大學圖書館
15卷1期（民國100年3月） 頁68-86

歐美數位資源存取管理聯盟及其Shibboleth系統運作之比較

A Comparative Study of Using Shibboleth for Access Management for Electronic Resources in Europe and the US

張迺貞 Naicheng Chang
大同大學通識教育中心助理教授
Assistant Professor, General Education Center, Tatung University
E-mail: ncchang@ttu.edu.tw

陳麗美 Limei Chen
中央研究院地球科學研究所編審
Librarian, the Institute of Earth Sciences, Academia Sinica
E-mail: april@earth.sinica.edu.tw

【摘 要】

為了改善數位資源存取管理問題，美國Internet2發展的Shibboleth存取管理系統，已漸漸被很多已開發國家使用。Shibboleth是一個依據標準的開放源碼套裝軟體，提供機關內或跨機關間的網頁單一登入（Single Sign-On，簡稱SSO）及屬性交換的架構，容許網站對個人存取線上數位資源時，使用單一以及機關所控制的辨識方法，並且以保護隱私的方式作確認性的授權決定，讓使用者無接縫的存取機關內部與外部的資源，減少現行使用者在使用不同領域的多種資源時，必須局限在一個校園或要去維護多個密碼；並且為身分提供者及服務提供者簡化了身分管理及存取許可。本研究分析比較英國、美國、澳洲、以及瑞士四個國家的聯盟組織以及採用的技術與政策，進而分析探討就規劃臺灣的數位資源存取管理聯盟提出建議。

【Abstract】

In order to solve the electronic access problems, Shibboleth has been developed by Internet2 in U.S.A., and has become an emerging solution for access management of electronic resources in a growing number of developed countries. The Shibboleth system is a standard based, open source software package for web Single Sign-On (SSO)

收稿日期：民國99年10月12日；接受日期：民國99年11月23日

across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner, for Identify Providers (IdPs) and Service Providers (SPs) simplify identity management and access permission.

This study compares the organization structures, technologies and policies adopted by four federations: InCommon (USA), UK Federation, Australian Federation, and SWITCHaai (Switzerland). The comparison leads to further analysis and suggestion for a federation system model for future development of digital archives in Taiwan.

關 鍵 字：Shibboleth；存取管理；認證與授權
Keywords：Shibboleth; Access management; Authentication and authorization

壹、前言

目前國內外圖書館在存取數位資源時，使用的方法及其缺點為：(1)在校園的IP範圍內使用：此種方法出了校園便無法使用；(2)在校園內使用IP限制，校園外則用Proxy伺服器：此種方法在校園外藉助中介伺服器，提供使用者與IP限制資源的虛擬連線。Proxy目前演進到EZProxy中介軟體，有些數位期刊及資料庫對EZProxy的設定可能有技術上問題，亦即有些資源無法透過EZProxy使用，必須設定傳統Proxy才能使用，其技術和使用穩定度尚未成熟；(3)使用虛擬私有網路連線（Virtual Private Network）：若使用者具有兩個以上單位的數位資源使用權，此種方法還是要分別登入不同單位的資源；(4)使用共用的密碼（“Shared”Passwords）：此種方法密碼容易外洩給社群以外的人，進而威脅到資源的安全；(5)針對不同資源，使用者分別註冊密碼：使用者若是將自己的個人資料提供校園內的單位，例如圖書館，是沒有問題的，但是如果要將個人資料提供給外來的服務提供者（Service Provider，簡稱SP），例如出版社，則使用者因所使用的資料可能牽涉科學、商業、以及政治敏感，而不願意洩漏個人身分；況且，在身分提供者（Identity Provider，簡稱IdP），例如大學圖書館，與服務提供者，例如出版社，之間交換個人資料，恐怕有身分不實的問題（Garibyan, 2007；張迺貞，2008）。

其他存取管理問題例如商業服務提供者（亦稱資源提供者）有他們自己的系統，不易與開放系統協定互相整合。從比較宏觀的角度看，一個全球的合作（Global Collaborative Initiatives）以建置合適的存取系統基礎建設，必然有很多挑戰，例如認證

架構的不確定性，影響範圍會是區域性、國家級、或是全球性；資訊基礎建設隨後的連結會是可行的電子商業模式（E-commerce Models）；資訊服務基礎建設的能力，可以延伸到數位學習服務模式；跨國界進行數位資源存取管理系統合作發展的能量有多少等議題值得進一步研究。

為了改善上述的電子資源存取管理問題，美、英等國積極投入Shibboleth（2010）存取管理系統的發展。Shibboleth服務提供者的信心建立在使用者所屬的機關要有一健全且即時更新的認證系統，此種因信賴的需求而導致聯盟管理的觀念。聯盟是由同性質機構，例如大學，同意一共同的政策，通常是建立在國家層級的政策，例如美國高等教育界已建立一國家性的政策聯盟稱InCommon（2010），瑞士稱SWITCHaai（2010）。Garibyan（2007）指出，依聯盟技術所發展的新一代存取管理架構如 Shibboleth，已逐漸被國際所認同。因此，本研究目的為：

1.比較英、美等國發展的Shibboleth存取管理系統之運作，瞭解其在數位環境下之授權、認證及存取管理之做法。
2.評估Shibboleth應用在臺灣高等教育環境電子資源存取管理的可行性、效能及影響。進而引起臺灣高等教育界認識注意Shibboleth的技術與發展，能儘速積極規劃一套完善的適合臺灣高等教育界環境的電子資源的整合存取管理系統。

