臺北市教育人員統一身份驗證服務

資料介接手冊

壹、資料介接專案申請流程

請以電子郵件與專案聯絡人申請資料介接，並填寫申請表。

專案聯絡人：謝琪文

電子郵件：chiwen168@gmail.com

貳、授權模式：

本系統所提供之資料，包含：學校公開資訊、個人資訊等兩種不同保密要求之資料，依照資料的分類及允許處理資料的方式，共提供三種不同授權方式，應用程式開發者應在不同場合，使用不同授權模式進行資料介接。

一、專案授權：

讀取學校公開資訊，請使用此授權模式。審核通過之專案，可以憑藉專案代號（client\_id，為專案流水號）及專案密碼（client\_secret，為雜湊字串），向伺服器交換授權金鑰（access\_token）即可進行相關資料查詢，無需使用者介入。

二、個資授權：

讀取學校人員資訊，須由個資當事人進行授權，若個資當事人未滿 13 歲，應先取得家長之書面同意後，始可使用此模式進行存取。進行使用者授權時，將由使用者依據應用程式想要存取的資料欄位，自行決定是否同意提供該資料給應用程式，並可於事後隨時取消授權。

三、代理授權：

進行學校資料維護操作，例如：新增、刪除、修改學校或人員之資料，必須由各校管理人員於本系統管理介面，預先製作授權金鑰，然後將金鑰交予應用程式，應用程式可以代理該管理人員，使用金鑰介接系統並進行資料操作。

参、資料授權範圍：

|  |  |  |  |
| --- | --- | --- | --- |
| **Scope** | **授權模式** | **資料操作** | **資料內容** |
| oauth | - | 取得、交換授權碼及金鑰 | 授權碼、金鑰 |
| user | 個資授權 | 讀取，修改電子郵件與手機號碼，啟用或關閉替代登入功能 | 使用者之唯一編號、姓名、電子郵件、手機號碼等四個欄位 |
| idno | 個資授權 | 讀取 | 使用者之身分證字號 |
| profile | 個資授權 | 讀取 | 使用者之角色、性別、生日、所屬學校、單位、職稱、就讀班級、座號等八個欄位 |
| account | 個資授權 | 修改自訂帳號及密碼 | 不提供任何資料 |
| school | 專案授權 | 讀取 | 移除個資之後的各項學校資料 |
| schoolAdmin | 代理授權 | 讀取全校所有人員資料，修改學校單位、職務、班級資料，新增、刪除、修改學校教師或學生資料 | 提供取得授權學校之所有資料 |

