

# 數位服務個人化 ( MyData ) 服務提供者技術開發說明

# 簡報大綱

## 壹、服務提供者申請流程

## 貳、服務流程

- 民眾前台服務流程說明
  - 下載個人資料
  - 線上申辦
  - 臨櫃檢驗
- 後台服務流程說明
- 可運用資料集查詢

## 參、技術規範說明

- MyData 整合網址及參數說明
- SP-API
- MyData-API
- MyData 資料結構與驗簽
- 資料查核相關網頁與 API

# 壹、服務提供者申請流程

1 請至 **MyData GitHub** 下載介接申請文件  
<https://tinyurl.com/u2kofxj>

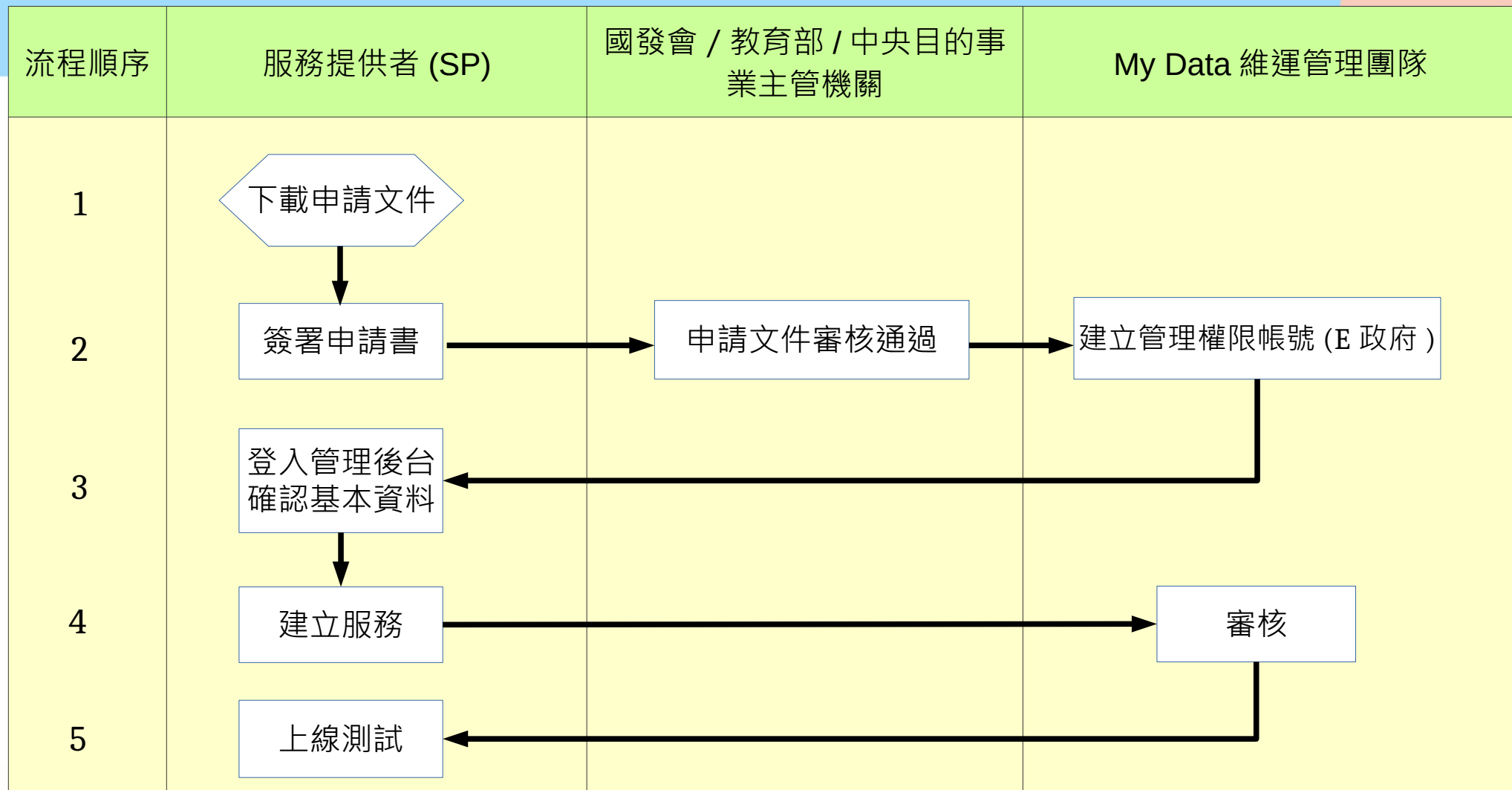
2 簽署「服務提供者介接申請表」，並依照「**MyData**  
平臺介接作業試辦要點」向相關單位提出申請

介接申請表簽署前，  
請先提供MyData團隊  
確認填寫內容

3 管理團隊建立申請人 E 政府公務帳號後台  
使用權限

4 申請人使用帳號登入後台並確認基本資料無誤

5 申請人開始使用管理後台之服務提供者  
(SP) 相關功能



## 貳、服務流程

# 民眾線上申辦 服務流程說明

## STEP 1 使用者從 MyData 網站點擊“線上服務”，選擇服務項目

網站地圖 常見問題 字級：中 前往個人專區

MyData 數位服務個人化 關於 MyData MyData 服務項目

下載個人資料  
線上服務

首頁 > MyData 服務項目

### 線上服務

點選下列線上服務，系統將會自動連結到服務提供端(機關/機構)的網站服務

#### 消費金融

◎ 第一銀行信用卡MyData介接

服務提供單位：第一商業銀行

#### 教育學習

◎ 高級中等學校低收入戶及中低收入戶學生線上申辦學雜費減免服務

服務提供單位：教育部國民及學前教育署



## 或直接由申辦服務機關進入 MyData 服務



教育部全國高級中等學校  
助學補助系統



國立暨南國際大學

### 高級中等學校低

本服務由教育部國民及學  
請於使用本服務前詳閱本

一、服務目的與內容  
為協助高級中等學

#### 五、服務條款修訂

1. 本服務條款因故需進行修改或變更時，本部國教署將取消您對本服務之授權內容，同時停止提供本服務；若您需要使用本服務，請同意最新版本之本服務條款，並重新授權本部國教署要求的個人資料。
2. 本部國教署因服務條款修改或變更而停止提供本服務期間，本部國教署對於您因無法使用本服務而造成的損害，不負任何賠償責任。

#### 六、注意事項

1. 您得自由選擇是否提供個人資料，惟您若拒絕提供相關個人資料，本部國教署將無法進行必要之審核及處理相關作業，致無法受理您前揭權利之行使或提供您相關服務。
2. 本告知事項日後如有更新內容，將於本部網站另行公告。

☒ 我已詳實了解此服務內容，並同意上述服務條款。

請輸入學生身分證字號：

使用MyData取得低收/中低收身分證明

## STEP 2 同意服務聲明並選擇驗證身分 ( 自然人憑證 )

教育學習

高級中等學校助學

伍、諮詢服務

若您對本平臺服務條款有任何疑問，歡迎您隨時與我們聯絡。

客服電話：(02)2192-7111， 客服信箱：[mydata@ndc.gov.tw](mailto:mydata@ndc.gov.tw)

☒ 我已了解此服務內容，並同意上述服務條款。

Step

1

資料下載及

國家發展委員

驗作業，期

本平臺前詳

壹、個人資

1. 本平

臺不

2. 本平

貳、個人資

2

身分驗證

申請人身分證字號\*英文字母為大寫

8004281XX1

生日\*請輸入西元年月日

請輸入生日8碼(例：19990101)

您可以選用下列其中一種方式驗證身分：



自然人憑證



健保卡



雙證件驗證

## STEP 3 進行登入、驗證

簽章中



載與身分驗證

同意數位服務個人化 ( MyData ) 平臺取得的個人資料集為：

入戶及中低收入戶證明

字號\* 英文字母為大寫

生日\* 請輸入西元年月日

您可以選用下列其中一種方式驗證身分：



自然人憑證



TW FidO



健保卡



雙證件驗證

請插入您的自然人憑證，並輸入PIN碼\*

\*\*\*\*\*

初次使用自然人憑證驗證嗎？

備妥晶片讀卡機及插卡輸入 PIN 碼就可以完成驗證，完整說明請參考 [常見問題](#) 或 [元件測試網頁](#)。

確認

## STEP 4 同意資料申請

4

提交申請

申請人資訊

姓名：胡\*林

身分證字號：— ■ ■ ■ ■ \*

已完成身分驗證。我願意將上述資料提供給「教育部國民及學前教育署」辦理「高級中等學校助學系統低收/中低收身份線上查驗」使用。

我本次同意數位服務個人化 ( MyData ) 平臺取得的個人資料集為：

1.低收入戶及中低收入戶證明



不同意

同意

## STEP 5 跳轉至資料頁面，實際以申請者身分資料為主



身分證字號	FO00000000	姓名	
學校名稱			
有效起訖			
身份別	衛服部系統查無低收或中低收身分		
系統查不到您的低收入戶或中低收入戶資料！請您向戶籍所在地之鄉/鎮/市/區公所確認申請人的低收/中低收身分申請，是否已經報經戶籍所在地的直轄市、縣(市)主管機關審通過，並於審核通過後24小時再次使用助學補助系統申請			
因資料有誤，不送出申請			

