
IDCore 140 Java-based Smart Card

Brand: Gemalto

Product Code: SMAO1039582



Short Description

IDCore 140 Java Card

IDCore 140 is a contact open smart card, compliant with Java Card 3.0.4 and Global Platform 2.2.1 standards. Offering enhanced cryptographic support, this smart card is CC EAL6+/PP Javacard certified for the Java platform and CC EAL6+ certified for the chip.

Description

IDCore 140 Java Card

IDCore 140 is a contact open smart card, compliant with Java Card 3.0.4 and Global Platform 2.2.1 standards. Offering enhanced cryptographic support, this smart card is CC EAL6+/PP Javacard certified for the Java platform and CC EAL6+ certified for the chip.

IDCore 140 Smart Card

SafeNet IDCore 140 is the newest release in the SafeNet IDCore portfolio and benefits from the latest release of Java Card technology standards. This Java Card platform is available as an open, multi-applicationcard 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 140 is CC EAL5+ / PP Java Card certified and complies with the latest international standards including:

- Java Card 3.0.4
- Global Platform 2.2.1
- ISO 7816

The SafeNet IDCore 140 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, SafeNet IDCore solutions support applications such as logical and physical access, PKI services and digital transactions. Additional benefits from Smartjac's proven Java Card experience and product offer include support, personalization services and integration to Card Management systems.

Flash memory

The SafeNet IDCore 140 has 160 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 Gemalto 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 140 Virtual machine has been highly optimized to offer maximum software performance, making it one of the fastest Java Open Platforms available.

Performance and Flexibility

The SafeNet IDCore 140 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 CC EAL5+ / PP Java Card certification of its Java Card Operating System, the SafeNet IDCore 140 platform implements the most advanced security counter measures for enforcing protection of all sensitive data and functions in the card. The SafeNet 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.

Specifications

Product characteristics

Flash memory

160KB Flash memory available for applications and data

Standards

Java Card 3.0.4

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)

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 140 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 140 is CC EAL5+ / PP Java Card certified