

Java Card Platform, basis for NIST certified FIPS 201 card

TOP DM GX4 (earlier named GemCombi'Xpresso R4) was introduced in 2005 and benefits from the latest standards release and **dual interface** that provides operation of the card either through a **contact** interface or a **contactless** one. The card with applet (which makes up the **SafesITe PIV TPC DM FIPS** smart ID badge) has achieved Personal Identification Verification (PIV) compliance certification from the US National Institute of Standards and Technology (NIST), thus complying with the FIPS 201 and FIPS-140 standard in line with HSPD 12.



This Java Card platform is also available from Gemalto as an open multiapplication card. It particularly aims at addressing markets such as Identity, Security/Access or Healthcare. It is a Public Key Java Card designed to meet the most advanced security requirements of long term multi-application programs such as the ones launched by government & large corporations. It complies with the latest international standards:

- **Java Card 2.2.1**
- **Global Platform 2.1.1** (amendment A)
- **ISO 7816 parts 1, 2, 3, 4, 5, 6, 8 & 9 for contact interface**
- **ISO 14443 part 1, 2, 3 and 4 for contactless interface (type A)**

The product passed FIPS140-2 level 2 certifications one with the SafesITe FIPS 201 applet.

Key Benefits

Dual Interface communication

Permits both, operation in contact mode for conventional smartcard applications where reader cost is a concern (ex: Digital signature), and also operation in contactless mode that is more and more demanded for user convenience in Identification applications and Access-Control.

Ready available ROMed* reference Applets without impairing available EEPROM:

GemSafe V2 for digital signature, **GemSafe V1** also available for previous systems compatibility
MPCOS fully compatible with high-runner native MPCOS,
 an **ICAO** compliant applet allowing interoperability in contactless mode with electronic passport.

Very large memory extends application, data capacity and lifetime

Due to ROMed applets about 68KB is still available to store data and to host additional applets to cope with application evolutions foreseen during the expected card lifetime.

Real Garbage Collector

New in JC2.2 spec, platform memory can be real-time released to the platform at object deletion and made available to the applets.

Part of a full range of product and services

Benefits from Gemalto proven JavaCard experience and environment offer: Support and training, Development kit, Middleware, Perso services, Card Management system ...

TOP DM GX4 provides backward compatibility for running applets developed for previous GXP3.x, JC2.1, GP2.0.1' products. Proprietary commands are available to significantly simplify migration of issuance and personalization systems.

Flexibility and Modularity

Open platform principle and interoperability allow separation of application development (Applet) from the platform. Aggressive time to market for introduction of new applications. Existing third party applets from most vendors can be loaded and thus generate cards compatible with already existing ones.

No compromise on security

Acknowledged by FIPS-140 certification, the platform implements most advance security countermeasures enforcing protection of all sensitive data and function in the card.



TOP DM GX4 Technical Specifications (Preliminary)

General Features

- JavaCard Virtual Machine, RTE and API compliant with **JC2.2.1**
- Card Management & API compliant with **GP2.1.1**
SCP01 and SCP02 supported with scripting capability of Amendment A
- Cryptographic algorithms: 3DES (ECB, CBC), AES (128, 192, 256), **RSA up to 2048bit**, SHA-1
- On-card asymmetric **key pair generation**
- PK-based **DAP** (for better control of applets that can be loaded on the card)
- Delegated Management
- Multiple Logical Channel (permit selection of multiple applets at the same time)
- Contact Interface :
Protocols: T=0, T=1, PPS
Baud rates up to 230Kbps
- **Contactless Interface:**
ISO14443 type-A communication mode
ISO14443-4, T=CL supported
Mifare-1 emulation mode on a part of the memory

Pre-loaded applets in ROM*

- GemSafe V1 applet
- GemSafe V2 applet also present
- MPCOS applet
- ICAO applet

Optional EEPROM loaded applet for FIPS-201 compliance

For delivery of a FIPS-201 certified card, the certified Gemalto applet is loaded in EEPROM and pre-personalized to provide a SafesITe FIPS-201 card.

Ordering Options

The exact product configuration is defined at card manufacturing depending on ordering options. It particularly defines the exact combination of ROMed applets that will be left as "loaded" in the delivered product. Other applets are logically deleted.

Chip characteristics

TOP DM GX4 runs on the Philips P5CD072 chip:

- Last generation Smartcard micro-controller
- EEPROM size: up to 72K Bytes
- Dual Interface Contact and Contactless
- Embedded security controller for asymmetric cryptography
- True random generator
- CC EAL5+ certified

Performance

TOP DM GX4 Virtual machine has been highly optimized in order to offer maximum software performance without any compromise on security. Combined with high performance of last generation silicon this provides one of the fastest Java Open Platform available.



Security

The TOP DM GX4 includes multiple hardware and software countermeasure against various attacks:

- Side channel attacks
- Invasive attacks
- Advanced fault attacks
- Other types of attack.

Virtual Machine resources

TOP DM GX4 provides a large amount of memory resources for applications:

- APDU Buffer Size: 261 Bytes
- **Persistent Heap: exceed 64KB (up to 68KB depending on ordering options)**

Memory management

TOP DM GX4 advance memory management supports the following features

- Applet deletion
- **Real Garbage collector (JC 2.2.1 specification) memory space can be recovered after individual object deletion**

*ROMed applet means Applet Package is preloaded in ROM thus not using EEPROM memory. At time of Manufacturing, depending on customer choice, ROMed applet packages may be available or deleted. This has no impact on EEPROM capacity.