thalestct.com

THALES

SafeNet IDPrime 3940

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.

The SafeNet IDPrime 3940 is a dual-interface smart card, allowing communication either via a contact interface or via a contactless ISO 14443 interface, also compatible with some NFC readers.

Compatible with Any Environment

In addition to its seamless integration into Windows ecosystems, the SafeNet IDPrime 3940 is a dual interface smart card and is compatible with any environment through support by the SafeNet Authentication Client.

Strong Security

SafeNet IDPrime 3940 Smart Cards are secured with both RSA up to 4096 and Elliptic curves algorithms up to 521 bits, 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 3940 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 3940 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.

Product characteristics	
Memory	• SafeNet IDPrime 3940 is based on a 400 KB Java Flash memory chip. SafeNet IDPrime 3940 comes as standard with 20 key containers. The memory available for certificates and other applets & 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 and ISO 14443
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) • T=CL, ISO 14443 type A, with speed up to 848 Kbps
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 3940 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.

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

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com

encryption, key management, and access control requirements.

For more information, visit www.thalestct.com