PRODUCT BRIEF

IDPrime 3811 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. These include SafeNet Identity and Access Management solutions, featuring PKI technology that offers the strongest security without compromising convenience or efficiency.

The IDPrime MD 3811 is a dual-interface smart card, based on a single chip, offering full PKI services either via a contact interface or via a contactless ISO14443 interface, also compatible with the NFC standard, already widely used by smartphones and tablets.

Convenient converged badge for logical and physical access

Many organizations have a need to logical and physical access. The IDPrime MD 3811 allow for both PAC [physical access controls] and LAC [logical access controls] in a single credential. IDPrime MD 3811 are set with either Mifare® Classic and/or DESFire EV1® emulation, to allow for PAC and perfect for an enterprise converged badge solution.

IDPrime MD 3811 integrates seamlessly with third-party applications through SafeNet Authentication development tools, supports SafeNet PKI and password management applications and software development tools, and allows customization of applications and extension of functionality through on-board Java applets. It is also supported by SafeNet Authentication Manager, which reduces IT overhead by streamlining all authentication operations, including deployment, provisioning, enrollment, and ongoing maintenance, as well as offering support for lost tokens.

Strong Security

The IDPrime MD 3811 smart cards implement the most advanced security countermeasures for enforcing protection of all sensitive data and functions in the card.

IDPrime MD smart cards are secured with both RSA 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.

Benefits

> Perfect integration in Windows environment—Certified and distributed by Microsoft, the IDPrime MD minidriver ensures immediate integration with all Microsoft environments, plus Plug & Play service up to Windows 10.
> Centralized management control—IDPrime MD 3811 is fully supported by SafeNet Minidriver and/or a Card Management System, which reduces IT overhead by streamlining all authentication operations, including deployment, for provisioning, enrollment, and ongoing maintenance, as well as offering support lost tokens.
> NFC Compliant—IDPrime MD 3811 smart cards are compliant to ISO14443 / NFC, and offer both an ISO7816 contact interface and an ISO14443 contactless interface, also compatible with the NFC standard already widely used by smartphones and tablets.
> Compatible with any environment—Fully supported by SafeNet Authentication Client on Windows, MAC, Linux, Android, iOS.

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.
# Product Characteristics

<table>
<thead>
<tr>
<th>Memory</th>
<th>IDPrime MD memory allows the storage of up to 15 RSA or Elliptic curve key containers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards</td>
<td>BaseCSP Minidriver v7 [SafeNet Minidriver] PKCS#11 and CSP [SAC]</td>
</tr>
<tr>
<td>Operating systems</td>
<td>Windows, MAC, Linux, Android, iOS</td>
</tr>
<tr>
<td>Cryptographic algorithms</td>
<td>Hash: SHA-1, SHA-256, SHA-384, SHA-512. RSA: up to RSA 2048 bits RSA OAEP &amp; RSA PSS Elliptic curves: P-256, P-384, P-521 bits, ECDSA, ECDH On-card asymmetric key pair generation (RSA up to RSA2048 &amp; Elliptic curves) Symmetric: 3DES (ECB, CBC), AES – For secure messaging and Microsoft Challenge/Response only</td>
</tr>
<tr>
<td>Communication protocols</td>
<td>T=0, T=1, PPS, with baud up to 230 Kbps T=CL type A, T=CL, compatible to NFC standard, with speed up to 848 Kbps</td>
</tr>
<tr>
<td>Other features</td>
<td>Onboard PIN Policy IDPrime family of cards can be customized (card body and programming) to fit customers’ needs.</td>
</tr>
</tbody>
</table>

## Gemalto Applets (optional)

- MPCOS: E-purse & secure data management application

## Physical Access Control options

- Mifare® Classic: 4K
- DESFire EV1®: 4K or 8K

## 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.

---

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

**Follow Us:** blog.gemalto.com/security