本研究採用文獻分析法以及網站資料收集法，於民國99年1月間上網查詢資料及網站，比較分析四個國家存取管理聯盟：美國聯盟（InCommon Federation，以下稱InCommon）（2010）、英國聯盟（UK Access Management Federation for Education and Research，以下稱UKF）（2010）、澳洲聯盟（Australian Access Federation，以下稱AAF）（2010）、以及瑞士聯盟（SWITCHaai），做為將來規劃臺灣聯盟之借鏡。

貳、文獻探討

Lynch（1998）代表美國網路資訊聯盟（Coalition for Networked Information，簡稱CNI）提出一個存取管理系統的需求分析及評估，其主要概念如下：

一、可行性（Feasibility）及可應用性（Deployability）

從使用者角度看一個認證及存取系統應該要具有以下特性：(1)能加速取用；(2)減少冗長的認證互動；(3)提供單一登入（Single Sign-On，簡稱SSO）；(4)親和力高的使用者介面（User-friendly）；(5)可以量測使用者的規模 （Scale）；(6)對機關而言，可以管理大而動態的社群；(7)要

健全且簡單，使用者問題容易處理，例如忘記密碼，應該很容易處理。軟體應為一公用的套裝組合（Common Package），例如使用者用網頁瀏覽器就可以使用。只要使用者所屬的圖書館被授權可以使用的資源，使用者的使用權限應獨立於其實體地點，例如一個使用者可透過商業的網路服務提供者（Internet Service Provider，簡稱ISP）、無線網際網路中的行動IP技術（Mobile IP）、或是從家裡的有線電視的網路連線，以存取資源。

二、認證強度（Authentication Strength）

資源提供者的憑證在一個好的存取控制系統不會輕易遭受駭客攻擊，身分提供者的憑證不會輕易在網路上被盜取。一個好的存取管理系統應該在資源提供者端予以監控以及使用其他控制措施來補強，減少侵害的影響。

三、細微度（Granularity）及擴展性（Extensibility）

細微度的存取控制構想來自數位指定參考用書及遠距教學，例如一個機構要限制資源的存取到某一課程註冊的個人，例如限定法律系及企管系學生才能存取等。

四、隱私考量（Privacy Considerations）

使用者以匿名方式使用數位資源時，隱私要能被確保，例如匿名存取（Anonymous Access）。值得注意的是，一個機構如何提供使用社群之成員，享受加值服務而又不暴露他們的身分給資源提供者是很重要的。有些國家受立法保護的資料包括高等教育機構對學生、公共圖書館對讀者、以及醫療機構對患者資料的隱私，受到法律規範；而有些隱私不完全是政治或道德問題，研究人員在一個競爭的環境中追求專利、申請經費補助、或是探索發現或是發明，提供保密檢索是很重要的議題。

五、使用者與資源提供者應負的責任與義務（Accountability）

在談判授權合約時，每一方都應該共識被授權資源的價值及資源擁有者的權利應該被尊重。通常，被授權機關應教育其使用社群之成員，關於授權條款之規定及限制，並協助資源提供者辨識、調查、以及阻止資源之不當使用。

六、有能力蒐集管理資料（Ability to Collect Management Data）

管理資料可能涉及兩個層面：第一種是從使用者，包括從IP位址來

源、從使用者身分（名字）、或是從使用者屬性來做合約授權之決定。第二種是從被存取的物件或是使用的服務等。管理資料是目前存取架構的最大問題；大部分的問題是機關政策層級就可解決，有些機關可能透過立法限制收集某些管理資料。管理資料的蒐集有不同的情境，目前最實用的方法是：(1)由被授權機關或資源提供者追蹤使用情形。因為資源提供者能計算次數，其在衡量資源的利用上會比較有意義，例如從期刊計算使用次數而非從存取頁數；(2)由資源提供者依個人（虛構名或身分辨識）來統計使用情形，再將使用日誌傳給被授權機關，被授權機關依資料加以處理，得到使用者分布面的使用統計報告；(3)被授權機關與資源提供者同意依使用者資料來統計，故使用者資料由存取管理系統傳給資源提供者，資源提供者依使用者資料做成使用統計報告。

Van Halm（1999）認為數位圖書館是存取管理的催生者，而數位圖書館的任務之一是將在不同地點、不同格式、以及不同領域，例如圖書館、檔案館、以及博物館等的異質資訊資源整合在一個適當的組織及合法的架構下。Van Halm進一步認為一個數位化圖書館的存取系統應包括四個主要元素：(1)存取介面系統；(2)存取控制系統；(3)計價；(4)帳單/結算/收費等。因此，為因應異質數位資源的多元化，圖書館的存取管理系統已開始逐漸被重視。Van Halm認為一個存取控制系統功能應包括：(1)校內/外的存取；(2)歷程控制（Session Control）；(3)認證（Authentication）；(4)授權（Authorization）；(5)使用者（含群組及訪客）統計以及中央和地方使用者管理。存取控制系統的其他特質尚包括：其連到資料庫內容應是標準介面、有獨立的資料庫、標準架構、系統的效能和監控（Performance and System Monitoring）、以及整體安全。

