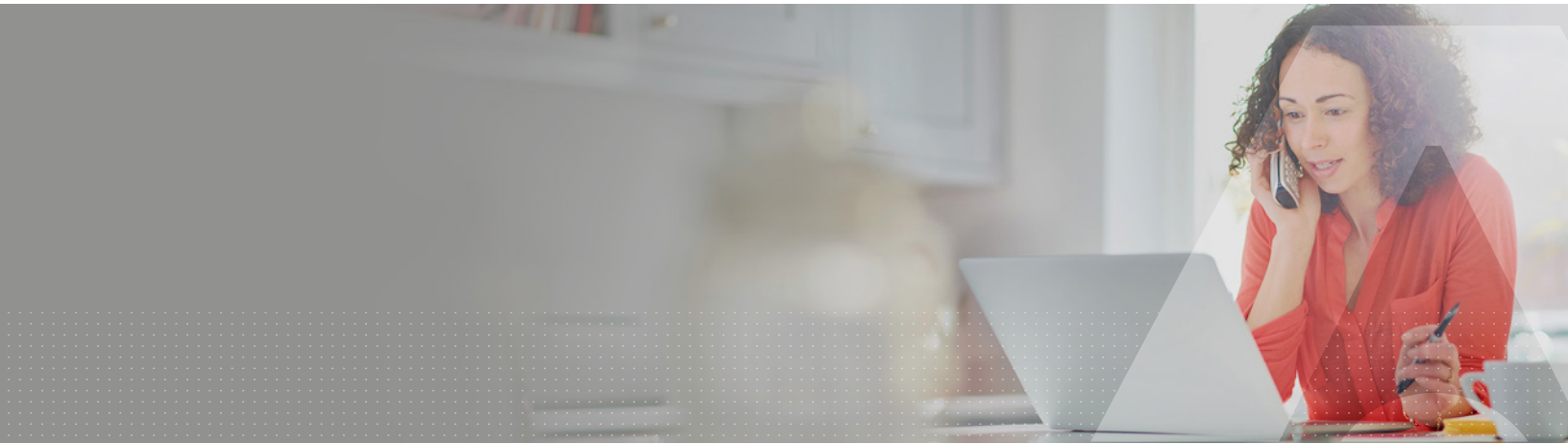**THALES**
Building a future we can all trust

SafeNet FIDO2 Passwordless Devices
Decrease the risk of security breaches with Passwordless Multi-factor Authentication

Organizations expanding their digital transformation are moving applications and data to the cloud to (1) enable accessibility from anywhere and (2) decrease operating costs. As users log in to an increasing number of cloud-based applications, weak passwords are emerging as the primary cause of identity theft and security breaches.

To reduce risk to your Windows logon, SaaS applications, users with high privilege and users in general, Thales supports FIDO passwordless authentication using multi factor-authentication (MFA) hardware devices.

Replacing passwords with FIDO authenticator hardware introduces a modern passwordless MFA experience that is resistant to phishing attacks and account takeovers, and enables compliance.

Thales multi-factor authentication devices use current and emerging protocols to support multiple applications at the same time. Use one key that combines support for FIDO2, WebAuthn, U2F, and PKI to access both physical spaces and logical resources.

Passwordless FIDO2 Authentication

Passwordless FIDO authentication decreases the risk of security breaches by replacing vulnerable textual passwords with FIDO authentication.

FIDO authentication has gained traction as a modern form of MFA because of its considerable benefits in easing the log in experience for users and overcoming the inherent vulnerabilities of text-based passwords. Advantages include less friction for users and a high level of security.

Enable Multiple User Authentication Journeys

Thales, the world leader in digital security, supports numerous passwordless authentication journeys with a powerful range of FIDO devices

FIDO with Converged Badge

Physical Access- For optimum convenience, Thales FIDO smart cards support physical access enabling users to access both physical spaces and logical resources with a single customizable smart card.

Extend Modern Authentication to PKI Environments - 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.

Remote Access

Whether working from home or while traveling, users may log into cloud based business applications from multiple devices in multiple locations.

Thales FIDO authenticators provide secure remote access with MFA to protect your organization regardless of the endpoint device and the location.

Windows PC and Network Login

FIDO authenticators provide passwordless MFA, enabling users to securely access Windows PCs and tablets. With the combined FIDO PKI cards, we can offer a single device for securely logging into any OS, including Windows 10, 8, and 7, Windows Server OS, macOS, and Linux. This means that organizations can use Thales FIDO-PKI devices to support both FIDO and PKI authentication and digital signature needs.

