IBM 全球服務事業部 (IGS)
管理技術報告

單一登入：使用者至上

管理摘要 — 在今日的環境中，身分識別、鑑別及授權，通常都需要使用一連串的使用者名稱和密碼來完成。對於使用者來說，實在非常不方便又令人感到氣餒，而對客服中心的人員而言，更是令人頭痛。由於密碼很容易被猜中、共用、抄在紙上，或複製到不安全的檔案中，因此依賴密碼也會造成安全漏洞。單一登入 (SSO) 可以減少所需的密碼數目並自動化授權，避免這個問題。每種服務都有其優點，但就整體而言，也都能再改進，爲使用者排除障礙，提供更多價值。

您輸入 ID 及密碼登入網路，瀏覽了一些喜愛的網站及新聞群組後，該是開始專心工作的時候了。這時您按下有 貴公司標誌的圖示，然後系統請您提供拇指指紋或標記代碼。因爲您就在辦公室裏，所以在輸入板上按了一下指紋，然後進入系統。現在您可以開始使用每個小組工作區、聊天室或應用程式。接著，有個公告通知您，某位客戶已接受您的最終提案；因此您已不能再存取該小組的資源了。您突然注意到一些新訊息 — 幾個優質社群在評估您的成就及興趣資料後，決定提供您會員資格。您挑了幾個做記號，準備進一步研究。

這一切是怎麼發生的

密碼不只是件麻煩事，也可能造成障礙，這點有好有壞；好處是可以協助確保適當的身分識別、鑑別、授權及資源配置；壞處則是讓其他人無法合法參與資訊系統，因而阻擋了有所貢獻或可提供協助的人。由於目前的密碼鑑別問題層出不窮（從忘記密碼到某些英數格式被拒絕，再到與系統要求不一致），許多人因此放棄，再也不造訪需要鑑別身分的免費網站，也爲了避免重新註冊的麻煩，而停止向零售商購物，或寧可向同樣是會員的親友借 ID 來，進行一次性的交易。

單一登入 (SSO) 便是一種嘗試減少這種障礙，但又不犧牲安全性的方法。SSO 不但可協助使用者，還可藉由大幅減少密碼協助要求（客服中心排名第一的問題）的次數，以及快速輕鬆取消拒絕付費的客戶或離職員工的權限，解決管理上的問題。實施 SSO 的方法有很多種，但每種都有其優點及限制。

用戶端型 使用者可以使用密碼管理工具（如 Vince Sorensen 的共享軟體 Passwords Plus 等），讓系統「記住」眾多的 ID 及密碼，並自動送出。對使用者來說，這種方式在設定和使用上都相當簡單，但每次新增應用程式、網站或社群時，都需要進行設定。然而，缺乏業界標準的密碼格式也是個問題。此外，以 PC 爲中心的解決方案，在使用上來說非常缺乏彈性，因爲使用者只要一離開工作地點（例如外出旅行），登入便有困難。對於管理員來說，則沒有機制可徹底拒絕與支援。

伺服器型 中央伺服器可以負責所有不同密碼的管理作業。使用這種方法，使用

者可以免除一些更新方面的瑣碎工作（例如因爲轉換工作而必須重新設定），並可從許多用戶端登入。管理員也可以控制密碼的品質，例如免除不必要的密碼、定期更新密碼，甚至在必要時終止服務。此外，利用伺服器管理密碼的系統，可讓使用者在旅行或使用不同的裝置連線時，也能輕鬆存取。這種方法的限制在於，其仍需考量用戶端系統，以及使用者和伺服器之間整體環境的安全性和管理問題。而目前缺乏標準化的情形，讓這個問題更形複雜。在這種情形下，伺服器的服務不能中斷，因爲使用者在線上的一切活動，可能都必須倚賴這部伺服器。

服務型　　密碼管理也可以成爲一項服務。例如，Microsoft® Passport 便使用集中式的伺服器、Cookies 以及標準化服務，爲訂閱業務處理密碼方面的瑣碎工作。從使用者的觀點來說，在 Microsoft 伺服器和各個網站之間，可讓他們登入多個網站，並進行交易的同一組密碼非常清楚。但只有在眾多目的地均使用同一專屬服務時，服務型 SSO 對使用者才有便利可言。讓企業願意參與的一個誘因是，他們可以擷取使用者在不同網站的互動情形，以得到更全面性的客戶資料。然而，這種商業利益卻已引起各界對使用者隱私權的關切。

