Brochure

FIDO2 Security Keys Specifications

cpl.thalesgroup.com

THALES
Building a future we can all trust

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
Applet Features						
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
FIDO Thales Extended capabilities	N/A	N/A	N/A	N/A	N/A	N/A
FIDO Authentication algorithms	ECC 256 ECDSA	ECC 256 ECDSA	ECC 256 ECDSA	ECC 256 ECDSA	ECC 256 ECDSA	ECC 256 ECDSA
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
FIDO2.0	✔	✔	✔	✔	✔	FIDO2.1
U2F	✔	✔	✔	✔	✔	✔
Base CSP minidriver (SafeNet minidriver)	✔	✔	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
Cryptographic algorithms (PKI)						
Hash: SHA-1, SHA-256, SHA-384, SHA-512.	✔	✔	N/A	✔	✔	N/A
RSA: up to RSA 4096 bits	✔ (2) RSA 3K available on demand	✔	N/A	✔ (2) RSA 3K available on demand	✔	N/A
RSA OAEP & RSA PSS	✔	✔	N/A	✔	✔	N/A
P-256 bits ECDSA, ECDH P-384 & P-521 bits ECDSA	✔ (2) ECC 384 & 521 available on demand	✔	N/A	✔ (2) ECC 384 & 521 available on demand	✔	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
Certifications						
Chip: CC EAL6+	✔	✔	✔	✔	✔	✔
NIST certification	N/A	FIPS 140-2 L2 Certificate #4517	N/A	N/A	FIPS 140-2 L2 Certificate #4517	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	✔ 2018/24	N/A	N/A	✔ 2018/24	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

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
Physical Access						
Mifare Classic & DesFire configurations	N/A	N/A	Mifare 4k Desfire EV1 4k/8k	Mifare 4k Desfire EV1 4k/8k	Mifare 4k Desfire EV1 4k/8k	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
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	✔	✔	✔	N/A

Token – Form Factor

Product Characteristics	 SafeNet eToken FIDO	 SafeNet eToken FIDO	 SafeNet eToken Fusion	 SafeNet eToken Fusion Common Criteria (CC)	 SafeNet eToken Fusion FIPS	 SafeNet eToken Fusion NFC PIV	 SafeNet eToken Fusion NFC FIPS
Form Factor	USB-A	USB-C	USB-A or USB-C	USB-A or USB-C	USB-A or USB-C	USB-C	USB-C
Contact (ISO 7816)	FIDO	FIDO	FIDO & PKI	FIDO & PKI	FIDO & PKI	FIDO & PKI	FIDO & PKI
Contactless (ISO 14443)	N/A	N/A	N/A	N/A	N/A	FIDO & PKI	FIDO & PKI
Memory							
Memory chip	400 KB Flash	400 KB Flash	400 KB Flash	400 KB Flash	400 KB Flash	512 KB Flash	400 KB Flash
Free memory available for resident keys, certificates, additional applets & data	90 KB	55 KB	55 KB	52 KB	55 KB	110 KB	42 KB
Applet Features							
FIDO resident keys	Up to 8	Up to 8	Up to 8	Up to 8	Up to 8	Up to 100 [1]	Up to 25
PKI key containers	N/A	N/A	20	20	20	24 [1]	20
FIDO Thales Extended capabilities	N/A	N/A	N/A	N/A	N/A	✔	N/A
FIDO Authentication algorithms	ECC 256 ECDSA	ECC 256 ECDSA	ECC 256 ECDSA	ECC 256 ECDSA	ECC 256 ECDSA	ECC 256 ECDSA	ECC 256 ECDSA
Standards Supported							
Java Card	3.0.4	3.0.4	3.0.4	3.0.4	3.0.4	3.1.0	3.0.4
Global Platform	2.2.1	2.2.1	2.2.1	2.2.1	2.2.1	2.2.1 2.3 (CTLess)	2.2.1
FIDO2.0	✔	✔	✔	✔	✔	FIDO2.1	✔
PKI	N/A	N/A	IDPrime 930	IDPrime 940	IDPrime 930	PIV v4.0	IDPrime 3930
U2F	✔	✔	✔	✔	✔	✔	✔
Base CSP minidriver (SafeNet minidriver)	N./A	N./A	✔	✔	✔	✔	✔

Token – Form Factor (continued)

Product Characteristics	 SafeNet eToken FIDO	 SafeNet eToken FIDO	 SafeNet eToken Fusion	 SafeNet eToken Fusion Common Criteria (CC)	 SafeNet eToken Fusion FIPS	 SafeNet eToken Fusion NFC PIV	 SafeNet eToken Fusion NFC FIPS
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	✔	✔ (2) RSA 3K available on demand	✔	✔	✔
RSA OAEP & RSA PSS	N/A	N/A	✔	✔	✔	✔	✔
P-256 bits ECDSA, ECDH. P-384 & P-521bits ECDSA,	N/A	N/A	✔	✔ (2) ECC 384 & 521 available on demand	✔	✔	✔
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	✔	✔	✔	✔	✔
Certifications							
Chip: CC EAL6+	✔	✔	✔	✔	✔	✔	✔
NIST certification	N/A	N/A	N/A	N/A	FIPS 140-2 L2 Certificate #4517	FIPS 140-3 L2 In progress	FIPS 140-2 L2 Certificate #4517
Java platform: CC EAL5+/ PP java card certified	N/A	N/A	N/A	✔	N/A	N/A	N/A
Java platform + PKI applet: CC EAL5+/PP QSCD	N/A	N/A	N/A	✔ 2018/24	N/A	N/A	N/A

Token – Form Factor (continued)

Product Characteristics	 SafeNet eToken FIDO	 SafeNet eToken FIDO	 SafeNet eToken Fusion	 SafeNet eToken Fusion Common Criteria (CC)	 SafeNet eToken Fusion FIPS	 SafeNet eToken Fusion NFC PIV	 SafeNet eToken Fusion NFC FIPS
Certifications (continued)							
eIDAS qualified for both eSignature and eSeal	N/A	N/A	N/A	✔	N/A	N/A	N/A
French ANSSI	N/A	N/A	N/A	✔	N/A	N/A	N/A
FIDO2	L1	L1	L1	L1	L1	L1 L2 to come	L1
Physical Access							
Mifare Classic & DesFire configurations	N/A	N/A	N/A	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	✔	✔	✔	✔	✔
User verification	PIN	PIN	PIN	PIN	PIN	PIN	PIN
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	✔	✔	✔	✔	✔

(1) Memory is shared between PKI and Fido applications; number of PKI Key containers and FIDO Credential are triggered by free remaining memory at creation time.

(2) RSA 3K and ECC 384 & 521 are not in default standard CC profile. A customization is needed to get such algorithms

THALES

Building a future we can all trust

Contact us

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

cpl.thalesgroup.com