

Solution Brief

Thales FIDO2 Security Keys:

Stop Phishing Attacks
with Strong Passwordless
Multi-Factor Authentication

thalestct.com

THALES
Building a future we can all trust

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 security keys 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 security keys 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 Phishing-Resistant MFA

FIDO2 authentication removes the risk of account take-over by replacing vulnerable passwords with a phishing-resistant WebAuth 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 U2F certified and FIDO2/FIDO2.1 - Level 1 or Level 2. The combined PKI-FIDO keys are compliant with the US Executive Order mandate for phishing-resistant MFA and NIST regulations. They are FIPS 140-2, 140-3*, FIPS 201* (for PIV) 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.

*Certification in progress



Best in class security

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



Compliant with high security market standards

- U2F and FIDO2 certified
- FIPS and CC certified
- Compliant with US and EU regulations for phishing-resistant authentication
- Manufacturing in Europe and Trade Agreement Act (TAA) compliance in option

Enable Multiple User Authentication Journeys

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



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. In addition this card meets the highest security standards FIDO2.1 L2.



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 phishing-resistant MFA, enabling users such as frontline workers to securely access shared devices such as Windows PCs, mobile phones 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.



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

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 keys enable users to authenticate to any web resources from their mobile devices. This enables users to access their resources either by taping their contactless smart card or token on their device using NFC, or by plugging one of our wide range of USB-C tokens 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.

Devices, Platforms and Services Compatibility

Thales FIDO2 security keys are compatible with any cloud or on-premise system that supports the FIDO2 standard. Check Thales Website for a list of validated Identity Providers (IDP's), Credential Management Systems (CMS) and online services:

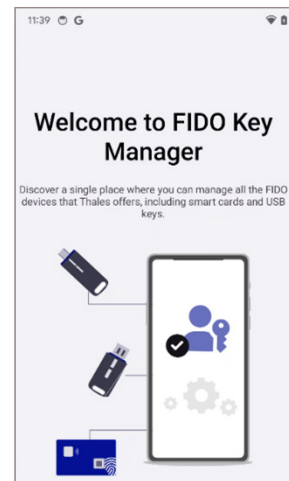
<https://cpl.thalesgroup.com/access-management/fido-compatible-services>

Thales FIDO security keys support a large variety of operating systems such as iOS, Android, Windows 11, 10, 8, Windows Server OS, macOS, and Linux making them compatible with the majority of devices used in an organization.

Configure easily and securely your Thales FIDO keys with SafeNet FIDO Key Manager

SafeNet FIDO Key Manager is a standalone offline application available on Mobile and Desktop platforms that allows administrators and end users to set up and manage Thales' FIDO USB tokens and Smartcards all along their life cycle.

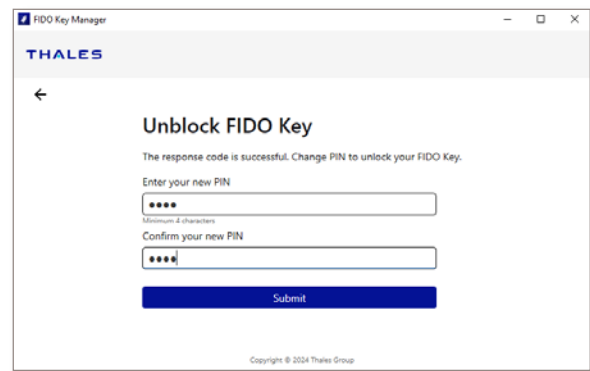
With SafeNet FIDO Key Manager, you can configure the Thales FIDO keys according to the FIDO2.1 specifications from FIDO Alliance and benefit from the unique set of additional FIDO enterprise features that Thales offer for better security and convenience. Your administrators and end users can install this application on their various platforms with no additional charge.



Control your FIDO keys' life cycle thanks to Thales FIDO Enterprise features .

Thales FIDO enterprise features allow organizations to manage their FIDO keys securely and easily throughout their life cycle. They add an administration layer and configuration policies to help IT teams deploy, administer, and support the end user. Beyond the FIDO Alliance FIDO2.1 specifications, Thales FIDO enterprise features offer organizations:

- **Better security** - Enforcing user verification during authentication from any device, managing the minimum PIN length and protecting the PIN policy set, preventing data in fido keys from malicious or non-intentional deletion.
- **Appropriate usage of organization assets** - Limiting the usage of the FIDO authenticators to a list of preferred services.
- **Reduced IT costs & better user experience** - Unlocking the FIDO key without resetting all key data, allowing end users to set and change their PIN code in self-service.



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



Enterprise FIDO Ready

- Comply with FIDO2.1 specifications
- Benefit from Thales FIDO Enterprise features
- Use SafeNet FIDO key Manager for free

Cards – Form Factor

Main Characteristics**	Mode			Certification		Applet	
Product List	Contact	Contactless (NFC)	Physical access	FIPS	Common Criteria	PKI	FIDO
IDPrime 931 FIDO	PKI	FIDO	Mifare Desfire	FIPS 140-2 L2 & L3		IDPrime 930	FIDO2.0 L1
IDPrime 3930 FIDO	FIDO, PKI	FIDO, PKI		FIPS 140-2 L2		IDPrime 3930	FIDO2.0 L1
IDPrime 3940 FIDO	FIDO, PKI	FIDO, PKI			✓	IDPrime 3940	FIDO2.0 L1
IDPrime 941 FIDO	PKI	FIDO	Mifare Desfire		✓	IDPrime 940	FIDO2.0 L1
IDPrime 3121 FIDO		FIDO	Mifare Desfire				FIDO2.0 L1
IDPrime FIDO Bio	PKI	FIDO					FIDO2.1 L1

Tokens – Form Factor

Main Characteristics**	Mode		Certification		Applet		
Product List	Contact/USB	Contactless (NFC)	FIPS	Common Criteria	PKI	FIDO	Thales FIDO enterprise features
eToken FIDO USB-A/USB-C	FIDO					FIDO2.0 L1	
eToken Fusion USB-A/USB-C	FIDO, PKI				IDPrime 930	FIDO2.0 L1	
eToken Fusion CC USB-A/USB-C	FIDO, PKI			✓	IDPrime 940	FIDO2.0 L1	
eToken Fusion FIPS USB-A/USB-C	FIDO, PKI		FIPS 140-2 L2 secure element		IDPrime 930	FIDO2.0 L1	
eToken Fusion NFC PIV USB-C	FIDO, PKI	FIDO, PKI	FIPS 140-3 L2* secure element		PIV 4.0	FIDO2.1 L1 and L2*	✓
eToken Fusion NFC FIPS USB-C	FIDO, PKI	FIDO, PKI	FIPS 140-2 L2 secure element		IDPrime 3930	FIDO2.0	

*Certification in progress

**For more details about each product, consult the FIDO2 Security Keys Specifications Brochure

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 Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com