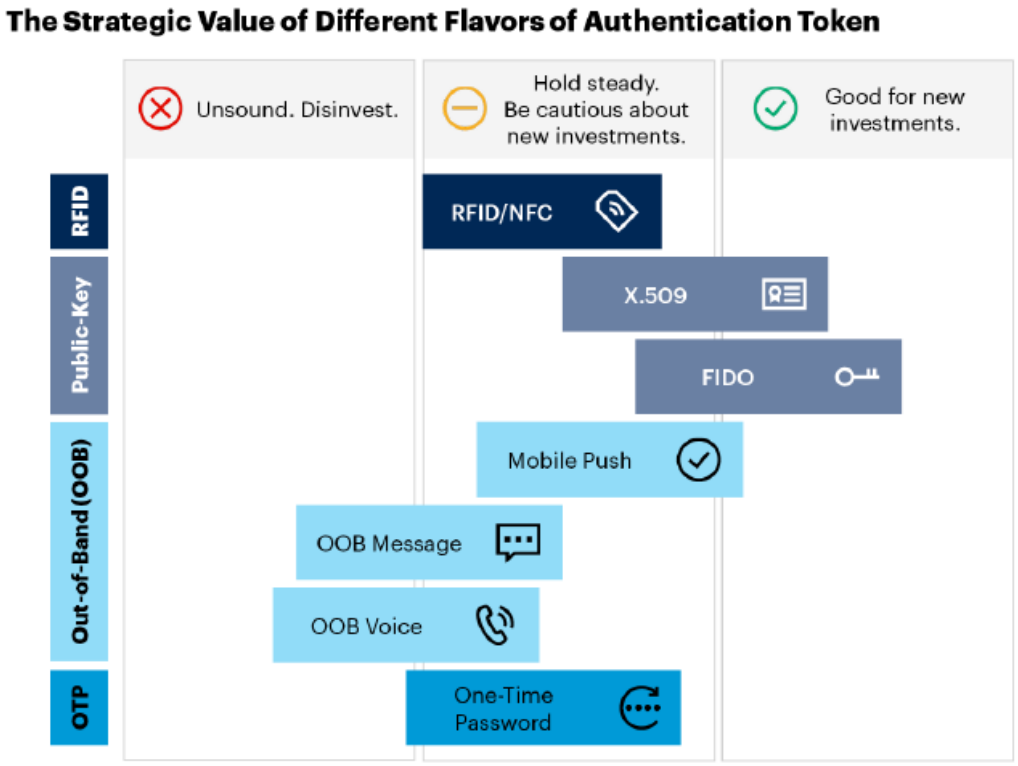
Practical Considerations: How to Comply with Phishing-Resistant MFA Requirements

Follow a hybrid approach

Despite FIDO2 being a future-proof authentication protocol, it is essential to highlight that it is not a panacea and cannot support use cases with legacy IT resources. FIDO2 protocol is designed to support only modern apps compatible with the WebAuthn standard.

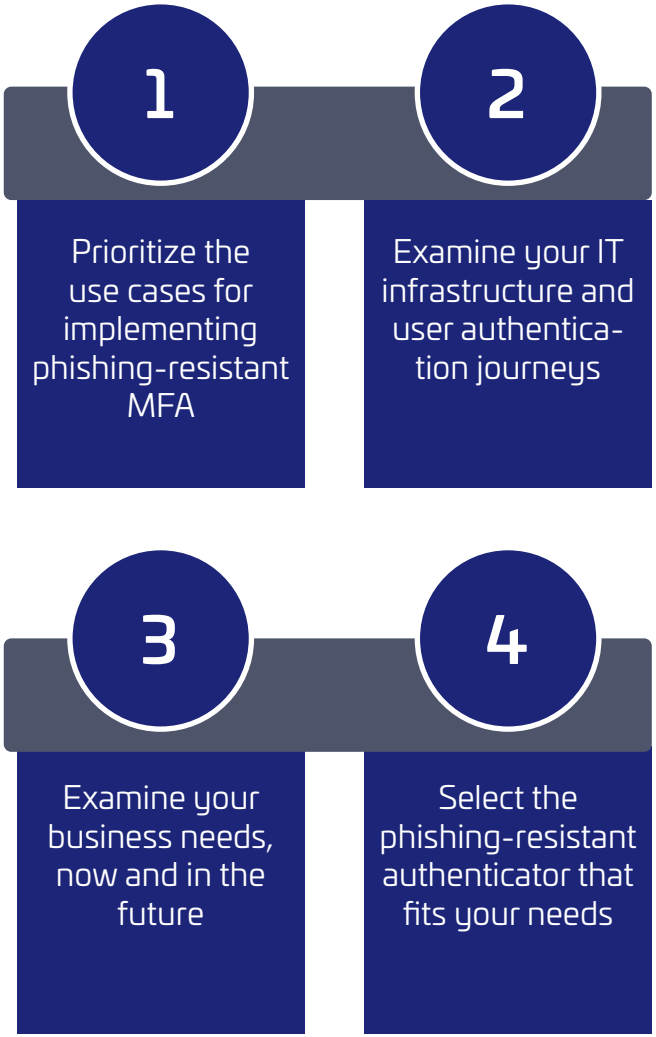
Some organizations, particularly those in critical infrastructure, healthcare, public administration, and finance, have outdated IT infrastructure that cannot support FIDO authentication and instead rely on PKI to defend against phishing and other cyber-attacks. Furthermore, FIDO may not be able to support specific operations that PKI does, such as digital signatures and file encryption. As a result, some businesses are slowly transitioning from PKI to FIDO as they update their IT systems and applications.

