

身份管理

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

免責聲明：政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

目錄

摘要.....	2
I. 介紹.....	3
何謂身份管理？	3
模式和技術	3
II. 身份管理之挑戰	6
身份盜竊.....	6
身份管理之採用和優點	6
III. 結論	8

摘要

身份管理（Identity management）是過程和科技的結合體，幫助企業管理和保護組織內資訊和資源的接達。本文將討論一般的身份管理模式、認證技術和授權模式。鑑於身份盜竊的威脅日趨嚴重，企業和政府正使用最新的科技來加強保護身份，但單靠資訊保安科技是不夠的，用戶和使用身份管理系統的組織亦需要注意是否已採用了最適當的保安措施和最佳作業實務，包括採用密碼保護認證和單一登入（Single Sign-On, SSO）機制的身份管理系統。

I. 介紹

何謂身份管理？

身份管理是過程和科技的結合體，幫助企業管理和保護組織內資訊和資源的接達，同時也可保護用戶或客戶的個人檔案。整個身份管理的過程包括：決定誰可使用資源的接達權力和使用何種資源；適當地授予、改變和終結該項接達權力；管理和監控過程，以符合內部和外部政策。當個人必須確認他所宣稱的身份時，身份管理就適用了。確認方式通常是透過身份驗證，例如邊境控制（border control）所用的護照或身份證、網上銀行的登入憑證、提款機的生物特徵識別技術等。

身份管理由兩項基本要素組成：身份認證管理和身份授權管理¹。身份認證管理指的是核發和使用數位身份、憑證的過程（例如用戶名稱和密碼），以作為認證之用。身份授權管理是合併已被證明的用戶身份和授權過程，以取得接達權進入組織使用資源。稍後，本文將會討論認證和授權。

模式和技術

身份管理模式

一個實體（entity）的身份有其生命周期。例如，一個可讓員工接達公司網絡的登入帳戶，會在不同的系統平台上建立、維護、整合和刪除。用戶資訊供給（user provisioning）過程可建立員工登入憑證以及適當的接達權利，不論新的許可特權是否分派給該名員工，因應該員工的內部調職、升遷或降職等原因，對該帳戶作出維護及更新。此外，該員工的資料或密碼將透過不同資訊科技系統和平台來整合。最後，員工的登入憑證會因為離職或是退休而遭刪除。移除使用資源接達權利的過程稱為用戶資訊取消（user de-provisioning）。

三個常見的身份管理模式為²：

獨立身份管理（Isolated identity management）

¹ Peter Wood, “Implementing identity management security - an ethical hacker's view”, **Network Security**, Volume 2005, Issue 9, September 2005, Pages 12-15.

² <http://sky.fit.qut.edu.au/~josang/papers/JP2005-AusCERT.pdf>

此模式要求每一個用戶都擁有身份認證工具，以便接達每一個獨立的服務。該系統大多使用於網上服務和資源，因為服務提供者要管理該系統比較容易，但是對於用戶而言，管理是一件難事。隨著網上服務的快速增長，令用戶需要牢記繁多的身份認證工具和憑證（不同的登入名稱和密碼），帳戶管理也愈來愈困難。因此，新的身份管理模式便應運而生。

聯邦身份管理（Federated identity management）

聯邦身份管理可簡化帳戶管理問題，不同的服務提供者共同制訂一系列的協議和標準，可以認可用戶在不同服務提供者上的身份認證。儘管這些服務隸屬於不同的服務提供者，一個特定服務提供者的客戶可使用一個身份認證工具，便可接達所有的服務。在此群組中運作和推行的常見資訊交換標準科技為 OASIS（先進結構化資訊標準組織）、SAML（安全斷言標記語言）³、開放源碼方案、Shibboleth⁴等。

集中化身份管理（Centralised identity management）

在此模式中，單一服務提供者使用相同身份認證工具和憑證，PKI 的推行便是一例，憑證管理中心（CA）核發憑證給用戶，用戶便能使用相同的憑證來接達不同服務。而在准許客戶接達服務之前，所有提供者將透過相同憑證來認證客戶。另一個例子是單一登入模式（Single sign-on, SSO），也就是要求用戶登入一次，然後其他服務提供者會自動認證該用戶身份。Kerberos 認證伺服器 and 微軟網絡護照都是推行單一登入模式的例子。該模式的缺點是，如果一個受信任的身份提供者失敗的話（例如受 DoS 攻擊），所有服務提供者的一般服務皆可能受影響。

認證和授權

認證技術可使用以下其一或更多的要素：

1. 使用者所知道的東西（例如密碼）
2. 使用者所擁有的東西（例如智能卡）
3. 使用者本身即有的東西（例如指紋）

假如以上要素中，需要具備兩樣要素才可成功認證，即稱為雙重認證（Two-factor authentication），此種認證方法通常更加安全，因此網上銀行等高風險系統目前都推行此項認證方法。

