Java Card Platform

The **IDCore 40** smartcard benefits from the latest release of Java Card technology standards. 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 40 complies with the latest international standards:

- Java Card 2.2.2 (& 3.0.1 for the elliptic curves algorithms)
- Global Platform 2.1.1 (amendment A)
- ISO 7816

The IDCore 40 java card Operating System is both **CC EAL5+ / PP Javacard** certified and **FIPS 140-2 Level 3** certified.

Key Benefits

Easy application deployment thanks to the **Gemalto applet** that can optionally be installed:
- 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.

Optimized memory (with MPCOS applet code stored in ROM area) extends multi-application capability, large data capacity and lifetime.

Real Garbage Collector
Memory can be released to the platform in real-time upon object deletion and made available to the applets.

Performance
IDCore 40 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.

Part of a full range of product and services
Additional benefits from Gemalto's proven Java Card experience and product offer include support, personalization services and integration to Card Management systems.

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.

No compromise on security
As reflected by the **CC EAL5+ / PP Javacard** certification and the **FIPS 140-2 Level 3** certification of its java card Operating System, the IDCore 40 platform implements the most advanced security countermeasures for enforcing protection of all sensitive data and functions in the card.

Product characteristics	
EEPROM Memory	**80 KB**
Standards	JC2.2.2 (and JC3.0.1 for ECC algos) GP2.1.1 (with SCP01 and SCP02)
Cryptographic algos	Symmetric: 3DES (ECB, CBC), AES (128, 192, 256) Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. RSA: up to RSA 2048 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 230 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)
Gemalto applets (optional)	
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 minimum 25 years
Certification	CC EAL5+
Security	
The IDCore 40 includes multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks. The IDCore 40 java card Operating System is both **CC EAL5+ / PP Javacard** certified and **FIPS 140-2 Level 3** certified	