勞委會「單一帳號暨認證授權控管應用整合平台」介紹

壹、 前言

本會為因應未來知識經濟社會的需要及勞工行政資訊發展的目標，訂定本會「電子化政府資訊發展計畫」，以達成電子化政府的願景：「充分運用資訊和通訊科技，一方面提高勞工行政效能，創新政府的服務，一方面提昇便民服務品質，落實政府再造，邁向全民智慧型政府」。本會電子化政府之目標是要提供革新的辦事方法，讓同仁處理公務可以藉助現代資訊及網路通信科技大幅改造，使得本會為勞工服務的方式更為精巧靈活，服務的速度更為加快，服務的時間更為延長，服務的據點更為普及，服務的選擇更為多樣，服務的成本更為降低，讓勞工朋友可以在任何時間、任何地點、透過多種管道很方便地得到本會的查詢資訊、申辦服務等各項服務。依據上述本會電子化政府之願景與目標，推動各項資訊發展計畫，其中推動措施之一是建置「單一帳號暨認證授權控管應用整合平台」。

鑒於本會之網路應用日益蓬勃發展，每位同仁期望在會內會外之不同環境都可藉由網路來完成各項線上行政管理作業及業務訊息傳遞；讓同仁處理公務可以藉助現代資訊及網路通信科技之協助，為勞工服務的方式更為精巧靈活，如圖 1 說明。然而，同仁在網路上所從事的各項活動必須是在安全、完整且保密的環境下完成。本會於今年度規劃委外建置「單一帳號暨認證授權控管應用整合平台」，使同仁在這種開放式的網路環境下，無論在遠端或近端使用，都可經由本系統平台確認身份的合法性及存取權限設定，提供一個安全的網路安全存取作業環境，發揮更多的網路應用效益，以達到簡化行政作業流程及提升為民服務效率之目的。

