## Java Card Platform – FIPS Certified

The **IDCore 3020** 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 3020 is a dual interface (**contact & contactless**) smartcard that complies with the latest international standards:

- Java Card 2.2.1, and JavaCard 2.2.2 & 3.0.1 for the elliptic curves algorithms.
- Global Platform 2.1.1 (amendment A), and Global Platform 2.2 for SCP03 protocol.
- ISO 7816 parts 1, 2, 3, 4, 5, 6, 8 & 9
- ISO 14443

IDCore 3020 is also both **FIPS140-2 level 3** and **ICP Brazil** certified.

## Key Benefits

**Available with embedded Gemalto applets**:
- PIV applet offers full compliancy to FIPS 201 standard.
- 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.

**Very large memory** extends multi-application capability, data capacity and lifetime.
The 128KB of memory of IDCore 3020 is available to store application data, and host additional applets for application evolution during the expected card lifetime.

**Performance**
IDCore 3020 virtual machine has been optimized to offer maximum software performance without compromising security.

**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 FIPS-140 certification, the IDCore 3020 platform implements the most advance security countermeasures for enforcing protection of all sensitive data and functions in the card.

# IDCore 3020

| Product characteristics | |
|---|---|
| Memory | EEPROM size: 128K Bytes |
| Standards | Java Card Virtual Machine, compliant with JC2.2.1 (and JC2.2.2/3.0.1 for ECC algos)<br>Card Management & API compliant with GP2.1.1 (and GP 2.2 for SCP03). Full support of SCP01, SCP02 & SCP03. |
| Cryptographic algos | Symmetric: 3DES (ECB, CBC), AES (128, 192, 256 bits)<br>Hash: SHA-1, SHA-256, SHA-384, SHA-512.<br>**RSA**: up to RSA 2048 bits<br>**Elliptic curves**: P-160, P-192, P-224, P-256, P-384, P-521 bits<br>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<br>T=CL type A & type B, with speed up to 848 Kbps<br>Mifare emulation |
| Other features | PK-based **DAP** for better control of applets that can be loaded on the card<br>Delegated Management<br>Multiple Logical Channel<br>Real Garbage collector (JC 2.2 specification) |
| **Gemalto optional applets** | |
| OATH OTP | One Time Password application |
| MPCOS | E-purse & secure data management application |
| PIV | For full compliancy to FIPS 201 standard |
| **Chip characteristics** | |
| Technology | Embedded crypto engine for symmetric and asymmetric cryptography<br>True random number generator |
| Lifetime | Minimum 500,000 write/erase cycles<br>Data retention for minimum 25 years |
| Certification | **CC EAL5+** |
| **Security** | |
| The IDCore 3020 smart cards include multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks.<br>The IDCore 3020 is both **FIPS 140-2 Level 3** and **ICP Brazil** certified. | |