PKI smart cards conform to SIS standard

The IDPrime SIS smart cards are based on IDPrime MD smart cards that are designed for Public-Key based applications, and offer all the necessary services (with both RSA and elliptic curves algorithms) to secure an IT Security and ID access infrastructure.

The IDPrime SIS 3840 is compliant to the Swedish standard. It's a dual-interface smart card, allowing communication either via a contact interface or via a contactless ISO14443 interface, also compatible with the NFC standard. The contactless interface also allows for emulation of physical access control technologies such as Mifare® Classic or DESFire EV1 ®.

Key Benefits

Conform to the Swedish standard
The IDPrime SIS is designed to comply with the data model of the Swedish standard SS 614332.

Compliant with European Digital Signature law
IDPrime SIS smart cards are CC EAL4+ / PP SSCD certified offering state-of-the-art security and a solution fully compliant with European Digital Signature law. Its java platform is also CC EAL4+ / PP Javacard certified.

Compliant to ISO14443 / NFC
IDPrime SIS 3840 smart cards offer both an ISO7816 contact interface and an ISO14443 contactless interface, which is also compatible with the NFC standard already widely used by smartphones and tablets.

Part of the Gemalto IDPrime range
IDPrime SIS 3840 is part of a large range of Gemalto IDPrime smartcards (IDPrime .NET & other IDPrime MD smartcards) and benefit from the wide and long experience of Gemalto with high end PKI smart cards.

OTP option
IDPrime MD are multi-application smart cards, and can have onboard the optional OATH One Time Password applet, offering a very flexible authentication service, combining both PKI and OTP.

Enhanced cryptographic support
IDPrime MD offers PKI services with both RSA and elliptic curves.

MPCOS option
IDPrime MD are multi-application smart cards, and can have onboard the optional MPCOS applet, which offers both e-purse and data management services.
**Product characteristics**

<table>
<thead>
<tr>
<th>Memory</th>
<th>IDPrime SIS 3840 memory allows the storage of up to 15 RSA and/or Elliptic curve key containers</th>
</tr>
</thead>
</table>
| Cryptographic algs | Symmetric: 3DES (ECB, CBC), AES (128, 192, 256 bits)  
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) |
| 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 | Multi-PIN support |

**Physical Access Control options**

- Mifare® Classic: 1K or 4K
- DESFire EV1 ®: 4K or 8K
- Other: Compatibility with the Legic Advant® applet

**Gemalto optional applets**

- OATH OTP: One Time Password application (event based)
- MPCOS: E-purse & secure data management application

**Chip characteristics**

<table>
<thead>
<tr>
<th>Technology</th>
<th>Embedded crypto engine for symmetric and asymmetric cryptography</th>
</tr>
</thead>
</table>
| 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 SIS 3840 is both **CC EAL4+ / PP Javacard** certified for the java platform and **CC EAL4+ / PP SSCD** certified for the combination of java platform plus PKI applet.