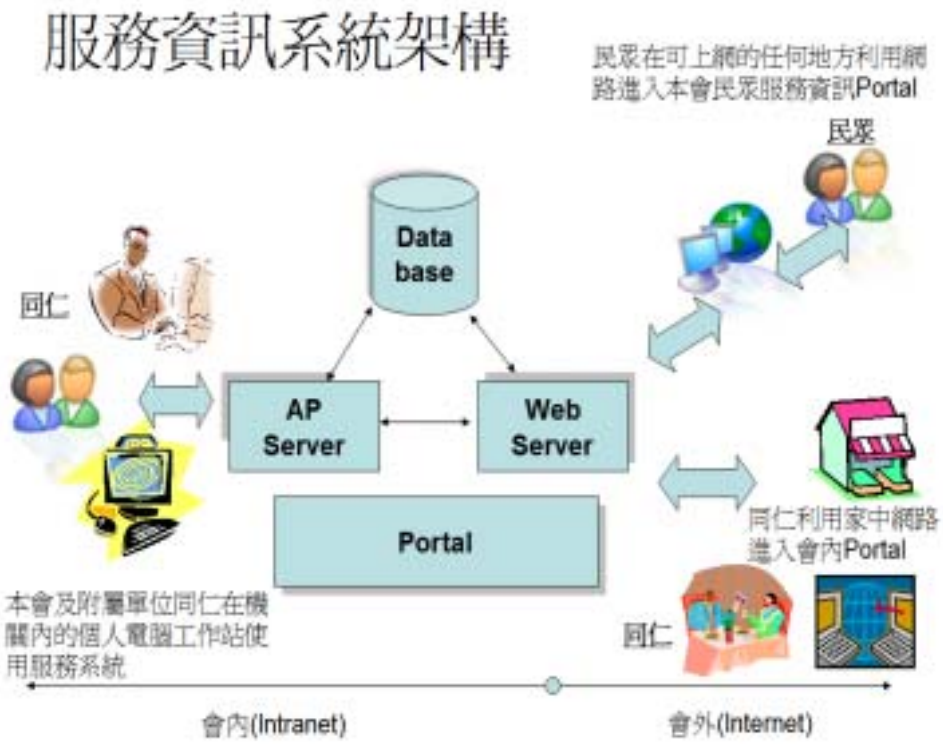

圖 1　本會網路服務圖

貳、 整體系

本會建置之整體系統運作架構包含前端的使用者、憑證管理中心、線上申辦應用系統、帳號註冊管理系統(帳號整合系統)與身份認證管理系統(單一認證暨授權管理平台)，使用者必須事先向內政部憑證管理中心申請自然人憑證，各單位管理者透過帳號註冊管理系統建立使用者的身份帳號資訊，並將所屬的自然人憑證上傳匯入系統中，以建立帳號與憑證的身份對應關係。其次，當使用者以自然人憑證進行身份認證時，便將相關的認證請求傳遞給身份認證管理系統，通過身份認證管理系統來驗證使用者的身份，並取得使用者的授權資訊，最後再將相關資訊回應給應用系統，如下圖 2 說明：

