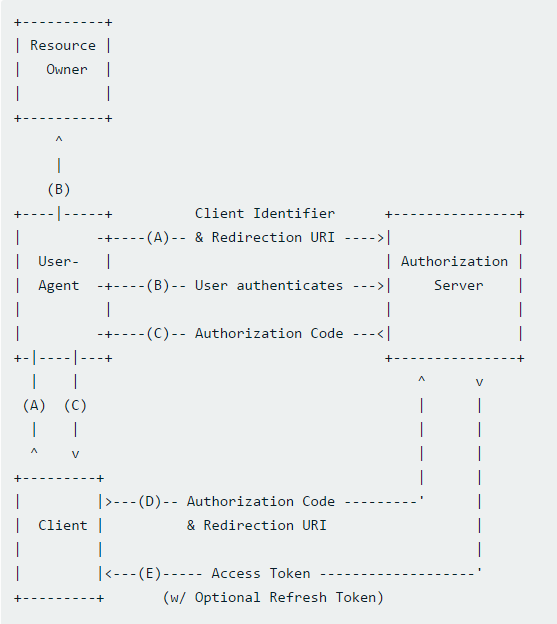
**流程介紹**

IAM採用OAuth 2.0規範流程中的Authorization Grant Code Flow:



流程為

1. Authorization Request
2. User Authenticate (使用者與IAM互動進行認證，系統不須處理)

(C) Authorization Response

(D) Access Token Request

(E) Access Token Response

前置作業

1. 資訊系統需提出介接申請，提供認證名稱作為存取依據
2. 申請時須提供redirect url供IAM記錄，以擋掉不合法的URL

* 預設根網址 (base URL):
  + 請依使用情境替換本文中所有的 {base URL} 為以下兩種設定
    - 測試環境: iam-qa.cht.com.tw
    - 正式環境: iam.cht.com.tw

1. Authorization Request

URL:

https://{base URL}/auth/realms/B2E/protocol/openid-connect/auth

HTTP method: GET

呼叫時須帶上GET參數如下:

|  |  |  |
| --- | --- | --- |
| 參數 | 說明 | 範例 |
| client\_id | 前置作業App申請的ID | mDAS (雙因子)  chtapp(單因子) |
| redirect\_uri | 回傳給應用服務之URI(完成認證後導回App的URL) | http://domain:port/xxx |
| response\_type | 回傳種類,固定值 | code |
| state | 應用服務端,會回傳讓系統確認state是否一樣。如果有參數需要保留，也可以編碼在此參數中 | sessionID@client\_ip |
| nonce | 亂數,長度12,會編進token | 隨機產生亂數(UTF-8)後使用Base64 encode |
| login\_hint | LDAP ID,若資訊系統有記錄過去登入紀錄，可帶上此參數讓使用者少敲一個資訊 | optional |
| scope | 只做認證可不帶入此參數。  帶入scope=openid可使用OpenID Connect介面，IAM會回傳ID Token。帶入scope=ldap可取得工號資料。  可同時帶多個scope，使用空格(%20)分隔。 | openid  ldap |
| acr\_values | 必須同時帶入scope=openid才有作用，acr\_values=two作為特級系統認證 | two |

1. Authorization Response

IAM會將code放到redirect\_uri後面,

ex: http://domain:port/xxx?session\_state=e58d3eb9-1e25-4752-821f-ac12619a1a14&code=omt3jTDlWLtZKO0gH2tCTqvm-n63I9XhV4qeuGnpgcs.d0662c92-033f-41b0-a143-c1bf8930f941&state=sessionID

* 取得code後，使用code在步驟(D)進行access token的申請
* state可用於安全驗證，確認(A)步驟的state中的sessionID是否一致
* session\_state是deprecated的參數，不須理會
  + https://openid.net/specs/openid-connect-session-1\_0.html

1. Access/Refresh Token Request

URL:

https://{base URL}/auth/realms/B2E/protocol/openid-connect/token

HTTP method: POST

Content-Type: application/x-www-form-urlencoded，用step (C) 取得的code交換access token, 呼叫時須帶上參數如下:

|  |  |  |
| --- | --- | --- |
| 參數 | 說明 | 範例 |
| client\_id | 前置作業資訊系統申請的認證名稱 | mDAS |
| redirect\_uri | 用於驗證是否合法 | http://domain:port/xxx |
| code | 於step(C)取得的code |  |
| grant\_type | 認證方式，使用者認證用authorization\_code，系統認證用client\_credentials | authorization\_code  client\_credentials |
| client\_secret | 確認後端系統身分(選填) |  |