[回到助學系統MyData申請首頁](#)

[前往國發會MyData下載紙本證明](#)

# 民眾臨櫃檢驗 服務流程說明

# 民眾臨櫃檢驗

## STEP 1 使用者從 MyData 網站點擊“下載個人資料”



# 民眾臨櫃檢驗

## STEP 2 選擇資料類別

### 個人資料

我想一次下載多筆資料

從個人生活至醫療教育，提供全方位個人資訊



戶役政



勞保



地政



健保



財稅



醫療



社福



商工



金融



交通



教育



法務



其他





## STEP 3 選擇項目 (以個人戶籍資料查詢為例)

首頁 > MyData服務項目 > 戶役政

### 項目一覽

#### ◎ 個人戶籍資料查詢

資料提供單位：內政部戶政司 ^

##### 您可下載的資料內容

1. 個人記事
2. 出生地
3. 出生日期
4. 國民身分證統一編號
5. 姓名
6. 婚姻狀況
7. 戶籍地址
8. 教育程度
9. 遷入日期

我要下載 0

#### ◎ 現戶全戶戶籍資料

資料提供單位：內政部戶政司 ^

#### ◎ 親屬關係資料 (範圍為父母、配偶、子女) 查詢

資料提供單位：內政部戶政司 ^

## STEP 4 同意 MyData 服務條款，並選擇身分驗證

### 個人戶籍資料查詢

#### Step 資料下載及線上服務條款

1

國家發展委員會（以下簡稱本會），於本載、線上服務或臨櫃資料核驗作業，期望務之功能與內容，以及保障您個人之權益視為您已充分閱讀、瞭解並同意接受本服

#### 壹、個人資料下載及申辦服務內容

1. 本服務協助您取得的個人資料均由來源機關單位聯繫，本服務不負責
2. 本服務限您本人及您授權之申辦服務由您自行負責。
3. 使用本服務時，須填寫個人資料進款內容。

#### 貳、個人資料保護聲明

1. 目的：本服務經由驗證您的身分與服務或臨櫃資料核驗作業。
2. 資料類別：經由驗證您的身分與服務或臨櫃資料核驗作業所需之資料。
3. 其餘個人資料使用與保護政策，請

### 參、資料保管及使用

1. 當您使用本服務取得個人資料後請妥善保管，其下載資料後續的保管、使用方式及其所造成之影響，本服務不負任何保管、管理以及損害賠償責任。
2. 使用本服務所取得個人之資料，包含資料自行下載儲存或提供給第三方機關（構）進行線上服務作業，資料一旦經取用後，系統將立即刪除您的個人資料；若資料未下載儲存或提供予第三方使用，本服務將於八小時後自動刪除您的個人資料，若需重新取得檔案，需重新進行授權作業。

### 肆、服務條款修訂

1. 本服務有權於任何時間修改、變更本服務服務條款之內容，修改或變更時，本服務將進行公告，不再個別通知使用者，建議您定期查閱本服務服務條款。如依法或其他相關規定須為通知時，本服務得以張貼於本服務服務網頁、電子郵件或其他合理之方式通知您。
2. 如您於本服務服務條款修改或變更後仍續使用本服務服務，則視為您（暨您的監護人）已閱讀、瞭解與同意接受本服務服務條款修改或變更。若您不同意本服務服務條款之修改或變更，應立即停止使用。

### 伍、諮詢服務

若您對本服務服務條款有任何疑問，歡迎您隨時與我們聯絡。

客服電話：[\(02\)2192-7111](tel:0221927111)， 客服信箱：[mydata@ndc.gov.tw](mailto:mydata@ndc.gov.tw)

☒ 我已了解此服務內容，並同意上述服務條款。

# 民眾臨櫃檢驗

2

## 同意下載與身分驗證

我本次同意數位服務個人化 ( MyData ) 平臺取得的個人資料集為：

個人戶籍資料查詢

身分證字號\* 英文字母為大寫

A999999999

生日\* 請輸入西元年月日

19991231

您可以選用下列其中一種方式驗證身分：



自然人憑證



TW FidO

# 民眾臨櫃檢驗

## STEP 5 進行登入、驗證



The screenshot shows a web browser window with the address bar displaying "localhost:61161/pop..." and the URL "t.gov.tw/mydata-dev-beta-testing/personal/cate/1/list". The page content includes a green heading "以選用下列其中一種方式驗證身分：" (Select one of the following ways to verify your identity:). Below this are two buttons: "自然人憑證" (Natural Person Certificate) and "TW FidO". A text input field is labeled "插入您的自然人憑證，並輸入PIN碼\*" (Insert your Natural Person Certificate and enter PIN code\*). To the right of the input field is a link: "初次使用自然人憑證驗證嗎？備妥晶片讀卡機及插卡輸入 PIN 碼就可以完成驗證，完整說明請參考 [常見問題](#)或 [元件測試網頁](#)。" (First time using Natural Person Certificate for verification? Prepare a chip reader and insert the card to complete verification. For full instructions, please refer to [Common Questions](#) or [Component Test Webpage](#)). A green "確認" (Confirm) button is at the bottom right. A white overlay box on the left side of the browser window is titled "簽章中" (Signing) and contains a circular progress indicator with the text "請稍候" (Please wait). A green arrow points from the bottom of this overlay box down towards the bottom of the slide.

## STEP 6 驗證通過後選擇「前往資料條碼區」

3

取用資料

下載完成

100%

你可選擇下列方式使用已下載的資料檔案：開啟檔案的密碼是身分證字號（英文為大寫）

線上預覽檔案

轉存到我的電腦

前往資料條碼區

## STEP 7 取得條碼資料

### 資料條碼區

若您有下載個人資料，將於本區顯示 **資料集最長保存 8 小時**

### 個人資料



#### 個人戶籍資料

請將此條碼提供給業務申辦櫃臺人員，櫃臺人員可在您下載資料 8 小時內，使用此條碼取得下載的資料檔案。

補充：為提高資料安全性，此條碼有效時間尚餘 19 分鐘，之後將再產生新條碼。



kh6tups0



手動更新條碼

你可選擇下列方式使用已下載的資料檔案：開啟檔案的密碼是身分證字號（英文為大寫）

線上預覽檔案


轉存到我的電腦

# 民眾臨櫃檢驗

## STEP 8 查詢申辦過的條碼 (於畫面右上方條碼圖案)

...

網站地圖 我想要更多 常見問題 字級：中 我的個人專區

 MyData 數位服務個人化


關於 MyData MyData 服務項目 前往資料條碼區


... 首頁 > MyData服務項目 > 資料條碼區

### 資料條碼區

若您有下載個人資料，將於本區顯示，資料集最長保存 8 小時。

#### 個人資料


 個人戶籍資料

 戶政國民身分證影像

個人資料

個人戶籍資料

請將此條碼提供給業務申辦櫃臺人員，櫃臺人員可在您下載資料 8 小時內，使用此條碼取得下載的資料檔案。  
補充：為提高資料安全性，此條碼有效時間尚餘 14 分鐘，之後將再產生新條碼。





kh6tups0

您可選擇下列方式使用已下載的資料檔案：開啟檔案的密碼是身分證字號（英文為大寫）

線上預覽檔案

轉存到我的電腦

手動更新條碼



# 機關人員臨櫃檢驗 服務流程說明



# 機關人員臨櫃檢驗

**STEP 1** 進入機關人員臨櫃檢驗頁面，輸入「資料條碼」，並勾選「我不是機器人」項目

網站地圖 常見問題 我想要更多 字級：中 前往個人專區

MyData 數位服務個人化 關於MyData MyData服務項目

首頁 > 資料條碼取用資料

### 資料條碼取用資料

Step 1 輸入條碼

請輸入資料條碼：\*

☐ 我不是機器人

reCAPTCHA 隱私權 - 條款

下一步

reuuu3fd

# 機關人員臨櫃檢驗

**STEP 2** 系統將發送「驗證密碼」至民眾手機或電子郵件信箱，  
請民眾提供臨櫃人員

2

## 輸入驗證密碼

此驗證密碼將依照申請人指定之聯絡方式傳送，請申請人留意個人行動電話簡訊或電子信箱。

驗證密碼\*

請輸入驗證密碼

下一步

# 機關人員臨櫃檢驗

## STEP 3 驗證通過，資料取得

↓  
3

條碼取用

下載完成

100%

你可選擇下列方式使用已下載的資料：密碼是當事人的身分證字號（英文為大寫）

線上預覽檔案

轉存到我的電腦

# 請機關配合提供臨櫃檢驗事項

1. 法規調適(除個人證明文件之正本外，  
也可透過MyData臨櫃檢驗提供證明資料)
2. 機關人員的教育訓練
3. 民眾操作說明

# 後台服務流程說明

## STEP 1 MyData 根據機關單位提交申請資料建立「MyData 註冊管理後台使用權限帳號」，並以電話及電子郵件告知開通。

### 機關單位註冊

申請日期： 106/06/01

\* 機關單位名稱：

請選擇

\* 機關單位地址：

請輸入單位聯絡地址

\* 申請人姓名：

請輸入申請人之姓名(與E政府帳號同一人)

