

Java Card Platform – CC EAL5+ Certified

The **IDCore 3010** benefits from the latest standard release of Java Card technology, and embed all the recent cryptographic algorithms, including elliptic curves.

This Java Card platform is available from Gemalto 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.

IDCore 3010 is a dual interface (**contact & contactless**) smartcard that complies with the latest international standards:

- JavaCard 2.2.2 (& 3.0.1 for the elliptic curves and other recent algorithms).
- Global Platform 2.1.1 (amendment A), and Global Platform 2.2 for SCP03 protocol.
- ISO 7816
- ISO 14443

IDCore 3010 Operating System is also **certified CC EAL5+ with Javacard Protection Profile**.

Key Benefits

Available with optional Gemalto applets:

- MPCOS applet is fully compatible with high performance native MPCOS and available for data management and/or purse applications.
- OATH OTP applet offers One Time Password services.

Large memory

extends multi-application capability, data capacity and lifetime. The 80KB of memory of IDCore 3010 is available to store application data, and host additional applets for application evolution during the expected card lifetime.

Performance

IDCore 3010 virtual machine has been 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.

Part of a full range of product and services

Additional benefits from Gemalto's proven Java Card experience and product offering include support, middleware, personalization services and integration to Card Management systems.

Flexibility and Modularity

The open platform principle and interoperability enable 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 Javacard** certification, the IDCore 3010 platform implements the most advanced security countermeasures for enforcing protection of all sensitive data and functions in the card.

IDCore 3010 – Rev B

Product characteristics	
EEPROM Memory	80KB
Standards	Java Card Virtual Machine, compliant with JC2.2.2 (and JC3.0.1 for ECC and other recent algos) Card Management & API compliant with GP2.1.1. Full support of SCP01, SCP02 & SCP03
Cryptographic algos	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: up to P-521 bits On-card asymmetric key pair generation (RSA up to RSA2048 & Elliptic curves)
Communication protocols	T=0, T=1, PPS, with baud up to 230 Kbps T=CL type A & type B, with speed up to 848 Kbps
Other features	PK-based DAP for better control of applets that can be loaded on the card Delegated Management Support of Extended Length APDU Multiple Logical Channel Real Garbage collector
Gemalto optional applets	
OATH OTP	One Time Password application
MPCOS	E-purse & secure data management application
Chip characteristics	
Technology	80K EEPROM area Embedded crypto engine for symmetric and asymmetric cryptography
Lifetime	Minimum 500,000 write/erase cycles Data retention for minimum 25 years
Certification	CC EAL5+
Security	
<p>The IDCore 3010 smart cards include multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks.</p> <p>The IDCore 3010 Operating System is also certified CC EAL5+ with Javacard Protection Profile.</p>	