IDPrime MD 840

Plug & Play PKI smart cards

The **IDPrime MD** smart cards are designed for Public-Key based applications, and come with a **IDGo 800** minidriver that offers a perfect integration with native support from the **Microsoft®** environments, up to Windows 8.1 **(without any additional middleware**).

The IDPrime MD smart cards offer all the necessary services (with both **RSA and elliptic curves** algorithms) to secure an IT Security and ID access infrastructure.
Their IDGo 800 PKCS#11 libraries extend the compatibility of these smart cards to any type of applications, and any environment (**Windows, MAC, Linux**) that may be in used in an IT Security solution.
IDPrime MD smartcards are also fully supported by the **IDGo 800 middleware & SDK for Mobiles (Android, iOS)**.

The IDPrime MD 840 is a contact interface smart card, both **CC EAL5+ / PP Javacard** certified for the java platform and **CC EAL5+ / PP SSCD** certified for the combination of java platform plus PKI applet.

Key Benefits

Perfect integration in Windows environment.
The IDPrime MD minidriver is certified and distributed by Microsoft. It ensures immediate integration with all Microsoft environments, plus Plug & Play service on Windows 7, Windows 8 and Windows 8.1.

Compatible with any environment
Fully supported by the IDGo 800 suite on **Windows, MAC, Linux, Android, iOS**.

Compliant with European Digital Signature law
IDPrime MD 840 is **CC EAL5+ / PP SSCD** 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** certified.

OTP option
IDPrime MD are multi-application smart cards, and can have onboard the optional OATH One Time Password applet, offering a very flexible authentication service, combining both PKI and OTP.

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

MPCOS option
IDPrime MD are multi-application smart cards, and can have onboard the optional MPCOS applet, which offers both **e-purse** and data management services.

Part of the Gemalto IDPrime range
IDPrime MD 840 is part of a large range of Gemalto IDPrime smartcards (IDPrime .NET & other IDPrime MD smartcards) and benefit from the wide and long experience of Gemalto with minidriver enabled smart cards.

IDPrime MD 840

Product characteristics	
Memory	IDPrime MD memory allows the storage of up to 15 RSA or Elliptic curve key containers (depending on the card profile)
Standards	BaseCSP Minidriver v7 (IDGo 800 Minidriver) PKCS#11 v2.20 (IDGo 800 libraries)
Operating systems	Windows, MAC, Linux, Android, iOS
Cryptographic algos	Symmetric: 3DES (ECB, CBC), AES (128, 192, 256 bits) Hash: SHA-1, SHA-256, SHA-384, SHA-512. RSA: up to RSA 2048 bits (and optionally up to 4096 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)
Communication protocols	T=0, T=1, PPS, with baud up to 230 Kbps
Other features	Onboard PIN Policy Multi-PIN support (including a dedicated IDGo 800 Credential Provider)
Gemalto optional applets	
OATH OTP	One Time Password application (event based)
MPCOS	E-purse & secure data management application
Chip characteristics	
Technology	Embedded crypto engine for symmetric and asymmetric cryptography
Lifetime	Minimum 500,000 write/erase cycles Data retention for minimum 25 years
Certification	**CC EAL5+**
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. The IDPrime MD 840 is both **CC EAL5+ / PP Javacard** certified for the java platform and **CC EAL5+ / PP SSCD** certified for the combination of java platform plus PKI applet.	