Smartjac Industries Inc. - Kanalvägen 1A
2nd floor
SE-194 61 Upplands Väsby
Sweden
www.smartjac.com / www.smartjac.biz

Phone: +46(8)41071230 - Email: order@smartjac.com

IDPrime MD 830 - Minidriver Enabled PKI Java Card. Plug & Play

Brand: Gemalto
Product Code: SMAGO1055604

Short Description

IDPrime MD 830 is a Plug and Play contact interface smart card and is available in two version with different security certification. One is FIPS 140-2 Level 3, and the other is FIPS 140-2 Level 2 certified, for both the Java platform and the combination of Java platform plus PKI applet.

Description

IDPrime MD 830 is a Plug and Play contact interface smart card and is available in two version with different security certification. One is FIPS 140-2 Level 3, and the other is FIPS 140-2 Level 2 certified, for both the Java platform and the combination of Java platform plus PKI applet.

Plug & Play IDPrime MD 830 contact interface smart card

The IDPrime MD 830 is a contact interface smart card, FIPS 140-2 Level 3 & FIPS 140-2 Level 2 certified for both
the java platform and the combination of java platform plus PKI applet.

Future-Proofed and Scalable with Centralized Management Control

IDPrime MD 830 is based on the advanced Gemalto IDCore 30 platform, and integrates seamlessly with third-party applications through SafeNet Authentication development tools, supports SafeNet PKI and password management applications and software development tools, and allows customization of applications and extension of functionality through on-board Java applets. It is also supported by SafeNet Authentication Manager, which reduces IT overhead by streamlining all authentication operations, including deployment, provisioning, enrollment, and ongoing maintenance, as well as offering support for lost tokens.

Benefits

Perfect integration in Windows environment—Certified and distributed by Microsoft, the IDPrime MD minidriver ensures immediate integration with all Microsoft environments, plus Plug & Play service up to Windows 10, based on a secure chip flashmask with a total capacity of 300KB.

Centralized management control— IDPrime 830 is fully supported by SafeNet Authentication Manager, which
reduces IT overhead by streamlining all authentication operations, including deployment, provisioning, enrollment, and ongoing maintenance, as well as offering support for lost tokens.

No compromise on security—As reflected by the FIPS 140-2 Level 3 certification of the combination of java platform and the PKI applet, the IDPrime MD 830 smart cards implement the most advanced security countermeasures for enforcing protection of all sensitive data and functions in the card.

Enhanced cryptographic support—IDPrime MD offers PKI services with both RSA and elliptic curves.

Strong Security

As reflected by the FIPS 140-2 Level 3 certification of the combination of java platform and the PKI applet,
the IDPrime MD 830 smart cards implement the most advanced security countermeasures for enforcing
protection of all sensitive data and functions in the card. IDPrime MD smart cards are secured with both RSA and
elliptic curves algorithms, and address a range of use cases that require PKI security, including secure access,
email encryption, secure data storage, digital signatures and secure online transactions for end users.

Specifications
Product characteristics

Memory
IDPrime MD memory allows the storage of up to 15 RSA or Elliptic curve key containers

Standards
BaseCSP Minidriver v7 (IDGo 800 Minidriver) PKCS#11 & CSP (SafeNet Authentication Client)

Operating systems
Windows, MAC, Linux, Android, iOS

Cryptographic algorithms
Hash: SHA-1, SHA-256, SHA-384, SHA-512
RSA: up to RSA 2048 bits
RSA OAEP & RSA PSS
Elliptic curves: P-256, P-384, P-521 bits, ECDSA, ECDH
On-card asymmetric key pair generation (RSA up to RSA2048 & Elliptic curves, RSA 1024 support
available in FIPS 140-2 Level 2 configuration)

Symmetric: 3DES (ECB, CBC), AES – For secure messaging and Microsoft Challenge/Response only

Communication protocols
T=0, T=1, PPS, with baud up to 460 Kbps

Other features
Onboard PIN Policy
IDPrime family of cards can be customized (card body and programming) to fit customers' needs.

Technology
Embedded crypto engine for symmetric and asymmetric cryptography

Lifetime
Minimum 500,000 write/erase cycles
Data retention for minimum 25 years

Certification

(Chip) - CC EAL6+
Certification (Java and applet)
FIPS 140-2 Level 3
Gemalto original applets
MPCOS E-purse & secure data management application

Security
The IDPrime MD smart cards include multiple hardware and software countermeasures against various attacks:
side channel attacks, invasive attacks, advanced fault attacks and other types of attacks.

IDPrime MD 830 is FIPS 140-2 Level 3 for both the Java platform and the combination of the Java platform and the PKI applet