身份驗證與權限管理中台
設計說明

摘要

本文件旨在描述本專案規劃的帳號權限管理模組之使用者生命週期管理流程。以 EIP 系統作為資料中台，計劃建立一個統一的帳號與角色權限管理平台，以提升管理效率和安全性。

目錄

身份驗證與權限管理中台設計說明

一、目的說明

本文件旨在描述本專案規劃一帳號權限管理模組之使用者生命週期管理流程，並以 EIP 系統作為資料中台，規劃統一的帳號與角色權限管理平台。該平台將作為內部系統間身份驗證與授權資料交換樞紐，實現以下目標：

1. **簡化新進人員入職流程**：優化帳號開通流程，減少重複操作與手動干預，提升工作效率。
2. **集中化角色管理**：統一管理部內系統的使用者角色，確保角色分配與權限設定的一致性。
3. **實現資料交換中樞功能**：為內部各系統提供使用者角色與權限整合與交換的可靠平台。

二、設計說明

本專案以 EIP 作為核心資料中台，並根據需求採用 Microsoft Azure 平台中的 Microsoft Entra ID ，作為雲端應用服務的核心，負責提供部內系統間身份驗證與授權資料的安全交換與存取功能，用以實現多系統間的統一認證與權限管理。具體設計規劃如下：

2.1 資料整合中台

EIP 系統 作為資料中台，負責彙整部內其他系統的基本資訊和使用者帳號資訊。此中台將成為所有部內系統的數據交換樞紐，整合後的資訊將包括：

1. EIP 應用程式對應 Microsoft Entra ID 之設定

本專案需求採用 Microsoft Azure 平台中的 Microsoft Entra ID，作為身份驗證與角色權限資訊同步之雲端應用服務。藉由 Microsoft Graph API 服務，將使用者對應各部內系統之存取設定與角色相關資訊寫入其帳號的 Microsoft Entra ID-Directory Extensions。具體設定如下說明：

A. Microsoft Entra ID 之應用程式註冊：

在 Azure 平台服務中之 Microsoft Entra ID 服務中進行 EIP 系統之應用程式註冊。註冊後取得以下應用程式相關資訊。實際系統開發上，得將相關資訊設定於環境變數中。

- `CLIENT_ID`：應用程式(用戶端)識別碼
- `OBJECT_ID`：物件識別碼
- `TENANT_ID`：目錄(租用戶)識別碼
- `CLIENT_SECRET`：用戶端密碼

B. 取得應用程式 `Access Token`：

藉由應用程式識別碼、目錄識別碼和用戶端密碼，透過 OAuth 2.0 授權流程與 Microsoft Entra ID 授權伺服器請求取得 Access Token 資訊。取得 Access Token 資訊後，即可藉由 Access Token 建立應用程式的 Directory Extensions。

2. 集中管理各業務系統之角色資訊

本專案所規劃之 EIP 系統作為部內各系統使用者角色權限管理之資料中台，需透過統一的角色管理平台進行系統角色的建立。系統角色的建立與管理作業可透過本專案所規劃角色管理 API 服務進行設定，其內容可參閱所提供之雲原生公務系統研究設計案之 API 服務說明中關於功能權限中角色管理之 API 說明，其 API 路徑為/basic/role。

3. 統一設定部內各業務系統的基礎資料

由於部內系統以 EIP 系統作為使用者角色與權限資料取得之來源。因此，EIP 需先將各系統註冊至 EIP 系統，並完成其擴充欄位的設定。

A. 註冊部內各系統資訊：

本專案已規劃具體 API，其詳細內容可參閱所提供之雲原生公務系統研究設計案之 API 服務說明中關於部內系統交易之 API 說明。以下將以註冊一公文系統作為一模擬情境做範例說明，執行此 API 時，會同步在 Microsoft Entra ID 中以 "code" 的內容新增 Extension 欄位。

API 路徑	/applications
HTTP 方法	POST

Request	{
	"header": {
	"usercode": "admin@moda.gov.tw",
	"datetime": "2025-01-09T17:33:12+08:00",
	"jwt": "modaeipapi"
	},
	"message": {
	"code": "DMS",
	"displayName": "公文系統",
	"status": 1
	}
	}

B. 管理部內系統擴充欄位：

本專案已規劃具體 API，其詳細內容可參閱所提供之雲原生公務系統研究設計案之 API 服務說明中關於部內系統的擴充欄位交易之 API 說明。以下將以新增部內系統之角色清單為例進行說明。其中{appid}為註冊部內系統 Response.message.data.id。

API 路徑	/applications/{appid}/extensionProperties
HTTP 方法	POST

Request	{
	"header": {
	"usercode": "admin@moda.gov.tw",
	"datetime": "2025-01-09T17:33:12+08:00",
	"jwt": "modaeipapi"
	},
	"message": {
	"name": "role",
	"dataType": "Array",
	"options": "[{\"code\":\"admin\",\"name\":\"管理者
	\"},{\"code\":\"user\",\"name\":\"使用者\"}]"
	}
	}