肆、資料存取端口

網址：https://ldap.tp.edu.tw

|  |  |  |  |
| --- | --- | --- | --- |
| **endpoint** | **scope** | **HTTP協定** | **功能說明** |
| /oauth/authorize | oauth | GET | 應用程式請求個資授權，將導向到使用者登入頁面以及授權頁面，授權成功後，將授權碼傳送到專案之重導向網址（redirect\_uri） |
| /oauth/token | oauth | POST | 應用程式傳送授權碼向伺服器請求金鑰，系統將產生存取金鑰與交換金鑰，並回傳金鑰給 client。 |
| 應用程式在存取金鑰過期（1天）後，可以傳送交換金鑰以取得更新後之存取金鑰，交換金鑰可使用期限為30天。 |
| 應用程式傳送專案代號及密碼，並取得專案授權之存取金鑰。 |
| /api/logout | 任意 | POST | 登出使用者，並移除授權金鑰 |
| /api/email | email | GET | 取得目前登入者的電子郵件信箱 |
| /api/me | me | GET | 取得目前登入者的姓名與電子郵件信箱 |
| /api/user | user | GET | 取得目前登入者的UUID、身份別、姓名、電子郵件信箱、手機號碼、登入設定 |
| /api/user | user | PATCH | 修改目前登入者的身份別、電子郵件信箱、手機號碼、取用或取消使用電郵或手機登入 |
| /api/idno | idno | GET | 取得目前登入者的身分證字號 |
| /api/profile | profile | GET | 取得目前登入者的身份識別資料，包含：身份別、隸屬機構、隸屬單位、職稱、配課資訊、特殊身份註記、就讀班級、班級名稱、座號等。 |
| /api/account | account | PATCH | 修改目前登入者的自訂帳號或密碼 |
| /api/school | school | GET | 取得臺北市所有學校之列表 |
| /api/school/{dc} | school | GET | 取得指定學校之詳細資訊，參數{dc}為學校代號 |
| /api/school/{dc}/ou | school | GET | 取得指定學校之行政部門列表，參數{dc}為學校代號 |
| /api/school/{dc}/ou/{ou} | school | GET | 取得指定部門之資訊，參數{dc}為學校代號，{ou}為部門代號 |
| /api/school/{dc}/ou/{ou}/role | school | GET | 取得指定部門之職稱列表，參數{dc}為學校代號，{ou}為部門代號 |
| /api/school/{dc}/ou/{ou}/role/{ro} | school | GET | 取得指定職稱之資訊，參數{dc}為學校代號，{ou}為部門代號，{ro}為職稱代號 |
| /api/school/{dc}/class | school | GET | 取得指定學校之班級列表，參數{dc}為學校代號 |
| /api/school/{dc}/class/{cid} | school | GET | 取得指定班級之名稱，參數{dc}為學校代號，{cid}為班級代號 |
| /api/school/{dc}/class/{cid}/teachers | school | GET | 取得指定班級之授課教師列表，參數{dc}為學校代號，{cid}為班級代號 |
| /api/school/{dc}/class/{cid}/students | school | GET | 取得指定班級之學生列表，參數{dc}為學校代號，{cid}為班級代號 |
| /api/school/{dc} | schoolAdmin | PATCH | 修改指定學校之資訊，參數{dc}為學校代號 |
| /api/school/{dc}/people | schoolAdmin | POST | 新增學校教育人員（教師或學生），參數{dc}為學校代號 |
| /api/school/{dc}/people/{uuid} | schoolAdmin | GET | 取得指定人員之詳細資訊，參數{dc}為學校代號，{uuid}為人員唯一編號 |
| /api/school/{dc}/people/{uuid} | schoolAdmin | PATCH | 修改指定人員之資訊，參數{dc}為學校代號，{uuid}為人員唯一編號 |
| /api/school/{dc}/people/{uuid} | schoolAdmin | DELETE | 修改指定之人員，參數{dc}為學校代號，{uuid}為人員唯一編號 |

伍、資料介接流程說明

ㄧ、專案授權

Request: POST <https://ldap.tp.edu.tw/oauth/token>

格式：form-data 或 json

欄位範例：

{

"grant\_type": "client\_credentials",

"client\_id": 3,

"client\_secret": "kpvnkKpqTsziTLq6EdQE81BUCPzeGfQiDJdc6qMg",

"scope": "school"

}

Response:

{

"token\_type": "Bearer",

"expires\_in": 86400,

"access\_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjA0MjgwNTliNzE5YTUzZjQ3OGY3NDhmZmNmN2YzODFkNTlkNTcyMmRhOGM4NjdiNjE1Y2I4ZGYyYmZmMGU1YmJmMjZmMmI2YTgyNTI4MTM2In0.eyJhdWQiOiIxIiwianRpIjoiMDQyODA1OWI3MTlhNTNmNDc4Zjc0OGZmY2Y3ZjM4MWQ1OWQ1NzIyZGE4Yzg2N2I2MTVjYjhkZjJiZmYwZTViYmYyNmYyYjZhODI1MjgxMzYiLCJpYXQiOjE1MTk1Mzg0OTcsIm5iZiI6MTUxOTUzODQ5NywiZXhwIjoxNTE5NjI0ODk3LCJzdWIiOiIiLCJzY29wZXMiOltdfQ.e5NQmSCcb7EkJtk9yftEnir2iRrEpVELDV6N8jXM9PVplcRjB9UGYKRlt9t7zZ7kZHZY6XpXFKdPsWXBP1R5tnNVL7QR4FNsgpBBYFls7X8qVivcnNChJz89xppomzdc9fa-GDifEJVnhNy3zcugSYhZXPyWxtKSIr0caUeExy-oxGDYbSGlDEom0ZdqNEqExwcTat9lQDWNX5pkyvdPQsXzmwli4ebwI7e1QZZfH4YSwPLvcZ9lneipy4t1rO0xzHCB2EEJBt5aUL8\_oUmlgrFOIyH7iP1NPiJkFUgWjQT52Tzb7tt70I1BmBwzkQxp-KAfvNbS5OQXIFmtgCvH9s7th2BdhJX9eIqy2LaMnsSc\_kvqzjXBqxrXTzTmixEZhWtRVJCHlwgmEkyMlXL2FfoPurHd0qajFwR5STl1HcGlB0d1fW1zZFLHXKT7c-EkBKEtPc6iS2Hqc50W6zBDC8J4yo3Sm7Zp3K9Kl6iS7nh7DGyt8vDNXBY9X1F13IyoENzYIBcQGkWqPP7oLW5WcDFz7hvvS9oR7rmrXBuZSzem0XbWkkMh4vQqMnTWHXruZqpAP687uN4ASXfFgM7c0ul1pF-1YoRE0zQ8vOZujjYv2zAkJBPN-NzHbde4MPfarUdqmCF\_61mRT02dYX1vnSN1A3jKSGoMsAF2o4Z3xkI"