Security executives and CISOs are tasked with complying with regulations while also ensuring that their IT infrastructure and operations are not disrupted. The most effective approach to support these various use cases is through a hybrid or fused method of authentication that is resistant to phishing attempts. Gartner notes, "FIDO2 promises a universal, standardized approach to passwordless authentication, but at least in the near term, alternative and hybrid approaches will be needed. "



Four steps to phishing-resistant MFA compliance

Businesses and organizations can apply the following four-step approach to comply with the phishing-resistant MFA requirement.



1. Prioritize the use cases for implementing phishing-resistant MFA.

When making decisions, it's important to consider the risks of cyberattacks on users and IT resources. To ensure safety, CISA recommends that high-value staff like system administrators, attorneys, HR staff, and top management executives use phishing-resistant MFA. Protecting highly targeted resources such as email systems, file servers, and remote access systems with phishing-resistant MFA should be a top priority.

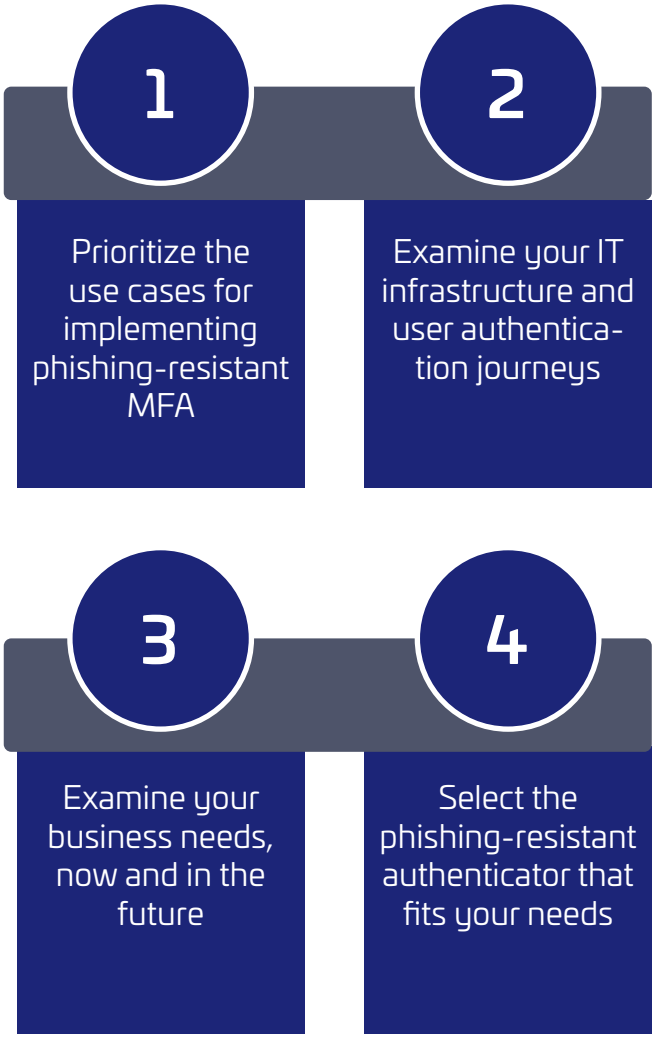
IT leaders need to identify all systems that may not support phishing-resistant authentication and find alternatives. For instance, small and medium-sized companies that cannot immediately implement phishing-resistant MFA should focus on enhancing their mobile One-Time Passcodes (OTP). Adding security features such as number matching will limit the potential of successful MFA bombing phishing attacks.

2. Examine your IT infrastructure and user authentication journeys.

Clear visibility into your infrastructure and ecosystem – Operational Technology (OT) and IT systems, apps, endpoints, etc. – will allow you to determine where to implement FIDO and PKI Certificate Based Authentication (CBA). It is essential to remember that legacy systems and apps will require PKI CBA, while modern apps are compatible with FIDO.