授權是一個決定是否讓實體進入使用特定資產或資源的過程，常見的接達控制模式為⁵：

³ http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

⁴ <http://shibboleth.internet2.edu/>

⁵ <http://csrc.nist.gov/rbac/NIST-ITL-RBAC-bulletin.html>

1. 自主接達控制 (Discretionary Access Control, DAC)：用戶擁有可以控制的物件，個別用戶有權決定接達控制權的許可或是撤回。
2. 強制接達控制 (Mandatory Access Control, MAC)：限制用戶接達到具敏感性資訊的物件，並且對想接達敏感資訊的用戶進行正式授權。
3. 基於角色接達控制 (Role-based access control, RBAC)：接達決定權基於個別用戶在組織中的角色。

當分配接達權利給實體時，強烈建議依據最小權限原則和職務分工原則。最小權限原則指的是在執行個人職務時所需的最低特權權限，職務分工原則指的是將重要功能分配給不同的人，以避免一個人便可暗中破壞重要的過程。

II. 身份管理之挑戰

身份盜竊

目前互聯網涵蓋全世界和大部份的經濟領域，認證問題已成為互聯網電子商務的一個主要挑戰。在互聯網上，並沒有一個確定的方式，去知道接達的對象其實是誰或是什麼地方。根據 Gartner 2007 年的調查，自 2003 年以來，美國身份盜竊受害人的數量已經增加了超過 50% 以上⁶。

許多資訊系統採用用戶名稱和密碼作為認證用途，早期互聯網銀行便是採用此項認證機制。網絡日益增加的身份盜竊事件（例如仿冒詐騙 Phishing）已促使相關組織使用更加先進的認證機制，以確認它們的客戶。香港金融管理局也建議網上銀行應使用更健全的客戶認證機制⁷，有一些香港的網上銀行系統現已要求客戶登入時需輸入雙重認證，銀行客戶需輸入由銀行保安權標（security token）產生的限用一次密碼（one-time password），以及其用戶名稱和密碼才可登入。

身份管理之採用和優點

身份管理科技的進步有助加強整體身份保護，相對依賴傳統密碼科技而言，生物特徵識別技術的雙重認證正逐漸成長中，原因是生物特徵識別硬件和軟件的价格滑落。一些可作為身份確認的生物特徵識別為：指紋、掌形、視網膜辨識（retina scans）、虹膜掃描（iris scans）、面部識別系統和聲紋分析。

生物特徵認證有其優點，也有其缺點。生物特徵的身份鑑別系統並不是完全可信賴的，在認證用戶之前，用戶發現有時候需要嘗試數次才會成功。使用生物特徵識別系統的前提是客戶必須要將其生物特徵登記到系統中，而此舉可能牽涉到個人私隱之議題。

公共領域中的身份管理需要更強大的認證方法，自 2003 年 6 月 23 日起，香港政府已經發行智能身份證，使香港居民安全地接達至政府電子服務的工具⁸。另一個例子是美國推行的電子護照計劃，可提供自動身份檢驗和更寬廣的邊境保護和保安⁹。面部識別，指紋或虹膜掃描等生物特徵皆可儲存到電子護照中。

⁶ <http://www.gartner.com/it/page.jsp?id=501912>

⁷ <http://www.info.gov.hk/hkma/eng/bank/spma/attach/TM-E-1.pdf>

⁸ <http://www.smartid.gov.hk/en/index.html>

⁹ http://travel.state.gov/passport/eppt/eppt_2788.html

身份管理的好處

除了保安上的改善，執行完善的身份管理系統可為企業帶來至少兩項好處：降低成本和改善服務質素。

當企業身份管理系統建置完整時，人力資源部門不再需要處理個別使用者的身份識別，因此，只需少數人員便可處理身份管理的活動，使資訊科技操作的成本降低。此外，支援熱線要處理的身份識別問題也會減少，這也可以節省成本。

企業內的用戶常抱怨資訊科技服務的應變太慢，有了自動身份管理系統的幫助，有關處理用戶身份問題（如重設用戶名稱或其它身份管理功能）所需要的應變時間將會獲得改善，資訊科技服務的水準和用戶身份管理事項的質素便相應提高。

III. 結論

密碼仍是相當普遍的認證方法，為了降低密碼被暴力攻擊破解的可能性，應該限制登入時連續失敗的次數，也就是說在登入失敗數次之後，該帳戶便失效。此外，增加在每一次嘗試登入之間的耽誤時間，也可預防密碼猜測的活動。

在單一登入模式中，用戶只需要記得一個憑證，攻擊者一旦知道憑證時，便可侵入用戶已被授權進入的所有系統。因此，當推行單一登入機制時，額外的保安措施是必要的，以便保護重要憑證。應強制執行嚴格的密碼政策和經常更換密碼，以防密碼被猜估。額外的認證方法也可加強認證過程，例如生物特徵識別或雙重認證。要進入另一個等級的功能時，也應重新認證。此外，應設定閒置對話超時登出，以防攻擊者竊取閒置對話。

此外，建立個人職責也可確保員工對其行為負責。在資訊系統中，職責可透過確認和認證系統用戶的身份來完成，用戶名稱應只屬於單一用戶，如此，要是發生意外事故或違反資訊科技保安政策時，便有可能追蹤用戶在系統上的活動。除非是特定的商業需求，否則應加以禁止分享或共同使用同一個用戶名稱。