



PRODUCT BRIEF

IDPrime 840

Plug & Play Smart Cards

As cybercriminals get smarter and more determined than ever, more and more businesses and government agencies are coming to the realization that single-factor authentication solutions using simple usernames and passwords are not enough. Gemalto, the world leader in digital security, offers an extensive portfolio of strong authentication solutions to help address the need for multi-factor authentication.

IDPrime MD smart cards are designed for PKI-based applications, and come with an IDGo 800 minidriver that offers perfect integration with native support for Microsoft® environments (through Windows 10), without any additional middleware.

Compatible with Any Environment

In addition to its seamless integration into Windows ecosystems, the IDPrime MD 840 is a contact interface smart card and is compatible with any environment through support by the SafeNet Authentication Client and the IDGo 800 libraries. IDPrime MD smart cards are also fully supported by the IDGo 800 middleware and SDK for Mobile (Android, iOS).

Strong Security

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.

IDPrime MD 840 is CC EAL5+ / PP Java Card certified for

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. Secure chip EEPROM capacities of 80 KB
- > **Compatible with any environment**—The MD 840 is fully supported by the SafeNet Authentication Client and IDGo 800 mobile for Android and iOS.
- > **Compliant with eIDAS regulations**—IDPrime MD 840 is CC EAL5+ / PP QSCD certified offering state-of-the-art security and is fully compliant with European eIDAS regulations. Its Java platform is also CC EAL5+ / PP Java Card certified.
- > **Multi-application smart cards**— IDPrime MD cards can have optional onboard applet for MPCOS e-purse
- > **Enhanced cryptographic support**—IDPrime MD offers PKI services with both RSA and elliptic curves.

the Java platform and CC EAL5+ / PP QSCD certified for the combination of Java platform and PKI applet. The CC EAL5+ / PP QSCD certification is based on the Protection Profiles EN 419211 part 1 to 6, as mandated by eIDAS regulations.

Optional Onboard Applets

IDPrime MD cards are multi-application smart cards, meaning they can have optional onboard applets for various functions. An MPCOS applet can be added to provide both e-purse and data management services.

Product characteristics	
Memory	> 80KB total, including 50KB available for data, certificates and additional applets. 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) > CSP and PKCS#11 (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 (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) > Symmetric: 3DES (ECB, CBC), AES – For secure messaging and Microsoft Challenge/Response only
Communication protocols	> T=0, T=1, PPS, with baud up to 230 Kbps
Other features	> Onboard PIN Policy > Multi-PIN support > IP Prime family of cards can be customized (card body and programming) to fit customers' needs.
Gemalto applets (optional)	
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 Java Card certified for the java platform and CC EAL5+ / PP QSCD certified for the combination of java platform plus PKI applet.

Why Gemalto

IDPrime MD 840 is part of a large range of Gemalto IDPrime smart cards and benefits from Gemalto's extensive experience with minidriver enabled smart cards. Gemalto's Identity Protection solutions enable enterprises, financial organizations and service providers to protect the daily digital interactions of employees, partners and customers by ensuring secure access to online resources and securing financial transactions. Gemalto's flexible management platforms and broad range of strong authentication technologies and form factors, allow organizations to adopt a forward-looking identity management strategy, ensuring that their security needs are met as new threats and use cases evolve.

To learn more about Gemalto's complete portfolio of authentication solutions, visit our website at:

www.gemalto.com/identity.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com

Follow Us: blog.gemalto.com/security

 GEMALTO.COM

gemalto
security to be free