

# GEMPLUS



## GemSafeXpresso 16K/32K

Product Information

Edition 10/04

---

### Introduction

GemSafeXpresso is a smartcard designed for Public-key based applications. GemSafeXpresso is immediately compatible with the GemSafe software suite (which includes GemSafe Libraries and GemSafe Logon).

GemSafeXpresso is based on both the GemXpresso Pro R3.2 JavaCard platform and the GemSafe applet, and take full advantages of these two components in order to offer all the necessary services to build an Identity or Corporate Security solution together with the GemSafe softwares.

- GemXpresso Pro R3.2 is a Public Key JavaCard platform which complies with the latest international standards (JavaCard 2.1.1, Open Plaform 2.0.1', ISO 7816 part 1, 2 & 3)
- GemSafe applet is a Public-key based applet running on JavaCard platforms. This applet implements all the cryptographic features necessary for Public Key based applications, plus file management and associated security.

### Key Benefits

#### Part of the GemSafe solution

GemSafeXpresso is part of a complete GemSafe solution, which includes also the GemSafe Libraries and GemSafe Logon, being used by over 50 large clients all over the world.

GemSafeXpresso is also part of an interoperable product range: GemSafeXpresso and the native OS GPK16000 are interoperable since they are both supported by the GemSafe Libraries.

#### Strong support for public key

With GemSafeXpresso any PKI service is available in a single card.

GemSafeXpresso supports all the necessary Public-Key features in order to be integrated in a PKI application:

- Digital Signature
- On-Board-Key-Generation
- Session Key Decipherment

GemSafeXpresso supports RSA keys from 512 to 2048 bits.

#### Save valuable EEPROM

Since the GemSafe applet is present in the ROM of the GemSafeXpresso smartcard, the EEPROM area of the java platform can be fully dedicated to the application data.

#### Strong performance

GemSafeXpresso shows excellent RSA performances (measured at APDU level):

RSA 1024 signature: 0.25 sec

RSA 2048 signature : 1.4 sec



---

## GemSafeXpresso 16K/32K Technical Specifications

### General Features

- Based on JavaCard Virtual Machine, compliant with JC2.1.1
- Card Management & API compliant with OP2.0.1'
- Baud rates up to 115Kbps

### Cryptographic features

- Cryptographic algorithms: 3DES (ECB, CBC), RSA up to 2048bit & SHA-1
- 6 x RSA key containers (GemSafeXpresso 16K)
- 10 x RSA key containers (GemSafeXpresso 32K)
- RSA key length up to 2048 bits
- On board Key Generation
- RSA Key injection
- Digital Signature
- Session key decipherment
- Secure messaging
- Entrust (v6 and above) compliant.
- User PIN and Admin PIN support

### Security

GemSafeXpresso supports all the necessary security mechanisms to protect sensitive data: protection by PIN, External Authentication, Role, Secure messaging.

This product includes also multiple hardware and software counter measures against the following attacks:

- Side channel attacks (SPA, DPA, Timing attacks,...)
- Invasive attacks
- Fault attacks
- Other types of attacks

### *GemSafeXpresso used in Identity and Security solutions:*

ResIDent , the Gemplus secure ID solution including secure card body, smartcards, readers, biometrics, client/server software, issuance software, integration services

SafesITe , the Gemplus closed community security solution including PKI smartcards, readers, client/server software, issuance software, integration services.