cpl.thalesgroup.com

THALES

存取管理手冊

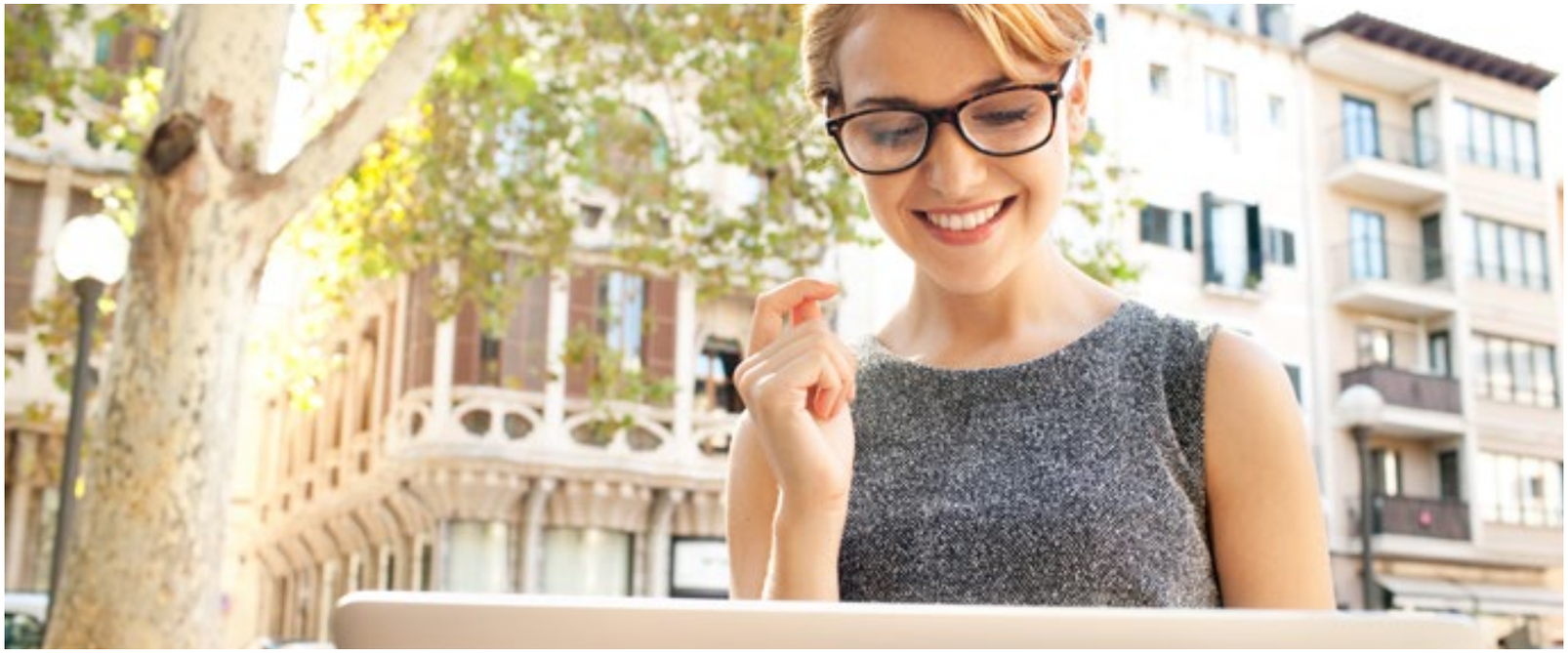
目錄

簡介

多年來，您或許已聽過很多關於存取管理的話題。事實上，我們傾向於將驗證(authentication)和存取管理(access management)當成同一件事看待。但實際上二者是不同的。驗證指的是驗證使用者的身分，而存取管理則用於判定使用者是否具有某一特定資源的存取權並且執行一些已針對該資源設定的存取政策。

存取管理對於雲端資源的存取管控而言非常重要。使用者現在一天當中都會存取多種雲端應用程式，這對於使用者和IT部門而言都很繁瑣，因為使用者必須記住無數的密碼，而IT則需要不斷的重設那些被遺忘的密碼。解決這個問題的方法就是單一登入(SSO)：以一個認證憑證適用於所有雲端應用程式，使用者可以輕鬆的一次登入數個應用程式，而IT也省下密碼重設的時間。

