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 identity and access management including a wide range of multi-factor authentication methods.

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

The SafeNet IDPrime 3940 is a dual-interface smart card, allowing communication either via a contact interface or via a contactless ISO14443 interface, also compatible with some NFC readers.

**Compatible with Any Environment**

In addition to its seamless integration into Windows ecosystems, the SafeNet IDPrime 3940 is a dual interface smart card and is compatible with any environment through support by the SafeNet Authentication Client.

**Strong Security**

SafeNet IDPrime 3940 Smart Cards are secured with both RSA up to 4096 and Elliptic curves algorithms up to 521 bits, 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**

- **Dual interface**—SafeNet IDPrime 3940 offers both an ISO7816 contact interface and an ISO14443 contactless interface, also compatible with some NFC readers.
- **Perfect integration in Windows environment**—Certified and distributed by Microsoft, the SafeNet minidriver ensures immediate integration with all Microsoft environments, plus Plug & Play service up to Windows 10.
- **Secure Flash mask chip**—400KB.
- **Compatible with any environment**—SafeNet IDPrime 3940 is fully supported by the SafeNet Authentication Client.
- **Compliant with eIDAS regulations**—SafeNet IDPrime 3940 is fully qualified according the eIDAS regulations for both eSignature and eSeal applications, and is qualified by the French ANSSI. Its Java platform is also CC EAL5+/PP Java Card certified.
- **Multi-application smart cards**—SafeNet IDPrime smart cards can have optional onboard applet for MPCOS e-purse.
- **Enhanced cryptographic support**—SafeNet IDPrime 3940 offers PKI services with both RSA up to 4096 and elliptic curves up to 521 bits.

SafeNet IDPrime 3940 is CC EAL5+/PP Java Card certified for the Java platform and CC EAL5+/PP QSCD certified for the combination of Java platform and PKI applet. SafeNet IDPrime 3940 is qualified by the French ANSSI and is qualified according to the eIDAS regulations for both the eSignature and the eSeal applications.

**Optional Onboard Applets**

SafeNet IDPrime 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
- SafeNet IDPrime 3940 is based on a 400 KB Java Flash memory chip. SafeNet IDPrime 3940 comes as standard with 20 key containers. The memory available for certificates and other applets & data in this standard configuration is 73 KB.

### Standards
- BaseCSP minidriver (SafeNet minidriver)
- Global Platform 2.2.1
- Java Card 3.0.4
- ISO 7816 and ISO 14443

### Operating systems
- Windows, MAC, Linux

### Cryptographic algorithms
- RSA: up to RSA 4096 bits
- RSA OAEP & RSA PSS
- P-256 bits ECDSA, ECDH. P-384 & P-521bits ECDSA, ECDH are available via a custom configuration
- On-card asymmetric key pair generation (RSA up to 4096 bits & Elliptic curves up to 521 bits)
- Symmetric: AES—For secure messaging and 3DES for Microsoft Challenge/Response only

### Communication protocols
- T=0, T=1, PPS, with baud rate up to 446 Kbps at 3.57 MZ (TA1=97h)
- T=CL, ISO 14443 type A, with speed up to 848 Kbps

### Other features
- Onboard PIN Policy
- Multi-PIN support
- SafeNet IDPrime 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 EAL6+

### Security
- SafeNet IDPrime 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 SafeNet IDPrime 3940 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, is eIDAS qualified for both eSignature and eSeal, and qualified by the French ANSSI.

## About Gemalto’s SafeNet Identity and Access Management Solutions

Gemalto’s industry-leading Identity and Access Management solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively manage risk, maintain regulatory compliance, gain visibility into all access events and simplify the login experience for their users.

To learn more, please visit: [safenet.gemalto.com/multi-factor-authentication](https://safenet.gemalto.com/multi-factor-authentication)

---

**Contact Us:** For all office locations and contact information, please visit safenet.gemalto.com  
**Follow Us:** blog.gemalto.com/security  

©Gemalto 2018. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries. PB (EN) - Oct 31, 2018 - Design: ELC