Brochure

FIDO2 Security Keys Specifications

cpl.thalesgroup.com

THALES
Building a future we can all trust

Smart Card – Form Factor

SafeNet Product Name	IDPrime 3940 FIDO	IDPrime 3930 FIDO	IDPrime FIDO Bio	IDPrime PIV FIDO	IDPrime FIDO	IDPrime PIV FIDO Enterprise	IDPrime FIDO Enterprise
Contact (ISO 7816)	FIDO & PKI	FIDO & PKI	FIDO	FIDO & PKI	FIDO	FIDO & PKI	FIDO
Contactless (ISO 14443)	FIDO & PKI	FIDO & PKI	FIDO	FIDO & PKI	FIDO	FIDO & PKI	FIDO
Memory							
Memory chip	400 KB Java Flash	400 KB Java Flash	206KB	512 KB Flash	512 KB Flash	512 KB Flash	512 KB Flash
Free memory available for resident keys, certificates, additional applets & data	73 KB	55 KB	4.8 KB	104 KB	159 KB	107 KB	162 KB
Applet Features							
FIDO discoverable credentials (resident keys)	Up to 8	Up to 8	Up to 32	Up to 100 [1]	Up to 100 [1]	Up to 100 [1]	Up to 100 [1]
PKI key containers	20	Up to 32	N/A	24 [1]	N/A	24 [1]	N/A
Thales FIDO Enterprise features	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	3.0.5	3.0.5	3.1.0	3.1.0	3.1.0	3.1.0
Global Platform	2.2.1	2.2.1	2.2.1	2.2.1 2.3 (CTLess)	2.2.1 2.3 (CTLess)	2.2.1 2.3 (CTLess)	2.2.1 2.3 (CTLess)
FIDO2.0 / FIDO 2.1	FIDO 2.0	FIDO 2.0	FIDO 2.1	FIDO 2.1	FIDO 2.1	FIDO 2.1	FIDO 2.1
PKI	IDPrime 3940	IDPrime 3930	N/A	IDPrime PIV 4.0	N/A	IDPrime PIV 4.0	N/A
U2F	✓	✓	✓	✓	✓	✓	✓
Base CSP minidriver (SafeNet minidriver)	✓	✓	N/A	✓	N/A	✓	N/A

Smart Card – Form Factor (continued)

SafeNet Product Name	IDPrime 3940 FIDO	IDPrime 3930 FIDO	IDPrime FIDO Bio	IDPrime PIV FIDO	IDPrime FIDO	IDPrime PIV FIDO Enterprise	IDPrime FIDO Enterprise
Cryptographic algorithms (PKI)							
Hash: SHA-1, SHA-256, SHA-384, SHA-512.	✓	✓	N/A	✓	N/A	✓	N/A
RSA: up to RSA 4096 bits	✓ (2) RSA 3K available on demand	✓	N/A	✓	N/A	✓	N/A
RSA OAEP & RSA PSS	✓	✓	N/A	✓	N/A	✓	N/A
P-256 bits ECDSA, ECDH P-384 & P-521 bits ECDSA	✓ (2) ECC 384 & 521 available on demand	✓	N/A	✓	N/A	✓	N/A
ECDH are available via a custom configuration	✓	✓	N/A	✓	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	✓	N/A
Symmetric: AES—For secure messaging and 3DES for Microsoft Challenge/Response only	✓	✓	N/A	✓	N/A	✓	N/A
Certifications							
Chip: CC EAL6+	✓	✓	✓	✓	✓	✓	✓
NIST FIPS 140-2/140-3	N/A	FIPS 140-2 L2 Certificate #4517	N/A	FIPS 140-3 L2 In progress platform - Certificate #4772	FIPS 140-3 L2 In progress platform - Certificate #4772	FIPS 140-3 L2 In progress platform - Certificate #4772	FIPS 140-3 L2 In progress platform - Certificate #4772
NIST FIPS 201 (PIV)	N/A	N/A	N/A	In progress	N/A	In progress	N/A
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	2018/24	N/A	N/A	N/A	N/A	N/A	N/A

Smart Card – Form Factor (continued)