\* 聯絡電話：

請輸入申請人之聯絡電話號碼

\* 聯絡E-mail：

請輸入申請人之E-mail信箱

\* E政府帳號：

請輸入申請人之E帳府帳號

## STEP 2

機關單位使用申請之「E 政府公務帳號」登入「MyData 註冊管理後台」，開始使用相關功能。

網址：<https://mydata.nat.gov.tw/mydata-backend/signin>



MyData管理後台

帳號

密碼

請輸入驗證碼

arch 

登入後台

## STEP 3

登入管理後台後，請先前往機關單位管理中「企業組織基本資料」確認基本資料是否正確。

### 單位資訊

申請日期： 2018-03-02

單位名稱： 行政院內政部戶政司

單位地址： 臺北市徐州路5號6樓

\* 申請人姓名： 薛仁奇

\* 聯絡電話： 02-23976703

\* 聯絡E-mail： will.hsueh@udngroup.com.tw

\* E政府帳號： mydatatest

SP服務條款： 已同意，2018-03-22 15:09:35

DP服務條款： 已同意，2018-03-22 15:11:44

修改人員： mydatatest

修改時間： 2018-03-21 20:24:04



## STEP 4

請先前往「服務提供者管理 / 服務列表」功能，點擊新增服務，開始進行服務註冊。



## STEP 5

請依序填寫相關欄位內容，欄位填寫若有疑問，請洽 MyData 維運管理團隊，填寫完成後請點擊送審。

請審服務

建立日期： 2018-02-26

機關單位名稱： 國家發展委員會

申請人： 國發會管理帳號

聯絡電話： 02-21927111

聯絡E-mail： mydata@ndc.gov.tw

\* 服務類別： 請選擇

\* 服務名稱： 請輸入服務名稱(例如：e管家福利自己查)

\* 服務網址： 請輸入服務網址(例如：https://mydata.nat.gov.tw/)

\* 服務說明： 請輸入該服務簡單之說明文字 (一般民眾瀏覽使用)(例如：國發會e管家網站福利自己查資料授權)

\* client id： CLInOzeW23AVz

\* 上傳服務同意申請書： File not selected

\* 需求資料集： 請選擇資料提供單位

\* 服務跳轉網址： 請輸入服務跳轉網址(例如：https://mydata.nat.gov.tw/MyDataResult)

\* SP-API： 請輸入服務SP-API(例如：https://mydata.nat.gov.tw/SP-API)

\* 允許連線IP： 請輸入IP(機關/企業 要連線到MyData後台及SP-API) 增加輸入IP欄位

修改人員： juliehu

取消 送審

## STEP 6

送審之服務，經 MyData 管理團隊審核完成即上架至 MyData “所有服務列表”，表示服務提供者可開始提供服務。

MyData

機關單位管理

服務提供者管理

資料提供者管理

查詢列表

所有服務列表

所有資料集列表

申請日期

單位名稱

服務類別

服務名稱

狀態

2017-09-01

行政院國家發展委員會

社會福利/ 線上申請/ 生育津貼

桃園市生育津貼線上申辦

啟用

2017-09-01

行政院衛生福利部桃園醫院

醫療照護/ 健康管理/ 產前檢查

孕婦健康手冊

啟用

2017-09-01

行政院衛生福利部桃園醫院

醫療照護/ 健康管理/ 幼兒疫苗接種

兒童健康手冊

啟用

2018-03-07

行政院國家發展委員會

民生消費/ 財務管理

個人戶籍資料查詢

啟用

# 可運用資料集查詢

機關單位管理

服務提供者管理

資料提供者管理

審核

查詢列表

顯示所有  
資料集清單

☒ 所有服務列表

☒ 所有資料集列表

統計數據

系統管理

登出

顯示特定  
資料集內容

所有資料集列表

搜尋:

顯示 10 條

項次	resource_id	資料集名稱	SOCPE	需要的身分驗證安全等級	資料提供機關單位名稱	
1	tygh.resource.prenatal	產前檢查紀錄	tygh.resource.prenatal.read	自然人憑證	衛生福利部桃園醫院	<a href="#">查看資料集</a>
2	tygh.resource.vaccine	未滿7歲之子女疫苗注射紀錄	tygh.resource.vaccine.insert tygh.resource.vaccine.read tygh.resource.vaccine.update	自然人憑證	衛生福利部桃園醫院	<a href="#">查看資料集</a>
3	API.UbwT0oJLZ1	高級中等學校學生畢業資料	search	自然人憑證	教育部國民及學前教育署	<a href="#">查看資料集</a>
4	API.7QovE2Gev6	個人戶籍資料查詢	ris_review_one	自然人憑證	內政部戶政司	<a href="#">查看資料集</a>
5	API.fS9bsX4web	個人資料查驗	ris_check	自然人憑證	內政部戶政司	<a href="#">查看資料集</a>
6	API.wH2r0nBb3O	核發使用牌照稅繳納證明	etax.service.oldvabi001.owner	自然人憑證	財政部財政資訊中心	<a href="#">查看資料集</a>
7	API.KvyRZSc5K	地籍及實價資料	MoiLandReadMyData	自然人憑證	內政部地政司	<a href="#">查看資料集</a>

resource\_id : API.7QovE2Gev6

資料集名稱 : 個人戶籍資料查詢

下載 : [點擊下載](#)

提供方式 : 即時

需要的身分驗證安全等級 : 自然人憑證

資料提供者 : 內政部戶政司

資料集欄位 :

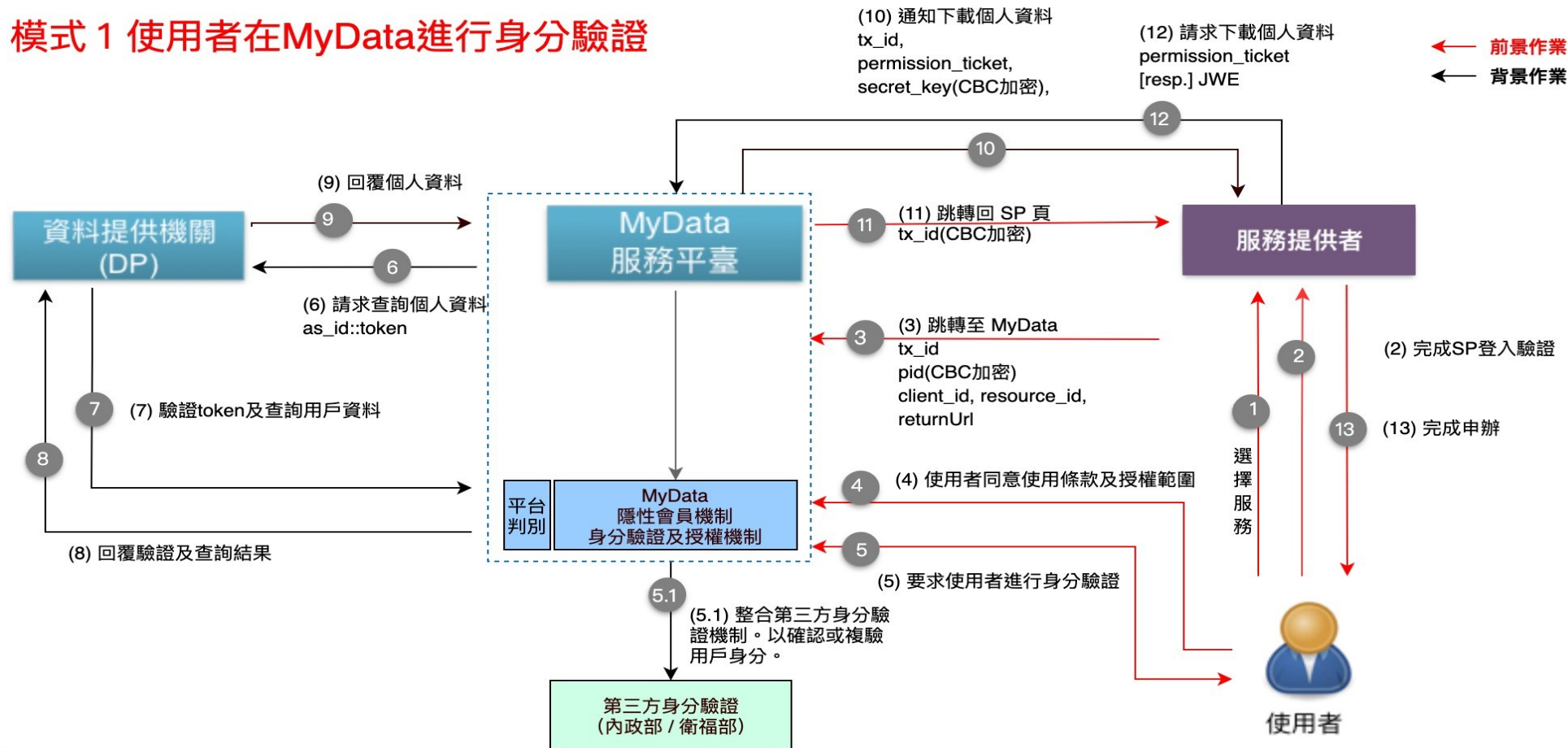
- 個人記事
- 出生地
- 出生日期
- 國民身分證統一編號
- 姓名
- 婚姻狀況
- 戶籍地址
- 教育程度
- 遷入日期