單一身分識別的安全取決於用來確認身分的驗證方法，因此驗證方法是維護雲端存取安全的最重要因素。為此，存取管理方案和單一登入必須針對每一應用程式的存取政策提供細緻分級的管控。在高風險環境要求額外的驗證因子，將可維護零摩擦的使用者體驗。



存取管理術語

驗證與存取管理

驗證與存取管理方案是由身分識別治理與管理(Identity Governance and Administration; IGA)和存取管理(Access Management; AM)功能組合而成。IAM提供一種方法架構以授予應用程式存取權(IGA)、執行存取控制(AM)和確保存取事件的能見度(AM)。由於大多數組織都個別部署IGA和AM元件，因此這些措施越來越被視為個別的獨立方案，而非一種單一驗證與存取管理套件的組合功能。

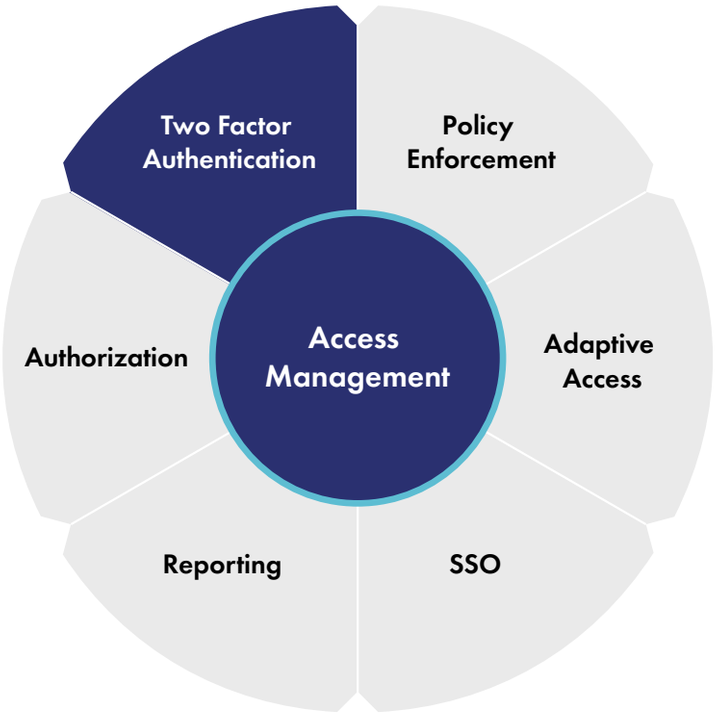
存取管理

存取管理用於判定使用者是否具有某一特定資源的存取權並且執行一些已針對該資源設定的存取政策。

存取管理是根據IT管理者訂定的存取政策而建置，其資訊包括允許那些使用者群組(例如銷售、研發、人力資源)存取那些雲端應用程式(例如Salesforce、Office 365、Jira、Taleo)，以及存取該等應用程式所需的使用者屬性(例如信任網路、密碼、OTP)。

存取政策可以依照雲端應用程式的敏感程度，要求評定更多或較少的使用者屬性。這些屬性的評定是依照風險或脈絡(context)進行驗證，這也是執行每一雲端應用程式不同存取政策的核心(詳見：脈絡驗證)。

同樣屬於雲端存取管理核心的單元就是單一登入(single sign-on)，這項機制允許使用一組單一的使用者名稱密碼登入使用者的所有雲端應用程式(詳見：單一登入)。