}

二、個資授權

步驟一：

Request: GET https://ldap.tp.edu.tw/oauth/authorize?client\_id=3&redirect\_uri=https://yourapp.com/api/callback&response\_type=code&scope=user,profile

格式：query string

Response:

https://yourapp.com/api/callback?code=授權碼

步驟二：

Request: POST <https://ldap.tp.edu.tw/oauth/token>

格式：form-data 或 json

欄位範例：

{

"grant\_type": "authorization\_code",

"client\_id": 3,

"client\_secret": "kpvnkKpqTsziTLq6EdQE81BUCPzeGfQiDJdc6qMg",

"redirect\_uri": "https://yourapp.com/api/callback",

"code": "步驟一所取得之授權碼"

}

Response:

{

"token\_type": "Bearer",

"expires\_in": 86400,

"access\_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6IjJkZmQxNGFiNDRhNGI5MGQzOThjZmU5MzU1ZDViZTIyN2UzMmQ5ZTgwZjU5OGE5ZDlkYzY0ZWExYWViNTAzYTk2MjgwZWMzOGZhODhhM2NlIn0.eyJhdWQiOiIyIiwianRpIjoiMmRmZDE0YWI0NGE0YjkwZDM5OGNmZTkzNTVkNWJlMjI3ZTMyZDllODBmNTk4YTlkOWRjNjRlYTFhZWI1MDNhOTYyODBlYzM4ZmE4OGEzY2UiLCJpYXQiOjE1MTk2NTcxNDQsIm5iZiI6MTUxOTY1NzE0NCwiZXhwIjoxNTE5NzQzNTQ0LCJzdWIiOiIyIiwic2NvcGVzIjpbIioiXX0.CSGq4vQ7HjNyfhC3h5kEYOilAntmluLAijIE0-tR7zUCmWhBdfgqw8gZuFBDUbZ1TMOpmZEmRY-ccW\_M3sD4ukS7ZWvljAVjZOYSUFgo3pULzxYAstTHns7sukohcuzgiKcELT7BwnMyV61AT8Hr7oRwkffKPnK0e0aeDoF3jjxXFuMcgTe5FsfbGR9FgBFfdyvFK4JmH4oH\_D-Q9MNXGx9YjSl0P\_Se9rZ4yX3UHjI6Z-uD8gOlv4KcNVSslzIT09EMoOjSGIM7p7SNxxEGIU692Zl7tdXk9av4UMkkVpUAaKTatuNsDD0ARnNrhP5tG0U\_1TvLJygZwsCzGq16BaP1BVwy6jDaFppr5Q-B-1d2Jtwz5NA1TSgjImSCMuFft8v5mYPJqVTWoif0b\_kI2zhjHhoj\_HOYdpaeIbqTiY7PEJ2BmkWC8aC3noqx5GzHRzCR4Y33x4jYxXi\_C8TrgjzYR\_Ha340wuosoM82jVa0v0U7ZKMmrvgdapuOe9ALLBMUNsyjTYdgmM3jhaX5kIm8mlDIbvLDukAoeO\_1T13Uzxt1DwvqTfANVkGbUIZD7UtR6YkJw0RasV-fXdnTDvoS-Y78NG2iw3xujQpF-a5fs4U34wCFEqLrGtkQnodEp0O09nN\_JlKg1uJJczVSe4gCw5aCnxBGOXcf9TbmS7MU",

"refresh\_token": ""

}

步驟三：存取金鑰過期之處理方式

Request: POST <https://ldap.tp.edu.tw/oauth/token>

格式：form-data 或 json

欄位範例：

{

"grant\_type": "refresh\_token",

"refresh\_token": “步驟二所取得之refresh token",

"client\_id": 3,

"client\_secret": "kpvnkKpqTsziTLq6EdQE81BUCPzeGfQiDJdc6qMg",

"scope": "user"

}

Response:

同上

三、代理授權

學校管理員登入 <https://ldap.tp.edu.tw/oauth> 金鑰管理介面，建立個人存取金鑰。



**四、REST** 資料存取請求

Request: [GET|POST|PATCH|DELETE] https://ldap.tp.edu.tw/api/….略....

