



Classic MDE TPC

Product Information

Edition Sept 08

Introduction

Classic MDE TPC stands for “**Classic Minidriver Enabled** Trusted PKI Card”. It’s a smartcard designed for Public-key based applications that is immediately compatible with Microsoft Smart Card Base Cryptographic Service Provider (Base CSP) thanks to the Classic MDE TPC Minidriver.

The Classic MDE TPC Minidriver has successfully passed the Microsoft test suite, and is available for download from the Microsoft web site.

The Classic MDE TPC is also supported by the Classic Client software, offering a PKCS#11 interface to the PKI applications.

Classic MDE TPC is based on both the TOP GX4 JavaCard platform and a dedicated MDE applet, and takes full advantages of these two components in order to offer all the necessary services to build an Identity and Access Management solution based either on Microsoft Base CSP or PKCS#11 API.

- TOP GX4 is a Public Key JavaCard platform which complies with the latest international standards (JavaCard 2.1.1, Global Platform 2.0.1’, ISO 7816 part 1, 2 & 3). TOP GX4 is also **FIPS 140-2 level 3 certified**.

Key Benefits

Minidriver for Base CSP available from Microsoft site

The Minidriver for Classic MDE TPC has successfully passed the Microsoft test suite and is available for download from the Microsoft web site. This Minidriver allows integrating the Classic MDE TPC with any PKI application running on a Windows 2000, XP (with Microsoft’s Base Smartcard CSP) or Vista environment.

PKCS#11 API with Classic Client

Classic MDE TPC is also supported by Classic Client, being used by over 50 large clients all over the world. With Classic Client, the Classic MDE TPC is part of an interoperable product range that includes all the Classic TPC cards.

Strong support for public key

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

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

Classic MDE TPC supports RSA keys up to 2048 bits.

Strong performance

Classic MDE TPC benefits from the excellent performances of:

- TOP GX4 Virtual machine, optimized for high performance.
- TOP GX4 latest generation silicon.

No compromise on security

Classic MDE TPC is based on the TOP GX4 JavaCard which is FIPS 140-2 level 3 certified.

Classic MDE TPC IM Technical Specifications

General Features

- Based on platform compliant to JavaCard (JC 2.2.1) and Global Platform (GP2.1.1)
- Baud rates up to 230 Kbps

Data organisation

Classic MDE TPC comes standard with a data organization ensuring both PKCS #11 and Minidriver compliance:

- PKCS #11:
 - data objects
 - 6 x RSA key containers up to RSA2048, for Read/Write operations with PKCS#11, and Read operations with Minidriver
- Minidriver:
 - data objects
 - 12 x RSA key containers up to RSA2048, for Read/Write operations with Minidriver, and Read operations with PKCS #11

Cryptographic features

- Cryptographic algorithms: DES - 3DES (ECB, CBC), RSA up to 2048bit & SHA-1
- RSA key length up to 2048 bits
- On board Key Generation
- RSA Key injection
- Digital Signature
- Authentication
- Session key decipherment
- User PIN and Admin PIN support

Security

Classic MDE TPC includes 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 MDE TPC is based on the TOP GX4 JavaCard which is **FIPS 140-2 level 3 certified**