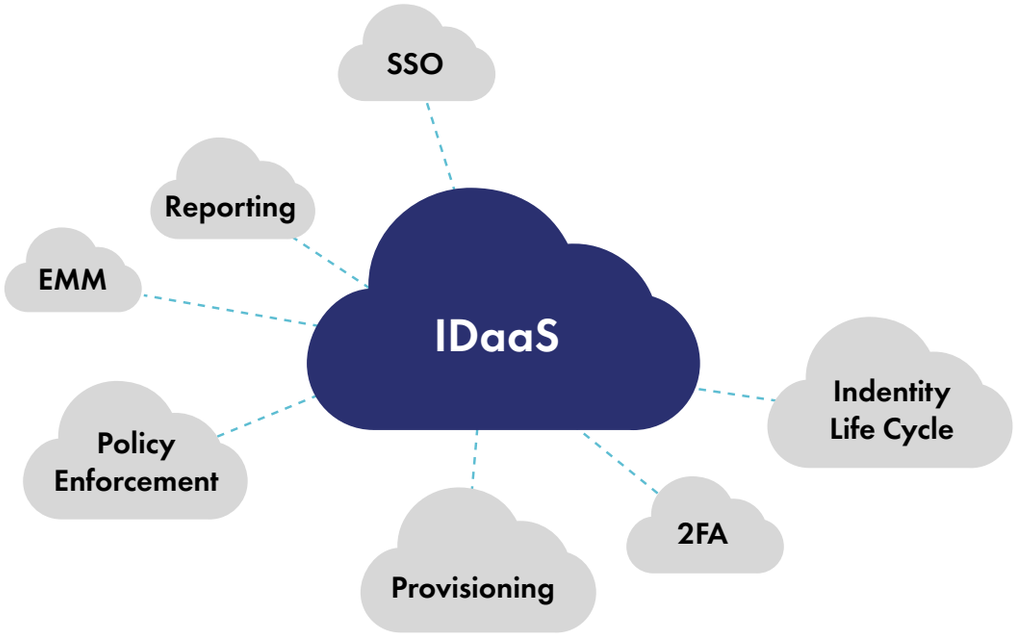


IDaaS

IDaaS全名是IAM-as-a-Service，也稱為身分識別服務(identity-as-a-service)，它是以雲端服務交付模式提供存取管理與驗證的一種身分識別與存取管理(Identity and Access Management (IAM)方案。IDaaS雖然這幾年來被視為一個個別的市場，但以最近的市場趨勢來看，未來將會被視為二項個別的技術，亦即存取管理和IGA，其交付方法包括地端、軟體或雲端平台。

身分識別治理與管理

身分識別治理與管理(Identity Governance and Administration; IGA)方案協助回答以下問題：「誰應獲得存取權？」、「誰允許存取何種應用程式？」、「誰由何人於何時授予何種應用程式的存取權？」等。例如，IGA方案可協助設定允許研發人員存取特定開發應用程式，例如GitHub、Jira和Confluence - IGA方案可以根據他們的研發團隊成員，自動配置這些應用程式的存取權。研發人員也可以請求其他應用程式的存取權，而此等請求將需通過某些IGA方案支援的管理審核程序。



聯合身分識別

聯合身分識別(identity federation)是透過一個稱為信任身分識別供應者(Identity Provider; IdP)的單一系統執行使用者身分驗證，每當使用者嘗試存取雲端應用程式時，應用程式將把驗證程序轉傳到身分識別供應者。聯合身分識別協助企業解決必須個別管理多個Web應用程式(不論內部或外部應用程式)使用者認證所帶來的挑戰與挫折。聯合身分識別仰賴一些協定例如SAML和Open ID Connect，以及一些專屬協定例如Microsoft的WS-Federation。

聯合登入

聯合登入(Federated login)是聯合協定例如SAML、Open ID Connect及其他的一項功能，它運用身分識別供應者模式對使用者進行身分驗證，並以一種驗證判定(authentication assertion)形式將驗證資訊轉傳至目標系統。判定內容包含一個「接受」或「拒絕」的回應，亦即否定或授予使用者存取權。

聯合登入讓使用者只需登入一次就可以同時存取他們的所有雲端應用程式。使用者不需要使用不同的帳密登入個別的雲端應用程式，而可以藉由聯合登入功能在上班時間從企業網路或下班後經由VPN登入office 365、Salesforce、AWS等。

聯合身分識別(identity federation)是透過一個稱為信任身分識別供應者(Identity Provider; IdP)的單一系統執行使用者身分驗證，每當使用者嘗試存取雲端應用程式時，應用程式將把驗證程序轉傳到身分識別供應者。

