IDCore

Flexible, Trusted Open Platform

FINANCIAL SERVICES & RETAIL

ENTERPRISE > SOLUTION

GOVERNMENT

TELECOMMUNICATIONS

TRANSPORT

gemalto

security to be free

IDCore

Flexible, Trusted Open Platform

The heart of problem

An increasing number of businesses and government agencies are coming to the realization that single authentication solutions using simple user names and passwords are not enough to keep today's cyber criminals at bay. And even though implementing stronger password solutions are better, they are simply not enough. Requiring long, cumbersome passwords with multiple characters, letters and numbers, typically results in users writing down their passwords and placing them near their computer. Scary to think the walls of an entire network could crumble because of what was jotted down on a single sticky note.

Strong authentication, combining something you know (PIN) with something you have (smart card or token) is the best method to ensure your networks are protected and cannot be compromised by the actions of a careless user. Gemalto, the world leader in digital security, offers a wide array of strong authentication solutions to help address this critical issue.

IDCore is a flexible open platform solution 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 and are available in credit card or USB key form factors for maximum use case support.

Integrate physical & logical access control

IDCore smart cards are a flexible platform give you the option to combine contact and contactless technologies so the same card can be used for access to both physical facilities and logical information assets throughout the organization. These hybrid cards use separate chips to control the contact and contactless interfaces which makes integrating legacy applications straightforward and efficient. It can be integrated with contactless technologies such as Mifare, DESFire, Legic Advant and HID Prox / Indala / iClass. In addition, this open platform can be customized to provides dual functionality to manage both contact and contactless interfaces and associated applications with a single chip.

IDCore is a flexible open platform solution that can be easily customized to fit into any corporate or public sector environment.

No compromise on security

IDCore smart cards using a Java Operating System incorporate advanced microcontrollers with strong security certification. The IDCore Java Card OSwas 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. The IDCore Java Card OS meets the industry's most stringent security certifications, such as FIPS 140-2 level 3, FIPS 201, and CC EAL4+ / PP SSCD.

Modular and flexible architecture

IDCore solutions are easy and fast to update through an open OS architecture that separates the platform from the application. This partitioning also reduces migration constraints, even after initial card issuance. Compliant applications can be loaded and cards that are compatible with existing ones can be produced quickly. Java Card technology offers fast deployment cycles for application development with rapid prototyping and implementation. No long and expensive re-masking is necessary; new applets are simply loaded in the Java Card memory. In addition, this technology enables various business models between issuer, application providers and operators, thanks to multiple security domains and dynamic application partitioning. The IDCore's virtual machine has been highly optimized to maximize software performance without compromising security. Combined with the latest generation of high performance microcontrollers, it provides one of the fastest Java Open Platforms available.

A strong foundation for any environment

Complete solutions can be built using IDCore products with other Gemalto digital security solutions including smart card readers, strong authentication and digital signature software, as well as smart card management systems. To allow you to get the solution that best fits your needs, several applets can be pre-loaded to provide a flexible multi-application platform for current requirements and future needs during the card lifecycle. With the most secure, flexible platform on the market, Gemalto offers a series of IDCore applets for authentication, access control, identification, digital signature, e-purse, data storage, customer loyalty, and other services.

Java Card Platform

The **IDCore 10** 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 10 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

Key Benefits

Easy application deployment thanks to the **Gemalto applets** 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.
- OATH OTP applet offers One Time Password services

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 10 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
The IDCore 10 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
OATH OTP	One Time Password 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 10 includes multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks.	

Java Card Platform

The **IDCore 30** 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 30 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 30 is **FIPS 140-2 Level 3** certified (pending)

Key Benefits

Flash memory ensures optimization of the memory allocation, extended multi-application capability, large data capacity and lifetime.

Easy application deployment thanks to the **Gemalto applets** that can optionally be loaded in the flash memory:
- 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.
- OATH OTP applet offers One Time Password services.

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

Performance
IDCore 30 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 **FIPS 140-2 Level 3** certification of its java card Operating System, the IDCore 30 platform implements the most advanced security countermeasures for enforcing protection of all sensitive data and functions in the card.

IDCore 30

Product characteristics	
Flash Memory	**122 KB Flash memory** available for applications and data
Standards	JC2.2.2 (and JC3.0.1 for ECC algos) GP2.1.1 (with SCP01 and SCP03)
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 **460Kbps**
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)	
OATH OTP	One Time Password application
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 IDCore 30 includes multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks. The IDCore 30 is **FIPS 140-2 Level 3** certified (pending)	

IDCore 40

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 is **CC EAL5+ / PP Javacard** certified and is also currently being **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 is **CC EAL5+ / PP Javacard** certified, and is also currently being **FIPS 140-2 Level 3** certified	