格式：header

欄位範例：

Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImp0aSI6Ijc3MjYwZWUw……

Accept: application/son

**五、REST** 資料存取回應

Request: POST https://ldap.tp.edu.tw/api/logout

Response:

HTTP 204

Request: GET https://ldap.tp.edu.tw/api/email

Response:

{"email":"leexxxxxxxne@gmail.com"}

Request: GET https://ldap.tp.edu.tw/api/me

Response:

{"name":"李忠憲","email":"leexxxxxxxne@gmail.com"}

Request: GET https://ldap.tp.edu.tw/api/user

Response:

{"role":"教師","uuid":"a4bcbfba-a678-1037-952c-15429bf75900","name":"李忠憲","email":"leexxxxxxxne@gmail.com","email\_login":false,"mobile":"09xxxxxxx8","mobile\_login":false}

Request: PATCH https://ldap.tp.edu.tw/api/user

{

"role":"教師",

"email": "shane@tc.xxps.tp.edu.tw",

"mobile": "09xxxxxxx2",

"email\_login": "true",

"mobile\_login": "true"

}

可修改以上四個欄位，不修改的欄位整欄省略，若給空字串，會顯示錯誤訊息。

email\_login 用來開啟使用電子郵件登入之功能，mobile\_login 用來開啟使用手機號碼登入之功能，可在不同載具上應用。

Request: GET https://ldap.tp.edu.tw/api/idno

Response:

{"idno":"P1xxxxxxx6"}

Request: GET https://ldap.tp.edu.tw/api/profile

Response:

{  
"role":"教師",  
"gender":1,  
"birthDate":"19690118",  
"o":"meps",  
"organization":"臺北市中正區國語國民小學",  
"unit":"科任教師",  
"title":"科任教師",  
"teachClass":["301,sub01","302,sub01"],  
"character":"巡迴教師"  
}

Another Response:

{  
"role":"學生",  
"gender":"1",  
"birthDate":"19690118",  
"o":"meps",  
"organization":"臺北市中正區國語國民小學",  
"studentId":"105307",  
"class":"301",  
"className":"三年一班",  
"seat":"13",  
"character":"特教生"  
}

Request: PATCH https://ldap.tp.edu.tw/api/account

{

"account": “newaccount"

"password": "xxxxxxxxxxxxx"

}

可修改以上兩個欄位，不修改的欄位整欄省略，若給空字串，會顯示錯誤訊息。

帳號只能接受英文字母或數字，密碼若有特殊符號需要在前面加\，例如：\\ 代表一個反斜線。

Request: GET https://ldap.tp.edu.tw/api/school

Response:

[  
{“o”:”bureau”,”tpUniformNumbers”:”399999”,"description":"臺北市政府教育局"},  
{"o":"yfes","tpUniformNumbers":"423612","description":"臺北市北投區義方國民小學"},  
{"o":"ssps","tpUniformNumbers":"313601","description":"臺北市松山區松山國民小學"},  
{"o":"sups","tpUniformNumbers":"313602","description":"臺北市松山區西松國民小學"},  
......  
]

欄位 o 為學校或機構代號，tpUniformNumbers 為會計統一編號，description 為學校全銜。

Request: GET https://ldap.tp.edu.tw/api/school/meps

Response:

{"o":"meps","businessCategory":"國民小學","st":"中正區","description":"臺北市中正區國語國民小學","telephoneNumber":"(02)23033555","PostalCode":"100","street":"臺北市中正區南海路58號","wWWHomePage":"http:\/\/www.meps.tp.edu.tw\/","tpUniformNumbers":"353604"}

以上資料欄位，依各校資料提供情形，會有資料量不一致的情形。欄位 businessCategory 為學程分類，st 為行政區，PostalCode 為郵遞區號，street 為郵遞地址，wWWHomePage 為學校網址。

Request: GET https://ldap.tp.edu.tw/api/school/meps/ou

Response:

[  
{“ou":"dept01","description":"校長室"},  
{"ou":"dept02","description":"教務處"},  
{"ou":"dept03","description":"學務處"},  
{"ou":"dept04","description":"總務處"},  
{"ou":"dept05","description":"輔導室"},  
......  
]

