企業為了符合資安國際標準ISO27001 需要加強登入密碼強度，卻常遭遇到以下困境？

過於繁複記不住

符合了密碼強度，卻連自己的密碼都記不住？

無限重覆共用

為免遺忘，各系統帳號密碼永遠使用同一組？

無隱私無保障

不得已將複雜難記的密碼抄寫後貼在電腦旁？

後疫情時代下居家辦公（ WFH, Work From Home ）帶來資安挑戰

疫情改變社會的工作型態，同時加速推動數位轉型，以建構企業營運的韌性。企業勢必採取混合辦公模式，在資安威脅事件暴增，駭客攻擊手法持續進化的壓力下，網路環境的日趨複雜，讓企業資安面臨前所未有的重大挑戰，如何讓資訊系統持續正常運作，是企業永續經營的關鍵。

居家辦公需採用虛擬私人網路（VPN，Virtual Private Network）、雲端或各種遠端工具，在連線時間變長、使用者變多、流量變高的狀況下，資安的風險也隨之放大，駭客盯上居家辦公的弱點，對於ＶＰＮ設備的攻擊、竊密、破解紛紛出籠，出現重大資安破口，以資安面來說，帳號密碼一向是最弱的環節，再複雜的密碼也可能會被駭客竊取，進而偽裝成合法身份者來連線，單純的加強密碼已經無法完全保證資訊安全，而從管理層面看來，人員權限控管實屬不易，常有離職員工依然可以登入企業內部權限的狀況，尤其在遠端工作的狀態下，連線身份也存有疑慮，因為無法真正確認另一端的登入對象的身份以及裝置的狀況，且外部人員帳號密碼共用也多有發生，提供給合作廠商的帳號密碼可能多人共用，合作結束時也持續保有權限等等，都有可能造成企業重大損失，而基於前列原因，企業資安部門勢必急需著重如何“提高遠端身份登入的安全強度“

疫情下WFH遠端登入存取的資安挑戰

VPN設備帳號密碼被破解

人員權限管理不易

無法確定使用者的實際身份

外部廠商帳號密碼多人共用

ABOUT US

致力於無密碼身份認證與機敏文件保護，建立企業資訊安全應用的強固基礎。除此之外，**KeyXentic**更強調「簡化資訊安全系統建置複雜度」、「降低管理者負擔」、「掌握資訊安全所有權」等影響企業組織核心競爭力的面向，提供無感式的資安產品，同時也提供客製化的服務，使產品能為企業組織強化競爭優勢，降低資安成本，大幅提昇企業組織的核心價值。

關楗股份有限公司
KeyXentic Inc.
Website | www.keyxentic.com
Email | contact@keyxentic.com
Phone | +886-2-2883-4283

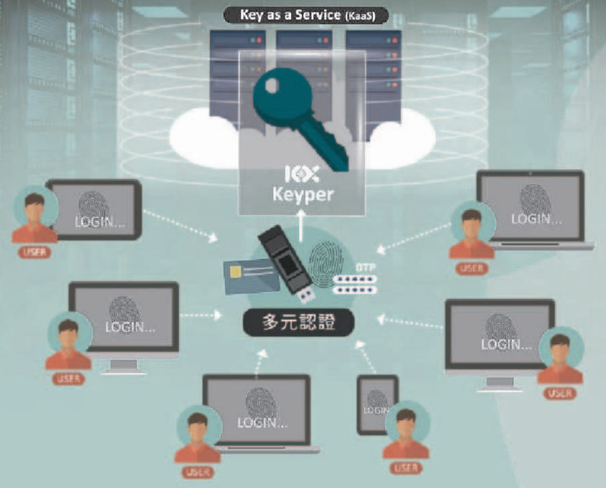
Keyper

無密碼身分認證 Passwordless Authentication

無痛雙因素驗證整合服務

Keyper

Passwordless Authentication
無痛雙因素驗證整合服務



一指登入 | 無痛整合 | 雙因認證 | 國際標準 | 管理方便

簡單智慧

- 整合各種身分認證機制，可根據使用者不同情境使用。
- 提供標準RESTful API整合，減少各種SaaS整合身分驗證機制的複雜度。
- 提供方便管理介面，降低資訊安全管理部門的工作量，輕鬆管控身分驗證與權限。

高度安全

- 強化帳號登入的安全性，能避免網路釣魚及鍵盤側錄竊取帳號密碼等攻擊
- 可加強採用實體安全金鑰或是指紋生物識別。
- 避免使用者設置簡單密碼易遭受駭客竊取以及帳號管理不當等資安風險。

