論述 》管理 · 資訊

# 全國主計網新版單一簽入平台之推動效益

行政院主計總處為順應行動化科技發展趨勢並整合新興身分識別機制，導入新版單一簽入平台，冀在資訊安全的前提下，強化主計資訊系統使用者身分及權限管理，充實多元資訊服務內容，以達成建置全國主計人員協作平台之目標。

蔡宏宜（行政院主計總處主計資訊處分析師）

## 壹、前言

行政院主計總處（以下簡稱本總處）爲提升資訊服務效能，持續運用創新資訊科技，發展主計資訊系統與應用服務。爲便利全國主計人員使用，本總處於 102 年藉由全國主計網（eBAS），建置集中式認證（以下簡稱 CAS 系統）機制（圖 1），提供身分驗證、帳號資料查詢等功能，作爲本總處各主計資訊系統之單一簽入服務基礎，包含歲計會計系統（GBA、SBA）、主計人員人事資訊系統及本總處內部服務系統等，以減輕主計人員在使用不同系統時，須記憶各系統使用帳號及密碼的負擔。

## 貳、面對的限制及難題

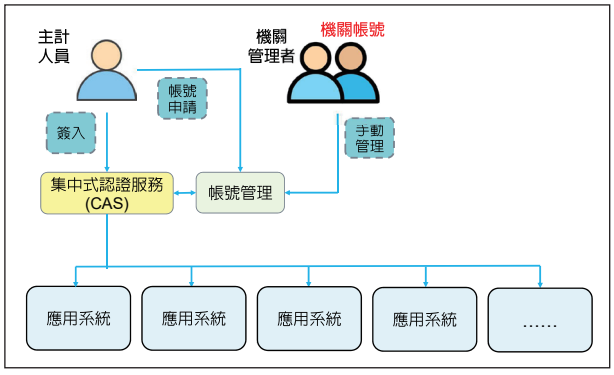
現行 CAS 系統功能（下頁圖 2）雖已有單一

圖 1　現行 CAS 系統簽入畫面


資料來源：行政院主計總處主計資訊處。

簽入的服務基礎，然其帳號管理機制係由主計機構指定人員擔任機關管理者，透過機關帳號進行使用者資料維護、權限設定、密碼管理及人員組織樹節點調整等，遇有作業層面的限制：

圖 2　現行 CAS 系統功能




資料來源：作者自行繪製。

一、機關管理人員以機關帳號簽入後，進行使用者帳號資料維護（圖 3），常因業務需求不同，未能有固定的管理人員；如有多人同時具備機關帳號權限時，將無法追查實際使用情形，潛藏資安風險。

圖 3　機關帳號

行政院主計總處主計資訊處 單位資料維護

| | |
|---|---|
| * 單位代號 | 321010000A |
| * 單位名稱 | 行政院主計總處主計資訊處 |
| 單位別 | ○主計機構 ◉內部單位 |
| eBAS帳號 | 32101 |
| 電子信箱 | [redacted] |
| 電話 | [redacted] |
| 傳真 | [redacted] |
| 通訊地址 | 台北市廣州街2號 |
| 信箱專責人員 | |
| 機構網頁 | |
| 排序 | 0_321010000A |

資料來源：行政院主計總處主計資訊處。

二、新進人員或非主計人員須等待機關管理人員預先於 eBAS 建立個人基本資料，才能進行使用者帳號之申請，未能切合使用者導向的操作流程；若基本資料有誤，更導致無法正常申請帳號。