SafeNet Product Name	IDPrime 3940 FIDO	IDPrime 3930 FIDO	IDPrime FIDO Bio	IDPrime PIV FIDO	IDPrime FIDO	IDPrime PIV FIDO Enterprise	IDPrime FIDO Enterprise
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
FIDO 2.0/ FIDO 2.1	FIDO 2.0 L1	FIDO 2.0 L1	FIDO 2.1 L2	FIDO 2.1 L1, L2 in progress	FIDO 2.1 L1, L2 in progress	N/A	N/A
Country of Origin (COO)	Poland	Poland	France	Poland	Poland	Poland	Poland
TAA Compliance	✓	✓	✓	✓	✓	✓	✓
Physical Access							
Mifare Classic & DesFire configurations	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Additional Features							
Onboard PKI PIN policy	✓	✓	N/A	✓	N/A	✓	N/A
PKI Multi-PIN support	✓	✓	N/A	✓	N/A	✓	N/A
Customization and branding	✓	✓	N/A	✓	N/A	✓	N/A
User verification	PIN	PIN	PIN and biometric fingerprint	PIN	PIN	PIN	PIN
VCI - Opacity Key and Pairing code (Ctless)	N/A	N/A	N/A	✓	N/A	✓	N/A
Biometry Match on Card (fingerprint)	N/A	N/A	✓	✓	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	✓	N/A

Smart Card – Form Factor (continued)

SafeNet Product Name	IDPrime CL 940 FIDO	IDPrime CL 930 FIDO	IDPrime DI 940 FIDO	IDPrime DI 930 FIDO
Contact (ISO 7816)	N/A	N/A	FIDO & PKI	FIDO & PKI
Contactless (ISO 14443)	FIDO & PKI	FIDO & PKI	FIDO & PKI	FIDO & PKI
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	73 KB	55 KB	73 KB	55 KB
Applet Features				
FIDO discoverable credentials (resident keys)	Up to 8	Up to 8	Up to 8	Up to 8
PKI key containers	20	Up to 32	20	Up to 32
Thales FIDO Enterprise features	N/A	N/A	N/A	N/A
FIDO Authentication algorithms	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	3.0.5
Global Platform	2.2.1	2.2.1	2.2.1	2.2.1
FIDO2.0 / FIDO 2.1	FIDO 2.0	FIDO 2.0	FIDO 2.0	FIDO 2.0
PKI	IDPrime 940	IDPrime 930	IDPrime 940	IDPrime 930
U2F	✓	✓	✓	✓
Base CSP minidriver (SafeNet minidriver)	✓	✓	✓	✓

Smart Card – Form Factor (continued)

SafeNet Product Name	IDPrime CL 940 FIDO	IDPrime CL 930 FIDO	IDPrime DI 940 FIDO	IDPrime DI 930 FIDO
Cryptographic algorithms (PKI)				
Hash: SHA-1, SHA-256, SHA-384, SHA-512.	✓	✓	✓	✓
RSA: up to RSA 4096 bits	✓ (2) RSA 3K available on demand	✓	✓ (2) RSA 3K available on demand	✓
RSA OAEP & RSA PSS	✓	✓	✓	✓
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	✓	✓	✓	✓
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	✓	✓	✓	✓
Certifications				
Chip: CC EAL6+	✓	✓	✓	✓
NIST FIPS 140-2/140-3	N/A	FIPS 140-2 L2 Certificate #4517	N/A	FIPS 140-2 L2 Certificate #4517
NIST FIPS 201 (PIV)	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	✓ 2018/24	N/A	✓ 2018/24	N/A

Smart Card – Form Factor (continued)