1. Access Token Response

取得回傳結果:

|  |  |  |
| --- | --- | --- |
| 參數 | 說明 | 範例 |
| access\_token | 用於存取API服務 |  |
| expires\_in | access token有效時間長度 | seconds |
| refresh\_token | 用於取得新的access token |  |
| refresh\_expires\_in | refresh token有效時間長度 | seconds |

登出

使用者完成登入後，IAM會在瀏覽器中存放session資料，在session時效內，使用者可以不須進行登入動作(直接通過step A)。如果想要提供使用者登出session的功能，資訊系統可以實作功能，選擇呼叫以下URL執行登出動作。

* 有確認視窗與使用者互動:
  + https://{base URL}/auth/realms/B2E/protocol/openid-connect/logout
* 直接登出
  + https://{base URL}/auth/realms/B2E/protocol/openid-connect/logout?post\_logout\_redirect\_uri={申請的redirect\_uri} &id\_token\_hint={id\_token}

備註:

1. scope帶入openid時，IAM會回傳id\_token
2. 呼叫直接登出API，如果登出的session不一致(ex. id\_token對應的session已登出過)，仍會跳出對話視窗而無法直接登出
3. id\_token的時效與access token相同，使用refresh token更換token，可以取得新的id\_token

**補充**

1. refresh token作法

使用(D) endpoint

|  |  |  |
| --- | --- | --- |
| 參數 | 說明 | 範例 |
| client\_id | 前置作業App申請的ID | mDAS |
| refresh\_token | 於先前取得的refresh token |  |
| grant\_type | 認證方式，固定值 | refresh\_token |

1. step(A)使用LDAP帳密進行認證
2. 認證強度管理:
   1. 作法一: 由資訊系統管理
      1. 若要實作1天1次(或每N小時1次)雙因子認證,可於step(E) 的回傳結果中取得該client的認證設定(單/雙因子認證)來判斷目前認證強度
      2. 使用兩組client來分別處理單雙因子的認證
      3. 如果雙因子時效到了，目前認證強度又只有單因子，就可以呼叫雙因子認證的client
   2. 作法二: 由IAM管理
      1. 採用遞升式身分驗證，認證時帶入acr\_values
      2. 資訊系統需要拆解token中的acr資訊來判斷目前登入的認證強度
3. LDAP資訊可以從token中解出

格式如下:

|  |  |  |
| --- | --- | --- |
| 參數 | 說明 | 範例 |
| uid | 員工代號 | btlin1025 |
| name | 員工姓名 | 林柏廷 |
| scope帶ldap | | |
| employeeNumber | 員工代號 | 842482 |
| title | 職稱 | 76 |
| 不提供 | | |
| dn | 識別名稱 | employeenumber=xxx,ou=xxx,o=xxx,o=xxx,o=xxx,o=xxx,o=cht,c=tw |

1. Introspection endpoint

後端系統可以申請使用檢驗Token API。IAM會配發給系統一組密碼，未來系統呼叫IAM API都需要帶上此密碼以驗證系統身分。

https://{base URL}/auth/realms/B2E/protocol/openid-connect/token/introspect

使用POST呼叫，content-type: application/x-www-form-urlencoded，須帶上參數如下:

|  |  |  |
| --- | --- | --- |
| 參數 | 說明 | 備註 |
| client\_id | 前置作業App申請的ID |  |
| client\_secret | 配發給App的密碼 |  |
| token | 要驗證的token |  |

取得回傳結果:

|  |  |  |
| --- | --- | --- |
| 參數 | 說明 | 備註 |
| active | 用於存取API服務 | 指示所提供的Token當前是否處於可用狀態 |
| exp | token過期的時間 | timestamp |
| client\_id | 該token 核發給的App的 ID |  |

備註:

1. 若browser已有NIAS的session，呼叫(A)步驟使用者不須再次登入

申請單範例:

1. 系統使用IAM來認證系統以呼叫APIM申請範例

一張含有 文字, 螢幕擷取畫面, 字型, 數字 的圖片

自動產生的描述

2. 系統使用IAM來認證使用者申請範例

一張含有 文字, 電子產品, 螢幕擷取畫面, 軟體 的圖片

自動產生的描述

3. 系統使用IAM來認證使用者新增轉導網址範例

一張含有 文字, 螢幕擷取畫面, 字型, 行 的圖片

自動產生的描述

**修改歷程**

* 230627:
  + 格式與文字調整
  + 新增[登出](#登出)說明
  + 新增[認證強度管理](#認證強度管理)方法說明
* 230725
  + 新增[Introspection endpoint](#Introspection_endpoint)介紹
* 230928
  + 新增申請單範例