

SafeNet IDPrime 3930

Plug & Play Smart Cards

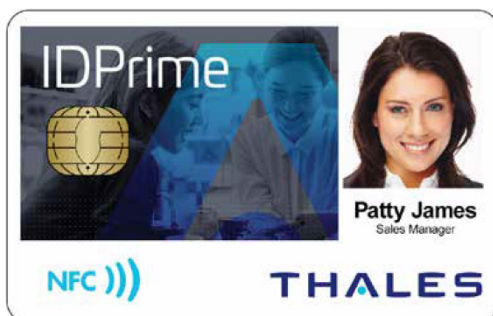
As cybercriminals get smarter and more determined than ever, more and more businesses and government agencies are coming to the realization that single-factor authentication solutions using simple usernames and passwords are not enough. Thales offers an extensive portfolio of identity and access management 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 (up to Windows 10), without any additional middleware.

The SafeNet IDPrime 3930 is a dual-interface smart card, allowing communication either via a contact interface or via a contactless ISO14443 interface, also compatible with some NFC readers.

Compatible with any environment

In addition to its seamless integration into Windows ecosystems, the SafeNet IDPrime 3930 is a dual interface smart card and is compatible with any environment through support by the SafeNet Authentication Client.



Benefits

- Dual interface—SafeNet IDPrime 3930 offers both an ISO7816 contact interface and an ISO14443 contactless interface, also compatible with some NFC readers.
- 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—400KB.
- Compatible with any environment—SafeNet IDPrime 3930 is fully supported by the SafeNet Authentication Client.
- Compliant with FIPS regulations—SafeNet IDPrime 3930 is FIPS 140-2 Level 2 certified for the combination of the Java platform and the PKI applet.
- Multi-application smart cards—SafeNet IDPrime smart cards can have optional onboard applets, for instance the MPCOS e-purse applet.
- Enhanced cryptographic support—SafeNet IDPrime 3930 offers PKI services with both RSA up to 4096 and elliptic curves up to 521 bits. SafeNet IDPrime 930
- Compliant with FIPS regulations—This card is FIPS 140-2 Level 2 certified for the combination of the Java platform and the PKI applet

Strong Security

SafeNet IDPrime 3930 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 3930 is FIPS 140-2 Level 2 certified for the combination of the Java platform and the PKI applet.

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.

Technical Specifications

Product Characteristics	
Memory	<ul style="list-style-type: none">SafeNet IDPrime 3930 is based on a 400 KB Java Flash memory chip. The memory available for certificates and other applets & data in this standard configuration is 78 KB.
Standards	<ul style="list-style-type: none">BaseCSP minidriver (SafeNet minidriver)Global Platform 2.2.1Java Card 3.0.5ISO 7816 and ISO 14443
Operating systems	<ul style="list-style-type: none">Windows, MAC, Linux
Cryptographic algorithms	<ul style="list-style-type: none">Hash: SHA-1, SHA-256, SHA-384, SHA-512.RSA: up to RSA 4096 bitsRSA OAEP & RSA PSSP-256 bits ECDSA, ECDH. P-384 & P-521 bits ECDSA, ECDHOn-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	<ul style="list-style-type: none">T=0, T=1, PPS, with baud rate up to 446 Kbps at 3.57 Mherz (TA1=97h)T=CL, ISO 14443 type A, with speed up to 848 Kbps
Other features	<ul style="list-style-type: none">Onboard PIN PolicyMulti-PIN supportSafeNet IDPrime family of cards can be customized (card body and programming) to fit customers' needs.
Thales Applets (optional)	
MPCOS	<ul style="list-style-type: none">E-purse & secure data management application
Chip Characteristics	
Technology	<ul style="list-style-type: none">Embedded crypto engine for symmetric and asymmetric cryptography
Lifetime	<ul style="list-style-type: none">Minimum 500,000 write/erase cyclesData retention for minimum 25 years
Certification	<ul style="list-style-type: none">CC EAL6+
Security	
Security	<ul style="list-style-type: none">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.SafeNet IDPrime 3930 is FIPS 140-2 Level 2 certified for the combination of the Java platform and the PKI applet.

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

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

[thalestct.com](#) [in](#) [t](#) [f](#) [v](#)