身分識別供應者

SAML及其他聯合身分識別協定能夠在非隸屬的網站之間安全交換身分識別資料，它們是奠基於一種身分識別供應者(Identity Provider; IdP)和服務供應者(Service Provider)的模型之上。當使用者存取雲端服務時將被重導至信任的身分識別供應者以接受驗證和授權。身分識別供應者驗證使用者資料(例如cookie、裝置、網路、OTP)並產生一個「接受」或「拒絕」的回應，然後送到服務供應者。授權資料可能包括允許從webmail帳號存取郵件地址，或者從社交網路帳號存取好友名單等資訊。

例如，SafeNet Trusted Access可以在使用者存取雲端應用程式時執行「身分識別供應者」功能。

安全代碼服務

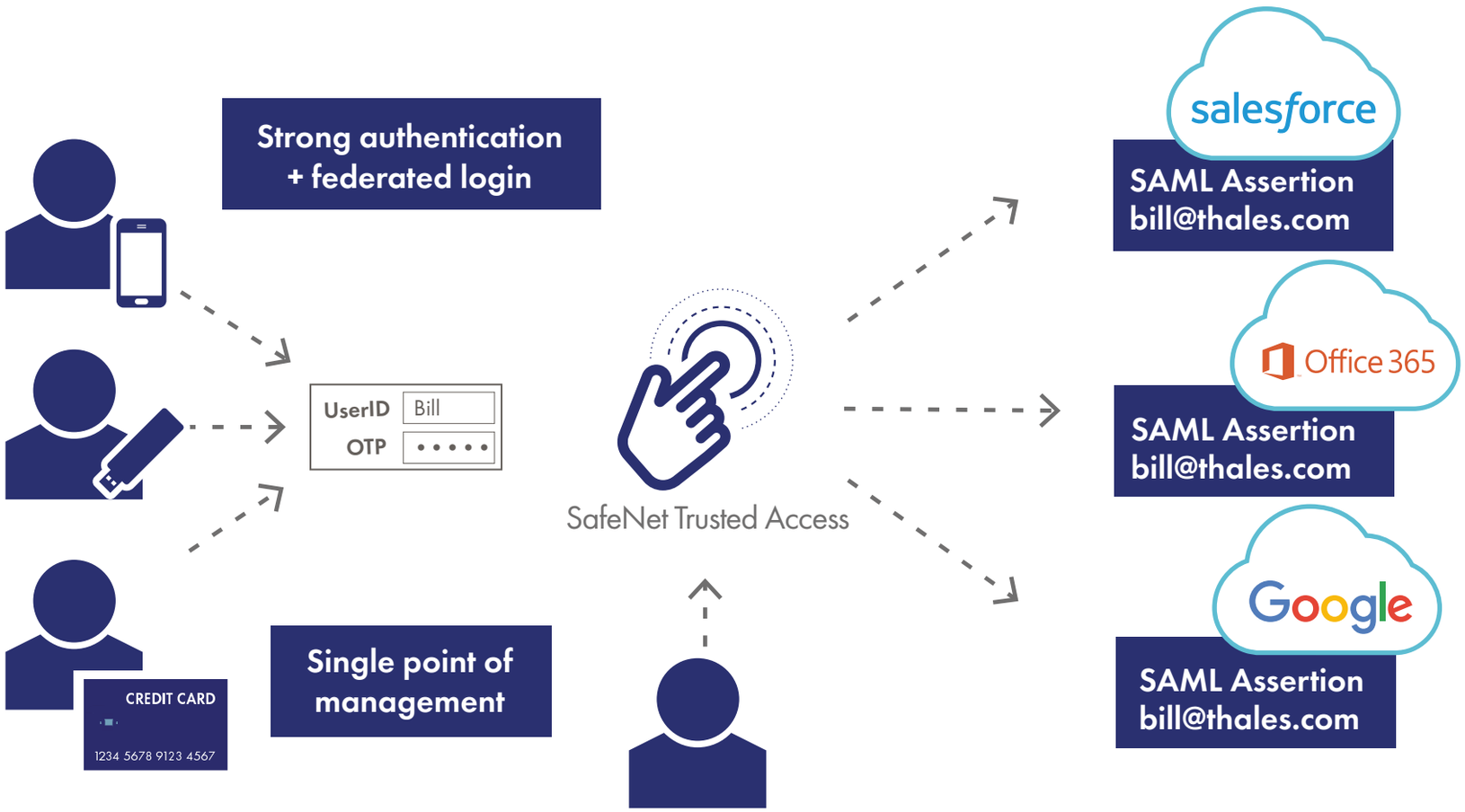
身分識別供應者模式也稱為以代碼為基礎的驗證或安全代碼服務(Security Token Service; STS)。安全代碼服務等同於一個身分識別供應者，而委託者(Relying Party; RP)則相當於一個服務供應者(Service Provider)。其交換的資訊不叫做SAML驗證判定，而稱之為安全代碼，名稱不同但概念一樣。

