cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales FIDO2 Devices:
Stop Phishing Attacks with Strong Passwordless Multi-Factor Authentication

Organizations expanding their digital transformation are moving applications and data to the cloud to enable accessibility from anywhere and 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.

Addressing this risk, Thales FIDO2 devices are offering organizations passwordless, phishing-resistant authentication, allowing them to stop account takeover and remove risk of unauthorized access to sensitive resources like SaaS applications and Windows endpoints.

Thales FIDO2 devices support multiple applications at the same time. Use one that combines FIDO2, U2F, PKI and RFID to access both physical spaces and logical resources.

Passwordless FIDO2 Authentication

FIDO2 authentication removes the risk of account take-over by replacing vulnerable passwords with a phishing-resistant WebAuthn credential.

FIDO2 authentication has gained traction as a modern form of MFA because of its considerable benefits in easing the login experience for users and overcoming the inherent vulnerabilities of passwords. Advantages include less friction for users and a high level of protection against phishing attacks. .

Meet stringent Compliance Mandates

Thales FIDO2 security keys, USB Tokens and smart cards let you meet all your regulatory needs. They are FIDO2 and U2F certified. The combined PKI-FIDO are compliant with NIST regulations, are FIPS 140-2 or Common Criteria (CC) certified, ANSSI qualified for the Java platform and the PKI applet. They also meet eIDAS regulations for both eSignature and eSeal applications.

Enable Multiple User Authentication Journeys

Thales supports numerous passwordless authentication journeys with a wide range of FIDO devices.

Secure Access to SaaS Apps

Since the majority of users reuse their passwords across apps, you can improve security dramatically and reduce calls to the Helpdesk, by equipping users with FIDO authenticators.

Network Login for Frontline Workers

FIDO2 security keys provide passwordless MFA, enabling users such as frontline workers to securely access shared devices such as Windows PCs and tablets.

Combine Physical & Logical 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.

Modernize PKI / CBA Environments

Organizations that rely on PKI and Certificate based Authentication (CBA) can now use a combined PKI-FIDO smart card or USB Token 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, they reduce operational costs and simplify User Experience.

Secure Remote Access

Whether working from home or while traveling, users may log into web-based 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.

Secure Mobile Access

Thales FIDO devices enable users to authenticate to any cloud resources from their mobile devices: either by taping their contactless smart card on their device using NFC, or by plugging the SafeNet eToken Fusion USB-C to their mobile phone.

Privileged Users Access Control

Privileged users with elevated permissions (administrators, VIP's ...) have ready access to sensitive data - their accounts are a prime target for spear phishing and whaling attacks.

Providing privileged users with FIDO2 security keys to replace vulnerable passwords ensures that only authorized users can access privileged resources.

IDP Compatibility

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

Check Thales website for a list of the tested and jointly validated IDPs: https://cpl.thalesgroup.com/access- management/authenticators/fido-devices

Supported Platforms

Thales PKI/FIDO security keys support a large variety of operating systems such as iOS, Android, Windows 11, 10, 8, Windows Server OS, macOS, and Linux, such as SafeNet Trusted Access and Microsoft Azure Active Directory.

Thales FIDO2 Benefits

Best in class security

- Thales controls the entire manufacturing cycle and develops its own FIDO crypto libraries, which reduces the risk of being compromised.

Support for multiple use cases

- Combine FIDO, PKI and physical access in a single device
- Experience a strong authentication from mobile endpoints

Compliant with high security standards

- U2F and FIDO2 certified
- Compliant with US and EU regulations for phishing-resistant authentication
- FIPS and CC certified for PKI operations

Robustness & Scalability for a long life duration

- Hard molded plastic, tamper evident USB FIDO keys
- No damage to USB ports thanks to sensitive presence detector
- Support for firmware updates for better maintenance and upgradability