參、Shibboleth計畫

Shibboleth是開始於2000年美國Internet2/MACE（Middleware Architecture Committee for Education）的一個計畫，稱Internet2 Middleware Initiative，簡稱I2MI（Internet2, 2008），由美國國家科學基金會（National Science Foundation, 簡稱NSF）資助發展Shibboleth 的架構、政策、以及應用技術。Shibboleth是一種依據SAML（Security Assertion Markup Language）（目前已演進到2.0版本）語言標準的開放源碼中介軟體（Open Source Middleware Software），以交換屬性的方式提供跨機關間之網頁單一登入（SSO），通常它是以聯盟（Federation）方式來運作，容許網站對個人存取線上數位資源時，以保護隱私的方式作確認性的授權決定。服務提供者不必再維護帳號與密碼，身分提供者提供使用者

資訊，而服務提供者依據使用者資訊提供安全的存取內容。Shibboleth本身並不執行認證與授權，而是定義一套協定使得身分資料可以在機關與服務提供者間安全通過。Shibboleth依賴機關來建立身分資料，提供使用者機構資料，並在服務提供者端確認存取權利。

Shibboleth系統的作業流程如圖1所示。Shibboleth身分提供者的四個元素：(1)屬性權威（Attribute Authority（AA））：代表母機關分發屬性；(2)管理服務（Handle Service（HS））：使用者登入服務。當一個使用者被授權後，Shibboleth的區域單位就會產生一個臨時的參照給使用者，稱Handle；(3)目錄服務（Directory Service）；(4)區域登入系統（Local Sign-On System（SSO））。服務提供者的三個元素：(1)聲明使用者服務（Assertion Consumer Service（ACS））：發出聲明指出使用者母機關端為何，其中WAYF（Where Are You From）是個「中央」的服務，代表Shibboleth聯盟的操作，提供機關的名單及那些使用者可存取資源。WAYF可能是由外部聯盟運作或由ACS執行；(2)屬性請求人（Attribute Requester（AR））：使用者請求登入服務提供者提供的

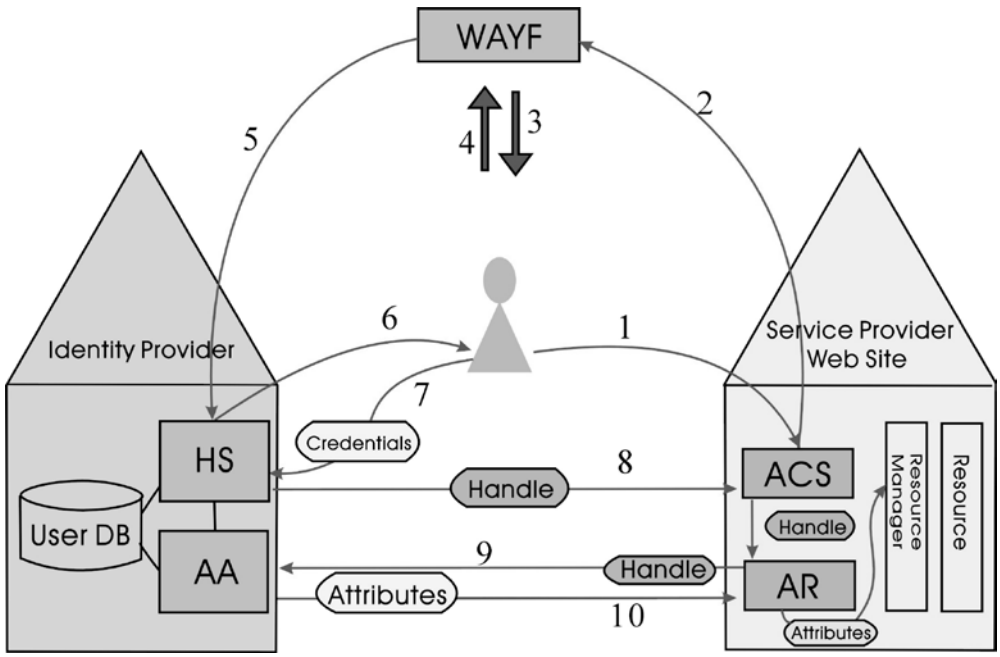

圖 1　Shibboleth作業流程圖示（摘自Swiss Education and Research Network，簡稱SWITCH（2010）原圖）。

資源；(3)資源管理人（Resource Manager（RM））。

流程說明：

1：使用者試圖到SP端的應用伺服器去存取Shibboleth所保護的資源。

2、**3**、**4**：使用者被指引到代表Shibboleth聯盟的中央服務操作「你從那裡來」（Where Are You From, WAYF）的伺服器，在WAYF，使用者指出其母機關端（IdP）。

5：使用者被指引到IdP端的管理服務系統（Handle Service）。

6、**7**：使用者在自己的IdP端使用區域的憑證（Local Credentials）來認證。

8：管理服務系統產生唯一的身分識別（稱ID或Handle），並指引使用者到服務提供者網站的聲明使用者服務（ACS），使用者服務證實該提供的聲明，產生一個歷程（Session），然後將使用者轉到屬性請求人端（Attribute Requestor）。

9、**10**：屬性請求人使用Handle從IdP端的屬性權威（Attribute Authority）去請求屬性，屬性權威根據屬性釋出政策來回應屬性聲明；服務提供者端使用屬性來做存取控制及其他應用層級的決定。