SAML

SAML全名為安全判定標記語言(Security Assertion Markup Language)，是以XML為基礎的開放標準，在非隸屬網站之間交換驗證資料，這項功能也稱為聯合身分識別或聯合身分驗證。聯合身分驗證將使用者現有的企業身分識別延伸到雲端，讓他們可以用企業帳密登入他們的雲端應用程式。雲端應用程式的SAML聯合身分驗證讓使用者可以用企業帳密登入他們所有的雲端應用程式，因此只需記憶一組帳密而不用維護一大串帳密。

SAML如何運作

當使用者嘗試登入一個雲端應用程式時，他們將被重導至一個信任的身分識別供應者以接受身分驗證。身分識別供應者收集使用者的信用憑證例如使用者名稱和動態密碼，然後產生一個回應給被存取的應用程式。這項回應稱為SAML判定，其內包含一個「接受」或「拒絕」回應。服務供應者(例如Salesforce、Office 365或DropBox)根據這項回應，阻斷或同意存取。



WS-Fed

WS-Federation Services (WS-Fed)是Microsoft的專屬聯合身分識別協定。WS-Fed是與Microsoft的Active Directory Federation Services (AD FS)共同作業，將儲存在Active Directory的身分識別延伸到Microsoft雲端應用程式例如Office 365和Azure。一如SAML，WS-Fed也使用一種身分識別供應者模式。當使用者存取Microsoft雲端應用程式時，他們將被重導至AD FS接受驗證，然後根據其回應而同意或拒絕使用者存取。