# 參、技術規範說明

## MyData整合網址及參數說明

# MyData 服務情境：線上申辦（模式 1）

## 模式 1 使用者在MyData進行身分驗證



# MyData 整合網址及參數說明

## 模式 1：使用者在 MyData 驗證自然人憑證

### 步驟 (3) SP 網站導向 MyData 整合網址時以 Path Parameter 帶入參數

整合網址：

GET /service/{client\_id}/{resource\_id\_base64encoded\_string}/{tx\_id}?

returnUrl={sp\_return\_url}&pid={personalId}

client\_id：SP 於 MyData 管理後台新增服務後所得的服務識別值。

resource\_id\_base64encoded\_string：Base64Encode( {resource\_id1}:{resource\_id2}:{resource\_id3} )

tx\_id：SP 核發的識別交易值。MyData 呼叫 SP 返回網址時會帶回給 SP。

sp\_return\_url：SP 的返回網址。

須以 UriEncode 編碼處理過。

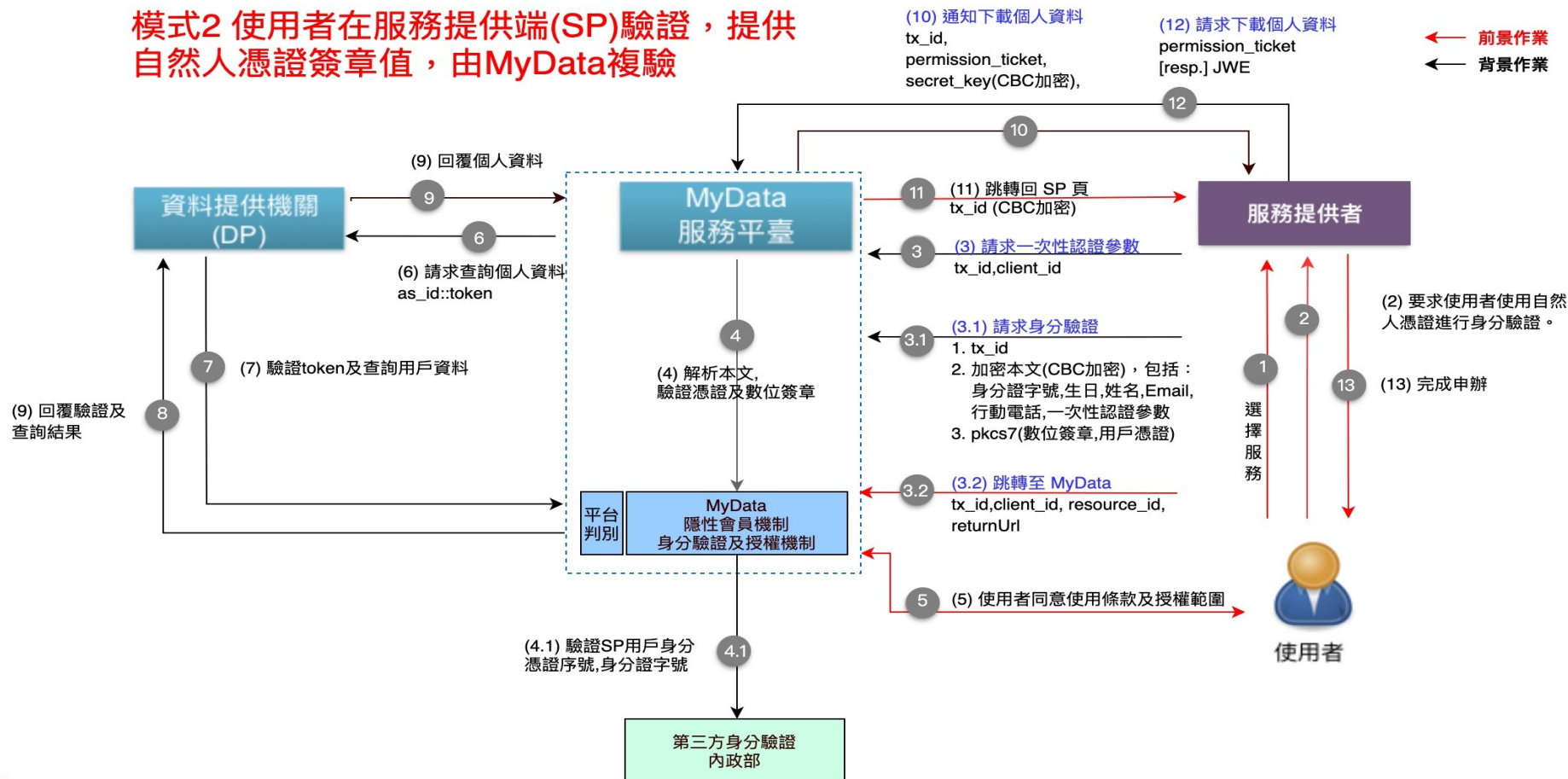
須符合 MyData 管理後台所登錄的返回網址。（只檢核 path url，不檢核 request parameter）

personalId：將用戶身分證字號以 AES/CBC/PKCS5PADDING 演算法進行加密。將 SP 的 client\_secret 合併 2 次為長度 256bit 的字串，當成是 AES 加密的金鑰。另外 CBC 加密向量值，請使用後台服務編輯頁「CBC IV」值為準。請輸入正確身分證字號。系統每次皆會檢核。



# MyData 服務情境：線上申辦（模式 2）

模式2 使用者在服務提供端(SP)驗證，提供自然人憑證簽章值，由MyData複驗



# MyData 整合網址及參數說明

模式 2：使用者在服務提供端 (SP) 驗證，提供自然人憑證簽章值，由 MyData 複驗

## 步驟 3 請求一次性認證參數

post /service/spsignature/{client\_id}

HTTP/1.1 TLS 1.2

Request body:

```
{  
  "tx_id": ${tx_id}  
}
```

Response body:

```
{  
  "tx_id": ${tx_id},  
  "salt": ${salt}  
}
```

salt：MyData 產生的一次性認證參數，有效期限 15 秒。

# MyData 整合網址及參數說明

模式 2：使用者在服務提供端 (SP) 驗證，提供自然人憑證簽章值，由 MyData 複驗

## 步驟 3.1 請求身分驗證

post /service/spsignature/{client\_id}  
HTTP/1.1 TLS 1.2

Request body:

```
{
  "tx_id": ${tx_id},
  "data": ${base64_encoded_aescbc-encrypted-data},
  "pkcs7": ${base64_encoded_pkcs7file-data}
}
```

**base64\_encoded\_pkcs7file-data：**  
PKCS7 檔案的 binary 以 Base64 編碼後的字串。

pkcs7 檔案中包含：

1. 以加密文本  
\${base64\_encoded\_aescbc-encrypted-data} 為對象  
所產製的數位簽章。簽章演算法使用 SHA256withRSA。
2. 自用戶自然人憑證卡讀出的憑證。

### 【說明】

**base64\_encoded\_aescbc-encrypted-data：**  
SP 用戶資料以 AES/CBC 加密後，再以 Base64 編碼後的字串。加密前的本文為 json。

用戶資料格式如下：

```
{
  "pid ": ${ 身分證字號 },
  "holder ": ${ 姓名 },
  "birthday" : ${ 生日，西元年月日 YYYY/MM/DD },
  "email" : ${ 電子郵件 },
  "mobile" : ${ 手機門號 },
  "salt ": ${salt}
}
```