In addition, you should map where your employees, partners, and suppliers authenticate from.

- Are they using shared devices or working in "air gapped" areas? In such cases, it is better to use roaming hardware authenticators instead of "platform" authenticators embedded in laptops or mobile devices.
- Are they using mobile devices or laptops? Mobile devices typically have USB-C connectors, while laptops support both USB-A and USB-C. It's important to determine which form factor you require.



3. Examine your business needs, now and in the future.

The following questions are worth considering before selecting an MFA vendor and solution.

- Does your business have any plans to move away from legacy systems and PKI CBA authentication?
- Does your business need to maintain a PKI infrastructure to support use cases such as digital signatures and data encryption?
- Do you intend to move processes and data to the cloud and access them through APIs or cloud-based apps?
- Is there a need to support a hybrid authentication environment – PKI CBA and FIDO?

4. Select the phishing-resistant authenticator that fits your needs.

With so many vendors offering MFA solutions, it is vital to examine their offerings.

- Are their authenticators certified by regulation bodies required by your market? For FIDO, it is important to look at authenticators certified by the FIDO Alliance .
- For PKI, many organizations on regulated markets or technology vendors must comply with international security standards such as Common Criteria , eIDAS, or FIPS . Deploying phishing-resistant authenticators certified by regulatory bodies such as NIST or ANSSI is a must and simplifies compliance to these standards.
- Opting for an authenticator that supports either FIDO or PKI CBA means you will deal with tool sprawl and increased complexity for your end users and IT team. Some vendors offer fused tokens supporting both FIDO and PKI CBA, giving the advantage of support to important additional use cases, such as qualified digital signature and data encryption for security, legal, and compliance purposes. A single authenticator can be optimal if you operate a hybrid environment.

It is essential to adapt the authentication method to the constraint of your IT resources and the user's context and find the right balance between security and user experience.

The following table provides high-level guidance on selecting the MFA method that meets your infrastructure and user requirements.

Use cases	Users	Device	Recommended MFA method
Combine physical access with digital access	Workforce • employees • contractors • suppliers	Laptops or mobile	Hybrid RFID/FIDO smart card (device-bound passkey)
Combine passwordless authentication with digital signature and file encryption			Hybrid PKI/FIDO USB Token (device-bound passkey)
Access to legacy resources/apps, digital signature		Laptops	PKI USB token or smart card
Windows, Mac, Linux logon			FIDO USB token or smart card (device-bound passkey)
Windows logon on shared desktops			
Access to modern web apps		Laptops or mobile	
Access to web apps when CBA/FIDO is not possible			Mobile Push + Number matching or Hardware OTP token (device-bound passkey)
Access to personal devices and online services	Consumers		Synced passkeys

The Thales FIDO security keys Advantage

Full range of FIDO security keys

Despite FIDO2 being a future-proof authentication protocol, it is essential to highlight that it is not a panacea and cannot support use cases with legacy IT resources. FIDO2 protocol is designed to support only modern apps compatible with the WebAuthn standard.

Some organizations, particularly those in critical infrastructure, healthcare, public administration, and finance, have outdated IT infrastructure that cannot support FIDO authentication and instead rely on PKI to defend against phishing and other cyber-attacks. Furthermore, FIDO may not be able to support specific operations that PKI does, such as digital signatures and file encryption. As a result, some businesses are slowly transitioning from PKI to FIDO as they update their IT systems and applications.

Security executives and CISOs are tasked with complying with regulations while also ensuring that their IT infrastructure and operations are not disrupted. The most effective approach to support these various use cases is through a hybrid or fused method of authentication that is resistant to phishing attempts. Gartner notes, "FIDO2 promises a universal, standardized approach to passwordless authentication, but at least in the near term, alternative and hybrid approaches will be needed."

Thales FIDO Security Keys Differentiators

Reduce risk of credential compromise with best in class security

- Thales controls the entire manufacturing cycle – hardware and software
- Thales develops its own crypto libraries for FIDO security keys
- Phishing resistant authentication offers superior assurance

Integrates seamlessly into your environment

- Compatible with Thales Authentication & Access Management Platform , Microsoft Entra ID and any other authentication platforms supporting FIDO2/ WebAuthn
- Extends value of PKI certificate authentication

Superior certifications

- U2F and FIDO2 certified
- Meets US and EU regulatory for phishing resistant authentication
- FIPS , CC, eIDAS, ANSSI certified

Enables broad range of use cases

- Phishing-resistant authentication from multiple endpoints (Windows Laptops and Mac, Mobile devices)
- eIDAS digital signing
- Network logon
- Remote access
- Cloud access
- Physical Access
- On Device Biometric Authentication

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com