thalescpl.com

THALES

# SafeNet IDPrime 940

## Plug & Play Smart Cards

隨著網路犯罪者變得比以往更聰明且有心，越來越多的企業和政府機構開始意識到：使用簡單的使用者名稱及密碼的單因素身分驗證是不夠的。Thales 是數位安全領域的世界領導者，提供多種的身分和訪問管理組合，包括廣泛的多重身分驗證方案。

SafeNet IDPrime 智慧卡是專為 PKI 的應用程式而設計，並配備了一個 SafeNet minidriver，可為 Microsoft® 的環境（透過 Windows 10），無須任何其他驅動。


## 與任何環境相容

除了無縫整合到 Windows 環境系統之外，SafeNet IDPrime 940 是一款接觸式介面智慧卡，透過 SafeNet 身份認證用戶端的支援，可與任何環境相容。

## 強大的安全性

SafeNet IDPrime 940 智慧卡通過高達 4096 的 RSA 和橢圓曲線演算法進行安全保護，並解決一系列需要 PKI 安全的案例，包括：安全登入、電子郵件加密、安全數據儲存、數位簽章和最終用戶的安全線上交易。

SafeNet IDPrime 940 已通過 Java 平台的 CC EAL5+ / PP Java 卡認證，以及針對 Jave 平台和 PKI applet 組合的 CC EAL5+ / PP QSCD 認證。SafeNet IDPrime 940 已經獲得法國 ANSSI 的認證，並根據 eIDAS 的法規和 eSeal 的應用程式進行了認證。

## 可選晶片內小程式

SafeNet IDPrime 是多用途的智慧卡，這代表它具有多功能的晶片內小程式可選擇。可以添加 MPCOS 程式以提供電子錢包和數據管理服務。

## 優點

- 在 Windows 環境中的完美整合—SafeNet minidriver 已獲得 Microsoft 的認證和分發，可確保所有與 Microsoft 環境的即時整合和即插即用的服務
- Flash mask 安全晶片—400 KB
- 與任何環境相容—SafeNet 身分驗證用戶端完全支援 SafeNet IDPrime 940
- 符合 eIDAS 法規—SafeNet IDPrime 940 完全符合 eIDAS 法規中關於 eSignature 和 eSeal 應用程序的資格，並通過法國 ANSSI 的認證。此 Java 平台同時也通過了 CC EAL5+ / PP Java 卡的認證。
- 多應用智慧卡—SafeNet IDPrime 智慧卡可以具有 MPCOS 電子錢包的可選晶片內小程式
- 強化加密支援—SafeNet IDPrime 940 提供高達 4096 的 RSA 和高達 521 bits 的橢圓曲線的 PKI 服務

| 產品特點 | |
|---|---|
| **記憶體容量** | • SafeNet IDPrime 940 擁有 400 KB Java Flash 晶片記憶體；標準的 SafeNet IDPrime 940 帶有 20 個密鑰容器。在此標準配置中，可用於憑證和其他小程式(Applet)跟數據的記憶體容量為 73 KB |
| **標準規範** | • BaseCSP minidriver (SafeNet minidriver)<br>• Global Platform 2.2.1<br>• Java 卡 3.0.4<br>• ISO 7816 |
| **支援的作業系統** | • Windows, MAC, Linux |
| **加密演算法** | • Hash: SHA-1, SHA-256, SHA-384, SHA-512.<br>• RSA: 最高 RSA 4096 bits<br>• RSA OAEP & RSA PSS<br>• P-256 bits ECDSA, ECDH. P-384 & P-521bits ECDSA, 可透過訂製規劃 ECDH<br>• 晶片內非對稱金鑰生成（高達 4096 bits 的 RSA 和高達 521 bits 的 Elliptic curves)<br>• 對稱式演算法：AES 可用於安全訊息傳遞及 3DES 用於 Microsoft® Challenge/Response |
| **通訊協定** | • T=0, T=1, PPS, 通訊速率可達 446 Kbps at 3.57 MZ (TA1=97h) |
| **其他特點** | • 晶片內建 PIN 的安全政策<br>• 支援多個 PIN 的功能<br>• SafeNet IDPrime 系列皆可客製(卡面和程式碼) |
| **Thales applets（可選擇）** | |
| **MPCOS** | • 電子錢包 & 安全數據管理應用程式 |
| **晶片特點** | |
| **技術** | • 用於對稱及非對稱的嵌入式加密式引擎 |
| **壽命** | • 至少 500,000 寫入 / 清除週期<br>• 數據保留至少 25 年 |
| **認證** | • CC EAL6+ |
| **安全性** | |
| | • SafeNet IDPrime 智慧卡包含針對各種硬體和軟體的多種攻擊策略：旁道攻擊(side-channel attacks),侵入攻擊(invasive attacks),進故障攻擊(advanced fault attacks)和其他類型的攻擊<br>• The SafeNet IDPrime 940 通過了 Java 平台的 CC EAL5+ / PP Java 卡認證 與 Java 平台和 PKI applet 組合的 CC EAL5+ / PP QSCD 認證,以及 eIDAS / Signature / eSeal 和法國的 ANSSI 認證 |