欄位 ou 為部門代號，description 為部門名稱。

Request: GET https://ldap.tp.edu.tw/api/school/meps/ou/dept02

Response:

{“ou":"dept02","businessCategory":"行政部門","description":"教務處"}

欄位 businessCategory 為單位分類。

Request: GET https://ldap.tp.edu.tw/api/school/meps/ou/dept02/role

Response:

[  
{"cn":"role002","description":"教務處主任"},  
{"cn":"role003","description":"教學組長"},  
{"cn":"role005","description":"資訊組長"},  
{"cn":"role006","description":"設備組長"},

......  
]

欄位 cn 為職稱代號。

Request: GET https://ldap.tp.edu.tw/api/school/meps/ou/dept02/role/roleC17

Response:

{“ou”:"dept02","cn":"roleC17","description":"系統管理師"}

Request: GET https://ldap.tp.edu.tw/api/school/meps/class

Response:

[  
{"ou":"101","description":"1年1班"},  
{"ou":"102","description":"1年2班"},  
{"ou":"103","description":"1年3班"},

{"ou":"104","description":"1年4班"},  
{"ou":"105","description":"1年5班"},  
{"ou":"106","description":"1年6班"},  
......  
]

Request: GET https://ldap.tp.edu.tw/api/school/meps/class/101

Response:

{"ou":"101","businessCategory":"教學班級","description":"1年1班"}

Request: GET https://ldap.tp.edu.tw/api/school/meps/class/101/teachers

Response:

{"a4bcbfba-a678-1037-952c-15429bf75900"]

Request: GET https://ldap.tp.edu.tw/api/school/meps/class/101/students

Response:

[  
"a4c4513a-a678-1037-955a-15429bf75900",  
"a4c473ae-a678-1037-955b-15429bf75900",  
"a4c496ae-a678-1037-955c-15429bf75900",  
"a4c4b95e-a678-1037-955d-15429bf75900",

......  
]

附錄、client 程式設計範例：

<?php  
session\_start();

if (!isset($\_GET['code']) && !isset($\_SESSION['token'])) {  
 $param = [  
 'client\_id' => '3',  
 'redirect\_uri' => 'redirect\_uri=https://yourapp.com/api/callback',  
 'response\_type' => 'code',  
 'scope' => 'user profile',  
 ];  
 http\_redirect('https://ldap.tp.edu.tw/oauth/authorize', $param);  
 exit;  
} elseif (!isset($\_SESSION['token'])) {  
 $param = [  
 'grant\_type' => 'authorization\_code',  
 'client\_id' => '3',  
 'client\_secret' => '5uyghc0DpeRJHsv43Di567fjasuy083kf6hiDAT',  
 'redirect\_uri' => 'redirect\_uri=https://yourapp.com/api/callback',  
 'code' => \_GET[‘code’],  
 ];  
 $response = http\_post\_fields('https://ldap.tp.edu.tw/oauth/token', $param);  
 $token = json\_decode($response);  
 ini\_set("session.gc\_maxlifetime", $token->expires\_in);  
 $\_SESSION['token'] = $token->access\_token;  
 $\_SESSION['refresh'] = $token->refresh\_token;  
 $\_SESSION['expire'] = time() + $token->expires\_in;  
} elseif (time() > $\_SESSION['expire']) {  
 $param = [  
 'grant\_type' => 'refresh\_token',  
 'refresh\_token' => $\_SESSION['refresh'],  
 'client\_id' => '3',  
 'client\_secret' => '5uyghc0DpeRJHsv43Di567fjasuy083kf6hiDAT',  
 'scope' => 'user profile',  
 ];  
 $response = http\_post\_fields('https://ldap.tp.edu.tw/oauth/token', $param);  
 $token = json\_decode($response);  
 ini\_set("session.gc\_maxlifetime", $token->expires\_in);  
 $\_SESSION['token'] = $token->access\_token;  
 $\_SESSION['refresh'] = $token->refresh\_token;  
 $\_SESSION['expire'] = time() + $token->expires\_in;  
}

$header = [  
 'Authorization' => 'Bearer '.$\_SESSION['token'],  
];  
$response = http\_get('https://ldap.tp.edu.tw/api/user', $header);  
$user = json\_decode($response);  
$response = http\_get('https://ldap.tp.edu.tw/api/profile', $header);  
$profile = json\_decode($response);  
?>