Shibboleth系統的認證與授權機制又稱為認證與授權的基礎建設（Authentication and Authorization Infrastructure，簡稱AAI）。AAI成員包括：(1)使用者（User）：屬於一個機構，該機構管理自己使用者的身分資料（個人屬性）；(2)聯盟管理者（Federated Manager）：通常是國家級機構來負責管理及審核不同當事人之間的信賴關係；(3)身分提供者（IdP）：安全而正確地管理使用者的屬性；(4)服務提供者或資源提供者（SP）：透過網頁對內部及外部使用者提供服務，其聚焦在核心的商業服務。

美國Internet2計畫的Shibboleth已形成領先以及被廣為採納。大部份使用在需要高標準隱私以及個人資料保護的政府和高等教育機構。Elsevier、EBSCO、OCLC、Microsoft等超過40家世界知名商業服務提供者包括圖書館自動化系統商，正計劃開創或已經使用Shibboleth的技術提供服務。除了Shibboleth之外，尚有其他AAI系統，大都只用在單一國家，例如西班牙學研網RedIRIS制定的PAPI（Shibboleth相容）（2009）；挪威於2008年納入一個泛北歐系統：Kalmar Union（2010）。創造一個安全又可信賴的環境是大勢所趨，因此，每個AAI系統正在積極導入主流標準（亦即SAML 2.0）以達到互通性，確保全球性規模的AAI系統基礎設施得以運作順暢。

肆、存取管理聯盟的比較

目前已有美國、澳洲、瑞士、

德國、以及英國等20餘Shibboleth聯盟（Terena, 2010）。其中，美國InCommon、英國UK Federation、瑞士SWITCHaai、以及澳洲Australian Access Federation四國的聯盟組織結構健全，由國家層級主導經營發展，聯盟經費來源穩定，主要服務在高等教育以及研究機構，是目前運作穩定成功的四個國家存取管理聯盟。

以下比較分析上述四個國家存取管理聯盟，分析的項目分成：(1)組織與現況；(2)政策與管理；(3)技術三方面。組織與現況之下細分為：聯盟組織結構與現況、聯盟參加者、以及聯盟參加者經費來源；政策與管理之下細分為：聯盟運作者及其責任與聯盟主要服務、是否跨聯盟、以及聯盟資料保護及隱私相關規定；技術之下細分為：聯盟技術協定、聯盟採用的Schema、以及聯盟接受的憑證。（表格中"-"表示沒有資料或資料不詳）：

一、組織與現況

InCommon是LLC的單一會員，由聯盟參與者組成公司以及由指導委員會（Steering Committee）管理，指導委員會由美國高等教育單位及公司等代表組成。聯盟另設有技術諮詢委員會（Technical Advisory Committee），負責提供InCommon有關技術方面的運作與管理建議，聯盟由Internet2員工運作，包括業務及政策的執行、技術操作、身分確認、以及支援InCommon及聯盟成員等工作。

英國聯盟下設有諮詢委員會（Advisory Board）和技術諮詢小組（Technical Advisory Group），經費由英國聯合資訊系統委員會JISC（Joint Information Systems Committee，簡稱JISC）（2010）與Becta（the British Educational Communications and Technology Agency，簡稱Becta）（是英國政府機構，領導與驅動學習技術的有效與創新）提供，由其提名三名會員至諮詢委員會並同意一個合聘主席。聯盟由JANET（是英國的教育與研究網路）來運作。瑞士聯盟下設有兩個委員會：諮詢委員會（Advisory Committee）和操作委員會（Operations Committee）。前者負責策略方面，後者則較重執行面。澳洲聯盟設有執行委員會，執行委員會下設政策及管理小組（Policy and Governance Reference Group）、技術小組（Technical Reference Group）、以及行銷及宣傳小組（Marketing and Publicity Reference Group）。

如表1所示，英國由負責國家研究及教育網路的JISC來主導，瑞士則由Swiss Education and Research Network（SWITCH）（2010）來主導；而美國、澳洲則另行成立法人，每個聯盟都設有委員會或工作小組監督聯盟運作。

InCommon成員分聯盟會員與贊助夥伴（InCommon稱服務提供者為

贊助夥伴（Sponsored Partners）），贊助夥伴需要會員保證，目前有450萬個使用者。英國聯盟會員不分層級，所有教育與研究機構皆可參加；商業機構提供資源服務給上述教育與研究機構者也符合加入會員資格，但是需要會員機構保證。瑞士聯盟會員為IdP或是身兼雙重身分（IdP兼SP）；提供資源服務的SP只能成為聯盟夥伴（Sponsored Partners）而不是聯盟會員。澳洲聯盟與瑞士相同，會員為IdP或是身兼雙重身分（IdP兼SP），SP也是只能成為聯盟夥伴。

如表2所示，四個國家聯盟除了美國與澳洲包括政府機關的會員之外，目前都著重在服務高等教育與研究機構；只有英國的SP可以成為聯盟會員，在美國、瑞士、以及澳洲SP只能成為聯盟夥伴。

美國聯盟運作的主要收入來自聯盟參與者，包括首次的登記費及年費。聯盟夥伴除首次的登記費外，依其年收入分等級收費。美國因發展Shibboleth技術，不同於其他三國聯盟，InCommon有來自聯盟贊助者NSF、IBM、以及Microsoft等的捐贈以協助Shibboleth的發展。

