cpl.thalesgroup.com

THALES
Building a future we can all trust

The FIDO Authentication Handbook

Contents

Passwords are not Viable

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

For enterprise IT departments, supporting and maintaining passwords is a burden that increases helpdesk costs, creates complexity, and leads to poor user experiences related to password-reset requirements. Most importantly, passwords are no longer adequate to protect against current cybersecurity threats and don't comply with corporate information security needs.

Data breach reports indicate that criminals leverage insecure passwords to launch attacks against organizations. Compromised, stolen, or weak passwords are a key vector for successful attacks to disclose personal data, impersonate legitimate user accounts and websites. Such attacks can have serious consequences for businesses and individuals alike.

61%

of data breaches involve credentials. Privilege misuse is the top misuse variety in data breaches

Privilege misuse is the top misuse variety in data breaches. Credentials are the top data variety compromised in data breaches.

39%

of organizations experienced an increase in credential stuffing and other password attacks

Organizations need to move beyond using just passwords for authenticating users and protecting data.

What is FIDO2?

While there are currently many solutions to implement passwordless authentication, Fast Identity Online (FIDO2) promises to deliver a truly frictionless and secure authentication mechanism.

The FIDO2 standard is intended to solve multiple user scenarios and provides for passwordless, multi-factor cryptographic tokens. A FIDO2 authenticator, also known as a FIDO security key, embeds one or more private keys, each dedicated to one online account. The protocols require 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.

FIDO2 security keys can entirely replace weak static password credentials with strong hardware or software public/private key credentials.

FIDO2 Benefits

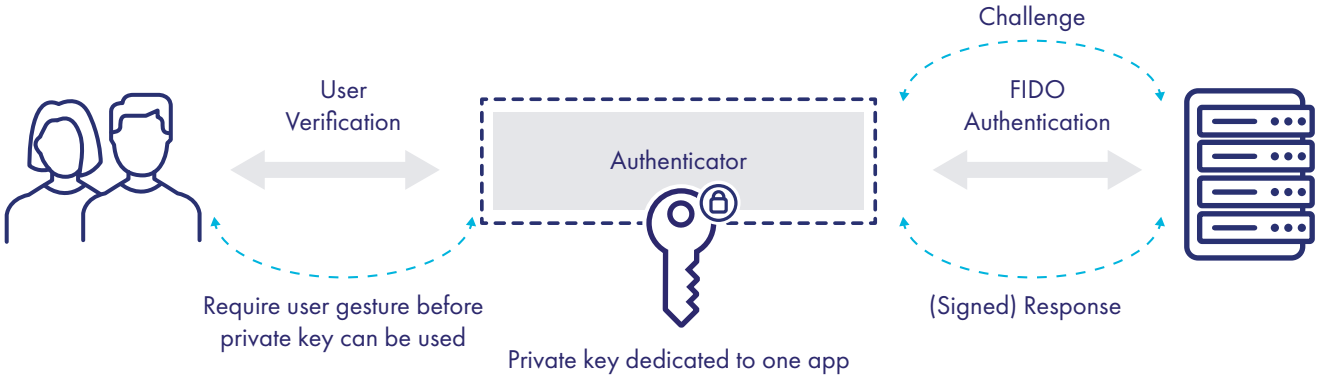
Security: Unique login credentials across every website, which are never stored on a server, eliminating the risks of phishing, all forms of password theft and replay attacks.

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 a simple JavaScript API call that is supported across all leading browsers and platforms.

How does FIDO Work?



FIDO2 and Regulatory Compliance

Businesses are governed by an increasingly complex network of regulations, jurisdictions, and standards which dictate security and privacy requirements. One common denominator in all regulations is the need for strong authentication.

Compliance with GDPR and CCPA

According to both regulations, data subjects, citizens of the EU and the State of California have the rights of access, rectification, erasure, and portability on their personal data. A key component of delivering these capabilities securely is to ensure the authenticity and validity of the identity of individuals exercising these data rights.

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

Compliance with PSD2

The European Union Payment Services Directive (PSD2) aims at creating an integrated European payments market, making payments safer and more secure to protect consumers. One of the key 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."

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

Meeting Requirements Specified by the US Executive Order on Cyber Security

Section 3.d of the Executive Order requires the implementation of multi-factor authentication. Thales FIDO devices and other authentication options offer the broadest range of authentication solutions and form factors, enabling federal and state agencies to meet the essential zero trust and authentication requirements specified in the US Executive Order.

Practical Considerations

Do we need to replace existing authentication methods?

To address increasing access security concerns, many organizations have invested in strong authentication schemes, including PKI-based authentication and OTP hardware or mobile solutions. It is not practical from a cost or operational perspective for them to rip and replace these solutions, especially if they meet business needs.

Organizations need to evaluate all available authentication solutions to find which solution satisfies the various use cases.

