

Gemalto SafeNet IDPrime 940 smartcard



The Gemalto IDPrime MD 940 card is a plug & play PKI smartcard that provides the necessary security services to implement a strong two-factor logical access and security infrastructure on Windows and other platforms. The IDPrime MD 940 is a contact interface smart card that supports the ISO 7816 standard, and is Common Criteria EAL6+ certified. It is also eIDAS compliant for eSignature and eSeal secure electronic signature generation, and qualified with the French ANSSI. The SafeNet IDPrime 940 is an enhanced version of the previous MD 840 series, with enhanced cryptographic support (including RSA up to 4096 bits).

Fully compliant with the latest Microsoft minidriver specifications for use on Windows, without the need for additional middleware, the necessary driver will install automatically and for free, using plug-and-play.

Plain white card.

If you need this card in a SIM-size just add our FREE SIM cutting service to your basket alongside this card.

Gemalto (SafeNet) part number O1132421

Contact PKI smartcard ideal for highly secure public-key based applications. Common Criteria EAL6+ and PP QSCD certified and eIDAS compliant for eSignature and eSeal. Free Windows minidriver. Gemalto part O1132421.

To buy, visit:

<https://www.smartcardfocus.com/shop/ilp/id~870/p/index.shtml>

This Product Briefing has been produced by [Dot Origin Ltd](#), the smart card experts behind [SmartcardFocus.com](#). If you have a query email sales@smartcardfocus.com or call us on +44 (0)1428 685250.

Gemalto IDPrime MD 940 smartcard

Technical Specifications

Memory: 400kB Flash, 20 key containers, 73kB for certificates/applets/data in standard configuration

Cryptographic algorithms: SHA-1, SHA-256, SHA-384, SHA-512; RSA up to 4096 bits; RSA OAEP & RSA PSS; On-card asymmetric key pair generation (RSA up to 4096 bits and elliptic curves up to 521 bits); AES symmetric keys for secure messaging; 3DES symmetric keys for Microsoft challenge/response only.

PIN: Onboard PIN Policy, Multi-PIN support

Lifetime: Minimum 500,000 write/erase cycles

Data retention: Minimum 25 years

Communications: T=0 or T=1 protocol , PPS, with rates up to 446 kbps

Compliance / Certification

ISO 7816, Java Card 3.0.4, Global Platform 2.2.1, BaseCSP minidriver (SafeNet minidriver), CC EAL6+

Operating System support

Windows, Linux, Mac

Manufacturer's part number: Gemalto (SafeNet) O1132421

Manufacturer: [Thales Gemalto](#)

Connection Method: USB