Solution Brief

Member of
Microsoft Intelligent
Security Association

Microsoft

Thales Phishing-Resistant FIDO2 & Certificate-Based Authentication for Azure AD, part of Microsoft Entra

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

As users log into 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 security keys support seamless integration with Azure AD, now part of Microsoft Entra, offering organizations highly secure passwordless authentication and allowing them to reduce risk of unauthorized access to Microsoft environments, SaaS applications and Windows endpoints.

Replacing passwords with FIDO2 security keys introduces a modern passwordless MFA experience that is resistant to phishing attacks and account takeovers, and meets current security guidelines and regulations.

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

Passwordless FIDO2 Authentication

Passwordless FIDO2 authentication decreases the risk of security breaches by replacing vulnerable passwords with a phishing – resistant WebAuthn credential.

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 passwords. Advantages include less friction for users and a high level of protection against phishing attacks.

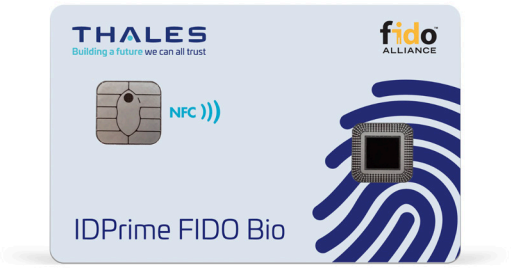
Meet stringent compliance mandates

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 the US Executive Order mandate for phishing-resistant MFA and 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, the world leader in digital security, integrates with Azure AD to support numerous passwordless authentication journeys with a powerful range of FIDO2 security keys.

Facilitate Users' Adoption with Biometric Authentication



Provide your end users a new passwordless authentication experience thanks to SafeNet IDPrime FIDO Bio Smart Card.

End users authenticate faster & easier by tapping the card on their device and putting their fingerprint on the sensor.

To protect users' data privacy, with fingerprint on-device authentication, users' data never leave the device.

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. Thales FIDO devices are fully compatible with Azure AD and ensure secure access to Azure AD managed applications.

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

With the new Azure AD cloud-native CBA support, organizations that rely on PKI and Certificate based Authentication (CBA) can now use a combined Thales 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, VIPs, etc.) 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.

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.

Thales FIDO2 Benefits

Full integration with Azure AD

- All Thales FIDO2 security keys are fully compatible and integrated with Azure AD. They have been verified by Microsoft technical teams.

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

User convenience for better adoption

- Support for biometric (fingerprint on smart card)
- Sensitive presence detector on USB FIDO key

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	SafeNet IDPrime FIDO Bio
Contact (ISO 7816)	FIDO & PKI	FIDO & PKI	N/A	PKI	PKI	FIDO
Contactless (ISO 14443)	FIDO & PKI	FIDO & PKI	FIDO & Physical Access	FIDO & Physical Access	FIDO & Physical Access	FIDO
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	206KB
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	4.8KB
Key Capacity						
FIDO resident keys	Up to 8	Up to 8	Up to 8	Up to 8	Up to 8	Up to 32
PKI key containers	20	20	N/A	20	20	N/A
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	3.0.5
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	2.2.1
FIDO 2.0	✔	✔	✔	✔	✔	FIDO 2.1
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,	✔	✔	N/A	✔	✔	N/A
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

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	SafeNet IDPrime FIDO Bio
Certifications						
Chip: CC EAL6+	✔	✔	✔	✔	✔	✔
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	✔	N/A	N/A
Java platform + PKI applet: CC EAL5+/PP QSCD	✔	N/A	N/A	✔	N/A	N/A
eIDAS qualified for both eSignature and eSeal	✔	N/A	N/A	✔	N/A	N/A
French ANSSI	✔	N/A	N/A	✔	N/A	N/A
Physical Access - Mifare Classic & DesFire configurations	N/A	N/A	✔	✔	✔	N/A
Other PKI Features						
Onboard PIN policy	✔	✔	N/A	✔	✔	N/A
Multi-PIN support	✔	✔	N/A	✔	✔	N/A
Customization and branding	✔	✔	N/A	✔	✔	N/A
User verification	PIN	PIN	PIN	PIN	PIN	PIN and biometric fingerprint
Certifications						
FIDO supported in Windows 10 and other FIDO-compliant operating systems	✔	✔	✔	✔	✔	✔
PKI supported in Windows, macOS X, and Linux	✔	✔	N/A	✔	✔	N/A

Token – Form Factor

Product Characteristics	 SafeNet eToken FIDO	 SafeNet eToken FIDO	 SafeNet eToken Fusion	 SafeNet eToken Fusion (CC)
Form Factor	USB-A	USB-C	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	400 KB Java Flash
Free memory available for resident keys, certificates, additional applets & data	90 KB	55 KB	55 KB	73 KB
Key Capacity				
FIDO resident keys	Up to 8	Up to 8	Up to 8	Up to 8
PKI key containers	N/A	N/A	20	20
Standards Supported				
Java Card	3.0.4	3.0.4	3.0.4	3.0.4
Global Platform	2.2.1	2.2.1	2.2.1	2.2.1
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,	N/A	N/A	✔	✔
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	✔	✔

Token – Form Factor (continued)

Product Characteristics	 SafeNet eToken FIDO	 SafeNet eToken FIDO	 SafeNet eToken Fusion	 SafeNet eToken Fusion (CC)
Form Factor	USB-A	USB-C	USB-A or USB-C	USB-A or USB-C
Certifications				
Chip: CC EAL6+	✔	N/A	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	N/A	N/A
Other PKI 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 OneWelcome Identity & Access Management Solutions

Thales' digital identity products and solutions empower billions of people and things with digital identities worldwide. The Thales OneWelcome Identity & Access Management portfolio enables organizations to build frictionless, trusted and secure digital journeys for customers, business partners and employees. The OneWelcome Identity Platform provides a variety of capabilities from identity verification, single sign-on, passwordless and multi-factor authentication to fraud management, adaptive access, dynamic authorization and consent & preference management for the highest levels of assurance. More than 30,000 organizations trust us with their IAM and data security needs, enabling them to deliver secure digital services to their users.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

cpl.thalesgroup.com

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

Thales - February 2024 • GHv8