gemalto

TOP DM CC

Java Card Platform

The **TOP DM CC** 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 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. TOP DM CC 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 parts 1, 2, 3, 4, 5, 6, 8 & 9

The TOP DM CC is also certified **CC EAL5+** with **Javacard** Protection Profile.

Key Benefits

Ready ROMed* reference Applets do not impact available EEPROM:
- Classic v3 applet is directly supported by Gemalto Classic Client software and enables building PKI
   applications.
- MPCOS applet is fully compatible with high performance native MPCOS and available for data
   management and/or purse applications.
- OATH OTP applet can optionally be loaded in order to offer One Time Password services.

Optimized memory extends multi-application capability, data capacity and lifetime.
Due to ROMed applets, approximately 72KB of EEPROM memory is available to store data and host additional applets for application evolution during the expected card lifetime.

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

Part of a full range of product and services
Additional benefits from Gemalto's proven Java Card experience and product offer include support, middleware, 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 **Common Criteria EAL5 +** certification of its java card Operating System, the TOP DM CC platform implements the most advanced security countermeasures for enforcing protection of all sensitive data and functions in the card.

gemalto

TOP DM CC Technical Specifications

General Features
- Java Card Virtual Machine, compliant with **JC2.2.2** (and JC3.0.1 for ECC algos)
- Card Management & API compliant with **GP2.1.1**
    SCP01 and SCP02 supported with scripting capability of Amendment A
- Cryptographic algorithms:
    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: up to P384 bits
- 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 Channels to allow selection of multiple applets at the same time
- Support of Extended Length APDU
- Contact interface: T=0, T=1, PPS, with baud rate up to **230Kbps**
- Contactless interface: ISO 14443 type A and Type B (T=CL), with baud rate up to **847Kbps**
- Mifare emulation

Memory management
TOP DM CC advanced memory management supports the following features
- Applet deletion
- **Real Garbage collector**: memory space can be recovered after individual object deletion

Optional Gemalto applets
- Classic v3 applet (ROMed*)
- MPCOS applet (ROMed*)
- OATH OTP applet

Chip characteristics
- Latest generation Smart Card microcontroller
- EEPROM size: 80K Bytes
- Embedded security controller for asymmetric cryptography
- Minimum 500,000 write/erase cycles
- Data retention for minimum 25 years
- Common Criteria EAL5+ certified

Performance
TOP DM CC 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.

Security
The TOP DM CC includes multiple hardware and software countermeasures against various attacks:
- Side channel attacks
- Invasive attacks
- Advanced fault attacks
- Other types of attacks.

The TOP DM CC is certified **CC EAL5+** with **Javacard** Protection Profile.

---

*ROMed applet means the Applet Package is preloaded in ROM without using EEPROM memory. Depending on customer preference, ROMed applet packages may be loaded or deleted during manufacturing with no impact on EEPROM capacity.

---

gemalto

TOP DL v2

Product Information — Edition Sept 10

Java Card Platform – FIPS Certified.

TOP DL v2 benefits from the latest standard release of Java Card technology, and embeds all the algorithms required in **the Suite B Cryptography** edited by the National Security Agency.

This Java Card platform is available from Gemalto as an open, multi-application card and 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. TOP DL v2 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

TOP DL v2 is also currently being **FIPS140-2 level 3 certified.**

Key Benefits

Ready ROMed* reference Applets do not impact available EEPROM:
- PIV applet offers full compliancy to FIPS 201 standard.
- Classic applet is directly supported by Gemalto Classic Client software and enables building PKI
  applications.
- 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.
- Biometric Match-On-Card algorithm and MoC applet.

Very large memory extends multi-application capability, data capacity and lifetime.
Due to ROMed applets, the 128KB of memory of TOP DL v2 is available to store application data, and host additional applets for application evolution during the expected card lifetime.

Real Garbage Collector
New in JC2.2 spec, memory can be released to the platform in real time upon object deletion and made available to the applets.

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 TOP DL v2 platform implements the most advance security countermeasures for enforcing protection of all sensitive data and functions in the card.

gemalto

TOP DL v2 Technical Specifications

General Features
- Java Card Virtual Machine, compliant with JC2.2.1 (and JC2.2.2/3.0.1 for ECC algos)
- Card Management & API compliant with GP2.1.1 (and GP 2.2 for SCP03)
    SCP01 and SCP02 supported with scripting capability of Amendment A
    SCP03 supported (according to GP2.2 Amendment D)
- Cryptographic algorithms:
    Symmetric: 3DES (ECB, CBC), AES (128, 192, 256)
    Hash: SHA-1, SHA-256, SHA-384, SHA-512
    RSA: up to 2048
    Elliptic curves: ECC p160 / p192 / p224 / p256 / p384 / p521.
- On-card asymmetric **key pair generation** (RSA & ECC)
- PK-based **DAP** for better control of applets that can be loaded on the card
- Delegated Management
- Multiple Logical Channel to permit selection of multiple applets at the same time
- Contact interface: T=0, T=1, PPS, with baud rates up to 230Kbps
- Contactless interface: ISO 14443 type A & type B, T=CL, with speed up to 848 Kbps
- Mifare emulation

Pre-loaded applets in ROM*
- PIV applet
- Classic v3 applet
- MPCOS applet
- OATH OTP applet
- Biometric Match-On-Card algorithm & MoC applet

Chip characteristics
- Latest generation Smart Card microcontroller
- EEPROM size: 128K Bytes
- Embedded security controller for asymmetric cryptography
- True random number generator

Performance
TOP DL v2 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.

Security
The TOP DL v2 includes multiple hardware and software countermeasures against various attacks:
- Side channel attacks
- Invasive attacks
- Advanced fault attacks
- Other types of attacks.

The TOP DL v2 is currently being **FIPS 140-2 Level 3** certified.

Memory management
TOP DL v2 advance memory management supports the following features
- Applet deletion
- **Real Garbage collector** (JC 2.2 specification) – memory space can be recovered after individual object deletion

*ROMed applet means the Applet Package is preloaded in ROM without using EEPROM memory. Depending on customer preference, ROMed applet packages may be loaded or deleted during manufacturing with no impact on EEPROM capacity.