上述欄位中，姓名、生日、電子郵件與手機門號為非必填，若無資料可直接省略該欄位。

# MyData 整合網址及參數說明

模式 2：使用者在服務提供端 (SP) 驗證，提供自然人憑證簽章值，由 MyData 複驗

## 步驟 3.2 跳轉至 MyData

GET/service/spsignature/{client\_id}/{resource\_id\_base64encoded\_string}/{tx\_id}?  
returnUrl={sp\_return\_url}  
HTTP/1.1 TLS 1.2

client\_id：SP 於 MyData 管理後台新增服務後所得的服務識別值。

resource\_id\_base64encoded\_string：Base64Encode( {resource\_id1}:{resource\_id2}:{resource\_id3} )

tx\_id：SP 核發的識別交易值。MyData 呼叫 SP 返回網址時會帶回給 SP。

sp\_return\_url：SP 的返回網址。

須以 UriEncode 編碼處理過。

須符合 MyData 管理後台所登錄的返回網址。（只檢核 path url，不檢核 request parameter）

# MyData 正常返回 SP 網址之處理方式說明

## 重導向回服務提供者網頁，帶回 tx\_id

GET {sp\_return\_url}?code={200}&tx\_id={aes-cbc\_encrypted\_txid}

HTTP/1.1 TLS 1.2

OR

GET {sp\_return\_url}?code={200}&tx\_id={aes-cbc\_encrypted\_txid}&{sp\_param\_key}={sp\_param\_value}

HTTP/1.1 TLS 1.2

code：HTTP 狀態碼。若為正常返回，固定為 200。

aes-cbc\_encrypted\_txid：

tx\_id 為 SP 產生的交易鍵值，格式為 version 4 UUID（36 字元，含 4 個 - 符號），MyData 以 AES/CBC/PKCS5PADDING 演算法進行加密，加密的金鑰為 client\_secret 合併 2 次為長度 256bit 字串。

加密向量值，請使用後台服務編輯頁「CBC IV」值為準。

{sp\_param\_key}={sp\_param\_value}：

用於示意表示 SP 原本附加的參數，MyData 將原值返回。



# MyData 異常返回 SP 網址之處理方式說明

## MyData 無法或拒絕處理，或發現參數檢核失敗時之異常狀況處理說明

GET {sp\_return\_url}?code={code}&tx\_id={aes-cbc\_encrypted\_txid}

HTTP/1.1 TLS 1.2

OR

GET {sp\_return\_url}?code={code}&tx\_id={aes-cbc\_encrypted\_txid}&{sp\_param\_key}={sp\_param\_value}

HTTP/1.1 TLS 1.2

205 : User 不同意傳送資料給 SP

400 : 無法順利解析 SP 帶入的 path parameter 。

401 : 權限錯誤。不允許此 IP 連線。未完成身分驗證或身分驗證失敗。無法順利解密或是驗簽章。

SP 所請求的 resource\_id 不屬於該服務的需求資料集。

403 : 拒絕存取。參數 ( tx\_id 或 client\_id ) 不存在。

404 : sp\_return\_url 不符合 MyData 管理後台中所登錄的設定。

408 : 交易逾時。

409 : 身分衝突。用戶身分證字號檢核失敗。 SP 傳送的 pid 與民眾於 MyData 填寫的身分證字號不符。

410 : SP-API 呼叫失敗。

501 : SP 請求的 DP 資料集之系統已停止服務。

504 : SP 請求的 DP 資料集之系統異常，無法傳送 DP 資料集。

# SP-API

# SP-API 請求及回覆規格說明

## MyData 呼叫 SP-API 傳遞 permission\_ticket 及 secret\_key 給 SP

MyData 發出請求， SP 處理請求。

POST /mydata-sp/notification

HTTP/1.1 TLS 1.2

Content-Type: application/json

```
{  
  tx_id: {uuid_v4_string},  
  permission_ticket: {uuid_v4_string},  
  secret_key: {base64encoded_256bit_secret_key_string}  
}
```

tx\_id：SP 核發的交易識別值。

permission\_ticket：MyData 核發，只有該次交易有效的交易識別碼，有效期最長超過 8 小時。

secret\_key：MyData 核發，只有該次交易有效的密鑰。

MyData 以 POST 觸發請求，並將傳遞內容以 JSON 格式置於 RequestBody。

SP-API Endpoint URI 可由 SP 自行決定，MyData 只規範傳遞的方式及內容格式。



# SP-API 請求及回覆規格說明

## MyData 呼叫 SP-API，告知 SP 無法給予資料檔

MyData 發出請求，SP 處理請求。

POST /mydata-sp/notification

HTTP/1.1 TLS 1.2

Content-Type: application/json

```
{  
  tx_id: {uuid_v4_string},  
  permission_ticket: {uuid_v4_string},  
  unable_to_deliver: [  
    {resource_id1},{resource_id2}  ]  
}
```

**unable\_to\_deliver**：MyData 已確認無法傳遞的資料集。以下情況，MyData 無法順利傳遞 DP 資料集檔案予 SP：

1. MyData 向 DP 發出請求成功後，等候逾時仍無法取得資料檔案。
2. MyData 向 DP 發出請求連線逾時。

### SP 回覆請求成功

HTTP/1.1 200 OK

Content-Type: application/json

### SP 回覆請求失敗

HTTP/1.1 403 Forbidden

Content-Type: application/json

SP 以 HTTP 狀態碼來表示回覆請求失敗的狀況



# MyData-API

# MyData-API 請求及回覆規格說明

SP 呼叫 MyData-API 以取得用戶的個人資料

SP 發出請求， MyData 處理請求。

正式環境：

GET /service/data

HTTP/1.1 TLS 1.2

Content-Type: application/json

permission\_ticket: {permission\_ticket}

permission\_ticket : MyData 核發，用於識別該次交易的交易識別碼。

SP 將 permission\_ticket 置於 HTTP Header，以 GET 觸發請求。

( 轉下頁 )

# MyData-API 請求及回覆規格說明

( 接上頁 )