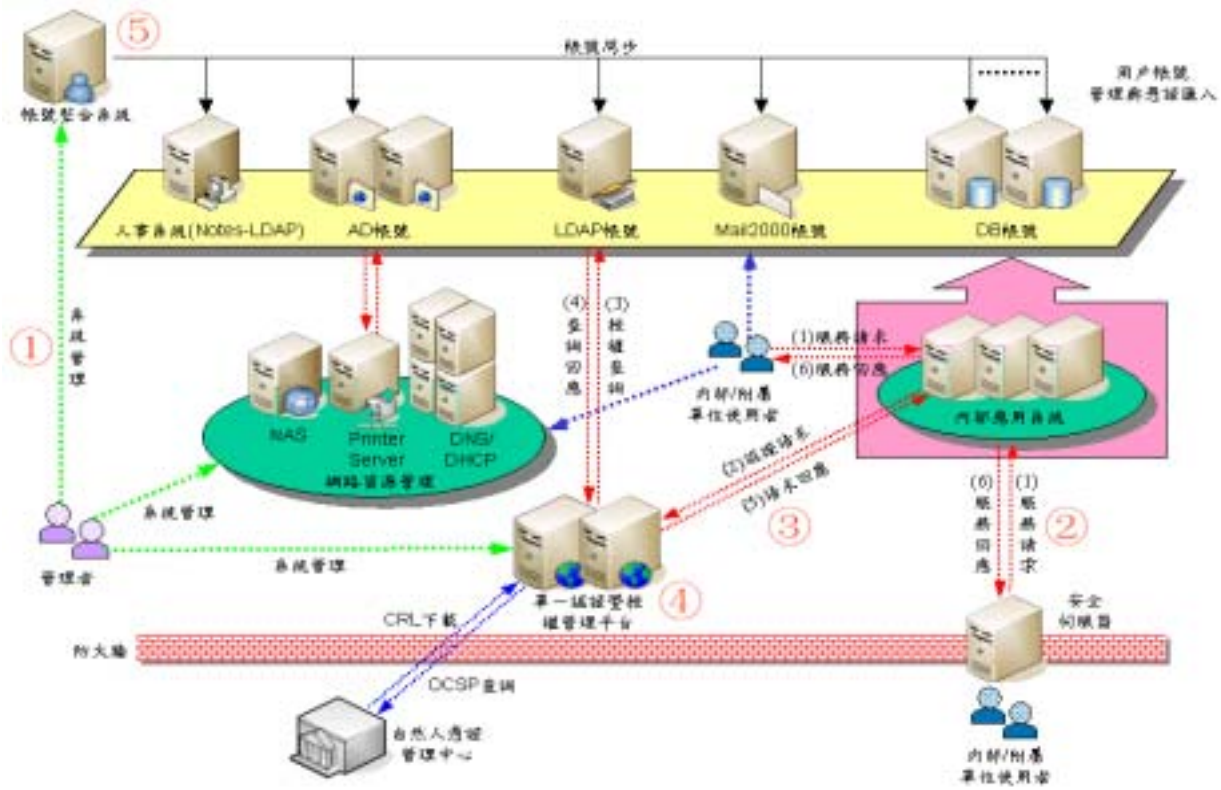

圖 2　整體系統運作架構圖

一、使用者註冊階段

管理者進入帳號註冊管理系統進行帳號註冊作業，並依據使用者的身份屬性將憑證匯入 LDAP 目錄伺服器中。使用者必須事先向內政部憑證管理中心申請自然人憑證。

二、使用者登入階段

使用者透過瀏覽器連接內部應用系統之單一簽入系統網頁。

三、遠端系統驗證階段

使用者必須輸入憑證 IC 智慧卡的 PIN 碼，開始讀取使用者的憑證資訊，並與身份認證管理系統進行簽章認證作業，確認使用者的身份。如使用帳號/密碼認證，則

不須簽章認證作業。

四、雙方會談階段

當使用者身份認證完成後，系統將個人憑證資訊或帳號資訊傳遞給相關應用系統。應用系統接收身份認證管理系統的認證請求回應，以及個人憑證資訊或帳號資訊，並直接對應系統內的使用者帳號資訊，最後帶出使用者的個人化資訊。

五、使用者變更密碼階段

當使用者以帳號/密碼進行身份驗證時，該使用者密碼便每隔一段時間，自行變更所屬密碼資訊，避免個人密碼遺失或外洩所造成的資訊安全風險。

參、 系統功能說明

一、帳號管理系統功能說明

本項系統功能為針對本會系統資源及資訊服務之使用，基於資訊安全考量，對使用者帳號予以標準化，亦即提供完整之帳號整合作業，以有效建立本之安全機制，並在本基礎下給予適當之授權，提供本會同仁與附屬單位同仁使用。如圖 3 之帳號管理系統作業流程說明：

