

SafeNet FIDO2裝置

為您的企業建構強大且安全的無密碼認證



跨入2020年，企業積極擴充數位轉型計畫並轉移到雲端，而大多數的安全事件都和身分識別竊盜有關。許多企業已投資強力認證方案，包括以PKI為基礎的認證。

面對物聯網的快速發展，企業在安全與便利上又將面臨新的挑戰，必須涵蓋一些新的使用例，同時在安全和便利之間維護最佳平衡。

企業如何做到讓使用者可以從任何裝置享有無縫且免密碼的登入體驗？他們如何支援這些新使用例而不用汰換認證系統？領先全球的數位安全公司Thales針對這些問題推出二款新的SafeNet FIDO2裝置：SafeNet IDPrime 3940 FIDO (智慧卡)與SafeNet eToken FIDO (USB token)。這些新方案讓企業藉由一個整合的存取管理與認證技術，確保安全的移轉到雲端以及維護混合環境的存取安全。

無密碼認證

無密碼認證是以其他身分識別方法取代傳統密碼，改善認證與便利性。這種認證方法因為能夠簡化使用者的登入體驗並排除文字密碼本身承襲的脆弱性，因此已獲得廣大肯定。其優勢包括減少摩擦、為每一應用程式提供更高安全性、以及免除傳統密碼。

PKI客戶的自在使用

這項方案最大效益之一就是仰賴PKI認證的企業現在可以使用PKI-FIDO智慧卡，讓使用者能夠安全的以一個單一認證裝置存取傳統應用程式、網域和雲端服務，加速企業的雲端和數位轉型。

FIDO2與PKI支援 - All in One裝置

SafeNet IDPrime 3940 FIDO智慧卡專為PKI-based應用而設計，搭載 SafeNet minidriver，能完美整合並支援Microsoft環境而無需任何額外的中介軟體。

這個雙介面智慧卡可藉由接觸式介面或非接觸式的ISO14443介面通訊，並且相容於一些NFC讀卡機。

SafeNet IDPrime 3940 FIDO智慧卡擁有支援Java平台的CC EAL5+/PP Java Card認證，以及支援Java平台和PKI applet的CC EAL5+/PP QSCD認證。SafeNet IDPrime 3940取得French ANSSI認證並且符合 eSignature與eSeal應用的eIDAS規範。再者，SafeNet IDPrime 3940 FIDO支援FIDO 2.0 and U2F標準。

具備接觸感測的USB 載具

SafeNet eToken FIDO為尋求部署無密碼認證的企業提供理想方案。這個認證器是一種小型化的防盜換(tamper-evident) USB token，提供第三個認證因子：你擁有的物件(實體載具)、你已知的東西(PIN)、你要做的事情(碰觸載具)。

關鍵效益

SafeNet FIDO2裝置協助你在任何環境構築強大且安全的無密碼認證。

關鍵效益包括：

- 藉由一個PKI/FIDO智慧卡確保安全的移轉到雲端以及維護混合環境的存取安全。
- 安全且容易在多重作業系統存取。
- 無密碼存取雲端應用程式和網域。
- 運用您的PKI認證基礎 - 無需汰換！
- 為使用者提供滿足所有需求的單一認證器。
- CC認證。
- 支援所有裝置和作業系統(無需部署中介軟體)。
- 完全可客製化。
- 數位簽章和電子郵件加密的理想方案。