SafeNet Product Name	IDPrime CL 940 FIDO	IDPrime CL 930 FIDO	IDPrime DI 940 FIDO	IDPrime DI 930 FIDO
Certifications (continued)				
eIDAS qualified for both eSignature and eSeal	✓	N/A	✓	N/A
French ANSSI	✓	N/A	✓	N/A
FIDO 2.0 / FIDO 2.1	FIDO 2.0 L1	FIDO 2.0 L1	FIDO 2.0 L1	FIDO 2.0 L1
Country of Origin (COO)	France	France	France	France
TAA Compliance	✓	✓	✓	✓
Physical Access				
Mifare Classic & DesFire configurations	Desfire EV3 8k with an option for additional Mifare/Desfire configurations	Desfire EV3 8k with an option for additional Mifare/Desfire configurations	Desfire EV3 8k with an option for additional Mifare/Desfire configurations	Desfire EV3 8k with an option for additional Mifare/Desfire configurations
Additional Features				
Onboard PKI PIN policy	✓	✓	✓	✓
PKI Multi-PIN support	✓	✓	✓	✓
Customization and branding	✓	✓	✓	✓
User verification	PIN	PIN	PIN	PIN
VCI - Opacity Key and Pairing code (Ctless)	N/A	N/A	N/A	N/A
Biometry Match on Card (fingerprint)	N/A	N/A	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	✓	✓	✓	✓

Token – Form Factor

SafeNet Product Name	 eToken FIDO	 eToken FIDO	 eToken Fusion	 eToken Fusion CC	 eToken Fusion FIPS
Form Factor	USB-A	USB-C	USB-A or USB-C	USB-A or USB-C	USB-A or USB-C
Contact (ISO 7816)	FIDO	FIDO	FIDO & PKI	FIDO & PKI	FIDO & PKI
Contactless (ISO 14443)	N/A	N/A	N/A	N/A	N/A
Memory					
Memory chip	400 KB Flash	400 KB Flash	400 KB Flash	400 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
Applet Features					
FIDO discoverable credentials (resident keys)	Up to 8	Up to 8	Up to 8	Up to 8	Up to 8
PKI key containers	N/A	N/A	Up to 32	20	Up to 32
Thales FIDO Enterprise features	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
Java Card	3.0.4	3.0.4	3.0.4	3.0.4	3.0.5
Global Platform	2.2.1	2.2.1	2.2.1	2.2.1	2.2.1
FIDO2.0	FIDO 2.0	FIDO 2.0	FIDO 2.0	FIDO 2.0	FIDO 2.0
PKI	N/A	N/A	IDPrime 930nc (MD 4.5 applet)	IDPrime 940	IDPrime 930 (MD 4.5 applet)
U2F	✓	✓	✓	✓	✓
Base CSP minidriver (SafeNet minidriver)	N/A	N/A	✓	✓	✓

Token – Form Factor (continued)

SafeNet Product Name	 eToken FIDO	 eToken FIDO	 eToken Fusion	 eToken Fusion CC	 eToken Fusion FIPS
Applet Features (continued)					
Hash: SHA-1, SHA-256, SHA-384, SHA-512	N/A	N/A	✓	✓	✓
RSA: up to RSA 4096 bits	N/A	N/A	✓	RSA 3K available on demand [2]	✓
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
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	2018/24	N/A
Country of Origin (COO)	China or Cambodia	China or Cambodia	China	China	China or Cambodia
TAA Compliance	✓	✓	N/A	N/A	✓

Token – Form Factor (continued)

SafeNet Product Name	 eToken FIDO	 eToken FIDO	 eToken Fusion	 eToken Fusion CC	 eToken Fusion FIPS
Certifications (continued)					
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
FIDO 2.0/ FIDO 2.1	FIDO 2.0 L1	FIDO 2.0 L1	FIDO 2.0 L1	FIDO 2.0 L1	FIDO 2.0 L1
Additional Features					
Onboard PIN policy	N/A	N/A	✓	✓	✓
PKI Multi-PIN support	N/A	N/A	✓	✓	✓
Customization and branding	✓	✓	✓	✓	✓
User verification	PIN	PIN	PIN	PIN	PIN
VCI - Opacity Key and Pairing code (Ctless)	N/A	N/A	N/A	N/A	N/A
Biometry Match on Card (fingerprint)	N/A	N/A	N/A	N/A	N/A
Operating Systems					
FIDO supported in all FIDO-compliant operating systems including Windows 10 and 11	✓	✓	✓	✓	✓
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

Token – Form Factor (continued)