Protect SaaS Apps

Since the majority of users re-use their passwords across apps, you can improve security dramatically, and reduce calls to the Helpdesk, by equipping users with FIDO authenticators. Thales FIDO devices are fully compatible with Azure AD and ensure secure access to Azure AD managed applications.

Secure Mobile Access

Thales FIDO devices enable modern authentication on any device by enabling users to authenticate using contactless to just 'tap and go' in order to gain secure access to any cloud resource from any mobile device.

Privileged Access Management

Privileged users with elevated permissions or the ability to log into PAM solutions, have ready access to sensitive data – their accounts are the ultimate goal of bad actors.

Providing privileged users with multi-factor authentication to replace vulnerable passwords ensures that only authorized users can access privileged resources.

IDP Compatibility

SafeNet FIDO2 Passwordless Devices are compatible with any Identity Provider (IDP) that supports the FIDO2 standard.

Please see our website for a list of the IDPs we have tested with and jointly validated, https://cpl.thalesgroup.com/access-management/authenticators/fido-devices

For all enterprises, offer your employees and contractors a single device for all of their authentication and access needs – whether they work from home or in an office. Permit physical access to buildings and controlled areas, and facilitate employee mobility. Consider your use cases and choose among SafeNet FIDO authenticators.

Product Characteristics	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Form Factor	Smart card	USB-A Token	Smart card	Smart card	Smart card
Contact (ISO 7816)	FIDO & PKI	N/A	N/A	PKI	PKI
Contactless (ISO144443)	FIDO & PKI	N/A	FIDO & Physical Access	FIDO & Physical Access	FIDO & Physical Access
Memory					
Memory chip	400 KB Java Flash	400 KB Java Flash	586 KB User ROM	Contact chip: 400KB Java Flash Contactless chip: 586 KB User ROM	Contact chip: 400KB Java Flash Contactless chip: 586 KB User ROM
Free memory available for resident keys, certificates, additional applets & data	73 KB	90 KB	88.3 – 98.3 KB	Contact: 73 KB Contactless: 88.3 – 98.3KB	Contact: 73 KB Contactless: 88.3 – 98.3KB
Key Capacity					
FIDO resident keys	Up to 8	Up to 8	Up to 8	Up to 8	Up to 8
PKI key containers	20	N/A	N/A	20	20
Standards Supported					
Java Card	3.0.4	3.0.4	N/A	3.0.4	3.0.5
Global Platform 2.2.1	✔	✔	N/A	✔	✔
FIDO 2.0	✔	✔	✔	✔	✔
U2F	✔	✔	✔	✔	✔
Base CSP minidriver (SafeNet minidriver)	✔	N/A	N/A	✔	✔
Cryptographic algorithms (PKI)					
Hash: SHA-1, SHA-256, SHA-384, SHA-512.	✔	N/A	N/A	✔	✔
RSA: up to RSA 4096 bits	✔	N/A	N/A	✔	✔
RSA OAEP & RSA PSS	✔	N/A	N/A	✔	✔
P-256 bits ECDSA, ECDH. P-384 & P-521 bits ECDSA, ECDH are available via a custom configuration	✔	N/A	N/A	✔	✔
On-card asymmetric key pair generation (RSA up to 4096 bits & Elliptic curves up to 521 bits)	✔	N/A	N/A	✔	✔
Symmetric: AES—For secure messaging and 3DES for Microsoft Challenge/Response only	✔	N/A	N/A	✔	✔

Product Characteristics	SafeNet IDPrime 3940 FIDO	SafeNet eToken FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Certifications					
Chip: CC EAL6+	✔	✔	N/A	✔	✔
NIST certification - FIPS 140-2 L2	N/A	N/A	N/A	N/A	✔
Java platform: CC EAL5+/ PP java card certified	✔	✔	N/A	✔	N/A
Java platform + PKI applet: CC EAL5+/PP QSCD	✔	N/A	N/A	✔	N/A
eIDAS qualified for both eSignature and eSeal	✔	N/A	N/A	✔	N/A
French ANSSI	✔	N/A	N/A	✔	N/A
Physical Access - Mifare Classic & DesFire configurations	N/A	N/A	✔	✔	✔
Other Features					
Onboard PIN policy	✔	N/A	N/A	✔	✔
Multi-PIN support	✔	N/A	N/A	✔	✔
Customization and branding	✔	N/A	N/A	✔	✔
Operating Systems					
FIDO supported in Windows 10 and other FIDO-compliant operating systems	✔	✔	✔	✔	✔
PKI supported in Windows, macOS X, and Linux	✔	N/A	N/A	✔	✔

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.