OAuth

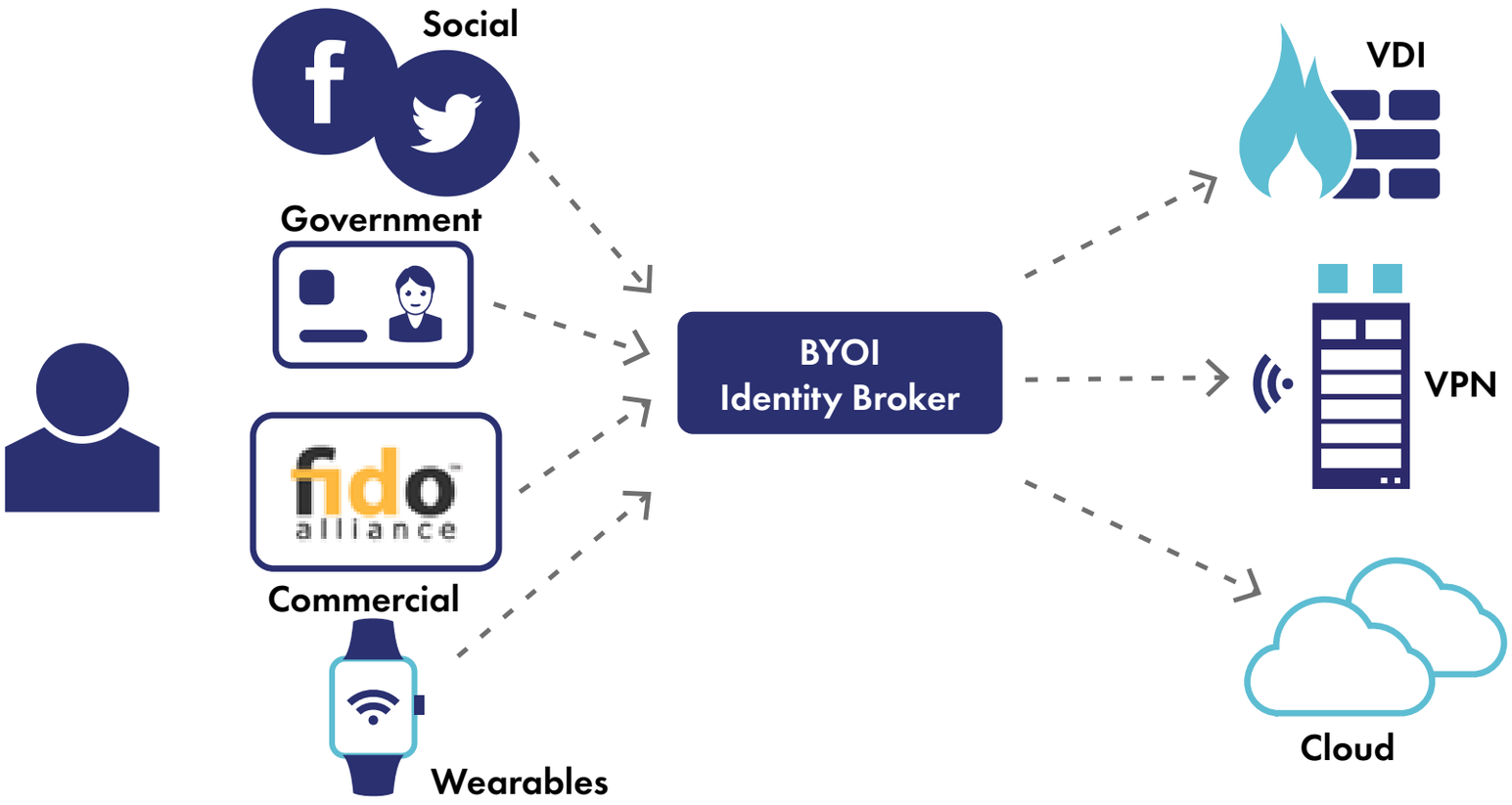
OAuth全名為開放授權(Open Authorization)，它是非隸屬網站之間聯合身分驗證或代碼授權的一種開放標準。一如其他聯合身分驗證協定例如SAML、Open ID Connect和WS-Fed，OAuth允許使用一個經由信任身分識別供應者驗證的帳密登入應用程式。OAuth不同於聯合驗證的是它允許使用者授權給委託網站存取特定帳戶資訊，例如通訊名稱與郵件地址。例如，社交網站利用OAuth協定以存取您的webmail好友名單，以及詢問您是否願意邀請您的webmail好友到您的社交網路。

Open ID Connect

一如SAML，Open ID Connect是一種採用身分識別供應者模式的開放標準聯合身分識別協定。不過，二者不同的是SAML使用cookie，所以只能適用於在瀏覽器開啟的應用程式，Open ID Connect提供一個單一登入框架，允許在以瀏覽器為基礎的應用程式、行動應用程式和桌上電腦用戶端(例如rich用戶端和一些VPN)之上建置單一登入。因此，儘管今日大多數單一登入只支援雲端和瀏覽器應用程式，但隨著越來越多身分識別供應者採納Open ID Connect，我們將可以只接受一次驗證就能同時存取我們所有的資源，不論是桌上電腦用戶端、瀏覽器的或行動應用程式。

攜帶自有身分識別(Bring Your Own Identity; BYOI)

在身分識別管理領域裡，廠商和組織正尋求方法讓員工和夥伴能夠使用他們自己的身分識別存取企業資源。理論上，此種身分識別可以是任何提供足夠確認身分的資訊，例如政府發行的身分證、健保卡，以及線上身分識別例如社交網路帳號、專業網路帳號和商業帳號例如FIDO。企業與消費者的世界日漸融合，使得企業安全團隊承受越來越大的壓力，需要建置如同消費者服務的典型認證方法。



