thalescpl.com

THALES

SafeNet IDCore 130

Java-based Smart Cards

Thales offers an extensive portfolio of identity and access management solutions including a wide range of multi-factor authentication methods.

The SafeNet IDCore 130 is the newest release in the IDCore portfolio and benefits from the latest release of Java Card technology standards. This Java Card platform is available from Thales as an open, multi-application card and is ideally suited for markets such as Identity or Security/Access. It is a Public Key Java Card (supporting both RSA and elliptic curves) that meets the most advanced security requirements of long-term, multi-application programs, including those being deployed by large global organizations. The SafeNet IDCore 130 is FIPS 140-2 Level 3 certified and complies with the latest international standards including:

- Java Card 3.0.5
- Global Platform 2.2.1
- ISO 7816

The SafeNet IDCore 130 is part of a portfolio of flexible open platform security solutions that can be easily customized to fit into any corporate or public sector environment. With a full range of multi-purpose smart cards, ID Core solutions support applications such as logical and physical access, PKI services and digital transactions. Additional benefits from Thales's proven Java Card experience and product offer include support, personalization services and integration to Card Management systems.

Flash memory

The SafeNet IDCore 130 has 146 KB flash memory available for applications and data, and ensures optimization of the memory allocation, extended multi-application capability, large data capacity and lifetime. Memory can be released to the platform in real-time upon object deletion and made available to the applets. In addition, an MPCOS applet can optionally be loaded into the flash memory, making application development easier. The MPCOS applet is fully compatible with the high performance native MPCOS Operating System and can be used for secure data management and e-purse applications.

Benefits

- **Flash memory**—Flash memory ensures optimization of the memory allocation, extended multi-application capability, large data capacity and lifetime. Easy application deployment thanks to the MPCOS Thales applet that can optionally be loaded in the flash memory.
- **Flexibility and modularity**—The open platform principle and interoperability enable the separation of application development (Applet) from the platform. This also supports aggressive time-to-market for introduction of new applications. Existing third-party applets from most vendors can be loaded and cards that are compatible with existing ones can be generated quickly.
- **High performance**—The SafeNet IDCore 130 virtual machine has been highly optimized to offer maximum software performance, making it one of the fastest Java Open Platforms available.

Optimized performance and flexibility

The SafeNet IDCore 130 virtual machine has been highly optimized to offer maximum software performance without compromising security. Combined with the latest generation of high performance silicon, this provides one of the fastest Java Open Platforms available. The open platform principle and interoperability enable the separation of application development (Applet) from the platform. This also supports aggressive time-to-market for introduction of new applications. Existing third-party applets from most vendors can be loaded and cards that are compatible with existing ones can be generated quickly.

No compromise on security

As reflected by the FIPS 140-2 Level 3 certification of its Java card Operating System, the SafeNet IDCore 130 platform implements the most advanced security countermeasures for enforcing protection of all sensitive data and functions in the card. The IDCore Java Card OS was developed by an industry-leading security team that designed it to implement counter measures against various threats, including side channel, invasive, advanced fault, and other types of attacks.

Product characteristics

Flash memory	• 146 KB Flash memory available for applications and data
Standards	• Java Card 3.0.5 • Global Platform 2.2.1 • ISO 7816
Cryptographic algorithms	• Symmetric: 3DES (ECB, CBC), AES (128, 192, 256 bits) • Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 • RSA: up to RSA 4096 bits • Elliptic curves: P-224, P-256, P-384, P-521 bits • On-card asymmetric key pair generation
Communication protocols	• T=0, T=1, PPS with baud rate up to 446 Kbps at at 3.57 MZ (TA1=97h)
Other OS features	• PK-based DAP (to control the applets that can be loaded on the card) • Delegated Management • Support of Extended Length APDU • Multiple Logical Channels • Real Garbage collector (memory space can be recovered after individual object deletion)

Thales Applets (optional)

MPCOS	• E-purse & secure data management application

Chip characteristics

Technology	• Flash memory • 16-bit microcontroller • 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

	• The SafeNet IDCore 130 includes multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks. • The SafeNet IDCore 130 is FIPS 140-2 Level 3 certified

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • 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