## MyData 回覆請求成功 - 即時回應

HTTP/1.1 TLS 1.2 200 OK

Content-Type: application/jwt

回傳內容格式為 JWT (JSON Web Token) 。

## MyData 回覆請求成功 - 等待處理

HTTP/1.1 TLS 1.2 429 Too Many Requests

Content-Type: application/jwt

Retry-After: {delay\_seconds}

delay\_seconds : SP 再次發動請求前，須等待的時間 (seconds) 。

考量 SP 系統整合的彈性，原則上若 DP 告知 MyData 須等待，MyData 也告知 SP 須等待。

## MyData 回覆請求失敗

HTTP/1.1 TLS 1.2 403 Forbidden

Content-Type: application/json

401：未完成身分驗證或身分驗證失敗。

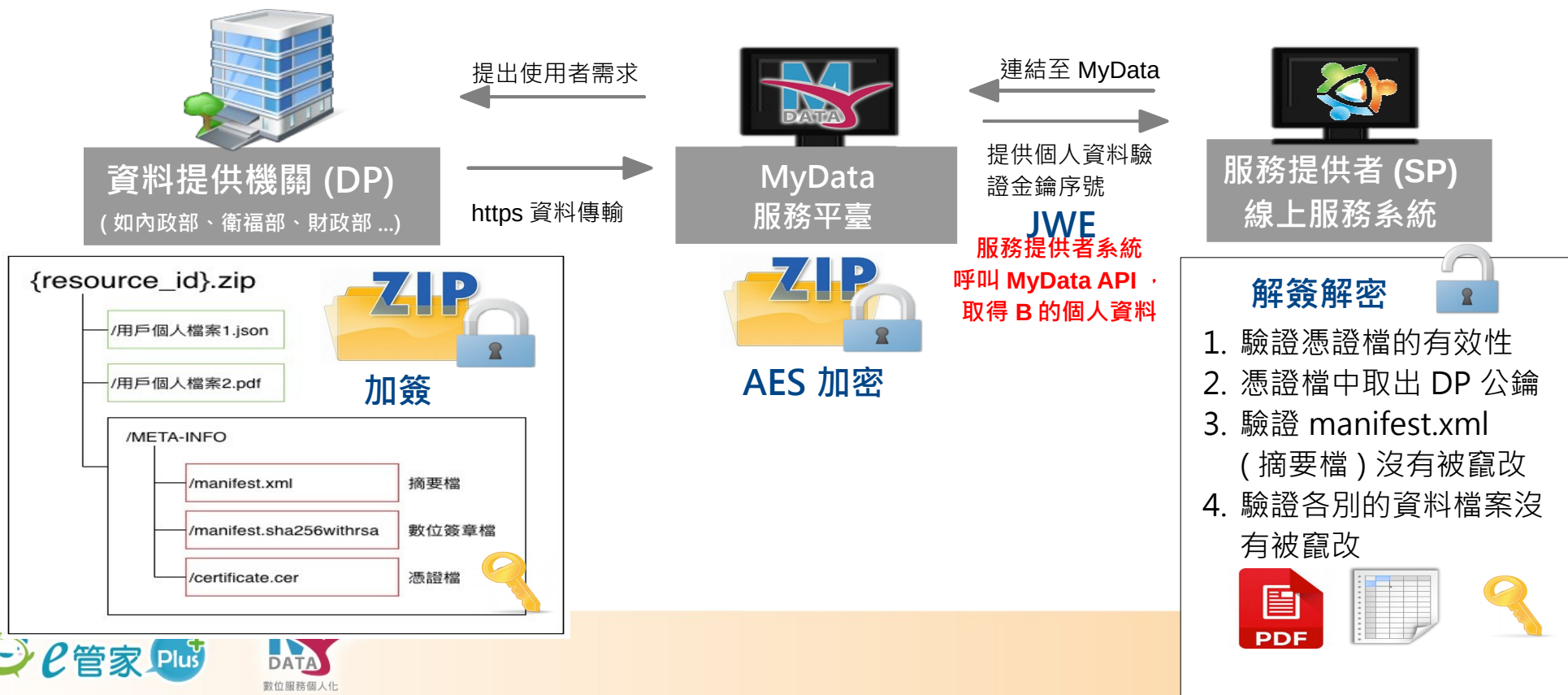
403：拒絕存取。若請求來源 IP 不合法，也會回應此狀態。

504：無法傳送 DP 個人資料檔案。



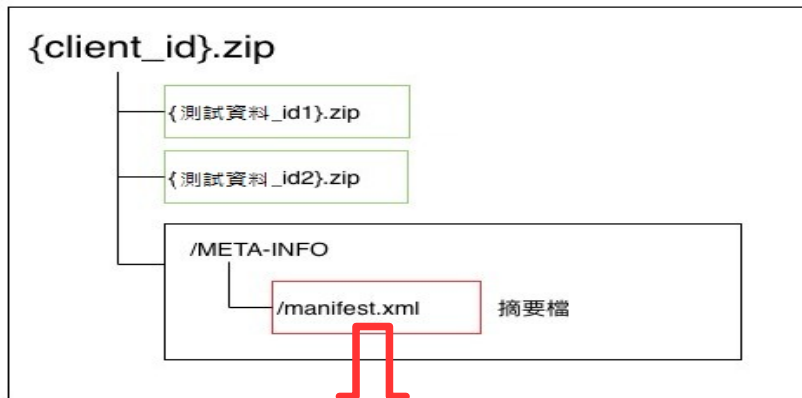
# 資料傳輸過程

## 安全的資料傳輸過程：資料加簽與加密

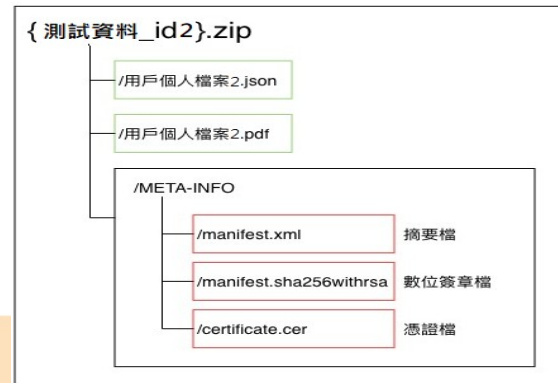
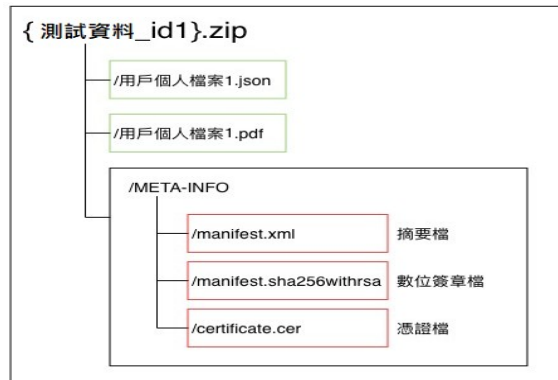


# 測試資料檔案結構

- MyData 個人資料測試檔，內含 2 個 DP 個人資料檔：  
/META-INFO/manifest.xml 描述各別個人資料檔的摘要值。  
/META-INFO/manifest.sha256withrsa SHA256withRSA 數位簽章檔。對象 manifest.xml  
/META-INFO/certificate.cer DP 申請的合法簽章憑證。 PEM 格式。



```
<?xml version="1.0" encoding="UTF-8"?>
<files>
  <file>
    <filename>{ 測試資料_id1}.zip</filename>
    <resource_id>{resource_id}</resource_id>
    <resource_name> 測試資料集名稱 1</resource_name>
    <code>204</code>
  </file>
  <file>
    <filename>{ 測試資料_id2}.zip</filename>
    <resource_id>{resource_id}</resource_id>
    <resource_name> 測試資料集名稱 2</resource_name>
    <code>204</code>
  </file>
</files>
```



# MyData資料結構與驗簽

JWE 資訊以 . 符號串接組合為一個字符串 => header.encrypted\_key.initialization\_vector.ciphertext.authentication\_tag

eyJhbGciOiJBbmJU2S1ciLCJlbmMiOiJBbmJU2Q0JDLUhTNTExIn0

1-mJQI42l08E3mz6Zac4OIhSNDXxz7g6DoAmJgayHmEVIUIiNhLMYS5kjWAKPI7LrsFZ0pmdFVqfC77688Mdfni0Xgu4PST

SHR6R1k3ZzFoTHk1Ymw5Ug

LMz7XIhl2p6FPQwXfHAhb0yZ7YjgiPsLXzR6J96Lxzc-z0G3dR5P5\_MB\_NBQmumD7exefh2GpXjCwwki277CD5htL7XzJodZLIqOwp1Ymhg

C7iWNo6BVCpamm3KlpuPxJYgCkcCh1QcTc8BzDKD3Sw

### (1) header

載明使用的演算法。 MyData 指定使用 A256KW 及 A256CBC-HS512 。

編碼前的 header 示意

```
{  
  "alg": "A256KW"  
  "enc": "A256CBC-HS512"  
}
```

### (1) header

載明使用的演算法。 MyData 指定使用 A256KW 及 A256CBC-HS512。

編碼前的 header 示意

```
{  
  "alg": "A256KW"  
  "enc": "A256CBC-HS512"  
}
```

### (1) header

載明使用的演算法。 MyData 指定使用 A256KW 及 A256CBC-HS512。

編碼前的 header 示意

```
{  
  "alg": "A256KW"  
  "enc": "A256CBC-HS512"  
}
```

(2) encrypted\_key

encrypted\_key 為以 A256KW 演算法封裝後的 CEK (Content Encryption Key)。

由於 MyData 指定使用 A256CBC-HS512 做為內容加密演算法，所以 CEK 的長度為 64 bytes (512bits)，CEK 中前 256bit 為 MAC key，後 256bits 為 AES key。

(2) encrypted\_key

encrypted\_key 為以 A256KW 演算法封裝後的 CEK (Content Encryption Key)。

由於 MyData 指定使用 A256CBC-HS512 做為內容加密演算法，所以 CEK 的長度為 64 bytes (512bits)，CEK 中前 256bit 為 MAC key，後 256bits 為 AES key。

(2) encrypted\_key

encrypted\_key 為以 A256KW 演算法封裝後的 CEK (Content Encryption Key)。

由於 MyData 指定使用 A256CBC-HS512 做為內容加密演算法，所以 CEK 的長度為 64 bytes (512bits)，CEK 中前 256bit 為 MAC key，後 256bits 為 AES key。



# MyData-API, JWE 內容說明

JWE 資訊以 . 符號串接組合為一個字符串 => `header.encrypted_key.initialization_vector.ciphertext.authentication_tag`

`eyJhbGciOiJBbmJU2S1ciLCJlbmMiOiJBbmJU2Q0JDLUhtNT`

`1-mJQI42l08E3mz6Zac4OIHsNDXxz7g6DoAmJqayHm`

`SHR6R1k3ZzFoTHk1Ymw5Ug`

`LMz7XIhl2p6FPQwXfHAhb0yZ7YjgPsLXzR6J96Lxzc-z0G3dR5P5_MB_NBQmumD7exefh2GpXjCvwkI277CD5htL7XzJodZLIqOwp1Ymhg`

`C7iWNo6BVCpamm3KlpuPxJYgCkcCh1QcTc8BzDKD3Sw`

## (3) initialization\_vector, IV

IV 為 AESCBC 運算所需的初始向量值。  
以 Base64Url decode 處理後即可取得。  
SP 系統應檢核此處所得 IV 值，是否與  
MyData 管理後台中取得的 IV 值相同，  
必需要相同才是正確的。

## (4) ciphertext

ciphertext 為加密後的內容。SP 進行內容解密之前  
應先利用 authentication tag 值來檢算正確性，以  
確保此 JWE 沒有被篡改。

AES\_CBC 加密前的內容，示意範例如下：

```
{  
  "filename": "abc.zip",  
  "data":  
    "application/zip;data:XsdfasCSFDSADFASVcxv"  
}
```

(5) authentication\_tag  
authentication tag 依  
規範有特定的生成方  
式，利用該值可用來檢  
算 JWE 的正確性。