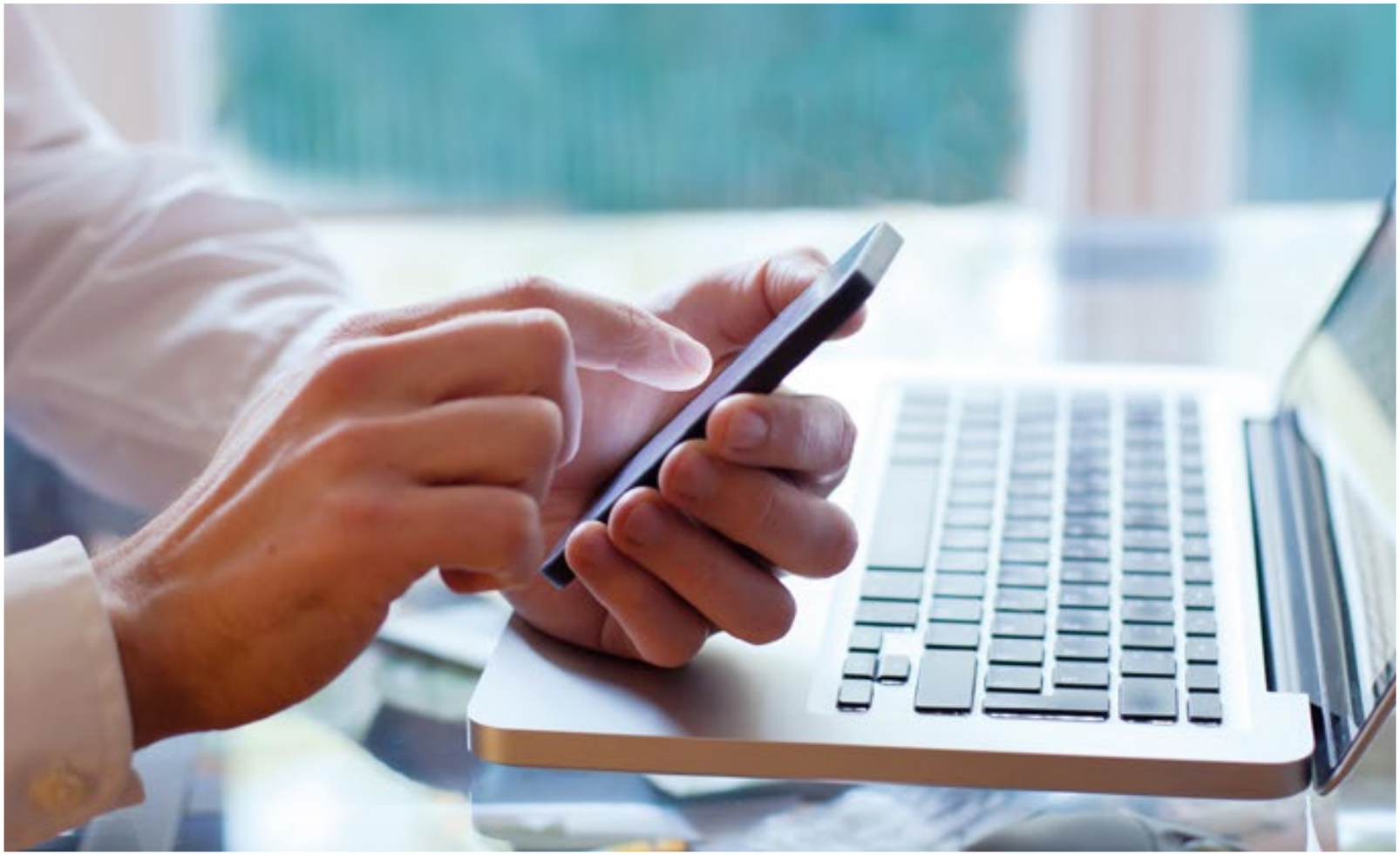
單一登入

單一登入(Single sign-on; SSO)只需驗證一次就能在其後存取資源時自動接受驗證。它免除了個別登入和驗證每一個應用程式與系統的需要，實質上擔任介於使用者和目標應用程式之間的中介者。目標應用程式和系統在背景仍保有它們自己的憑證資訊並催促使用者的系統執行登入，SSO回應那些催促並將憑證映射到一個單一的登入／密碼組。(Source: Gartner)

