Classic TPC

Product Information Edition Jan 09

Introduction

Classic Trusted PKI Card (or Classic TPC) is a smartcard designed for Public-key based applications. Classic TPC is immediately compatible with the Classic Client software.

Classic TPC is based on both the TOP JavaCard platform and the Classic applets, 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.

- TOP is a Public Key JavaCard platform which complies with the latest international standards (JavaCard, Global Plaform, ISO 7816 part 1, 2 & 3)

- Classic applets are Public-key based applets running on JavaCard platforms. These applets implement all the cryptographic features necessary for Public Key based applications, plus file management and associated security. Classic v2 and Classic v3 applets are also CC EAL4+ / PPSSCD certified.

Key Benefits

Part of the Classic solution
Classic TPC 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.
Classic TPC is also part of an interoperable product range: Classic TPC and the native OS GPK16000 are interoperable since they are both supported by the Classic Client software.

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.

Compliant to the European Digital Signature law
Classic TPC IM CC is CC EAL4+ / PPSSCD certified, offering then a solution fully compliant to the European Digital Signature law.

Save valuable EEPROM
Since the Classic applets are present in the ROM of the Classic TPC smartcards, the EEPROM area of the java platform can be fully dedicated to the application data.

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

Classic TPC Technical Specifications

Product range

- Classic TPC IS v2 (PKCS#15): 10 x RSA key containers (standard profile)
- Classic TPC IM (PKCS#15): 12 x RSA key containers (standard profile)
- Classic TPC IM CC (CC EAL4+ / PPSSCD certified, PKCS#15): 12 x RSA key containers (standard profile)

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 (Classic TPC IS v2 & IM)
- Global PIN for PIN sharing with other applications (Classic TPC IM CC with Classic v3 applet)

Cryptographic features

- Cryptographic algorithms:
  - 3DES (ECB, CBC), RSA up to 2048bit & SHA-1
  - SHA-256 (Classic TPC IM CC with Classic v3 applet)
- 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
- Entrust (v6 and above) compliant.
- User PIN and Admin PIN support
- PKCS #11 API and CSP API with the Classic Client
- PKCS#15 compliant profile

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

Classic TPC IM CC is CC EAL4+ / PPSSCD certified, so fully compliant to the European Digital Signature law.