Product Brief

SafeNet IDCore 230/3230

Java-based Smart Cards

thalestct.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

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

The SafeNet IDCore cards 230/3230 benefit from the state-of -the-art FIPS 140-3-L3 security features, required by US federal departments and agencies. These security enhancements are the newest releases of IDCore OS in the IDCore FIPS portfolio and benefit from the latest release of Java Card technology standards. These IDCore Java card platforms are available from Thales as open, multi-application cards and are ideally suited for markets such as Identity or Security/Access. SafeNet IDCore 230/3230 are public key Java Cards (supporting both RSA and elliptic curves) that meet the most advanced security requirements of long-term, multi- application programs, including the ones deployed by large global organizations.

SafeNet IDCore 230/3230 are FIPS 140-3 Level 3 certified and comply with the latest international standards including:

- Java Card 3.1.0
- Global Platform 2.2.1
- ISO 7816
- ISO 14443 for SafeNet IDCore 3230 only

These cards are 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, IDCore 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.

SafeNet IDCore 230 - Contact Card

SafeNet IDCore 3230 - Contact/Contactless Card

Communication interface

The SafeNet IDCore 230 is a contact interface smart card.

The SafeNet IDCore 3230 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.

Flash memory

The SafeNet IDCore 230/3230 have 197 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.

No compromise on flexibility

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.

State-of-the-art security

As reflected by the new FIPS 140-3 Level 3 certification of its Java card Operating System, the SafeNet IDCore 230/3230 platform implement the most advanced security countermeasures for enforcing protection of all sensitive data and functions in the card. The IDCore Java Card OS has been developed by an industry-leading security team and designed to implement countermeasures against various threats, including side channel, invasive, advanced fault, and other types of attacks.

Benefits

- **Flash memory:** Flash memory ensures optimization of the memory allocation, extended multi-application capability, large data capacity and lifetime. Easy application deployment is provided 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 230/3230 virtual machine benefits from the newest technologies, enhancing security and performances simultaneously.

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

Product characteristics

Flash memory	• 197 KB Flash memory available for applications and data
Standards	• Java Card 3.1.0 • Global Platform 2.2.1 and partially 2.3 • ISO 7816
Cryptographic algorithms	• Symmetric: 3DES (ECB, CBC), AES (128, 192, 256 bits) • Hash: SHA-1, SHA2 (224, 256, 384, 512), SHA3 (224, 256, 384, 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) • T=CL, ISO 14443 type A & type B, with speed up to 848 Kbps *
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) • OPACITY secure contactless protocol *

Thales applets (optional)

MPCOS	• E-purse & secure data management application

Chip characteristics

Technology	• 40nm structure and flexible Secure Flash memory • Fast ARM 32bit CPU with crypto co-processors • 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 230/3230 include multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks. • The SafeNet IDCore cards 230/3230 will benefit from the state-of -the-art FIPS 140-3-L3 security features, required by US federal departments and agencies.**

*Featured in SafeNet IDCore 3230 only ** NIST certification is in process