SSO不論是獨立方案或功能更大的存取管理方案，都可透過一系列聯合身分識別協定達成任務。這些包括開源協定例如SAML 2.0和Open ID Connect、專屬協定例如Microsoft的WS-Federation、以及其他技術例如密碼保存庫和反向代理(reverse proxies)。

密碼保存庫

聯合身分識別(identity federation)是透過一個稱為信任身分識別供應者(Identity Provider; IdP)的單一系統執行使用者身分驗證，每當使用者嘗試存取雲端應用程式時，應用程式將把驗證程序轉傳到身分識別供應者。聯合身分識別協助企業解決必須個別管理多個Web應用程式(不論內部或外部應用程式)使用者認證所帶來的挑戰與挫折。聯合身分識別仰賴一些協定例如SAML和Open ID Connect，以及一些專屬協定例如Microsoft的WS-Federation。



授權

授權(authorization)程序是為了確保獲得適當驗證的使用者僅能存取他們允許存取的資源，而使用者的存取權限是由該資源所有者或管理者設定。在消費者領域，授權也可以指使用者確保雲端應用程式(例如社交網路)僅能存取非隸屬網站的特定資訊(例如使用者的webmail帳號)。

驗證

驗證(authentication)是根據使用者登入應用程式、伺服器、電腦或數位環境時提供的憑證對其身分進行驗證。大多數憑證包含使用者擁有的資訊(例如使用者名稱)和使用者知道的資訊(例如密碼)。如果使用者提供的憑證符合應用程式或身分識別供應者儲存的資訊，使用者即成功通過驗證並取得存取權。

脈絡驗證

脈絡驗證(context-based Authentication)藉由評估使用者登入應用程式時提供的一系列輔助資訊，對使用者的身分進行驗證。使用者提供的最典型脈絡資訊包括使用者所在位置、時間、IP位址、裝置類型、URL和應用程式聲譽。脈絡驗證也稱為風險或調適性驗證，它是SSO與存取管理的核心，其目的是要盡可能的讓驗證程序透明且無痛。

單一登入和存取管理方案藉由評估使用者的登入屬性，不論其為脈絡(裝置、任務、地點)或行為(輸入速度、頁面瀏覽順序)，可以連續的以使用者的驗證層級比對每一應用程式設定的存取政策。如此，驗證程序是根據每一應用程式的存取政策以最沒有摩擦的方式進行，而非對所有企業資源採行一體適用的規則。

連續驗證

不論代碼、密碼或指紋，驗證基本上是一項是／否的決策：系統驗證使用者身分，然後允許或拒絕存取應用程式。

不過，較新的技術例如脈絡驗證或生物行為(例如輸入型態及其他物理跡證)使得驗證可以變成一種更連續性的程序。藉由評估一系列屬性例如IP位址、行動參數、已知裝置、作業系統等，脈絡或風險驗證法可以在使用者每次登入一個應用程式時進行連續的驗證。事實上，它可以在沒被使用者察覺的情形下執行這些程序。

脈絡驗證提供許多零摩擦的方法以驗證使用者身分，讓我們能夠在使用者便利性和數種雲端應用程式的分級存取控制之間取得平衡。這也是為何連續驗證概念(奠基於脈絡驗證)是雲端存取管理基礎的原因。

Thales 台灣辦公室

114 台北市內湖區瑞湖街 88 號 4 樓之 3（亞太經貿廣場C樓）

Tel : +886 2 7745 1888 ｜ Fax : +886 2 2658 3922

E-mail : apacsales.cpl@thalesgroup.com

>cpl.thalesgroup.com<