

# SafeNet IDPrime 940 and 940B

## 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. Thales, 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 11), without any additional middleware.

### Compatible with Any Environment

In addition to its seamless integration into Windows ecosystems, the SafeNet IDPrime 940 and 940B are contact interface smart cards and are compatible with any environment through support by the SafeNet Authentication Client.

### Strong Security

SafeNet IDPrime 940 and 940B smart cards are secured with both RSA up to 4096 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.



Both cards are 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 940 and 940B are fully qualified according the eIDAS regulations for both eSignature and eSeal applications.

SafeNet IDPrime 940 has also obtained the French "Qualification Renforcée" required by the French government, administration and military.

### 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.

## Benefits

### SafeNet IDPrime 940 and 940B

- 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 11
- SafeNet IDPrime 940 is based on a 400KB Flash memory chip
- SafeNet IDPrime 940B is based on a 500KB Flash memory chip
- Compatible with any environment—Both cards are fully supported by the SafeNet Authentication Client
- Compliant with eIDAS regulations—Both cards are fully qualified according the eIDAS regulations for both eSignature and eSeal applications.
- Java platform is CC EAL5+ / PP Java Card certified on both cards
- Multi-application smart cards—SafeNet IDPrime smart cards can have optional onboard applets for MPCOS e-purse
- Enhanced cryptographic support—Both cards offer PKI services with both RSA up to 4096 and elliptic curves up to 521 bits

### SafeNet IDPrime 940

- This card has obtained the French “Qualification Renforcée” from ANSSI.

Product characteristics	
Memory	<ul style="list-style-type: none"> <li>• SafeNet IDPrime 940 is based on a 400KB Flash memory chip. SafeNet IDPrime 940B is based on a 500KB Flash memory chip. Both cards come as standard with 20 key containers. The memory available for certificates and other applets and data in this standard configuration is at least 73 KB.</li> </ul>
Standards	<ul style="list-style-type: none"> <li>• BaseCSP minidriver (SafeNet minidriver)</li> <li>• Global Platform 2.2.1</li> <li>• Java Card 3.0.4</li> <li>• ISO 7816</li> </ul>
Operating systems	<ul style="list-style-type: none"> <li>• Windows, MAC, Linux</li> </ul>
Cryptographic algorithms	<ul style="list-style-type: none"> <li>• Hash: SHA-1, SHA-256, SHA-384, SHA-512.</li> <li>• RSA: up to RSA 4096 bits</li> <li>• RSA OAEP &amp; RSA PSS</li> <li>• P-256 bits ECDSA, ECDH. P-384 &amp; P-521 bits ECDSA, ECDH are available via a custom configuration</li> <li>• On-card asymmetric key pair generation (RSA up to 4096 bits &amp; Elliptic curves up to 521 bits)</li> <li>• Symmetric: AES—For secure messaging and 3DES for Microsoft Challenge/Response only</li> </ul>
Communication protocols	<ul style="list-style-type: none"> <li>• T=0, T=1, PPS, with baud rate up to 446 Kbps at 3.57 MZ (TA1=97h)</li> </ul>
Other features	<ul style="list-style-type: none"> <li>• Onboard PIN Policy</li> <li>• Multi-PIN support</li> <li>• SafeNet IDPrime family of cards can be customized (card body and programming) to fit customers’ needs.</li> </ul>
Thales applets (optional)	
MPCOS	<ul style="list-style-type: none"> <li>• E-purse &amp; secure data management application</li> </ul>
Chip characteristics	
Technology	<ul style="list-style-type: none"> <li>• Embedded crypto engine for symmetric and asymmetric cryptography</li> </ul>
Lifetime	<ul style="list-style-type: none"> <li>• Minimum 500,000 write/erase cycles</li> <li>• Data retention for minimum 25 years</li> </ul>
Certification	<ul style="list-style-type: none"> <li>• CC EAL6+</li> </ul>
Security	
	<ul style="list-style-type: none"> <li>• 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.</li> <li>• SafeNet IDPrime 940 and SafeNet IDPrime 940B 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, is eIDAS qualified for both eSignature and eSeal.</li> <li>• SafeNet IDPrime 940 has also obtained the French “Qualification Renforcée” required by the French government, administration and military.</li> </ul>