從表3可以看出聯盟的經費來源有：1.會員費（如InCommon）；2.政府補助（如UKF）；3.會員費及

表 1　聯盟組織結構與現況

美國InCommon	英國UKF	瑞士SWITCHaai	澳洲AAF
由在Delaware的Limited Liability Company（LLC）經營，公司名：InCommon, LLC。 2004年開始運作，目前有高等教育及研究機構會員151個，政府機構及非營利實驗室、研究中心等6個，贊助夥伴50個；使用者450萬人。	聯盟本身並非一個法人，與會員合約由JISC簽署。 2006年11月開始運作，目前有781個會員（含IdP及SP），約300萬個使用者。	SWITCHaai聯盟是SWITCH所提供給會員及夥伴的服務；與會員及聯盟夥伴各簽有不同合約。 2005年8月開始運作，目前有48個IdP，23個聯盟夥伴（即SP），382種資源；約27萬個使用者。	2009年在澳洲新南威爾斯依據澳洲1984年的法案「The Associates Incorporation Act, 1984」成立，名稱為：The Australian Access Federation Incorporated。 2009年7月開始運作，目前已有25個IdP，另有12個將加入；31個SP；約24萬個使用者。

表 2　聯盟參加者

美國InCommon	英國UKF	瑞士SWITCHaai	澳洲AAF
聯盟成員為高等教育單位及其商業夥伴、政府機關、非營利機構、以及實驗室等。	聯盟成員為高等教育及研究機構、進修教育與學校等。	聯盟成員為瑞士高等教育以及研究機構。	聯盟成員為高等教育與研究機構、政府機關、以及提供產品與服務給教育與研究機構的商業機構。

表 3　聯盟參加者經費來源

美國InCommon	英國UKF	瑞士SWITCHaai	澳洲AAF
預算與收入			
沒有經常的預算，主要收入來自聯盟參與者。	每年直接來自JISC與Becta約壹佰壹拾萬英磅的預算。	經常預算部分來自SWITCH，其他來自會員的基本服務費。	預算在2010年任命聯盟管理者時決定，除了會員訂購費的收入之外，經費由澳洲政府補助。
服務提供者收費政策			
依SP年收入等級收費。	不收費。	目前尚未收費。	目前不收費，但不排除將來收費。
委外服務			
由Internet2運作。	每日的運作委給EDINA（在英國內/外提供員工及學生高等教育及進修教育資源）。	沒有委外服務。	2010年任命聯盟管理者時決定。

政府補助兩種都有（如SWITCHaai及ＡＡＦ）；4.聯盟夥伴（如InCommon）。因為沒有來自政府的預算補助，InCommon是目前四個聯盟中唯一向SP收費的聯盟。

二、政策與管理

四國聯盟的服務，英國以圖書館的線上期刊及資料庫為首要服務，瑞士則聚焦在數位學習，之後各國聯盟的服務擴展到研究數據資料庫、科學運算、虛擬團隊的合作環境與工作空間、視訊會議、網頁服務如電子郵件、以及高等教育及研究管理系統等。

根據Davis and Shreeve（2007）跨聯盟（Inter-federation）模式有合作

表4　聯盟運作者及其責任與聯盟主要服務

美國InCommon	英國UKF	瑞士SWITCHaai	澳洲AAF
聯盟運作者是Internet 2員工，其責任在於後設資料管理、憑證授權運作、註冊中心操作、業務擴展、合約談判、以及營運管理等。 主要服務在高等教育以及研究機構。服務項目有後設資料管理（Metadata Management）、註冊中心（Registration Authority）、建構社群及其他等。	由英國教育與研究網ＪＡＮＥＴ運作，其責任在於會員登記、實體註冊（Entity Registration）以便會員機構的Metadata可以在英國聯盟中被發布或修正、會員訓練、健全聯盟以及安全機制等。 主要服務在支援英國國家研究與教育網NREN，包括線上期刊、資料庫及其他數位學習資源、電子郵件、視訊會議等，並將擴大由教育社群提供上述型態的服務及其他等。	聯盟運作者是瑞士的國家研究與教育網SWITCH，其責任在於做為： 1. 管理中心：運作一個測試的基礎工程建設以核對新設備的元件及建置關鍵技術、以及關鍵技術轉移等。 2. AAI工具：發展及實做AAI工具以加速資源的整合。 3. 策略與行銷。 主要服務在： 1. 建置及支援數位教材，為數位學習及網頁應用提供單一登入。 2. 科學運算、資訊及通術、電子郵件。 3. 聯盟認證與授權及憑證中心的基礎建設。 4. 策略及行銷。	聯盟運作者是AAF Inc.，其責任在於提供會員服務，包括提供Help Desk給使用者。 主要服務在數據網格（Data Grids）、科學儀器、模型（Modeling）、視覺化工具及運算資源、虛擬團隊的合作環境與工作空間、數位學習資源及學習物件、高等教育及研究管理系統及其他等。

聯盟（Con-federation）以及聯盟同儕（Federation Peering）等方式。Con-federation為數個聯盟一起合作，聯盟會員需要架構一個共同的信任模式、標準與政策；聯盟同儕的信任模式是建立在雙方或是多個聯盟獨立的協定；合作聯盟是集中式的，而聯盟同儕則為分散式的跨聯盟方式。隨著各國聯盟的發展逐漸趨於穩定與成熟，跨聯盟逐漸被考慮或進行中。

如表6所示，不論是美國、英國、瑞士、以及澳洲聯盟都有資料保護及隱私政策的規定，突顯Shibboleth系統對資料安全與隱私保護的重視，可以解決現行針對不同資源，使用者分別註冊密碼，而使用者個人身分容易被洩漏或有身分不實的問題。

