

Thales Fusion Authenticators

Two Forms of Phishing Resistant Multi-Factor Authentication in a Single Device

thalestct.com

THALES
Building a future we can all trust

In today's environment, more than ever, organizations need strong, phishing-resistant, Certificate based Authentication (CBA). At the same time, organizations are expanding their digital transformation and 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 Fusion authenticators are offering organizations FIDO2 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 Fusion authenticators not only support existing CBA functionality, but they also have FIDO2 support for multiple applications at the same time. This allows the cost savings of the use of a single token 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 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 USB tokens and smart cards let you meet all your regulatory needs. They are FIDO2 and U2F certified. The combined PKI-FIDO use cases are compliant with the US Executive Order mandate for phishing-resistant MFA and NIST regulations. They are FIPS or Common Criteria (CC) certified, ANSSI qualified for the Java platform and the PKI applet. These authenticators are also FIDO Alliance certified for the FIDO2 applet as well as NPVP certified for the PIV 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 authenticators provide passwordless phishing-resistant 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 have the Fusion capability to 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 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 Fusion devices enable users to authenticate to any cloud resources from their mobile devices: either by tapping 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 authenticators to replace vulnerable passwords ensures that only authorized users can access privileged resources.

IDP and CMS compatibility

Thales Fusion authenticators are compatible with any cloud or on premise system that supports the FIDO2 standard.

Check Thales Website for a list of the tested and jointly validated Identity Providers (IDP's) and Credential Management Systems (CMS): thalesct.com/FIDO

Supported Platforms

Thales PKI/FIDO authenticators support a large variety of operating systems such as iOS, Android, Windows 11, 10, 8, Windows Server OS, macOS, and Linux.

Thales Fusion 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
- Smartcard as well as USB-A & C form factors

User convenience for better adoption

- Sensitive presence detector on USB Fusion key

Compliant with high security standards

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

Robustness & Scalability for a long life duration

- Hard molded plastic, tamper evident USB Fusion 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 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	✓	✓
User verification	PIN	PIN	PIN	PIN	PIN
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
Fusion**



**SafeNet
eToken
Fusion (CC)**

Form Factor	USB-A or USB-C	USB-A or USB-C
Contact (ISO 7816)	FIDO & PKI	FIDO & PKI
Contactless (ISO 14443)	N/A	N/A
Memory		
Memory chip	400 KB Flash	400 KB Flash
Free memory available for resident keys, certificates, additional applets & data	55 KB	73 KB
Key Capacity		
FIDO resident keys	Up to 8	Up to 8
PKI key containers	20	20
Standards Supported		
Java Card	3.0.4	3.0.4
Global Platform	2.2.1	2.2.1
FIDO 2.0	✓	✓
PKI	IDPrime 930	IDPrime 940
U2F	✓	✓
Base CSP minidriver (SafeNet minidriver)	✓	✓
Cryptographic algorithms (PKI)		
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	✓	✓

Token – Form Factor (continued)

Product Characteristics



SafeNet
eToken
Fusion



SafeNet
eToken
Fusion (CC)

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

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