三、主計人員職務異動或機關單位調動時，常因未主動更新，造成帳號基本資料與實際不符，因此無法依使用者所在機關及身分，提供適當的資訊系統使用權限，進而影響業務運作。

CAS 系統迄今運作多年，現存使用者帳號眾多，因系統架構老舊且缺乏後續擴充可行性，以致在技術發展上，面臨下列難題：

一、無法支援新興身分識別機制，例如行動身分識別（TAIWAN-FidO）、動態密碼（OTP）、生物識別等。

二、針對新加入的資訊系統進行跨系統間身分識別整合時發生困難，例如經費結報系統、GBA、線上簽核系統等，使用者仍須切換不同帳號，造成操作不便利。

三、現行各主計機構所使用之 eBAS 機關帳號，常有多人共用帳號情形，不符合現行資訊安全規範要求。

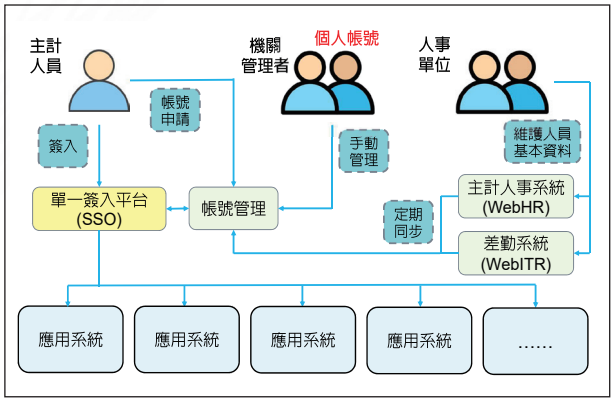
## 參、建置新版單一簽入平台

本總處為突破前述限制、克服難題，同時順應行動化應用發展趨勢、導入新興身分識別機制及建構各系統帳號的整合介接功能，作為主計資訊系統使用者識別流程一致化之基礎，並藉由單

# 論述 》管理 · 資訊

一存取控制機制，簡化使用者帳號、密碼管理成本及降低資安風險，進而建置「主計資訊系統單一簽入平台」（以下簡稱新版平台，圖 4），具有以下功能：

圖 4　新版單一簽入平台功能




資料來源：作者自行繪製。

一、提供多樣化身分驗證機制

（一）符合 OpenID Connect（OIDC）技術規範的單一帳號簽入（Single Sign On，SSO）服務，目前提供使用者選擇「帳號／密碼」或「自然人憑證」驗證方式（圖 5）簽入系統。

圖 5　新版單一簽入平台簽入介面


資料來源：行政院主計總處主計資訊處。

（二）提供使用者註冊管理自然人憑證功能，以利驗證自然人憑證之有效性，包含檢查憑證是否被列於「憑證廢止表列（Certificate Revocation List，CRL）」或透過線上憑證狀態協定（Online Certificate Status Protocol，OCSP）查詢憑證狀態等，可避免使用已廢止的憑證簽入系統，確保資訊安全。

（三）配合未來發展規劃，可擴充新驗證機制如行動身分識別（TAIWAN-FidO）、動態密碼（OTP）、生物識別等，以提升便利性及行動化應用。

二、運用單一簽入機制

（一）利用資訊系統單一簽入（SSO）的管理功能，未來新加入的資訊系統即以 SSO 應用程式介面（Application Programming Interface，API）規格介接，並透過管理介面進行適當設定即可完成，無須安裝任何元件。

（二）整合帳號認證、授權與管理，以簡化使用者帳號、密碼管理複雜度。當使用者完成簽入流程後，若須使用其他資訊系統，可透過 API 驗證使用者 Token 有效性，使用者無須重複簽入流程即可進入使用。

（三）系統管理者可依照使用者的單位角色來設定能夠存取的資訊系統，以限制使用者的存取權限。

三、建置新版 eBAS 組織樹

新版平台將作爲各主計資訊系統權限控管的基礎，未來主計人員能以一個身分簽入平台後，即可使用所需之多元資訊系統，且不因跨系統流

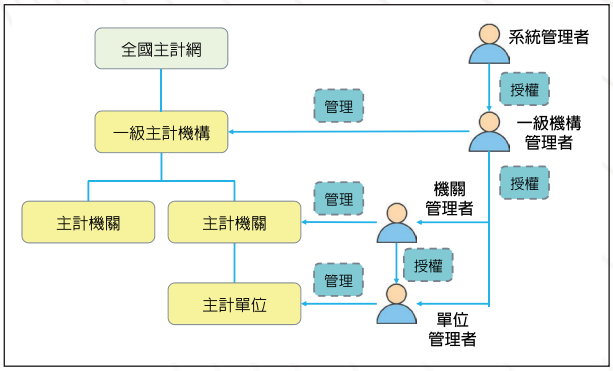
程，而有重新簽入不同系統的情形。為達成上述的單一簽入目標，首先必須擁有全國主計人員帳號資料，因此新版平台將定期同步主計人事系統 WebHR（主計機構人員）及差勤系統 WebITR（本總處人員）資料，以建立新版 eBAS 組織樹，並提供組織資料同步介接 API 規格，以利各主計資訊系統介接取得人員帳號資料，進而設定系統的使用權限。

在 eBAS 組織樹架構（圖 6）下，新版平台將提供分層授權功能（圖 7），經由授權各機關管理人員以個人帳號管理所屬機構人員資料，以明確區分權責及資安管理；又考量資訊系統使用者有時包含非主計人員（如臨時人員或其他人員等），未能自 WebHR 或 WebITR 等人事相關系統取得資料，故新版平台提供機關管理者可手動建立帳號資料的功能，以利彈性運用。

