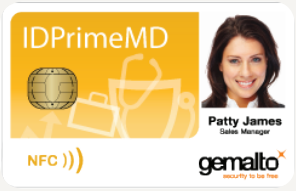

PRODUCT BRIEF

IDPrime 3840

Plug & Play Smart Cards

Gemalto, the world leader in digital security, offers an extensive portfolio of strong authentication solutions to help address the need for multi-factor authentication. The IDPrime MD 3840 is a dual-interface smart card, allowing communication either via a contact interface or via a contactless ISO14443 interface, also compatible with the NFC standard.

IDPrime MD smart cards are designed for PKI-based applications, and come with a IDGo 800 minidriver that offers a perfect integration with native support from the Microsoft® environments, up to Windows 10 (without any additional middleware). IDPrime MD 3840 is fully supported by SafeNet Authentication Client for more robust management support. SafeNet Authentication Client provides full local admin and support for advanced card and token management, events and deployment.

Compliance with European Digital Transaction and Signature Regulations

eIDAS is the European Regulation aimed at creating a framework for cross-border electronic identification and transactions across EU member countries. Common Criteria (CC) certification is a pre-requisite for qualified digital signatures under the eIDAS Regulation.

The IDPrime MD 3840 smart cards are 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. The CC EAL5+/ PP QSCD certification is based on the Protection Profile EN 419211 part 1 to 6, as mandated by eIDAS Regulation.

Advanced Functionality

IDPrime MD smart cards are multi-application smart cards 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.

Benefits

- NFC Compliant—IDPrime MD 3840 offers both an ISO7816 contact interface and an ISO14443 contactless interface, also compatible with the NFC standard already widely used by smartphones and tablets.
- Compliant with eIDAS regulations—IDPrime MD 3840 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.
- Compatible with any environment—The IDPrime MD 3840 is fully supported by SafeNet Authentication Client and IDGo 800 mobile for Android and iOS.
- Enhanced cryptographic support—IDPrime MD offers PKI services with both RSA and elliptic curves.

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.

Strong Security

The IDPrime MD 3840 smart cards implement the most advanced security countermeasures for enforcing protection of all sensitive data and functions in the card. As reflected by the CC EAL5+ / PP QSCD certificate, IDPrime MD smart cards include multiple hardware and software countermeasures against various attacks, including side channel attacks, invasive attacks, advanced fault attacks and other types of attacks.

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 and CSP (SAC)
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 > 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 > T=CL, ISO 14443 type A, compatible also to NFC standard, with speed up to 848 Kbps
Other features	> Onboard PIN Policy > Multi-PIN support
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 3840 is both CC EAL5+ / PP Javacard certified for the java platform and CC EAL5+ / PP QSCD certified for the combination of java platform plus PKI applet.

Why Gemalto

IDPrime MD 3840 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