知識天地

為什麼我們要用OpenID？

蕭景燈研究技師(資訊科技創新研究中心)

相信每個人都有一樣的經驗，每到了一個網站，總是要重新註冊一個帳號和一組密碼，而每個人在造訪過無數個網站後，就擁有了各式各樣的帳號密碼，為了安全起見，每個人也都盡量邀免每個網站的帳號密碼都一樣，免得被有心人士拿去做了不當利用，增加麻煩，但使用者真的都很有效的管理著自己的帳號密碼嗎？有些人甚至還需要利用excel表格來管理自己的帳號密碼，以免遺失自己重要的資訊，這樣的方式，一旦檔案被他人取得，所有網路上的個人帳號資料也都曝露在危險的環境下，2006年中由數個網路服務公司，整合既有的想法與技術，共同提出的OpenID規範，適度地解決這個問題，不但可以有效的管理自己個人網路上的身份，而且只要記住一組帳號密碼，就可以悠遊在網路的世界。

而這套開放標準除了可以讓使用者免除重複註冊新網站帳號的麻煩，也可讓自己在網路上的身份進行整合，非常的方便。簡單來說，OpenID是一個以使用者為中心所推出的網路身份認證服務，且具備了下列幾項特性：

方便性

使用者只要向OpenID帳號發行者（OpenID Provider，簡稱OP）註冊一組帳號密碼後，便可以登入所有支援OpenID認證的信賴憑證者網站（Relying Party，簡稱RP），不需再註冊新的帳號及設定對應的密碼，認證流程由OP來負責，OP也提供基本身份資料交換的機制，有些RP會需要使用者再額外填寫資料。

突破性

OpenID是Identity 2.01的實踐，符合Web2.0的使用情境，單一的OpenID機制即可完成服務，並可以結合OAuth或SAML等開放標準，衍生不同的服務以符合不同需求。2008年是OpenID迅速發展的一年，包括Google, Microsoft, Yahoo!與MySpace等大型網路服務陸續宣布支援OpenID，成為OP方便其會員登入RP網站；到了2009年MySpace的OP功能正式推出，而Facebook也適時加入，成為RP可以接受不同OP來源的使用者登入，顯示出OpenID在技術上與應用上獲得多數使用者與服務商的認同。

獨特性

OpenID是一個以使用者為中心(User-Centric)的身份認證機制，當註冊一組OpenID後，使用者就擁有專屬於自己的個人認證識別，而這個URI的格式與網際網路上通用的URL相同，由於這樣的設計讓OpenID URI除了是OP與RP之間認證用獨一無二的識別碼之外，OP也可以將此URI轉為URL做為該OpenID擁有者的個人資料頁面，個人頁面的內容會因OP的功能規劃而各不相同，大致來說，OpenID URI的個人頁面，可以顯示擁有者頭像照片，以增加辨識度，亦可以顯示個人願意公開的資料，例如：個人部落格網址、工作用的e-mail、暱稱……等。OpenID同時提供代理認證（Delegating Authentication, 詳閱3.4節）的機制，讓進階的OpenID使用者可以將自己的網頁空間網址做為OpenID登入帳號。

整合性

因為OpenID提供代理認證的機制，所以使用者便可利用這樣的機制整合網路上的身份，強化個人身份的真實性，並降低他人冒名的機會，舉例來說，一個知名的部落客通常都喜歡用自己習慣且大家熟悉的網址來代表自己，所以利用代理認證的機制將自己所能控制的網址變成OpenID帳號，這樣的好處是將網路上的身份全權交由OpenID發行者OP來管理，方便其他使用者辨認又可清楚代表自己，亦可以降低帳號被他人冒名發言的困擾。

除了上述的特性，OP都會給予使用者多種的服務，例如提供使用者安全的管理自己已認證的網站，使用者登入RP後，自動替使用者記錄網站的認證狀態，以利下次登入時以更精簡的方式登入相關網站使用服務；另外就是提供使用者登入過的網站歷史紀錄，讓使用者了解自己的使用習慣，以及追蹤不正常的登入情形。

什麼是OpenID？

OpenID是實現了Single Sign-On（單一簽入）技術的其中一種作法，所謂Single Sign-On就是使用者用一組帳號密碼，就可快速登入多個網站系統。所以，OpenID可以解決使用者在使用不同服務時，一再輸入帳號密碼等認證資料的問題。它是以網站為基礎的認證協定，適用於網路的服務，運作的方式是以使用者為中心，結合了認證、識別、信賴、授權等服務圍繞其外的概念。如圖1所示：

OpenID可為我們做什麼？

- OpenID讓使用者只需保有一組帳號密碼，即可以使用支援OpenID的所有網站服務。
- 使用者用OpenID登入拜訪過的網站，不會記住任何密碼，不易有密碼外洩問題。
- OpenID URI也是一個URL，使用者可將其身份相關資訊留在這個網址供人查閱。
- 在OpenID擁有者的同意之下， RP可以透過協定取得身份所有者願意公開交換的資料。
- OP自動記錄使用者的網站登入資料，方便使用者檢視追蹤使用習慣。