表 5　是否跨聯盟

美國InCommon	英國UKF	瑞士SWITCHaai	澳洲AAF
跨聯盟計畫			
與美國政府及UK Federation發展跨聯盟。	正在與InCommon及英國政府入口網擬合約草案中，將研究合作聯盟政策的可行性。	SWITCHaai與其他歐洲聯盟正在測試eduGAIN（2010）計畫（是歐洲的一個跨聯盟計畫，使得身分資料透過SAML的交換可以在聯盟間共享）。	透過全球性跨聯盟計畫Research and Education Federations（REFEDs）（2010）發展聯盟合作。
跨聯盟驅動力			
基於美國國內許多機構，例如National Institutes of Health表示合作聯盟的興趣以及支援歐洲的聯盟夥伴。	基於機構間的國際合作以及因為SP要去了解不同的聯盟政策，非常複雜。	為了引進其他國家的數位學習課程。	澳洲/紐西蘭計畫合作聯盟。

表 6　聯盟資料保護及隱私相關規定

美國InCommon	英國UKF	瑞士SWITCHaai	澳洲AAF
「InCommon聯盟：參與者操作應用」（InCommon Federation: Participant Operational Practices）中的隱私政策提及聯盟參與者應尊重其他參與者所提供屬性資訊的隱私限制，限制只為某些目的而使用。	「聯盟會員規章」（Federation Rules of Membership, UK Federation）及聯盟規範的「個人資料使用建議」（Recommendations for use of personal data, UK Federation）都言明聯盟的目的與設計都是以尊重及保護使用者隱私的方式來交換存取管理資訊。	「AAI服務同意書」（AAI Service Agreement）中的第十二款「資料保護」（Data protection）特別言明對使用者資料的保護。	「聯盟參與者規範」（Federation Rules for Participants）中的第十款「資料保護與隱私」規定聯盟參與者要遵守「1988年澳洲隱私法案」（Australian Privacy Act 1988）的相關規定。

三、技術方面

Shibboleth目前軟體發展的經費是來自Internet2，部份由NSF資助；Shibboleth除了在學術聯盟被使用之外，美國聯邦政府的數位化認證系統也是採用Shibboleth；另外，Google以及微軟也將計劃Google Scholar及微軟的CardSpace賦予Shibboleth的功能。

目前除英國少部份機構仍然採用OpenAthens外，大都採用Shibboleth技術及SAML協定，目前最新版本為2.x版，在安裝上建議採用最新版本，以便在聯盟間可以互通；另外，美國、英國、以及澳洲都同意使用LDAP來建置使用者資料。

使用者身分資料庫的建置是整個Shibboleth系統的核心，建置前周詳的規劃屬性規範是非常重要的；要決定每一物件應該包含那些屬性，那些是必備屬性等。eduPerson及eduOrg是由美國Internet2 MACE-Directories Working Group（MACE-dir）所發展及維護的；瑞士的SwissEduPerson以及澳洲的auEduPerson都是由美國Internet2 的eduPerson 衍生而來。

從表9可以看出目前聯盟憑證的簽發有三種方式：(1)自簽：身分提供者自行產生憑證，然後呈送給聯盟，經聯盟確認後將憑證資料加入後設資料；(2)聯盟所簽發；(3)聯盟信賴的憑證中心（Certification Authority，簡稱CA）所簽發。當Shibboleth的實體互相溝通時，首先就會去驗證夥伴“身

表 7　聯盟技術協定

美國InCommon	英國UKF	瑞士SWITCHaai	澳洲AAF
協定（Protocol）			
SAML；LDAP	Shibboleth 1.3，正逐漸移轉到Shibboleth 2.1；任何與SAML相容的軟體皆可；LDAP。	目前仍使用Shibboleth 1.x 版本及SAML 2.0 版本。	SAML1.1/SAML2.0；LDAP。
系統實作（Implementations）			
Shibboleth。	大部份使用者使用Shibboleth 1.3、2.1版本及OpenAthens。	約一半的IdP及SP仍使用Shibboleth 1.3.x版本；另一半則使用Shibboleth 2.x 版本。	將逐步淘汰Shibboleth 1.3.x版本；大部份的IdP及SP用Shibboleth 2.x版本。

表 8　聯盟採用的Schema

美國InCommon	英國UKF	瑞士SWITCHaai	澳洲AAF
Schema名稱			
eduPerson	eduPerson	SwissEduPerson	auEduPerson
參考的Schema			
eduPerson	核心屬性取自eduPerson的Schema	Person、OrgPerson、InetOrgPerson、eduPerson	Person、OrgPerson、InetOrgPerson、eduPerson、schac、auEduPerson
其他屬性的使用			
依合作者不同而定。	依IdP及SP雙方約定；聯盟推薦如何建構屬性是必要的，通常取自eduPerson。	依IdP及SP雙方約定。	依IdP及SP雙方約定。
必備屬性			
–	核心屬性：eduPerson-Affiliation、eduPerson-TargetedID、eduPerson-PrincipalName、eduPerson-Entitlement。	每一IdP負責其使用者的建置，必備屬性為：swissEdu-PersonUniqueID、sn、givenName、mail、swissEdu-PersonHome-Organization等。	所有IdP都要支援以下屬性：auEduPerson-SharedToken、cn、displayName、eduPerson-Affiliation等。

