iKey 2032

個人的 USB 認證與加密裝置

iKey™ 2032是一款雙因素認證裝置，提供網路認證、電子郵件加密與數位簽章應用程式的用戶端安全性。

SafeNet的 iKey 2032 是一款 USB 式攜帶型 PKI 認證裝置，可以產生與儲存私密金鑰及數位憑證，尺寸小且能繫在鑰匙圈上。iKey 2032 是智慧卡的延伸，只要插入 USB 埠就能提供強大的使用者認證功能，而不需要另購昂貴的讀卡裝置。iKey 2032 是專為支援廣泛的桌上型電腦應用程式和可攜式系統而設計的。成本低廉、外型小巧，為標準 USB 介面，iKey 2032 比其他麻煩的智慧卡或單次性 (one-time)PIN裝置更容易運用。其 FIPS Level 2 驗證硬體和機板內建的金鑰產生、金鑰儲存、加密及數位簽章，能確保用戶端應用程式的高度安全。

以雙因素認證取代脆弱的密碼

iKey 2032 將雙因素認證功能帶入需要高度安全性的應用程式中。和仰賴脆弱、容易被猜中的傳統密碼認證方式不同，iKey 2032需要實體裝置（即包含使用者唯一 PKI 金鑰的 iKey)和使用者的 PIN 才能完成認證程序。
錯誤PIN輸入超出限制次數會導致它鎖定,保護它在遺失後被拾獲者攻擊PIN進行非法使用。

獲數百套應用程式支援

iSafeNet 和軟硬體廠商共同合作，使得 iKey 成為最廣泛支援的安全解決方案。包括 Single Sign On/智慧卡登入、VPN 認證、電子郵件加密、數位簽章及其他許多來自 Microsoft、Entrust、Computer Association、VeriSign等領導廠商且內含 PKI 功能的應用程式都支援 iKey。iKey 2032 支援 PKCS#11 和 Microsoft CryptoAPI，可以輕易整合於自訂應用程式中。

通過 FIPS 140-1，Level 2 驗證的硬體安全性

iKey 2032 通過 FIPS 140-1，Level 2 的驗證，能為需要高度實體與運作安全性的應用程式提供高度的保護能力。

主要特性

小巧便利

iKey 2032 比一條口香糖還小，但能提供許多重要的安全功能。它的小巧外型與堅固耐用、防竄改型的結構使其便於攜帶，讓使用者能夠隨身攜帶其獨一無二的數位身分識別。

USB 連線部署容易

iKey 2032 提供智慧卡的安全性，而不需要智慧卡讀卡機。它具有一個內建的 USB 1.1/2.0 埠，可以輕鬆連接任何電腦。您不需要購買、維護昂貴的智慧卡讀卡機或特殊的生物測定裝置來加強您的安全應用程式 – iKey 讓您輕鬆享有智慧卡的安全性而省去這些麻煩。

機板內建的加密處理能力

和其他智慧卡或硬體裝置式 (token-based) 系統不同，iKey 2032 於機板上內建金鑰產生與加密處理功能，能確保加密金鑰與各功能的高度安全。

認證

FIPS 140-1 Level 2
Common Criteria EAL 2
RoHS
China RoHS
FCC Part 15 - Class B
CE

SafeNet®
The Foundation of Information Security

獲世界上許多安全應用程式採用

iKey 2032 已經被許多應用程式採用，包括 Single Sign On/智慧卡登入、VPN 認證、電子郵件加密、數位簽章及其他許多來自 Microsoft、Entrust、Computer Association、VeriSign 等領導廠商且內含 PKI 功能的應用程式。iKey 2032 支援 PKCS#11 和 Microsoft CryptoAPI，可以輕易整合於自訂應用程式中。

技術規格

系統需求

支援的作業系統

- Microsoft Windows 95、Windows 98、Windows NT (SP4)、Windows ME Windows 2000、Windows XP、Microsoft Vista Windows 2003
- Apple Mac OS 10.4.6 (Tiger) and above

加密式應用程式介面

- PKCS#11 v 2.01
- Microsoft CryptoAPI (CAPI) 2.0
- Microsoft PC/SC
- Apple Native PC/SC

硬體加密驗證

- 通過FIPS 140-1Level 2的驗證–憑證編號161

加密功能

- 非對稱金鑰對產生(RSA)
- 對稱金鑰產生(DES、3DES)
- 硬體防護式金鑰管理與儲存私鑰禁止匯出
- 機板內建數位簽章功能與密碼容錯次數管理(密碼長度4~20字元)、亂數產生器

加密效能

- 1024-bit與2048-bit RSA 金鑰運作
- 金鑰產生：90秒以內，含金鑰驗證
- 數位簽章：1秒鐘內

加密演算法

非對稱金鑰加密

- RSA 1024-bit，RSA 2048-bit

對稱金鑰演算法

- DES、3DES, RC2

數位簽章

- RSA 1024-bit、RSA 2048-bit

Hash Digest運算法

- SHA-1、MD5

另支援額外的演算法

實體特性

硬體系統

- 8-bit處理器
- 32K記憶體

連接能力

- USB 1.1/2.0相容
- 每秒傳輸1.5 Mbps

尺寸

15.875mm x 57.15mm x 7.9375mm

符合規範標準

ISO 7816-3 Compliant

另提供客戶自訂品牌圖樣。

SafeNet 台灣分公司

221台北縣汐止市新台五路一段75號6樓之5

電話：*+886 2 8698 1238 ext 168*　　*eMail: Info.apac@safenet-inc.com*

tw.safenet-inc.com

經銷商