Product Characteristics

SafeNet IDPrime 3940 FIDO Smart Card

Memory	<ul style="list-style-type: none"> • SafeNet IDPrime 3940 is based on a 400 KB Java Flash memory chip. A standard SafeNet IDPrime 3940 FIDO comes with 20 key containers. • The memory available for certificates and other applets & data in this standard configuration is 73 KB.
Standards	<ul style="list-style-type: none"> • BaseCSP minidriver (SafeNet minidriver) • Global Platform 2.2.1 • Java Card 3.0.4 • ISO 7816 and ISO 14443 • FIDO 2.0 and U2F certifications
Operating systems	<ul style="list-style-type: none"> • FIDO application supported in Windows 10 and other FIDO compliant operating systems. • Standard PKI application supported on Windows, MAC OS X and Linux
Cryptographic algorithms	<ul style="list-style-type: none"> • Hash: SHA-1, SHA-256, SHA-384, SHA-512. • RSA: up to RSA 4096 bits • RSA OAEP & RSA PSS • P-256 bits ECDSA, ECDH. P-384 & P-521 bits ECDSA, ECDH are available via a custom configuration • On-card asymmetric key pair generation (RSA up to 4096 bits & Elliptic curves up to 521 bits) • Symmetric: AES—For secure messaging and 3DES for Microsoft Challenge/Response only
Communication protocols	<ul style="list-style-type: none"> • T=1, T=0, PPS, with baud rate up to 446 Kbps at 3.57 MZ (TA1=97h) • T=CL, ISO 14443 type A, with speed up to 848 Kbps
Other features	<ul style="list-style-type: none"> • Onboard PIN Policy • Multi-PIN support • SafeNet IDPrime family of cards can be customized (card body and programming) to fit customers' needs.
Chip characteristics	
Technology	<ul style="list-style-type: none"> • Embedded crypto engine for symmetric and asymmetric cryptography
Lifetime	<ul style="list-style-type: none"> • Minimum 500,000 write/erase cycles • Data retention for minimum 25 years
Certification	<ul style="list-style-type: none"> • CC EAL6+
Security	<ul style="list-style-type: none"> • SafeNet IDPrime 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 SafeNet IDPrime 3940 FIDO is both CC EAL5+ / PP Java Card certified for the Java platform and CC EAL5+ / PP QSCD certified for the combination of Java platform plus PKI applet, is eIDAS qualified for both eSignature and eSeal, and qualified by the French ANSSI.



Product Characteristics

SafeNet eToken FIDO

Memory	<ul style="list-style-type: none">• 80K
Standards	<ul style="list-style-type: none">• API and Standards Support: FIDO 2.0 and U2F
Operating systems	<ul style="list-style-type: none">• FIDO application supported in Windows 10 and other FIDO compliant operating systems
Physical	
Dimensions	<ul style="list-style-type: none">• 6mm * 8mm * 40.5mm
Operating Temperature	<ul style="list-style-type: none">• 0° C to 70° C (32° F to 158° F)
Storage Temperature	<ul style="list-style-type: none">• -40° C to 85° C (-40° F to 185° F)
Humidity Rating	<ul style="list-style-type: none">• 0-100% without condensation
Water Resistance Certification	<ul style="list-style-type: none">• IP X7 – IEC 529 -
USB Connector	<ul style="list-style-type: none">• USB type A; supports USB 1.1 and 2.0 (full speed and high speed)
Casing	<ul style="list-style-type: none">• Hard molded plastic, tamper evident
Memory data retention	<ul style="list-style-type: none">• At least 10 years
Memory cell rewrites	<ul style="list-style-type: none">• At least 500,000

SafeNet IDPrime 3940 FIDO/ SafeNet eToken FIDO is compatible with Microsoft Azure Active Directory accounts.

關於Thales的SafeNet存取管理與認證方案

Thales領先業界的存取管理與認證方案讓企業能夠集中管理並確保安全存取企業IT、Web和雲端應用程式。企業可以運用以政策為基礎的單一登入與通用認證方法，有效預防入侵，安全轉移到雲端並簡化資料法規遵循程序。

關於Thales

不論任何企業在個資保護的技術上都透過Thales 保護他們的資料。在資料安全方面，企業面臨著越來越多的決定性時刻。無論是建置 加密策略，移轉到雲端還是滿足合規性要求，在邁向數位化轉型時，您可以依靠Thales來保護您的有價資料。