

SafeNet IDPrime 3930

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。

SafeNet IDPrime3930 是雙介面智慧卡，允許通過觸摸或非觸摸式連接 ISO14443 介面，也與大部分 NFC 讀卡機相容。



與任何環境相容

除了無縫整合到Windows 環境系統之外，SafeNet IDPrime 3930 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。

優點

- **雙介面**- SafeNet IDPrime 3930 提供ISO 7816 接觸式介面和 ISO 14443 非接觸式介面，也與大部 NFC 讀卡機相容
- **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**-400KB
- **與任何環境相容**- SafeNet Authentication Client完全支援SafeNet IDPrime 3930
- **符合FIPS法規**- SafeNet IDPrime 3930 通過Java 平台和API 程式的FIPS140-2 Level 2和Level 3
- **多應用智慧卡**- SafeNet IDPrime擁有晶片內小程序式可選擇。例如MPCOS的電子錢包程式。
- **強化加密支援**- SafeNet IDPrime 3930提供高達4096的RSA和高達521 bits的橢圓曲線的PKI服務

強大的安全性

SafeNet IDPrime 3930 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 3930通過Java平台和PKI 程式的FIPS140-2 Level 和Level 3認證。

可選晶片內的程式

SafeNet IDPrime 是多應用的智慧卡，代表晶片內有各種功能的程式可選擇，可增加MPCOS的程式來使用電子錢包和數據管理服務。

產品特點	
記憶體容量	<ul style="list-style-type: none">SafeNet IDPrime 3930 擁有 400 KB Java Flash 晶片記憶體。在此標準配置中，可用於憑證和其他小程式(Applet)和數據的記憶容量為 78 KB
標準規範	<ul style="list-style-type: none">BaseCSP minidriver (SafeNet minidriver)Global Platform 2.2.1Java Card 3.0.5ISO 7816 和 ISO 14443
支援系統	<ul style="list-style-type: none">Windows, MAC, Linux
加密演算法	<ul style="list-style-type: none">Hash: SHA-1, SHA-256, SHA-384, SHA-512.RSA: 最高 RSA 4096 bitsRSA OAEP & RSA PSSP-256 bits ECDSA, ECDH. P-384 & P-521bits ECDSA, ECDH晶片內非對稱金鑰生成 (高達 4096 bits 的 RSA 和高達 521 bits 的 Elliptic curves)對稱式演算法 AES 可用於安全訊息傳遞及 3DES 用於 Microsoft® Challenge/Response
通訊協議	<ul style="list-style-type: none">T=0, T=1, PPS, 通訊速率可達 446 Kbps at 3.57 MHerz (TA1=97h)T=CL, ISO 14443 速率高達 848 kbs 的 type A,
其他特點	<ul style="list-style-type: none">晶片內建 PIN 的安全政策支援多個 PIN 的功能SafeNet IDPrime 系列皆可客製(卡面和程式碼)
Thales applets (可選擇)	
MPCOS	<ul style="list-style-type: none">電子錢包 & 安全數據管理應用程式
晶片特點	
技術	<ul style="list-style-type: none">用於對稱及非對稱的嵌入式加密引擎
壽命	<ul style="list-style-type: none">至少 500,000 寫入 / 清除週期數據至少保留 25 年
認證	<ul style="list-style-type: none">CC EAL6+
安全性	
	<ul style="list-style-type: none">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),先進故障攻擊(advanced fault attacks)和其他類型的攻擊SafeNet IDPrime 3930 通過 Java 平台和 PKI 程式的 FIPS140-2 Level 2 和 Level 3 認證