# 解密 encrypted\_key 說明

SP 需使用 MyData 核發的 secret\_key 為金鑰以 A256KW 演算法 ( AESWrap ) 來解封裝 (unwrap) JWE 中的 encrypted\_key , 進而得到另一把隨機產生的、用於內容加密的金鑰 (CEK) , 該內容加密演算法使用 A256CBC-HS512 , 所以這把隨機產生的內容金鑰 (CEK) 長度為 512bits , 其中前 256bits 為 MAC key, 後 256bits 為 AES key 。

java 程式範例如下：

```
Cipher cipher = Cipher.getInstance( "AESWrap" );
cipher.init(Cipher.UNWRAP_MODE, kek);
SecretKey cek = (SecretKey) cipher.unwrap(
    base64UrlDecodedEncryptedCEK,
    "AES" ,
    Cipher.SECRET_KEY);
```

# 檢算 JWE 說明

利用 authentication tag 來檢算 JWE 正確性的做法如下：

1. 依 JWE 規範，重新計算 authentication tag 值。
2. 比較重製後的 tag 值，與自 JWE 中解析出的 authentication tag 值，兩者是否完全相同，完全相同才是正確的。

[ 補充資料 ]JWE Library

由於 JWE 規格複雜，jwt.io 網站提供各種程式語言適用的 Library 供參考。

<https://jwt.io/#libraries-io>

# 解密 ciphertext 說明

SP 解密 ciphertext 前必需先完成取得 CEK，使用 CEK 中 AES key 及 IV 值，才能順利以 AES\_CBC 演算法進行解密。

java 程式範例如下：

```
IvParameterSpec iv = new IvParameterSpec(base64UrlDecodedIV);  
Cipher cipher = Cipher.getInstance( "AES/CBC/PKCS5PADDING" );  
cipher.init(Cipher.DECRYPT_MODE, encKey, iv);  
byte[] result = cipher.doFinal(base64UrlDecodedCiphertext);
```

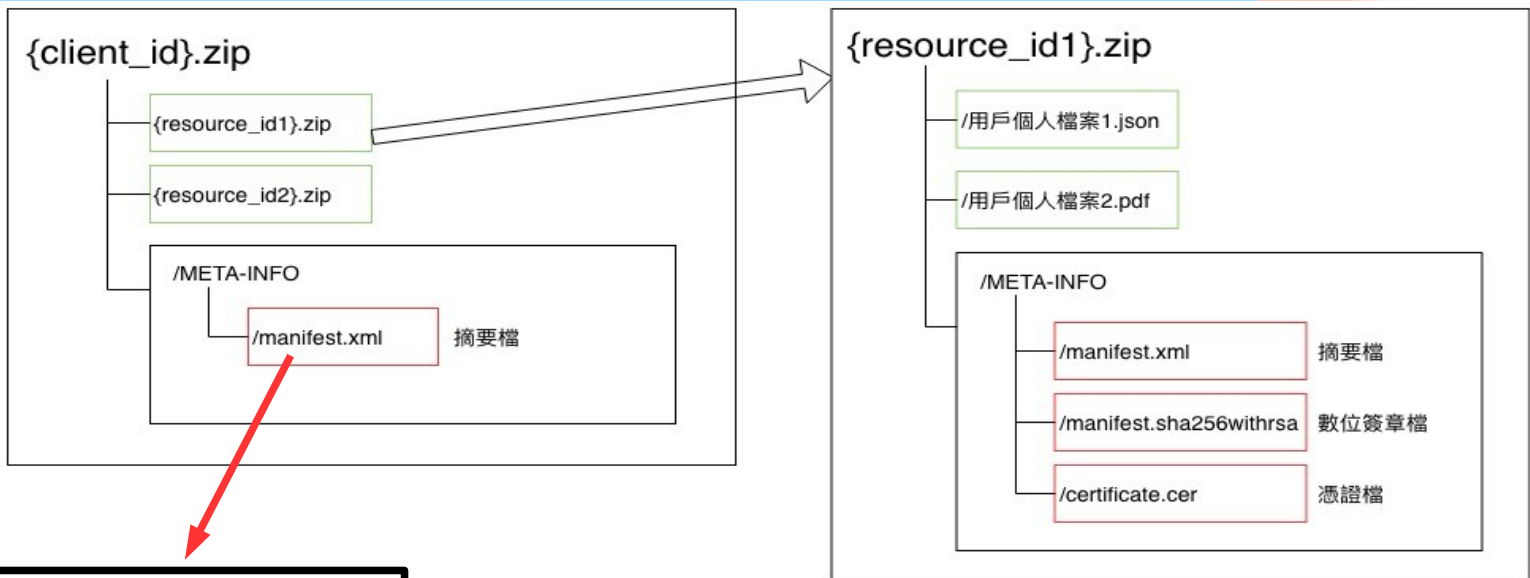
內容解密成功後，可得到一個 JSON 格式的資料內容，欄位說明如下：

欄位	說明
filename	代表打包檔的檔案名稱，目前一律是壓縮 zip 檔，檔案名稱為 {client_id}.zip，client_id 為變數代表該服務項目的識別值。
data	代表 MyData 資料打包檔以 Base64UrlEncode 編碼後的內容。其中 application/zip;data: 是前置碼，與資料內容無關，只是在說明 Base64UrlDecoder 解碼後的檔案格式為何。

SP 將上述 data 欄位值進行 Base64UrlDecoder 解碼處理後將 binary 儲存為 filename 中所述的檔案名稱即完成檔案保存。

# MyData 資料打包檔結構說明

MyData 個人資料打包檔，  
檔案結構示意：

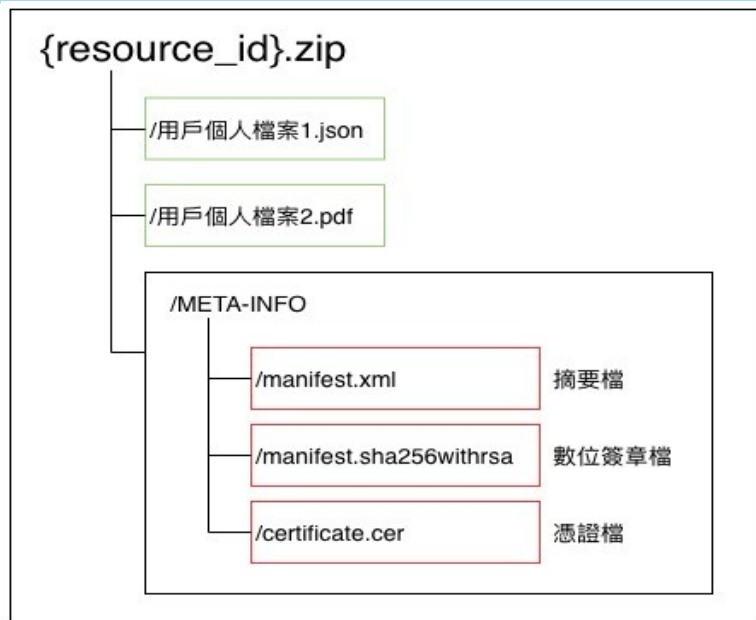


```
<?xml version=" 1.0" encoding=" UTF-8" >  
<files>  
  <file>  
    <filename>{resource_id1}.zip</filename>  
    <resource_id>{resource_id}</resource_id>  
    <resource_name> 資料集中文名稱 </resource_name>  
    <code>204</code>  
  </file>  
</files>
```

參數	說明
code	檔案處理狀態， 200：正常 204：查無使用者資料（封裝內無檔案）

# DP 資料打包檔結構說明

DP 個人資料打包檔，  
檔案結構示意：



DP 個人資料打包檔，內含多個 **DP 個人資料檔**。

`/META-INFO/manifest.xml` 描述各別個人資料檔的摘要值。

`/META-INFO/manifest.sha256withrsa` SHA256withRSA 數位簽章檔。對象 `manifest.xml`

`/META-INFO/certificate.cer` DP 申請的合法簽章憑證。 **PEM** 格式。

# SP 驗證 DP 個人資料檔是否被竄改

## 1. 驗證憑證檔的有效性

1. GCA 支援 CRL, OCSP 兩種驗證方式。

## 2. 憑證檔中取出 DP 公鑰

1. DP 憑證檔為 PEM 格式。

2. 從 DP 憑證檔中取出 DP 公鑰。

## 3. 驗證 manifest.xml 沒有被竄改

1. manifest.sha256withrsa：對 manifest.xml 以 SHA256withRSA 演算後獲得。

2. SP 以 DP 公鑰，對 manifest.sha256withrsa 解密，得到正確的摘要值。

3. SP 以 SHA256 演算 manifest.xml 後，比對前後兩者是否相符。

## 4. 驗證各別的資料檔案沒有被竄改

1. 若 manifest.xml 沒有被竄改，代表 manifest.xml 所載明的各檔案摘要值也沒有被竄改。

2. SP 讀取 manifest.xml 獲得正確的摘要值。

3. SP 對各別資料檔案以 SHA256 演算，比對前後兩者是否相符。

# SP 解析 DP 個人資料檔內容

DP 個人資料檔格式，目前只規範 DP 至少須提供一種機器可讀的格式（如：JSON），以及一種人易讀的格式（如：PDF，其中，PDF 以申請人之身分證字號作為檔案開啟密碼）。

