IDClassic 3340

Product Information Edition July 12

Introduction

IDClassic 3340 is a dual interface (contact & contactless) smartcard designed for Public-key based applications. The integration of IDClassic 3340 with any PKI application is simple and immediate thanks to its minidriver and to the IDGo 300 software.

IDClassic 3340 is based on both the IDCore 3010 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 Classic Client software.

- IDCore 3010 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 3340 is both certified **CC EAL5+** with **Javacard** Protection Profile & **CC EAL4+** with **SSCD** Digital Signature Protection Profile.

Key Benefits

Fully integrated in any PKI application
IDClassic 3340 is fully supported by the **IDGo 300 software** (being used by over 100 large clients all over the world) **and a minidriver**, Consequently IDClassic 3340 interfaces with any PKI application, via Microsoft BaseCSP / CSP or via PKCS#11.

Strong support for public key infrastructure
With IDClassic 3340 any PKI service is available in a single card, via either the contact or the contactless interface.
IDClassic 3340 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 3340 supports RSA keys up to 2048 bits.

Compliant with European Digital Signature law
IDClassic 3340 is CC EAL4+ / PPSSCD certified offering state-of-the-art security and a solution fully compliant with European Digital Signature law.

Multi-application
Other applications can reside on the IDClassic 3340 smartcard, using the optional **MPCOS** or **OTP OATH** applets, or a 3rd party applet.

Save valuable EEPROM
Since the Classic v3 and MPCOS applets are present in the ROM of the IDClassic 3340 smartcard, the EEPROM area of the java platform can be fully dedicated to the application data.

IDClassic 3340 Technical Specifications

General Features

- Based on Java Card Virtual Machine, compliant with JC2.2.2
- Card Management & API compliant with GP2.1.1
- Global PIN for PIN sharing with OTP, MPCOS or other applications
- Contact interface: T=0, T=1, PPS, with baud rate up to **230Kbps**
- Contactless interface: ISO 14443 type A and Type B (T=CL), with baud rate up to **847Kbps**

Cryptographic features

- Cryptographic algorithms: 3DES (ECB, CBC), RSA up to 2048bit & SHA-1 / **SHA-256**
- 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 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
- Multiple virtual slot support
- BaseCSP API (with **minidrive**r), PKCS #11 API and & CSP API with the Classic Client middleware
- PKCS#15 compliant profile

Optional applets

- MPCOS applet
- OATH OTP applet

Chip characteristics

- Latest generation Smart Card microcontroller
- EEPROM size: 80K Bytes
- Embedded security controller for asymmetric cryptography
- Minimum 500,000 write/erase cycles
- Data retention for minimum 25 years
- Common Criteria EAL5+ certified

Security

IDClassic 3340 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

IDClassic 3340 is both certified CC EAL5+ with Javacard Protection Profile & CC EAL4+ with SSCD Digital Signature Protection Profile