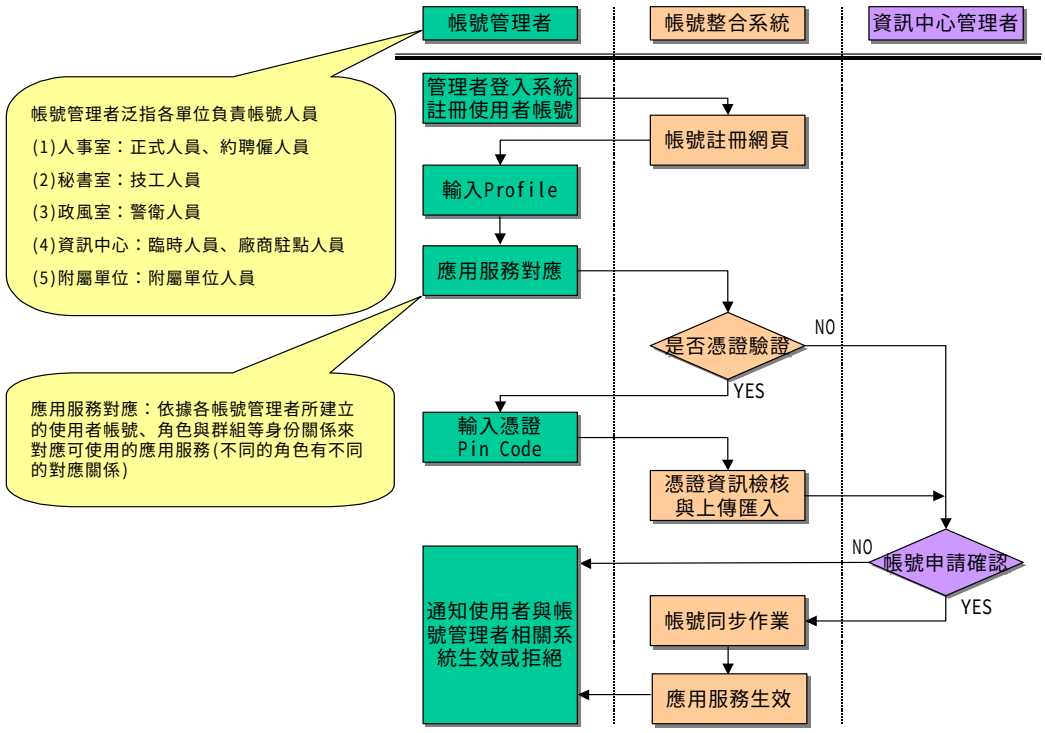

圖 3　帳號管理系統作業流程圖

系統開發採人性化 GUI 介面作為管理者與使用者的操作介面，主要由五大功能模

組及異質系統介接模組（Agent）構成，經由各模組分工處理後再整合於本系統內，各系統模組分別為「系統管理模組」、「同步事件處理模組」、「帳號管理者模組」、「使用者登入模組」和「授權審核模組」等，為安全考量本系統也納入本專案所建置單一認證暨授權管理平台之控管作業。

為建立統一集中之帳號管理系統，首先對於現有職工人員的基本帳號資訊作彙整處理，匯入現有帳號以建立一新完整之帳號系統，以供認證授權使用，並達成帳號之一致性，針對現有 Web 應用系統之帳號功能，需取消帳號註冊作業及帳號註銷作業，並取消現有之認證機制也就是取消密碼欄位與輸入，統一由單一認證暨授權管理平台處理。如圖 4 之帳號管理系統架構說明：

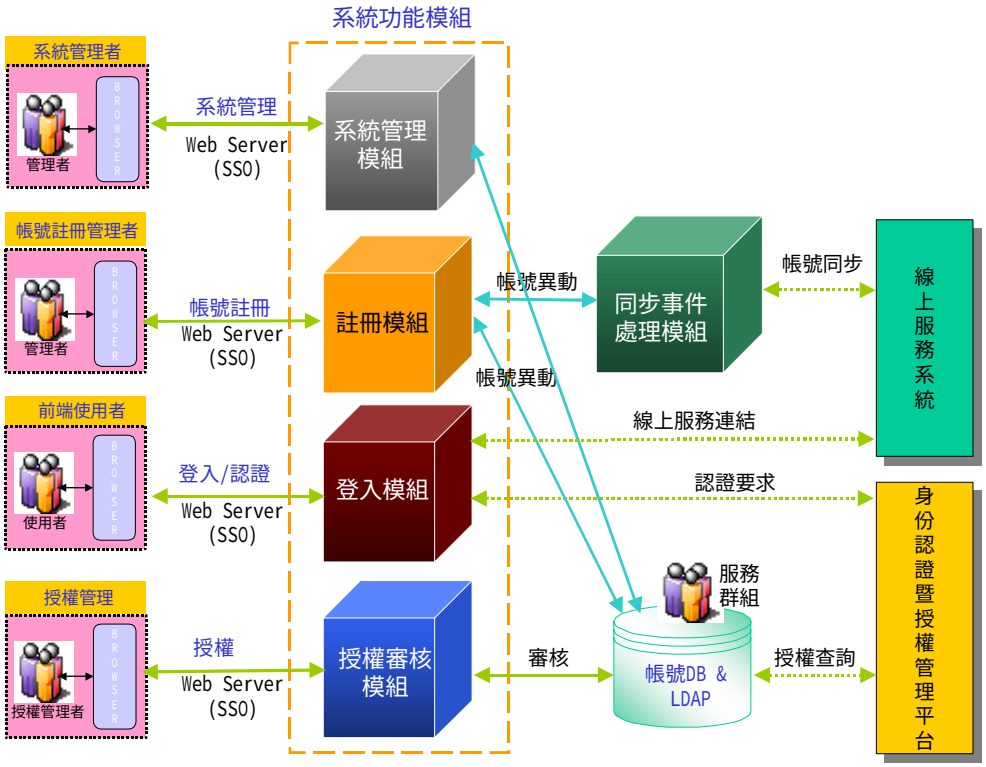

圖 4　帳號管理系統架構圖

二、單一認證暨授權管理平台功能說明

系統整合本會相關線上服務系統之認證與授權，使用者帳號與數位憑證可透過帳號管理系統，將各系統帳號資料匯整儲存於目錄伺服器。系統管理者可透過認證授權系統，完成具安全性與完整性之系統認證與授權作業。系統管理的方式，可直接透過 Web GUI 界面來設定完成，並以矩陣的方式進行授權政策管理。