表 9　聯盟接受的憑證

美國InCommon	英國UKF	瑞士SWITCHaai	澳洲AAF
從2010年起，將不再簽發憑證，而接受自簽（Self-signed）的憑證；也接受憑證中心（Comodo CA, Ltd）簽發的憑證。	由JANET或任何可信的憑證中心發行的憑證；也接受其認可的憑證中心所簽發的憑證。	SWITCHaai建議使用自簽憑證以直接嵌入後設資料，使用最長有效期三年；也接受憑證中心簽發的憑證。	由AAF Inc.發行憑證；也接受其認可的憑證中心所簽發的憑證。

分”的憑證，可見憑證對IdP及SP的重要性。在安裝Shibboleth的IdP及SP時就可以產生自簽憑證並嵌入後設資料。從四國聯盟發展可以看出自簽憑證以及憑證中心是一個趨勢。

一個成功的Shibboleth聯盟系統牽涉的層面非常廣，除了電腦的軟硬體技術之外，尚有聯盟的政策、管理等問題，因此，籌備期間縝密的規劃攸關國家聯盟成功與否。

伍、討論

規劃臺灣存取管理聯盟應該借鏡歐美成功的存取管理聯盟，以下分別就組織與現況、政策與管理以及技術三方面提出建議。組織與現況方面，臺灣建置存取管理聯盟時，一個強而有政策及技術主導權的聯盟運作單位做後盾是很重要的，因此，由國科會（2010b）掌舵實際負責臺灣存取管理聯盟的運作，應該有極佳的成功以及永續經營的機會。國科會透過「全國學術電子資訊資源共享聯盟」（CONsortium on Core Electronic Resources in Taiwan，簡稱CONCERT）（國科會，2010a）運作，一直與全國性機構會員、使用者和資源提供者保持良好的溝通管道與有效率的合作，而這正是臺灣存取管理聯盟運作成功的基本要求。此外，近年來網格服務漸漸成為世界各國重要的研究和教育網絡，提供以科學研究和教育為目的網格服務。臺灣存取管理聯盟將充分利用國科會的高品質學術研究網路TWAREN（TaiWan Advanced Research & Education Network）（2010）的網格服務提供資源，特別是在數位期刊、數位數據庫、科學計算，以及數位學習資源方面。臺灣存取管理聯盟初時可以先著重在服務高等教育與研究機構，由政府補助聯盟的經費支出。

政策與管理方面，國內「數位典藏與數位學習國家型科技計畫」（2010）至2010年已邁入第十二年，

目前該計畫已經有相當數量的數位學習內容成果展現，臺灣存取管理聯盟可以提供全國數位教學平台一個安全的機制來使用這些高品質數位學習內容資源。此外，「電腦處理個人資料保護法」已經於九十九年四月三讀通過「個人資料保護法」，其中包含隱私權與個人資料保護的相關規範，可見臺灣對資料安全及個人隱私保護亦越來越重視，而數位資源的存取日益頻繁，Shibboleth聯盟存取管理系統已逐漸被國際所認同，臺灣應該儘早研究規劃，加速資源的存取。

臺灣存取管理聯盟勢必會與鄰國建立對等關係，例如中國的CARSI-Fed/CERNET-Fed聯盟（2008）以及日本的UPKI聯盟（2010）。臺灣存取管理聯盟可以借鏡泛北歐聯盟，發展一個合作聯盟，連接亞洲太平洋地區，這將有助於建立一個串聯世界規模的全球村聯盟。有鑑於各國家法律和立法的分歧，發展合作聯盟將遭遇嚴厲的挑戰和潛在風險。Davies and Shreeve（2007）指出兩個可能的挑戰。為了建立一個共同的全球基礎設施、技術和政策相關架構，就技術層面而言，一個全球村聯盟共同的溝通語言是必需的，SAML正是目前全球接受的共同的溝通語言；而聯盟之間政策問題的互通性，挑戰難度遠大於技術方面的問題。當實際籌備合作聯盟時，從草案協議進一步規劃身分提供者以及服務提供者、聯盟運作者及其責任、以及資料保護及隱私相關規定等，要達到成功的跨聯盟互通性，很可能要跨越來自不同國家的法律和立法障礙。總之，這涉及聯盟成員是否願意遵守規則的問題，以建立信任關係。

臺灣存取管理聯盟的服務首先可以聚焦在圖書館數位資源（電子期刊、資料庫及電子書）的服務，其次為數位學習及數位教學資源，瑞士聯盟在提供數位學習服務方面是一個成功的典範，值得借鏡參考。另外，經濟部工業司建立的「數位內容學院」及「數位學習網路科學園區」、行政院人事行政局為推動公務人員終身學習而推出的「公務人員終身學習數位學習課程」、行政院研究發展考核委員會發展的「電子化政府網路文官學院」等、以及大專院校學生的數位教學內容都可以納入聯盟服務的範疇。進而包括研究機構實驗室或醫學中心的研究數據資料、科學運算及其他網頁服務，例如電子郵件等。

技術方面，SAML和LDAP已經是成熟的技術，而且被歐美聯盟存取管理系統所採用，值得借鏡遵循。前面章節提到使用者身分資料庫的建置是整個Shibboleth系統的核心，美國Internet2 MACE-dir發展及維護的eduPerson及eduOrg，因其規範明確與完整，值得參考以訂定臺灣聯盟的eduPerson。憑證中心簽發聯盟憑證是一個趨勢，建議可以採用授權方式由通過安全信賴的政府或是商業公司負責簽發憑證。