2.2 使用者帳號資訊與角色授權管理

1. 新進人員帳號與角色權限建置

現行數位發展部當有新進人員時，其帳號申請流程如下所示：

A. 人事單位透過電子郵件寄送給新進人員免登入填寫表單，此階段作業於現行既有的表單系統中執行，其作業內容並未包含於本案之規劃範疇。
B. 新進人員填寫之基本資訊完成後，資訊人員將於現行既有的表單系統中執行審核作業，其作業內容並未包含於本案之規劃範疇。
C. 資訊人員審核通過後，即可透過本專案所規劃之使用者建立 API 服務進行使用者帳號建立作業，新進人員帳號建立 API 服務如下所示：

API 路徑	/users
HTTP 方法	POST

Request	{
	"header": {
	"usercode": "admin@moda.gov.tw",
	"datetime": "2024-07-16T16:27:12+08:00",
	"jwt": "modaeipapi"

	<pre>},
	"message": {
	"userPrincipalName": "admin@moda.gov.tw",
	"password": "P@ssw0rd",
	"displayName": "MODAUSER",
	"department": "研發部",
	"jobTitle": "研發工程師",
	"status": 1
	}
	}</pre>

透過此 API 服務，將新增使用者資訊至 EIP 系統中，並同步於 Microsoft Entra ID 服務中新增使用者帳號資訊。其中，欄位「userPrincipalName」之電子信箱資訊必須為數位發展部之網域。

D. 新進人員報到後將可申請部內各系統角色權限，並等待各系統管理者審核。EIP 系統會根據前述之註冊部內系統與新增部內系統擴充欄位設定，輪詢各系統的存取權限及擴充欄位配置，並呼叫專案所規劃之新增使用者帳號對應部內系統存取設定 API 服務完成操作。其 API 規劃設計如下所示：

API 路徑	/users/{userPrincipalName}/userApplicationAccess
HTTP 方法	POST

Request	<pre>{
	"header": {
	"usercode": "admin@moda.gov.tw",
	"datetime": "2024-07-16T16:27:12+08:00",
	"jwt": "modaeipapi"
	},
	"message": {
	"accessList": [
	{
	"appid": "註冊部內系統 Response.message.data.id",
	"available": true, //true:可存取系統, false: 不可存取系統
	"extension": [
	{
	"id": "新增部內系統的擴充欄位 Response.message.data.id",
	"value": "user" //此範例設定角色為使用者
	}
	]
	}
	]
	}
	}</pre>

E. 若系統管理者同意新進人員之角色與存取權限申請，將可透過以下規劃之 API 服務更新其系統的存取權限及擴充欄位配置，並同步將配置內容寫入 Micorsoft Entra ID Extension。其 API 規劃設計如下所示：

API 路徑	/users/{userPrincipalName}/userApplicationAccess
HTTP 方法	PATCH
Request	{ "header": { "usercode": "admin@moda.gov.tw", "datetime": "2024-07-16T16:27:12+08:00", "jwt": "modaeipapi" }, "message": { "accessList": [{ "appid": "註冊部內系統 Response.message.data.id", "available": true, "extension": [{ "id": "新增部內系統擴充欄位 Response.message.data.id", "value": "user" }] }] } }

2. 既有使用者之角色權限資訊修改

A. 修改部內各系統角色權限後，等待各系統管理者審核。EIP 系統會根據前述之註冊部內系統與新增部內系統擴充欄位設定，輪詢各系統的存取權限及擴充欄位配置，並呼叫專案所規劃之修改使用者帳號對應部內系統存取設定 API 服務完成操作。其 API 規劃設計如下所示：

API 路徑	/users/{userPrincipalName}/userApplicationAccess
HTTP 方法	PUT
Request	{ "header": { "usercode": "admin@moda.gov.tw", "datetime": "2024-07-16T16:27:12+08:00", "jwt": "modaeipapi" },

	"message": {
	"accessList": [
	{
	"appid": "註冊部內系統 Response.message.data.id",
	"available": true, //true:可存取系統, false: 不可存取系統
	"extension": [
	{
	"id": "新增部內系統的擴充欄位 Response.message.data.id",
	"value": "user" //此範例設定角色為使用者
	}
	]
	}
	]
	}
	}

B. 若系統管理者同意人員之角色與存取權限修改，將可透過以下規劃之 API 服務更新其系統的存取權限及擴充欄位配置，並同步將配置內容寫入 Micorsoft Entra ID Extension。其 API 規劃設計如下所示：

API 路徑	/users/{userPrincipalName}/userApplicationAccess
HTTP 方法	PATCH

Request	{
	"header": {
	"usercode": "admin@moda.gov.tw",
	"datetime": "2024-07-16T16:27:12+08:00",
	"jwt": "modaeipapi"
	},
	"message": {
	"accessList": [
	{
	"appid": "註冊部內系統 Response.message.data.id",
	"available": true,
	"extension": [
	{
	"id": "新增部內系統擴充欄位 Response.message.data.id",
	"value": "user"
	}
	]
	}
	]
	}
	}