

Trusted Open Platform (TOP) Java Cards

||||| A complete family of secure multi-application smart cards



FINANCIAL SERVICES & RETAIL

ENTERPRISE > PRODUCT

INTERNET CONTENT PROVIDERS

PUBLIC SECTOR

TELECOMMUNICATIONS

TRANSPORT

Trusted Open Platform
Java Card



Alexandra
Miller



>network identity >smart card security >cryptographic capability

www.gemalto.com

gemalto
security to be free

gemalto
security to be free

Trusted Open Platform (TOP) Java Cards

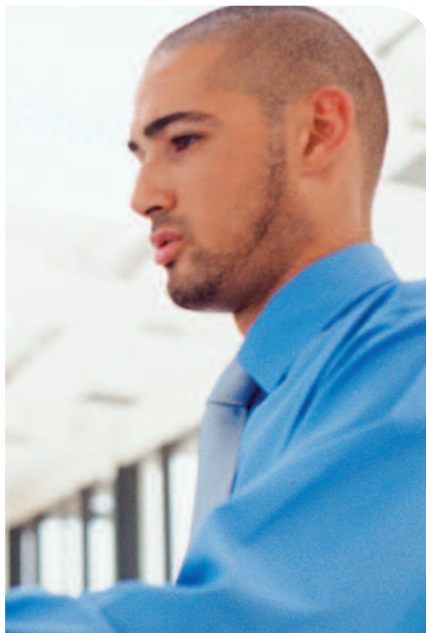
||||| A complete family of secure multi-application smart cards

Gemalto's Trusted Open Platform (TOP) family of Java Cards offers a comprehensive array of features and options for logical and physical access control applications. Support for key Java Card (JC) and Global Platform (GP) specifications, a broad range of memory capacities, and extensive set of proven applets make TOP Java Cards an optimal platform for business and public sector smart card deployments. They are ideally suited for all applications that require secure identity credentials, including one time password authentication, Public Key Infrastructure (PKI) services, digital transactions, e-purse and physical access control.

The perfect match for every smart card deployment project

> TOP Java Card family benefits:

- Full compliance with JC 2.2 and GP 2.1 specifications maximizes interoperability and application compatibility.
- EEPROM capacities from 36 KB to 128 KB and advanced memory management support a broad range of application requirements.
- Multiple applets can be pre-loaded to streamline development and accelerate the deployment process.
- Contact, contact-less, dual and USB interface options provide unsurpassed versatility.
- Available in credit card or USB key form factors for maximum use case support.
- Highest level of security is assured – certified for CC EAL4+, FIPS 140-2 level 3 and FIPS 201 specifications.



The Gemalto TOP Java Card family includes a full range of multi-purpose smart cards.

TOP Java Cards support applications such as logical and physical access, PKI services and digital transactions with a single card or USB key form factor.

Complete solutions can be built using TOP Java Cards with other Gemalto digital security products, including smart card readers, strong authentication and digital signature software, and smart card management systems. Gemalto also offers Allynis services for TOP Java Cards to assist with card issuance, customized personalization, and support services.

A versatile multi-application platform

Several applets can be pre-loaded to provide a flexible multi-application platform for current requirements and future needs during the card lifecycle. Gemalto offers a series of TOP Java Card applets for authentication, access control, identification, digital signature, e-purse, data storage, customer loyalty, and other services. They include:

- Access and Classic applets for PKI applications with PKCS#11, CSP and Microsoft® BaseCSP support
- OATH (Initiative for Open Authentication) compliant one-time password applet for use with Gemalto Strong Authentication Server
- MPCOS (Multi-application Payment Chip Operating System) applet for secure data management and/or e-purse applications
- Biometric Match on Card applet

These applets are stored in the microcontroller's ROM memory so full EEPROM capacity is preserved for applications and data that can be loaded at anytime, either pre- or post issuance. Multiple applications can be built using a combination of Gemalto applets and others provided by customers, Gemalto partners and third-party developers.

Open and compliant with industry standards

TOP Java Cards comply with the latest Java Card and Global Platform specifications to maximize interoperability across a full range of solution components and applications. This makes application development and management faster and easier by enabling code reuse and legacy application updates. As a thought leader and participant in several committees driving industry standards, Gemalto is also helping define platform enhancements that benefit all organizations that use Java Card technology.

Modular and flexible architecture

TOP Java Cards enable easy and fast updates 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.

Integrate Physical & Logical Access Control

TOP Java Cards can combine contact and contact-less technologies so the same card can be used for access to both physical facilities and logical information assets throughout the organization.

The hybrid TOP Java Card uses separate chips to control the contact and contact-less interfaces which makes integrating legacy applications straightforward and efficient. It can be integrated with contact-less technologies such as Mifare, DESFire, Legic Advant and HID Prox / Indala / iClass. In addition, a dual interface TOP Java Card that manages both contact and contact-less interfaces and associated applications with a single chip is also available.

No Compromise on Security

TOP Java Cards incorporate advanced microcontrollers with strong security certification. The TOP Java Card Operating System 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 attack. The TOP Java Card Operating System meets the industry's most stringent security certifications, such as FIPS 140-2 level 3, FIPS 201, and CC EAL4+ / PP SSCD.

High Performance Assured

The TOP Java Card 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.

Technical specifications

> GENERAL FEATURES

- Full compliance with JC2.2 and GP2.1
- Cryptographic algorithms: 3DES (ECB, CBC), AES (128-, 192-, 256-bit), RSA up to 2048 bit, SHA-1 & SHA-256
- On-card asymmetric key pair generation
- EEPROM size (available for application data): 36K to 128K
- PK-based Data Authentication Pattern
- Delegated Management
- Multiple Logical Channel
- ISO 7816 contact interface
- ISO 14443 contact-less interface
- USB key form factor available with optional Gemalto USB Shell or eSeal token
- Protocols: T=0, T=1, T=CL, PPS

Pre-loaded applets in ROM

- Classic applet
- MPCOS applet
- OATH OTP applet
- Biometric Match On Card applet

Security

- Chip CC EAL4/5+ certified
- Operating System FIPS 140-2 Level 3 certified
- Operating System CC EAL4+ / PPSSCD certified

Performance

- TOP Java Card virtual machine is optimized for maximum software performance

Memory management

- Applet deletion
- Real time garbage collector



TOP Java Card	EEPROM*	Interface Options	Java Card release	Global Platform release	Certification	Gemalto Applets in ROM
TOP IM FIPS CY2	68 KB	Contact, Contact-less, USB form factor	2.1	2.0.1	FIPS 140-2 Level 3	PBI Biometric Match on Card (optional)
TOP IM GX4	72 KB	Contact, Contact-less, USB form factor	2.2	2.1.1	FIPS 140-2 Level 3 (option) CC EAL4+ / PPSSCD with Classic applet (option)	Classic v1, v2, MPCOS, PBI Biometric Match on Card (optional)
TOP IS GX4	36 KB	Contact, Contact-less, USB form factor	2.2	2.1.1	FIPS 140-2 Level 3 (option)	Classic v1, v2, MPCOS, PBI Biometric Match on Card (optional)
TOP DM GX4	72 KB	Contact, Contact-less, Dual, USB form factor	2.2	2.1.1	FIPS 140-2 Level 2 (including PIV applet)	Classic v1, MPCOS
TOP DL GX4	128 KB	Contact, Contact-less, Dual, USB form factor	2.2	2.1.1	FIPS 140-2 Level 2 (including PIV applet)	Classic v1, MPCOS

||||| The world leader in digital security

www.gemalto.com

gemalto
security to be free