



EZIO Classic TPC IM Identrust

Product Information

Edition Apr 09

Introduction

EZIO Classic TPC IM Identrust is a smartcard dedicated for PKI e-banking. It is part of the generic Classic TPC range (Trusted PKI Card) designed for Public-key based applications and immediately compatible with the Classic Client software.

All Classic TPC cards are based on both a TOP JavaCard platform and the Classic applet, and take full advantages of these two components in order to offer all the necessary services to build a Network Identity solution together with the Classic Client software.

- The TOP platform used in EZIO Classic TPC IM Identrust is FIPS140 certified to comply with Certification Authority requirements. It is a Public Key JavaCard platform which complies with the latest international standards (JavaCard, Global Platform, ISO 7816 part 1, 2 & 3).
- The EZIO Classic TPC IM Identrust is using Classic applets (V1.11) which is a Public-key based applet implementing all the cryptographic features necessary for Public Key based applications, plus file management and associated security.
- Thanks to FIPS certification, associated with software suite, Classic Client and eSigner, the card is certified by Identrust as compliant with their high demanding security and operation scheme.

Key Benefits

Part of the Classic solution

Classic TPC IM Identrust is part of a complete Classic solution, which includes also the Classic Client software, being used by over 50 large clients all over the world.

Classic Client offers both a CSP API and a PKCS#11 API to allow interfacing with any PKI application in Read Only mode. In the current Classic Client releases, the PKCS#11 interface is the one to be used for updating certificates. CSP API will be supported for updating in later versions.

Strong support for public key

With Classic TPC any PKI service is available in a single card.

Classic TPC 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

Classic TPC supports RSA keys up to 2048 bits.

Identrust certified

Classic TPC IM Identrust as part a suite with Classic Client and EZIO eSigner is certified by Identrust as compliant with their specification and high demanding security level.

Save valuable EEPROM

Since the Classic applet is present in the ROM of the smartcard chip the EEPROM area of the java platform can be fully dedicated to the application data (room for certificates).

Strong performance

Classic TPC shows excellent performances for both data management and RSA operation, thanks to the high performance of the TOP JavaCard.

EZIO Classic TPC IM Identrust Technical Specifications

General Features

- Based on JavaCard Virtual Machine, compliant with JC2.1.1 / 2.2.1
- Card Management & API compliant with GP2.0.1' / 2.1.1
- Baud rates up to 115 Kbps or 230 Kbps
- Up to 64Kbytes of EEPROM available for keys, certificates and data containers

Cryptographic features

- Cryptographic algorithms: 3DES (ECB, CBC), RSA up to 2048bit & SHA-1
- Cryptographic profile can be adapted to client's needs (up to 16 x RSA key containers)
- RSA key length up to 2048 bits
- On board Key Generation
- RSA Key injection
- Digital Signature
- Session key decipherment
- Secure messaging
- User PIN and Admin PIN support
- PKCS #11 API and CSP API with the Classic Client

Security

Classic TPC 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

Typical project deployment approach with EZIO Classic TPC IM Identrust

E-banking PKI projects typically involve various integration tasks with different stake holders. This typically includes: card profile definition, selection of the Certification Authority that will issue the certificates to be loaded into the cards, definition of the card life cycle processes particularly issuance and others tasks.

Gemalto also provides consulting services, integration, support services, card personalization and fulfilment services to ensure that the cards and associated software are working efficiently at first use for the e-banking service provided to end users.

On top of the cards, Gemalto provides complementary and pre-integrated products:

- A cryptographic library named Classic Client
- A client digital signature software plug-in, integrated with the browser, named eSigner
- A wide range of card readers

Contact your Gemalto sales contact that will set in place the appropriate project team to support you towards success of your project.