以上各種方法中的密碼，都可以使用標記來加強或取代；標記在實質上是一種金鑰，其中可能包含動態產生的代碼或生物辨識功能（這項功能利用了使用者的身體特點，例如拇指指紋、臉部或語音辨識）。這些方法均可提高安全性，但也帶來一些問題，這些問題包括費用、系統相容性、正向誤判（false positive，將未獲授權的使用者辨識爲已獲授權的使用者），以及負向誤判（false negative，未辨識出已獲授權的使用者）等。
就整體而言，SSO 的缺點在於，萬一有安全漏洞，使用者的身分就會被盜用，而且盜用者可獲得全面性的授權。隨著生物辨識技術不斷發展，也許將來能有方法輕鬆確保正確辨識使用者的身分。然而，安全性和易存取性之間的基本衝突仍無法輕易解決，未來在使用可能嚴重危及網路安全的層級時，可能仍有某些特定的困難。

此外，SSO 也無法靈活動態回應使用者不斷變化的需求和權益。大部分的系統或要求使用者明確建立自己身分，或需要管理員根據標準定義（例如職稱或個人背景資訊）調整存取權限。利用協同合作過濾功能，以及使用社群作爲重要資料來源，可讓識別功能和電子身分更加緊密結合。

大部分 SSO 應用程式的整體設計都很簡單，而且通常會偏向使用者或管理員，視付費者是哪一方而定。到目前爲止，還沒有一個 SSO 方法是真正創新，而且可以完全解決安全性和使用簡便性之間的衝突。

這一點對您有何意義

單一登入其實只是一種授權技術，其中並無任何突破性的元素或明顯的創新。然而，這項技術卻對使用者和管理員同樣具有吸引力，而且也可能會對目前的使用者，以及尚未使用這項服務的人產生重大影響。

多重登入的問題仍然層出不窮，讓 IT 部門爲了找出令人滿意的解決方案而備感壓力。然而這個問題卻存在著一種矛盾。例如，SSO 解決方案所採用的方法，經常會將本身轉變成多重登入解決方案，因而降低了登入問題本身的重要性。如果找不到清楚明確的解決方案，左右買方選擇解決方案的因素，可能是行銷而非方案本身的優點。

隱私權有可能成爲 SSO 的主要問題。某些限制控制了資訊的共享時，這個問題就會變得更複雜。最後，個人資訊及基本資料的所有權，也是尚未解決的社會問題，這個問題也會限制 SSO 的價值以及各界的採用意願。理想的解決方案必須能解決便利性和安全性之間的基本衝突。

兩種產業：政府和金融

由於政府和選民之間的互動種類繁多，再加上其 IT 功能的限制，SSO 對於公家機關而言極具吸引力。事實上，如果某些群組必須通過繁複的存取控制，才能取得資源及協助，那麼對他們而言就非常不利。從正面來說，資料範圍廣泛的 SSO 應用程式可以預測使用者的需求，如此不但可加快提供服務的速度，也可改進計畫和預算所根據的資訊。

金融產業所提供的眾多產品和服務，對於安全性和使用便利性的要求差異非常大。例如，小孩也許可以使用父母的信用卡，但是不能賣掉他們的股票。資產如果要用來申請貸款，可能需要經過第三方驗證。政府如果要存取資料，可能也要經過合法程序，才能確保符合法律規定。就內部而言，金融機構可能必須管理各種不同的帳戶，但可能沒有合法理由存取其他帳戶或特定資訊（例如信用卡消費模式）。SSO 提供了一個內含許多標準的架構，依據不同安全層級及不斷增加的困難挑戰，將各種管理安全性和存取權限的方法，精簡成一種。由於這種方法有利於新的資訊組合，讓資金調度和新產品開發變得更容易。

技術展望
加密
個人化
協同合作過濾功能
XML
普及運算