IDClassic 340

Introduction

IDClassic 340 is a smartcard designed for Public-key based applications. The integration of IDClassic 340 with any PKI application is simple and immediate thanks to its minidriver and to the IDGo 300 (Classic Client) software.

IDClassic 340 is based on both the IDCore JavaCard platform and the Classic v3 applet, and takes full advantage of these two components in order to offer all the necessary services to build a Public-key based solution, together with the minidriver and the IDGo 300 (Classic Client) software.

- IDCore is a Public Key JavaCard platform which complies with the latest international standards (JavaCard, Global Plaform, ISO 7816)

- Classic v3 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.

IDClassic 340 is both **CC EAL4+ / PP SSCD** and **CC EAL5+ / PP Javacard** certified, and its java platform is also **FIPS 140-2 Level 3** certified (pending)

Key Benefits

Fully integrated in any PKI application
IDClassic 340 is fully supported by the IDGo 300 (Classic Client) software (being used by over 100 large clients all over the world) and a minidriver, Consequently IDClassic 340 interfaces with any PKI application, via Microsoft BaseCSP / CSP or via PKCS#11.

Strong support for public key infrastructure
With IDClassic 340 any PKI service is available in a single card.
IDClassic 340 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

IDClassic 340 supports RSA keys up to 2048 bits.

Compliant with European Digital Signature law
IDClassic 340 is **CC EAL4+ / PPSSCD** certified offering state-of-the-art security and a solution fully compliant with European Digital Signature law. Its java platform is also CC EAL5+ / PP Javacard and FIPS 140-2 Level 3 certified.

Multi-application
Other applications can reside on the IDClassic 340 smartcard, using for instance the optional MPCOS applet, or a 3rd party applet.

Save valuable EEPROM
Since the Classic v3 and MPCOS applets are present in the ROM of the IDClassic 340 smartcard, the EEPROM area of the java platform can be fully dedicated to the application data.

IDClassic 340

Product characteristics	
General features	JC2.2.2 GP2.1.1 (with SCP01 and SCP02) Global PIN
Cryptographic features	Cryptographic algorithms: 3DES (ECB, CBC), SHA-1, SHA-256, RSA up to RSA 2048 bits On-card asymmetric key pair generation Cryptographic profile can be adapted to client's needs (standard profile with 12 x RSA key containers, custom profile with up to 16 x RSA key containers) RSA Key injection Digital Signature Session Key Decipherment Secure Messaging User PIN and Admin PIN support Multiple virtual slot support BaseCSP API (with minidriver), PKCS #11 API and & CSP API with the Classic Client middleware PKCS#15 compliant profile
Communication protocols	T=0, T=1, PPS, with baud rate up to 230 Kbps
Gemalto applets (optional)	
MPCOS	E-purse & secure data management application
Chip characteristics	
Technology	80K EEPROM area Embedded crypto engine for symmetric and asymmetric cryptography
Lifetime	Minimum 500,000 write/erase cycles Data retention minimum 25 years
Certification	CC EAL5+

Security

The IDClassic 340 includes multiple hardware and software countermeasures against various attacks: side channel attacks, invasive attacks, advanced fault attacks and other types of attacks.

IDClassic 340 is both **CC EAL4+ / PP SSCD** and **CC EAL5+ / PP Javacard** certified, and its java platform is also **FIPS 140-2 Level 3** certified (pending).