## 圖 6　新版 eBAS 組織樹架構（以內政部會計處為例）


資料來源：行政院主計總處主計資訊處。

## 圖 7　分層授權示意圖



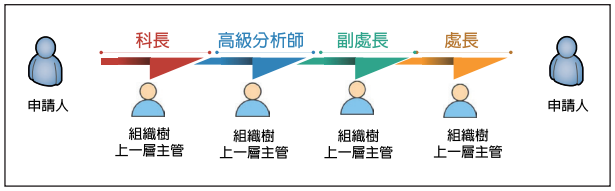

資料來源：作者自行繪製。

四、發展 eBAS 組織樹應用功能

藉由新版 eBAS 組織樹可即時提供帳號現況的優點，新版平台已結合現行本總處內部紙本流程表單與帳號資訊，建置線上電子表單（圖 8），預計本總處內部先行採用，透過電子表單系統自動遞送、線上簽核，進行 eBAS 組織維護作業，如使用者帳號申請單、帳號異動單、帳號刪除單、新進人員報到單、離職交代查核單等，以提升行政效率並落實減紙目標。

電子表單依據 eBAS 組織樹階層傳遞，申請人送出表單後，系統會依據組織樹層級，依序傳送上一層主管簽辦；另依據申請人角色（如科員、

## 圖 8　以 eBAS 組織樹架構設定表單流程




資料來源：作者自行繪製。

科長等）不同，可以設定啓動不同的電子表單流程。由於 eBAS 已與最新主計人事資料結合，本功能未來可作爲主計體系跨單位共用系統之建置基礎並推廣應用。

五、強化資訊安全管理

（一）爲符合「系統管理人員應避免共用管理者帳號」資安規範要求，新版平台將不提供機關帳號簽入機制，以使用個人帳號爲主。

（二）各主計機構管理人員將由單一簽入平台設定帳號管理權限，後續由該管理人員負責機關人員資料維護業務及資訊安全管理。

（三）新版平台提供詳盡操作（含簽入成功、簽入失敗、簽出成功及帳號遭到鎖定等）紀錄，並可匯出 Excel 格式檔案備查。

## 肆、達成效益

eBAS 導入新版單一簽入平台後的效益如下：

一、完整性

主計人事系統（WebHR）、主計總處差勤系統（WebITR）係由各級主計人事單位負責維護人員基本資料，新版平台藉與上述系統定期同步人員組織資料，以達成涵蓋全國各級機構主計人員的目標。

二、即時性

經由定期同步機制，取得最即時主計人員異動資訊（如到職、調職、退離、退休等資訊），避免產生資料落差情形。

三、正確性

因人員資料係由各級主計人事單位維護，可避免現行各機關（單位）管理人員誤繕使用者個人資料的情形發生。

四、安全性

以具有管理權限的使用者帳號辦理機關（單位）帳號管理作業，取代多人共用管理帳號機制，可強化資訊安全稽核能力，且避免高權限帳號被誤用情形。

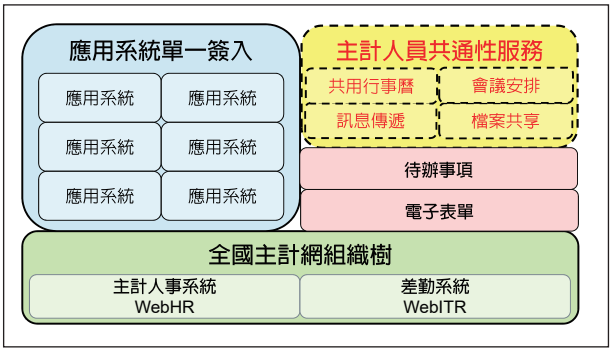
五、彈性

新版平台除提供自動化同步主計人員資料的機制外，亦提供手動新增人員的彈性做法，以確實貼近各業務單位使用上的需求。

## 伍、後續發展

導入新版單一簽入平台後，建立新 eBAS 組織樹，已打造各主計資訊系統單一簽入的新開始，並可進行業務資訊發布、跨組織線上表單傳遞，亦將陸續發展主計人員共通性服務（如訊息傳遞、檔案共享、會議安排及共用行事曆等），充實多元資訊服務內容，以達成作爲全國主計人員協作平台（圖 9）之目標。❖

圖 9　全國主計協作平台規劃




資料來源：作者自行繪製。