圖 1：OpenID 運作以使用者中心結合服務概念圖

- 若擁有個人網頁管理功能的進階使用者，在個人網頁的首頁寫入特定的Meta Information，就可以利用OpenID的代理認證功能。

OpenID怎麼運作的？

這個符號就是代表OpenID。在使用OpenID登入網站時，若帳號輸入框有符號就是要提示使用者輸入OpenID的意思。在輸入OpenID後，按下確定，會將畫面導至使用者當初申請OpenID的OpenID Provider（OpenID發行者，簡稱OP）的頁面；在輸入密碼之後，如密碼無誤認證完成便會導回使用者原本想進入的網站，叫做Relying Party（信賴憑證者，簡稱RP）也可稱作Consumer，在登入的過程中，OP與RP之間會透過協定取得使用者願意公開交換的資料，

所以當登入到網站時一樣會有使用者的暱稱、生日…等資料，這些資料便是在您同意下經由後端機制交換來的。

從圖2可以清楚表達使用者在操作OpenID時資料的流向：

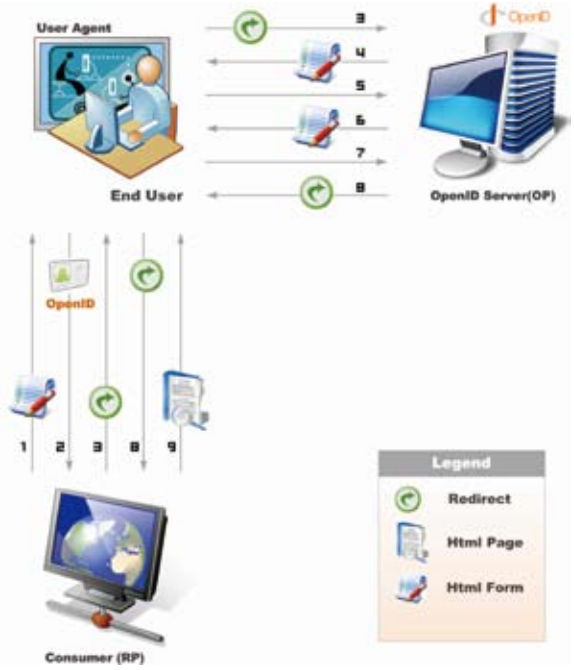

圖 2：使用者登入 OpenID 的資料流程圖

1. 使用者要登入一個可經由OpenID登入的網站，如wikitravel，這網站即是一個RP，所以RP便傳給使用者一個填入OpenID的頁面(HTML form)。
2. 使用者填入要使用的OpenID帳號（這裡不會出現填寫密碼的區塊）。
3. RP收到使用者的OpenID後，經過程式執行判斷，便透過使用者電腦向OpenID Server要求認證，OpenID Server也就是發給使用者OpenID的OP。
4. 此時，當OP收到認證請求後，便產生請OpenID 擁有者填入密碼的頁面，以供識別。
5. 使用者輸入密碼。
6. 當OP判斷密碼通過認證成功，OP便導向讓使用者勾選同意RP要求傳遞的個人資料選項網頁。
7. 使用者勾選同意OP交換給RP的資料項目。
8. OP收到使用者的同意之後，透過使用者將使用者資料回傳給RP。
9. 最後，RP信賴OP對使用者身份的認證及識別，同時也接收使用者同意交換的資訊，便授權讓使用者使用RP網站的內容。

從上述解釋我們知道，在使用OpenID的過程中，所有資料流都是經過使用者端來運作的，由使用者掌控，完成了認證、識別、信賴與授權的工作，亦實現了以使用者為中心的目的。

學學怎麼用myID.tw

myID.tw是中央研究院資訊科技創新研究中心（資創中心）為本地使用者特別打造的OpenID服務，是一個免費

的OpenID發行者（OpenIDProvider，簡稱OP），提供華文使用者的認證服務(Authentication service)與身份識別服務(Identity service)，到myID.tw申請一組帳號密碼（以下將myID.tw發行的OpenID稱為myID），即可以漫遊全球上萬個支援OpenID的網站5。這組帳號同時也可當作是URL，網路上所有使用者都可以連上這個URL觀看同意公開的身份資料。除了紀錄OpenID Simple Registration Extension 1.0定義的欄位之外，使用者可將其他社群網站身份填寫在這裡，實現以使用者為中心(Usercentric)的新型態運用。

學習如何在myID.tw註冊一個屬於自己的OpenID及下載「10分鐘學會 OpenID」，請連結資創中心之計畫網站http://myid.tw。

原載於2009年8月 資訊科技創新研究中心之計畫出版品：10分鐘學會 Open ID

計畫名稱：數位典藏與學習之學術與應用推廣計畫-Daodin社會網絡服務系統