關鍵無密碼身分認證解決方案，無痛整合各種應用的雙因素認證，提供無密碼身分登入驗證管理機制，可加強使用指紋生物辨識，完整解決複雜密碼疲勞的問題，有效幫助企業安全管理帳號密碼及加強資訊安全。

網路資料外洩已成為新常態，國際上知名企業幾乎都曾遭受重創，連科技巨擘微軟、Google也不例外，紛紛投入近千億的資安防護資金，並且宣布無密碼時代的來臨。
傳統以帳號密碼驗證身份的方式已不再是最安全可靠的登入途徑了，就在網路日漸發達、雲端服務四起的背景之下，造就了新世代的網路識別標準 FIDO2（Fast Identity Online II）的問世。
FIDO2 是指由非營利組織 FIDO 聯盟所訂定的一套網路識別標準，旨在確保登入流程中伺服器及終端裝置協定的安全性，其最大的特色在於採用分散式處理的方式將個資分別存放在使用者的終端裝置上，再透過公鑰及私鑰的架構來登入雲端服務，這樣一來，使用者的個資就不必被上傳到雲端，且使用者可以選擇透過指紋、聲音及隨機的驗證碼來作為線上登入。此標準支援各大系統平台以及網頁瀏覽器，這樣的協議能讓使用者再更多的平台及裝置上透過 FIDO2 標準進行身份驗證，拉開無密碼時代的序幕。

無密碼的新旅程生活

比密碼更安全的保護 雙因素驗證 2FA (Two Factor Authentication)

為解決帳號密碼的困境，除了無密碼的趨勢外，目前最快速有效的解決方法就是使用2FA雙因素驗證，輸入帳號密碼之餘，多增一道強化身份驗證的安全關卡與因子，用以確保資訊安全，如：回答安全問題、一次性密碼（OTP, One Time Password）、隨身攜帶安全性鑰匙等等，最終都是為了更加守護自己的數位資產。

增強2FA驗證機制 實體安全金鑰

值得注意的是，新型的駭客攻擊手法中，增加許多針對2FA破解的手法，像是利用釣魚網站來欺騙使用者回答安全問題，或是監看一次性簡訊，進而竊取身份，所以目前最高效益的做法依然是“隨身攜帶安全性鑰匙”，也就是擁有屬於自己的安全金鑰Token，並且隨身攜帶，實體資產有鑰匙保護，數位資產也需要一把鑰匙，並以此作為2FA的驗證方式，才能真正保護數位資產。

更智慧安全的 帳號登入選擇

關鍵無密碼遠端身份認證管理解決方案Keyper　也為此而生，無痛整合各種應用情境的雙因素認證，提供各種整合模組下載即可安裝使用，例如: KX-Radius-Agent瞬間增強企業VPN資安強度。另外在整合網站的雙因素驗證，可選擇使用手機OTP或是插入硬體式KX-Token執行2FA雙因素驗證即可，輕鬆掌握登入人員的身份及權限，確保各種行為的不可否認性，解決方案符合國際標準FIDO2，不僅易於操作，且可以確保人員權限，增強安全性，實現安全且便利的登入管理，進而提高企業生產力，是企業不可或缺的最佳方案。

便利的各種模組，滿足各種環境需求

Keyper 優勢特色 ADVANTAGES

無痛雙因素驗證整合服務

多元整合模組

- 減少各種SaaS的整合複雜度。
- 幫助企業快速上手，擺脫弱密碼威脅。

實體安全金鑰2FA

- 利用實體安全金鑰及生物辨識功能，來執行2FA加強保護帳號密碼登入安全。

支援FIDO國際認證

- 符合國際安全標準，提供企業無密碼登入、無密碼2FA選項

無痛整合VPN與2FA

- KX-Radius-Agent下載及安裝，即時加強遠端登入防護
- 透過周密無縫的登入防護及2FA消除安全漏洞
- 防堵透過VPN連線建立網路立足點的安全漏洞

Web介面管理系統

- 方便的Web化管理介面，輕鬆管控帳號與權限。
- 圖形式統計資料，降低資訊部門工作量，減少管理上疏失與遺漏。

電子簽章服務

- 整合各種文件與PDF電子簽章功能。
- 適用於各種雲端簽章系統。

遠端登入保護

- 支援Windows RDP登入
- 支援SSH遠端連線登入

加密貨幣協議

- 支援各種加密貨幣協議。
- 輕鬆整合加密貨幣交易所登入交易應用。