THALES

SafeNet FIDO2 Devices
Arm your Enterprise with Strong & Secure Passwordless Authentication

As enterprises enter the 2020s, expand their digital transformation and move to the cloud, the majority of security breaches are related to identity theft. Many organizations have invested in strong authentication schemes, including PKI-based authentication.

These organizations now face the challenge of having to address new use cases, while maintaining the optimal balance between security and convenience.

How can organizations achieve a seamless and passwordless logon experience from all devices? How can organizations address new use cases without having to rip and replace their authentication methods? Thales, the world leader in digital security, addresses these issues with two new SafeNet FIDO2 devices: the SafeNet IDPrime 3940 FIDO (Smart Card) and SafeNet eToken FIDO (USB token). These new solutions enable organizations to secure cloud adoption and bridge secure access across hybrid environments via an integrated access management and authentication offering.

Passwordless Authentication

Passwordless authentication replaces passwords with other methods of identity, improving the levels of assurance and convenience. This type of authentication has gained traction because of its considerable benefits in easing the login experience for users and surmounting the inherent vulnerabilities of text-based passwords. These advantages include less friction, a higher level of security that's offered for each app and the elimination of the legacy password.

Comfort for PKI Customers

One of the biggest benefits of the offering is organizations that rely on PKI authentication can now use a combined PKI-FIDO smart card to facilitate 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.

FIDO2 and PKI Support, All in One Device

The SafeNet IDPrime 3940 FIDO Smart Card is designed for PKI-based applications and comes with a SafeNet minidriver that offers perfect integration with native support for Microsoft® environments, without any additional middleware.

This dual-interface smart card, allowing communication either via a contact interface or via a contactless ISO 14443 interface, is also compatible with some NFC readers.

SafeNet IDPrime 3940 FIDO Smart Card is CC EAL5+/PP Java Card certified for the Java platform and CC EAL5+/PP QSCD certified for the combination of Java platform and PKI applet. SafeNet IDPrime 3940 is qualified by the French ANSSI and is qualified according to the eIDAS regulations for both the eSignature and the eSeal applications. In addition, SafeNet IDPrime 3940 FIDO supports FIDO 2.0 and U2F standards.

USB Token with Touch Sense Options

The SafeNet eToken FIDO is a USB token, an ideal solution for enterprises looking to deploy passwordless authentication for employees. This authenticator is a compact, tamper-evident USB with presence detection, which creates a third factor of authentication: Something you have (physical token), something you know (PIN), something you do (touching the token).

Key Benefits

SafeNet FIDO2 Devices arm your enterprise with strong and secure passwordless authentication to any environment.

Key benefits include:

- Secure cloud adoption and bridge secure access across hybrid environments with a combined PKI/FIDO smart card.
- Secure & easy access on multiple operating systems.
- Passwordless access to cloud apps & network domains.
- Leverage your PKI authentication scheme—No rip & replace!
- Offer your users a single authenticator for all their needs
- CC certified
- Supports all devices and OS (without middleware deployment)
- Fully customizable
- Ideal for digital signatures and email encryption.

Product Characteristics	SafeNet IDPrime 3940 FIDO Smart Card
Memory	• SafeNet IDPrime 3940 is based on a 400 KB Java Flash memory chip. A standard SafeNet IDPrime 3940 FIDO comes with 20 key containers. • The memory available for certificates and other applets & data in this standard configuration is 73 KB.
Standards	• BaseCSP minidriver (SafeNet minidriver) • Global Platform 2.2.1 • Java Card 3.0.4 • ISO 7816 and ISO 14443 • FIDO 2.0 and U2F certifications
Operating systems	• FIDO application supported in Windows 10 and other FIDO compliant operating systems. • Standard PKI application supported on Windows, MAC OS X and Linux
Cryptographic algorithms	• Hash: SHA-1, SHA-256, SHA-384, SHA-512. • RSA: up to RSA 4096 bits • RSA OAEP & RSA PSS • P-256 bits ECDSA, ECDH. P-384 & P-521 bits ECDSA, ECDH are available via a custom configuration • On-card asymmetric key pair generation (RSA up to 4096 bits & Elliptic curves up to 521 bits) • Symmetric: AES—For secure messaging and 3DES for Microsoft Challenge/Response only
Communication protocols	• T=1, T=0, PPS, with baud rate up to 446 Kbps at 3.57 MZ (TA1=97h) • T=CL, ISO 14443 type A, with speed up to 848 Kbps
Other features	• Onboard PIN Policy • Multi-PIN support • SafeNet IDPrime family of cards can be customized (card body and programming) to fit customers' needs.
Chip characteristics	
Technology	• Embedded crypto engine for symmetric and asymmetric cryptography
Lifetime	• Minimum 500,000 write/erase cycles • Data retention for minimum 25 years
Certification	• CC EAL6+
Security	• SafeNet IDPrime smart cards include multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks. • The SafeNet IDPrime 3940 FIDO is both CC EAL5+ / PP Java Card certified for the Java platform and CC EAL5+ / PP QSCD certified for the combination of Java platform plus PKI applet, is eIDAS qualified for both eSignature and eSeal, and qualified by the French ANSSI.

Product Characteristics	SafeNet eToken FIDO
Memory	• 80K
Standards	• API and Standards Support: FIDO 2.0 and U2F
Operating systems	• FIDO application supported in Windows 10 and other FIDO compliant operating systems
Physical	
Dimensions	• 6mm*8mm*40.5mm
Operating Temperature	• 0° C to 70° C (32° F to 158° F)
Storage Temperature	• -40° C to 85° C (-40° F to 185° F)
Humidity Rating	• 0-100% without condensation
Water Resistance Certification	• IP X7 – IEC 529 -
USB Connector	• USB type A; supports USB 1.1 and 2.0 (full speed and high speed)
Casing	• Hard molded plastic, tamper evident
Memory data retention	• At least 10 years
Memory cell rewrites	• At least 500,000

SafeNet IDPrime 3940 FIDO/ SafeNet eToken FIDO is compatible with Microsoft Azure Active Directory accounts.

About Thales's SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.