本專案提供之認證授權系統特色，除了簡單的授權管理工具外，亦延伸其本身的功能，並結合完整的存取控管系統，提供使用者及應用系統內容提供者間線上關係功能：

- 支援單一簽入（Single Sign-On ,SSO）
- 賦予使用者設定的能力
- 提供使用者密碼與設定管理
- 授權管理機制
- 提供點對點（end-to-end）的稽核系統
- 系統資源服務搜尋與註冊設定

(1) 支援單一簽入（SSO）

提供 Web 單一簽入（SSO）的能力，使用者可於存取系統資源時，只要簽入系統一次即可，系統會將其簽入資訊儲存起來，便於後續其它的存取動作。

(2) 賦予使用者設定檔的能力

當使用者隨組織進行異動時，使用者設定檔可進行動態資訊改變。當使用者設定檔的屬性改變時，其角色歸屬亦會相對異動。讓相關 Web 應用程式於發展時變得更簡易，程式開發人員不需為了取得使用者應有的相關權限，再去開發或維護複雜的目錄或資料庫存取程式碼。

(3) 提供使用者密碼與設定管理

系統密碼與設定檔管理，可簡化使用者處理線上服務，並對技術資源最小化需求，讓使用者在其他地方亦能最佳化地處理。

(4) 授權管理機制

授權管理系統可允許對使用者及政策授權，並對於分散式的管理，提供較多的控管。可針對多重層級（Multi-Tiers）的管理者提供次一階的授權，模仿真實環境中的組織圖。

(5) 點對點（end-to-end）的稽核系統

系統會連結安全稽核伺服器，不只可從分散式網路中的不同元件收集訊息，亦可對所有的稽核記錄進行數位簽章。

(6) 系統資源服務搜尋與註冊設定

系統提供彈性的應用服務資源搜尋與註冊設定作業，並可定義與執行授權機制，以便使用者能夠存取該資源，例如：使用者所處的位置，讓使用目錄伺服器作為中央儲存器，儲存資源列表中的政策資料。並允許建構特殊的 Plug-Ins 來掃描任何特定的應用服務資源。因此，系統會列舉所有可用的服務與資源，並透過該內建功能，以階層式的方式加入 Policy Builder 的 Policy Matrix 中，節省管理者時間並

改進準確度。

肆、 效益

一、將本會同仁之工作轉變為知識工作者，隨時隨地可利用網路擷取知識，取得有助工作之資訊，並經由同仁間知識分享、學習，加強組織能力及提昇服務品質與行政效率。
二、將本會相關資訊服務之使用者帳號管理及身份認證作業予以標準化，使本會同仁在安全、完整且保密的網路環境下完成各項資訊存取活動。
三、整合本會現有帳號管理系統，提供單一帳號整合服務管理功能，透過帳號管理介面新增、修改帳號資料，於帳號資料變動時，可同步更新帳號資料至本會相關線上系統。
四、建立本會對內與對外網路線上之身份認證整合，提供本會及附屬單位同仁使用單一簽入系統機制，推廣本會電子化政府應用之目標。

伍、 結論

建置本專案旨在立基於現有資訊系統的基礎上，加強網路的資訊流通，支援組織工作人員（決策層、管理層、承辦人員層等所有員工）有效獲取有用的網路資訊資源，提高工作效率，達到提高組織整體運作效率的目的，進而提昇便民服務品質，創新政府服務，為全國勞工謀求更大的福利。

（本文由勞委會資訊中心黃金福科長 提供）