Shibboleth數位資源存取管理系統在臺灣的實作經驗極為有限。本文作者於2008年7月參加澳洲測試聯盟（MAMS），並且在中央研究院地球科學研究所建置身分管理系統，同時邀請Elsevier出版商為資源提供者，以實際測試聯盟的運作方式，並瞭解其在數位環境下的Shibboleth認證與授權機制（陳麗美，2010）。樹德科技大學（2010）於2009年12月開始導入Google Apps，為了有效整合校園單一簽入機制，採用SAML技術的Shibboleth IdP服務與Google Apps進行整合。

陸、結論

近年來為支援以消費者為導向之網路電子商務以及以學習者為中心之網路數位學習，一連串關於跨機關間的認證與存取管理的新技術及政策議題逐漸浮現。因此，建立一個如Shibboleth新概念的模式；一個更健全的認證、授權、以及存取管理是擴大資訊服務規模必要的基礎建設，以提供經濟又安全的資訊存取，做為建立一個永續、有效的管理機制是為當務之急。

比起亞太地區聯盟存取管理發展，歐洲國際聯盟存取管理的發展極為活躍。中國的CARSI-Fed/CERNET-Fed聯盟仍處於試車階段，日本的UPKI聯盟已經於2010年正式營運；而臺灣存取管理聯盟仍未見國家級機構開始規劃。考慮到瑞士SWITCHaai聯盟花了4年時間從試車到正式營運；英國UKF則花了2年時間，我們敦促國內相關機構應當儘早開始規劃設立臺灣存取管理聯盟，誠如在討論章節分析評估，臺灣存取管理聯盟的環境已經成熟，應當加緊腳步設置臺灣存取管理聯盟並且參與相關的國際聯盟存取管理論壇，特別是在學術和研究方面，早日與國際聯盟存取管理接軌。

參考文獻

國科會（2010a）。*全國學術電子資訊資源共享聯盟*。上網日期：2010年8月12日，檢自http://www.stpi.org.tw/fdb/index.html

國科會（2010b）。*行政院國家科學委員會*。上網日期：2010年8月12日，檢自http://web1.nsc.gov.tw/mp.aspx?mp=1

張迺貞主持（2008）。*電子資源的整合存取管理系統：Shibboleth在臺灣高等教育環境的應用*（國科會研究成果報告，NSC 96-2413-H-036-001）。臺北市：大同大學通識教育中心。

陳麗美（2010）。*電子資源的聯盟存取管理系統：Shibboleth在臺灣學術及高等教育界的應用探討*。未出版之碩士論文，國立臺灣師範大學圖書資訊學研究

所圖書資訊學在職專班，臺北市。

樹德科技大學（2010）。上網日期：2010年8月12日，檢自http://www.stu.edu.tw

數位典藏與數位學習國家型科技計畫（2010）。上網日期：2010年8月12日，檢自http://teldap.tw/Introduction/introduction.php

Australian Access Federation (2010). *Australian Access Federation: Providing trusted access to services, resources and people*. Retrieved August 12, 2010, from http://www.aaf.edu.au

CARSI-Fed/CERNET-Fed (2008). Retrieved August 12, 2010, from http://carsi.edu.cn/index.jsp

Davies, C., & Shreeve, M. (2007). *Federated access management: International aspects*. Guildford: Curtis+Cartwright Consulting Ltd.

Garibyan, M. (2007). Building a national federated access management infrastructure: the U.K. experience. In A. Hopkinson (Chair), *Information techonlogies in education in the 21st centur*y. ITE 2007 Conference, Symposium held at Yerevan, Armenia.

InCommon (2010). *InCommon makes sharing protected online resources easier.* Retrieved August 12, 2010, from http://www.incommonfederation.org

Internet2 (2008). *Shibboleth: a project of the Internet2 middleware initiative*. Retrieved August 12, 2010, from http://shibboleth.internet2.edu

JISC (2010). *U.K. federated access management*. Retrieved August 12, 2010, from http://www.jisc.ac.uk/federation

Kalmar Union (2010). Retrieved August 12, 2010, from http://www.kalmar2.org/kalmar2web/front_page.html

Lynch, C. (1998). *A white paper on authentication and access management issues in cross-organizational use of networked information resources*. Coalition for Networked Information. Retrieved August 12, 2010, from http://www.cni.org/projects/authentication/authentication-wp.html

PAPI (2009). Retrieved August 12, 2010, from http://papi.rediris.es

Shibboleth (2010). Retrieved August 12, 2010, from http://shibboleth.internet2.edu

SWITCH (2010). *SWITCH: Serving Swiss Universities*. Retrieved August 12, 2010, from http://www.switch.ch/aai/index.html

Terena (2010). *Federations*. Retrieved August 14, 2010, from https://refeds.terena.org/index.php/Federations

TWAREN (2010). *TaiWan advanced research & education network*. Retrieved August

12, 2010, from http://www.twaren.net/english

UK Access Management Federation (2010). *UK Access Management Federation for education and research*. Retrieved August 12, 2010, from http://www.ukfederation.org.uk

UPKI (2010). *University public key infrastructure initiative*. Retrieved August 12, 2010, from https://upki-portal.nii.ac.jp/docs/fed/participants

Van Halm, J. (1999). The digital library as access management facilitator. *Information Services & Use*, *19*, 299-303.