	FIDO2 Devices	OTP hardware	OTP Push/ OTP Mobile App	X.509 smart cards	SMS
Network Logon	High	Medium	Medium	High	Low
Cloud/VPN Access	High	High	High	Low	Low
Privileged Access	High	High	High	High	Low

Solutions, including those offered by Thales, support a diverse range of authentication methods, technology and form factors. These solutions enable organizations to secure cloud adoption and bridge secure access across hybrid environments via an integrated access management and authentication offering, facilitating their cloud and digital transformation initiatives by providing their users with a single authentication device for securing access to legacy apps, network domains and cloud services.

Combining PKI Authentication with FIDO2 Authentication

Many organizations have invested in Public Key Infrastructure (PKI) to manage certificate-based authentication. Mandated by numerous security and privacy regulations, and standards that require a high level of assurance and strong authentication, PKI is used broadly by industries and organizations, including banks, healthcare, energy utilities, and others to secure access to data and apps.

Due to the complexity of managing digital certificates and PKI, enterprises are often forced to make trade-offs between business functionality and security, which can create serious gaps and leave them open to cyber-attacks.

Organizations that have invested in PKI to authenticate and secure access to traditional apps are not required to rip or replace their existing authentication environment. On the contrary, they can supplement PKI with FIDO2, build on their existing infrastructure and extend their existing security footprint to modern authentication methods to safeguard access to cloud-based apps.

Benefits

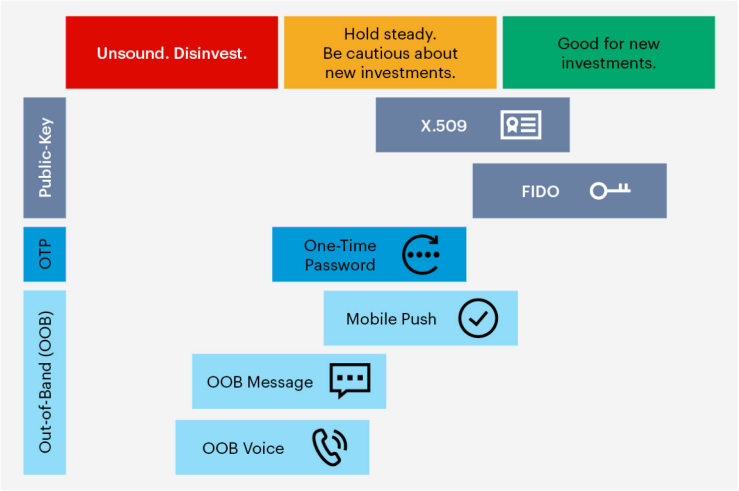
- Unified authentication and access security solution for both legacy apps and modern, cloud-based apps and data.
- Faster integration within applications for strong authentication based on the FIDO2 protocol's public key cryptography.
- Lower costs to the enterprise because they can build on the existing authentication infrastructure and extend their authentication mechanisms.
- Compliance with privacy laws for all use cases to ensure that private and sensible information are protected and prevent unauthorized exposure of such data to anyone.
- Reduced complexity for end-users, developers and administrators.

Investing in Solutions that are Future-ready

Gartner® predicts that by 2025, more than 25% of MFA transactions using a token will be based on FIDO authentication protocols, up from less than 5% today. In addition, Gartner recommends that security and risk management leaders must carefully evaluate which options best fit their tactical and strategic needs and should:

- Optimize the value of investments by choosing methods that can provide consistent, adequate, reasonable, and effective user authentication.
- Ensure user authentication methods (with or without tokens) meet these criteria by evaluating trust, total cost of ownership, user experience (UX) and other needs and constraints across different use cases.
- Reduce potential vulnerabilities in legacy implementations by disinvesting from known-weak legacy OOB modes, such as SMS, and migrating toward more effective methods.
- Plan to improve consistency over multiple use cases by preparing for strategic investments in FIDO2, seeking tactical opportunities to invest in the near term.

The Strategic Value of Different Kinds of Authentication Token



Source: Gartner
724226_C

Gartner.

Source: Gartner, Innovation Insight for Many Flavors of Authentication Token, Ant Allan, David Mahdi, Tricia Phillips, May 2021. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

The Thales FIDO Advantage

Full range of FIDO devices

There are many vendors that provide various authentication tokens. However, only Thales offers a complete range of FIDO devices to address all possible authentication use cases. Specifically, Thales SafeNet FIDO devices include:

- PKI-FIDO smart cards to address both PKI and FIDO use cases
- FIDO smart cards with NFC support, enabling FIDO authentication via mobile devices
- FIDO smart cards with combined logical access, enabling combined badge – logical access use cases
- USB FIDO devices with presence detection, enabling secure remote access to cloud services

Full Integration with Azure AD

All Thales FIDO devices are fully compatible and integrated with Azure AD managed services. SafeNet FIDO devices offer users a seamless and passwordless logon experience from all devices. Organizations using Thales FIDO2 devices can address new use cases while maintaining the optimal balance between security and convenience with passwordless authentication.

For more info and to learn what Gartner recommends read the 'Innovation Insight for Many Flavors of Authentication' report.

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 <