DP 個人資料檔內容的解析規則，目前依 DP 自行定義。



# 資料查核相關網頁與API

# 第三方身分驗證中心日誌查詢

流程：民眾→ SP 服務網頁→透過第三方身分驗證→ 由 SP 服務頁提供查看「授權紀錄」的按鈕，民眾點擊按鈕即可前往 MyData 網站調閱紀錄。

網址路徑：

GET /service/{client\_id}/log?as\_id={as\_id}&token={token}

HTTP/1.1 TLS 1.2

參數	說明
client_id	SP 於 MyData 管理後台新增服務後所得的 client 識別值。
as_id	第三方身分驗證中心
token	第三方身分驗證中心核發的 access_token 將 SP 的 client_secret 合併 2 次為長度 256bit 的字串，當成是 AES 加密的金鑰。 將 access_token 以 AES/CBC/PKCS5PADDING 演算法進行加密。另外 CBC 加密向量值，請使用後台服務編輯頁「CBC IV」值為準。

# Type-Valid

提供 SP 查詢服務申請者於 MyData 所使用之身分驗證方式。

## (一) 發出請求

網址路徑：

GET /service/type\_valid

HTTP/1.1 TLS 1.2

Content-Type: application/json

permission\_ticket: {permission\_ticket}

## (二) 驗證憑證檔的有效性

HTTP/1.1 TLS 1.2 200 OK

Content-Type: application/json

body:

{"verification": "{verification}"}

## (三) 失敗回應

HTTP 狀態碼	說明
401	不允許此 IP 連線。
403	拒絕存取、格式錯誤或該 permission_ticket 無效。

參數	說明
verification	CER：自然人憑證 FIC：晶片金融卡 FCH：硬體金融憑證 MOE：工商憑證 TFD：TW FidO 驗證 OTP：一次性密碼 NHI：健保卡 FCS：軟體金融憑證 PII：多因子 GOV：E 政府帳號



# Txid-Status

提供 SP 狀態查詢服務，查驗根據發出的「 tx\_id 」，查驗該筆交易處理的狀態。

(一) 發出請求

網址路徑：

GET /service/txid\_status

HTTP/1.1 TLS 1.2

Content-Type: application/json

tx\_id: {tx\_id}

(二) 驗證交易處理狀態

HTTP/1.1 TLS 1.2 200 OK

Content-Type: application/json

body:

{"code": "{code}", "text": "{text}"}

(三) 失敗回應

HTTP/1.1 TLS 1.2 403 Forbidden

Content-Type: application/json



## 交易狀態

201 : SP 已取用資料。

205 : User 不同意傳送資料給 SP 。

403 : 參數 ( tx\_id ) 不存在。部分資料集下載失敗  
[API.xxxxxxx] 。

404 : 無效的路徑。

408 : 交易逾時或交易未完成。

409 : 身分衝突。用戶身分證字號檢核失敗。

410 : SP-API 呼叫失敗。

501 : SP 請求的 DP 資料集之系統已停止服務。

504 : SP 請求的 DP 資料集之系統異常，無法傳送 DP 資料集。

## 失敗回應

400 : 參數格式或內容不正確，或是缺少必要參數。

401 : 權限錯誤。不允許此 IP 連線。

403 : 拒絕存取。

# 交易 Log 日誌查詢 (1/3)

提供 SP 狀態查詢服務，查驗根據發出的「tx\_id」，查驗該筆交易處理的狀態。

建立 DP、MyData、SP 之間的交易勾稽機制。

說明如下：

1. 各角色勾稽必要參數說明如下：

DP：transaction\_id, resource\_id, 交易事件代碼，日誌產生時間，請求來源 IP。

MyData：transaction\_id, client\_id, resource\_id, tx\_id, 交易事件代碼，身分證字號 / 統一編號，日誌產生時間，請求來源 IP。

SP：client\_id, resource\_id, tx\_id, 交易事件代碼，身分證字號 / 統一編號，日誌產生時間，請求來源 IP。

2. 交易日誌產生時機，如技術文件之說明。

# 交易 Log 日誌查詢 (2/3)

POST /log/sp  
HTTP/1.1 TLS 1.2  
Content-Type: application/json  
**requestBody:**

```
{  
  "client_id": "CLI.xxxxxxxx",  
  "stime": "yyyy-mm-dd",  
  "etime": "yyyy-mm-dd",  
  "tx_id": [ "", "" ],  
  "event": [ "", "" ],  
}
```

**responseBody:**

```
{  
  "client_id": "CLI.xxxxxxxx",  
  "data" : [  
    {  
      "tx_id": "",  
      "ctime": "yyyy-MM-dd hh24:MI:SS",  
      "event": "",  
      "ip": "",  
      "resource_id": [ "", "" ]  
    }  
  ]  
}
```

參數	說明
client_id	SP 於 MyData 管理後台新增服務後所得的 client 識別值。
stime	查詢起始時間。以 tx_id 的產生時間為依據。
etime	查詢結束時間。以 tx_id 的產生時間為依據。
ctime	交易日誌產生時間。
tx_id	SP 核發的交易識別值。非必填。 第二層過濾條件，查詢結果會滿足 stime, etime, tx_id 的條件交集結果。
event	事件代碼。非必填。 第三層過濾條件，查詢結果會滿足 stime, etime, tx_id, event 的條件交集結果。
ip	該事件的請求來源 IP。
resource_id	資料集鍵值。

# 交易 Log 日誌查詢 (3/3)

失敗回應

HTTP/1.1 TLS 1.2 403 Forbidden  
Content-Type: application/json

400 : 參數格式或內容不正確，或是缺少必要參數。

401 : 權限錯誤。不允許此 IP 連線。

403 : 參數 ( tx\_id, client\_id ) 不存在。

# 範例程式

提供完整 JAVA 範例程式如連結：

<https://github.com/ehousekeeper/emsg/blob/master/MyData%E7%AF%84%E4%BE%8B%E7%A8%8B%E5%BC%8F/sp-example.2.1.zip>



# 系統環境主機及網址資訊

# 系統環境主機及網址資訊 (正式機)

項目	IP 或網址
正式機負載平衡 IP	117.56.91.59
正式機 AP1 IP	117.56.91.72
正式機 AP2 IP	117.56.91.73
正式機 AP3 IP	117.56.91.245
正式機 MyData-API 網址	<a href="https://mydata.nat.gov.tw/service/data">https://mydata.nat.gov.tw/service/data</a>
正式機後臺登入網址	<a href="https://mydata.nat.gov.tw/mydata-backend">https://mydata.nat.gov.tw/mydata-backend</a>
正式機前臺首頁網址	<a href="https://mydata.nat.gov.tw">https://mydata.nat.gov.tw</a>

# 系統環境主機及網址資訊 (正式機)

項目	IP 或網址
正式機負載平衡 IP	117.56.91.59
正式機 AP1 IP	117.56.91.72
正式機 AP2 IP	117.56.91.73
正式機 AP3 IP	117.56.91.245
正式機 MyData-API 網址	<a href="https://mydata.nat.gov.tw/service/data">https://mydata.nat.gov.tw/service/data</a>
正式機後臺登入網址	<a href="https://mydata.nat.gov.tw/mydata-backend">https://mydata.nat.gov.tw/mydata-backend</a>
正式機前臺首頁網址	<a href="https://mydata.nat.gov.tw">https://mydata.nat.gov.tw</a>

# 系統環境主機及網址資訊 ( 測試機 )

項目	IP 或網址
測試機 IP	117.56.91.143
測試機 MyData-API 網址	<a href="https://mydatadev.nat.gov.tw/mydata/service/data">https://mydatadev.nat.gov.tw/mydata/service/data</a>
測試機後臺登入網址	<a href="https://mydatadev.nat.gov.tw/mydata-backend">https://mydatadev.nat.gov.tw/mydata-backend</a>
測試機前臺首頁網址	<a href="https://mydatadev.nat.gov.tw/mydata">https://mydatadev.nat.gov.tw/mydata</a>

# 參考附件

# MyData 使用者身分認證安全等級規劃

授權取用 資料集 最低安全 等級	安全 等級	安全等級對應之身分驗證方式
	1	自然人憑證、晶片金融卡、硬體金融憑證
	2	臺灣行動身分識別(T-FidO)、一次性密碼(OTP), 須使用 自然人憑證綁定
	3	健保卡、軟體金融憑證
	4	多因子驗證(健保卡號+戶號或健保卡號+身分證換補證日期)
	請填寫最低安全等級：第 ____ 等級 *安全等級由1到4遞減，等級1最高，例如選擇3，即表示1、2、3皆可驗證。 <input type="checkbox"/> 工商憑證 *若本資料集可提供給公司行號或法人服務使用，再行勾選	

加入 TW FidO(台灣行動身分識別)、晶片金融卡、硬體金融憑證、軟體金融憑證等身分驗證方式。