Smart Card – Form Factor

Product Characteristics	SafeNet IDPrime 3940 FIDO	SafeNet IDPrime 3930 FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Contact (ISO 7816)	FIDO & PKI	FIDO & PKI	N/A	PKI	PKI
Contactless (ISO 14443)	FIDO & PKI	FIDO & PKI	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	55 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	20	N/A	20	20
Standards Supported					
Java Card	3.0.4	3.0.5	3.0.4	3.0.4	Contact chip: 3.0.5 Contactless chip: 3.0.4
Global Platform	2.2.1	2.2.1	2.3	Contact chip: 2.2.1 Contactless chip: 2.3	Contact chip: 2.2.1 Contactless chip: 2.3
FIDO 2.0	✔	✔	✔	✔	✔
U2F	✔	✔	✔	✔	✔
Base CSP minidriver (SafeNet minidriver)	✔	✔	N/A	✔	✔
Cryptographic algorithms (PKI)					
Hash: SHA-1, SHA-256, SHA-384, SHA-512.	✔	✔	N/A	✔	✔
RSA: up to RSA 4096 bits	✔	✔	N/A	✔	✔
RSA OAEP & RSA PSS	✔	✔	N/A	✔	✔
P-256 bits ECDSA, ECDH. P-384 & P-521 bits ECDSA,	✔	✔	N/A	✔	✔
ECDH are available via a	✔	✔	N/A	✔	✔
custom configuration	✔	✔	N/A	✔	✔
On-card asymmetric key pair generation (RSA up to 4096 bits & Elliptic curves up to 521 bits)	✔	✔	N/A	✔	✔
Symmetric: AES—For secure messaging and 3DES for Microsoft Challenge/Response only	✔	✔	N/A	✔	✔

Smart Card – Form Factor (continued)

Product Characteristics	SafeNet IDPrime 3940 FIDO	SafeNet IDPrime 3930 FIDO	SafeNet IDCore 3121 FIDO	SafeNet IDPrime 941 FIDO	SafeNet IDPrime 931 FIDO
Certifications					
Chip: CC EAL6+	✔	✔	✔	✔	✔
NIST certification - FIPS 140-2 L2	N/A	✔	N/A	N/A	✔
Java platform: CC EAL5+/ PP java card certified	✔	N/A	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 PKI Features					
Onboard PIN policy	✔	✔	N/A	✔	✔
Multi-PIN support	✔	✔	N/A	✔	✔
Customization and branding	✔	✔	N/A	✔	✔
Certifications					
FIDO supported in Windows 10 and other FIDO-compliant operating systems	✔	✔	✔	✔	✔
PKI supported in Windows, macOS X, and Linux	✔	✔	N/A	✔	✔

Token – Form Factor

Product Characteristics	 SafeNet eToken FIDO	 SafeNet eToken Fusion	 SafeNet eToken Fusion Common Criteria (CC)
Form Factor	USB-A	USB-A or USB-C	USB-A or USB-C
Memory			
Memory chip	400 KB Java Flash	400 KB Java Flash	400 KB Java Flash
Free memory available for resident keys, certificates, additional applets & data	90 KB	55 KB	73 KB
Key Capacity			
FIDO resident keys	Up to 8	Up to 8	Up to 8
PKI key containers	N/A	20	20
Standards Supported			
Java Card	3.0.4	3.0.4	3.0.4
Global Platform	2.2.1	2.2.1	2.2.1
FIDO 2.0	✔	✔	✔
U2F	✔	✔	✔
Base CSP minidriver (SafeNet minidriver)	N./A	✔	✔
Cryptographic algorithms (PKI)			
Hash: SHA-1, SHA-256, SHA-384, SHA-512.	N/A	✔	✔
RSA: up to RSA 4096 bits	N/A	✔	✔
RSA OAEP & RSA PSS	N/A	✔	✔
P-256 bits ECDSA, ECDH. P-384 & P-521 bits ECDSA,	N/A	✔	✔
ECDH are available via a	N/A	✔	✔
custom configuration	N/A	✔	✔
On-card asymmetric key pair generation (RSA up to 4096 bits & Elliptic curves up to 521 bits)	N/A	✔	✔
Symmetric: AES—For secure messaging and 3DES for Microsoft Challenge/Response only	N/A	✔	✔

Product Characteristics	 SafeNet eToken FIDO	 SafeNet eToken Fusion USB-A or USB-C	 SafeNet eToken Fusion Common Criteria (CC)
Certifications			
Chip: CC EAL6+	✔	N/A	✔
NIST certification - FIPS 140-2 L2	N/A	N/A	N/A
Java platform: CC EAL5+/ PP java card certified	✔	N/A	✔
Java platform + PKI applet: CC EAL5+/PP QSCD	N/A	N/A	✔
eIDAS qualified for both eSignature and eSeal	N/A	N/A	✔
French ANSSI	N/A	N/A	✔
Physical Access - Mifare Classic & DesFire configurations	N/A	N/A	N/A
Other PKI Features			
Onboard PIN policy	N/A	✔	✔
Multi-PIN support	N/A	✔	✔
Customization and branding	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	✔	✔

About Thales OneWelcome Identity & Access Management Solutions

Thales's industry-leading Workforce and Customer Identity & Access Management (CIAM) 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.