TOP IM FIPS CY2

Product Information Edition Dec 07

Introduction

The TOP IM FIPS CY2 (formally named Cyberflex 64K v2) is a smart card aimed at assisting government agencies and corporations in securing their network infrastructures.
The TOP IM FIPS CY2 offers you the best of mature industry standards for Java-based open platform smart cards, combined with a variety of card body configurations supporting contactless chip, magnetic stripes, customer-issuance printing, etc.

This product passed **FIPS140-2 level 3 certification.**

Key Benefits

Secure multi-application and post-issuance support:
• powerful firewalls between applications
• fast and secured transaction cycle

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.

Full compliance, with the Java Card and Open Platform specifications.

Advanced cryptographic support
TOP IM FIPS CY2 offers on board all the necessary cryptographic algorithms, symmetric key based or public key based.

No compromise on security
Acknowledged by FIPS-140 certification, the platform implements most advance security countermeasures enforcing protection of all sensitive data and functions in the card.

TOP IM FIPS CY2 Technical Specifications

General Features

- JavaCard 2.1.1 (API, JCRE and JVM)
- Global Platform 2.0.1'
- Up to 64KB of free memory
- Biometry support (optional):
  - API for biometric operations compliant with Java Card Forum recommendations (V1.1)
  - Precise Biometrics Match-on-Card algorithm
- ISO 7816-1-2-3-4 (applicable sections), ISO 7810, 7813
- Standard I/O transfer speed up to 115 Kbps
- Negotiable PPS
- T=0 protocol

Cryptographic capabilities

- Global PIN Support:
  - configurable number of tries (min. 3)
  - Pin Unblock Number
- DES/DES3 (CBC, EBC), SHA-1 algorithm, AES 128
- RSA signature and verification up to 2048 bits keys
- On-board key generation:
  - RSA 1024-2048bits
  - DES/DES3
- Mutual authentication mechanism through Global Platform Secure Channel
- Global Platform DAP (DES, RSA)
- Global Platform Mandated DAP
- Delegated Management

Chip characteristics

- Infineon SLE66 family
- 8bits micro-controller in advanced CMOS technology
- EEPROM endurance: 500,000 write/erase cycles
- Data retention: 10 years (ambient temperature)
- Cryptographic co-processor for faster RSA and DES3
- True Random Number Generator – FIPS 180
- Exception sensors for voltage, frequency, temperature

Security

The TOP IM FIPS CY2 includes multiple hardware and software countermeasure against various attacks.
The TOP IM FIPS CY2 is FIPS 140-2 Level 3 certified.