SafeNet Product Name	 eToken Fusion NFC FIPS	 eToken Fusion NFC PIV	 eToken FIDO NFC	 eToken Fusion NFC PIV Enterprise	 eToken FIDO NFC Enterprise
Form Factor	USB-A or USB-C	USB-A or USB-C	USB-A or USB-C	USB-A or USB-C	USB-A or USB-C
Contact (ISO 7816)	FIDO & PKI	FIDO & PKI	FIDO	FIDO & PKI	FIDO
Contactless (ISO 14443)	FIDO & PKI	FIDO & PKI	FIDO	FIDO & PKI	FIDO
Memory					
Memory chip	400 KB Flash	512 KB Flash	512 KB Flash	512 KB Flash	512 KB Flash
Free memory available for resident keys, certificates, additional applets & data	42 KB	104 KB	159 KB	107 KB	162 KB
Applet Features					
FIDO discoverable credentials (resident keys)	Up to 8	Up to 100 [1]	Up to 100 [1]	Up to 100 [1]	Up to 100 [1]
PKI key containers	Up to 32	24 [1]	N/A	24 [1]	N/A
Thales FIDO Enterprise features	N/A	N/A	N/A	✓	✓
FIDO Authentication algorithms	ECC 256 ECDSA	ECC 256 ECDSA	ECC 256 ECDSA	ECC 256 ECDSA	ECC 256 ECDSA
Standards Supported					
Java Card	3.0.4	3.1.0	3.1.0	3.1.0	3.1.0
Global Platform	2.2.1	2.2.1 2.3 (CTLess)	2.2.1 2.3 (CTLess)	2.2.1 2.3 (CTLess)	2.2.1 2.3 (CTLess)
FIDO 2.0/ FIDO 2.1	FIDO 2.0	FIDO 2.1	FIDO 2.1	FIDO 2.1	FIDO 2.1
PKI	IDPrime 3930 (MD 4.5 applet)	PIV v4.0	N/A	PIV v4.0	N/A
U2F	✓	✓	✓	✓	✓
Base CSP minidriver (SafeNet minidriver)	✓	✓	N/A	✓	N/A

Token – Form Factor (continued)

SafeNet Product Name	 eToken Fusion NFC FIPS	 eToken Fusion NFC PIV	 eToken FIDO NFC	 eToken Fusion NFC PIV Enterprise	 eToken FIDO NFC Enterprise
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
Certifications					
Chip: CC EAL6+	✓	✓	✓	✓	✓
NIST certification	FIPS 140-2 L2 Certificate #4517	FIPS 140-3 L2 In progress platform - Certificate #4772	FIPS 140-3 L2 In progress platform - Certificate #4772	FIPS 140-3 L2 In progress platform - Certificate #4772	FIPS 140-3 L2 In progress platform - Certificate #4772
Java platform: CC EAL5+/ PP java card certified	N/A	N/A	N/A	N/A	N/A
Java platform + PKI applet: CC EAL5+/PP QSCD	N/A	N/A	N/A	N/A	N/A
Country of Origin (COO)	France	France	France	France	France
TAA Compliance	✓	✓	✓	✓	✓

Token – Form Factor (continued)

SafeNet Product Name	 eToken Fusion NFC FIPS	 eToken Fusion NFC PIV	 eToken FIDO NFC	 eToken Fusion NFC PIV Enterprise	 eToken FIDO NFC Enterprise
Certifications (continued)					
eIDAS qualified for both eSignature and eSeal	N/A	N/A	N/A	N/A	N/A
French ANSSI	N/A	N/A	N/A	N/A	N/A
FIDO 2.0/ FIDO 2.1	FIDO 2.0 L1	FIDO 2.1 L1 L2 in progress	FIDO 2.1 L1 L2 in progress	N/A	N/A
Additional Features					
Onboard PIN policy	✓	✓	N/A	✓	N/A
PKI Multi-PIN support	✓	✓	N/A	✓	N/A
Customization and branding	✓	✓	✓	✓	✓
User verification	PIN	PIN	PIN	PIN	PIN
VCI - Opacity Key and Pairing code (Ctless)	N/A	✓	N/A	✓	N/A
Biometry Match on Card (fingerprint)	N/A	✓	N/A	✓	N/A
Operating Systems					
FIDO supported in all FIDO-compliant operating systems including Windows 10 and 11	✓	✓	✓	✓	✓
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