thalescpl.com

THALES

SafeNet IDPrime 940

Plug & Play Smart Cards

As cybercriminals get smarter and more determined than ever, more and more businesses and government agencies are coming to the realization that single-factor authentication solutions using simple usernames and passwords are not enough. Thales, the world leader in digital security, offers an extensive portfolio of identity and access management including a wide range of multi-factor authentication methods.

SafeNet IDPrime smart cards are designed for PKI-based applications, and come with a SafeNet minidriver that offers perfect integration with native support for Microsoft® environments (through Windows 10), without any additional middleware.

Compatible with Any Environment

In addition to its seamless integration into Windows ecosystems, the SafeNet IDPrime 940 is a contact interface smart card and is compatible with any environment through support by the SafeNet Authentication Client.

Strong Security

SafeNet IDPrime 940 Smart Cards are secured with both RSA up to 4096 and Elliptic curves algorithms, and address a range of use cases that require PKI security, including secure access, email encryption, secure data storage, digital signatures and secure online transactions for end users.

SafeNet IDPrime 940 is CC EAL5+ / PP Java Card certified for the Java platform and CC EAL5+ / PP QSCD certified for the combination of Java platform and PKI applet. SafeNet IDPrime 940 is qualified by the French ANSSI and is qualified according to the eIDAS regulations for both the eSignature and the eSeal applications.

Optional Onboard Applets

SafeNet IDPrime cards are multi-application smart cards, meaning they can have optional onboard applets for various functions. An MPCOS applet can be added to provide both e-purse and data management services.

Benefits

- Perfect integration in Windows environment—Certified and distributed by Microsoft, the SafeNet minidriver ensures immediate integration with all Microsoft environments, plus Plug & Play service up to Windows 10.
- Secure Flash mask chip—400 KB.
- Compatible with any environment—SafeNet IDPrime 940 is fully supported by the SafeNet Authentication Client.
- Compliant with eIDAS regulations—SafeNet IDPrime 940 is is fully qualified according the eIDAS regulations for both eSignature and eSeal applications, and is qualified by the French ANSSI. Its Java platform is also CC EAL5+ / PP Java Card certified.
- Multi-application smart cards—SafeNet IDPrime smart cards can have optional onboard applets for MPCOS e-purse.
- Enhanced cryptographic support—SafeNet IDPrime 940 offers PKI services with both RSA up to 4096 and elliptic curves up to 521 bits.

Product characteristics	
Memory	• SafeNet IDPrime 940 is based on a 400KB Flash memory chip. SafeNet IDPrime 940 comes as standard with 20 key containers. The memory available for certificates and other applets and data in this standard configuration is 73 KB.
Standards	• BaseCSP minidriver (SafeNet minidriver) • Global Platform 2.2.1 • Java Card 3.0.4 • ISO 7816
Operating systems	• Windows, MAC, Linux
Cryptographic algorithms	• 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-521bits 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
Communication protocols	• T=0, T=1, PPS, with baud rate up to 446 Kbps at at 3.57 MZ (TA1=97h)
Other features	• Onboard PIN Policy • Multi-PIN support • SafeNet IDPrime family of cards can be customized (card body and programming) to fit customers' needs.
Thales applets (optional)	
MPCOS	• E-purse & secure data management application
Chip characteristics	
Technology	• Embedded crypto engine for symmetric and asymmetric cryptography
Lifetime	• Minimum 500,000 write/erase cycles • Data retention for minimum 25 years
Certification	• CC EAL6+
Security	
	• SafeNet IDPrime smart cards include multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks. • The SafeNet IDPrime 940 is both CC EAL5+ / PP Java Card certified for the Java platform and CC EAL5+ / PP QSCD certified for the combination of Java platform plus PKI applet, is eIDAS qualified for both eSignature and eSeal, and qualified by the French ANSSI.

> thalescpl.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com