

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
 - 線上申辦
 - 臨櫃檢驗
- 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
- 交易 Log 日誌查詢 API
- 範例程式

壹、服務提供者申請流程

服務介接申請流程說明

1 申請人至 **MyData** 平臺(<https://mydata.nat.gov.tw>)->最新消息->介接試辦要點，下載與填寫申請表，並經**MyData**團隊確認內容
(為避免資料填寫不正確或不齊，請先電話或**E-mail**聯繫**MyData**團隊)

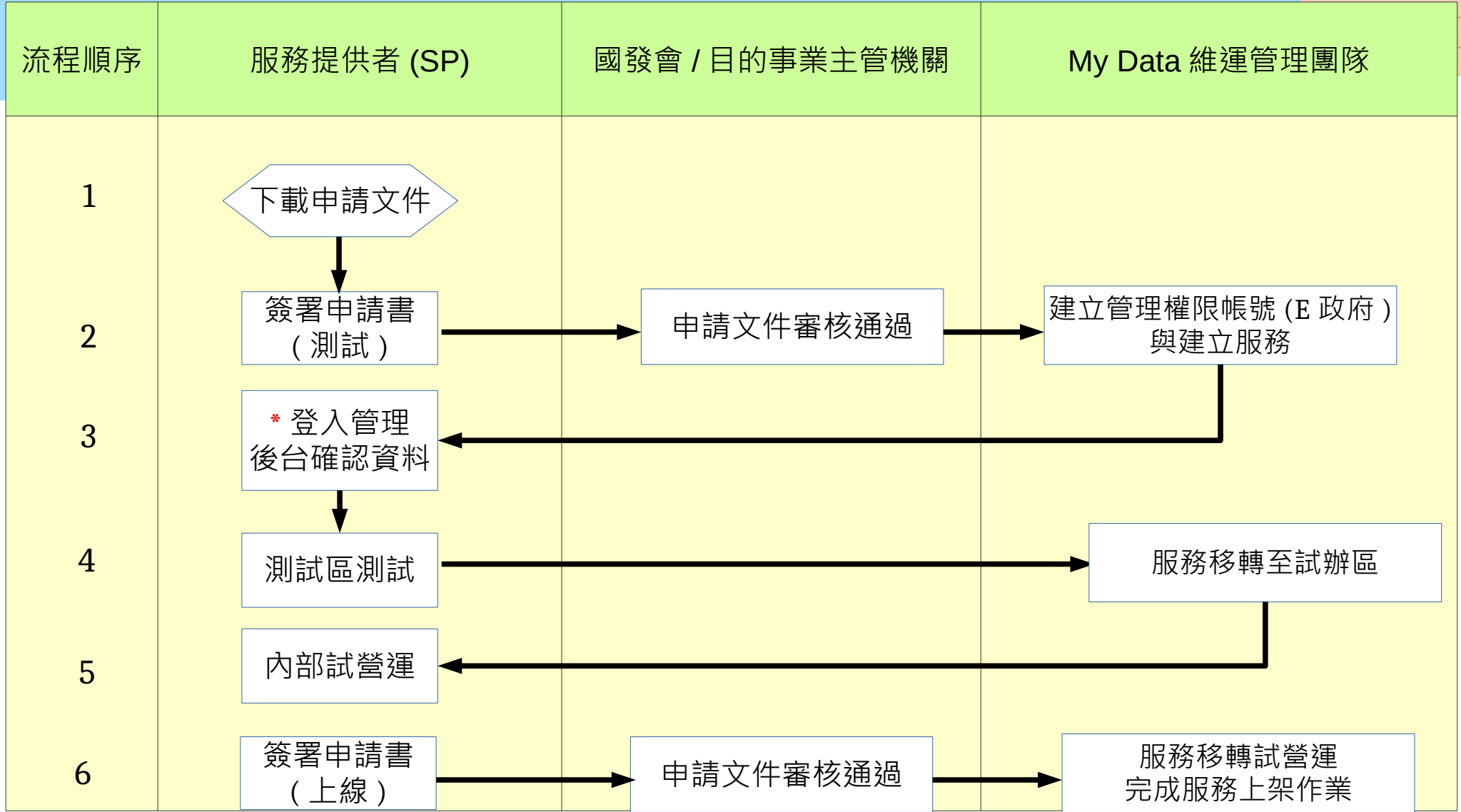
2

- 公務機關：填具申請表並函送本會
- 非公務機關：填具申請表及用印後，函送目的事業主管機關，由目的事業主管機關同意後函送本會

3 **MyData**團隊依申請表建立申請人權限及服務內容

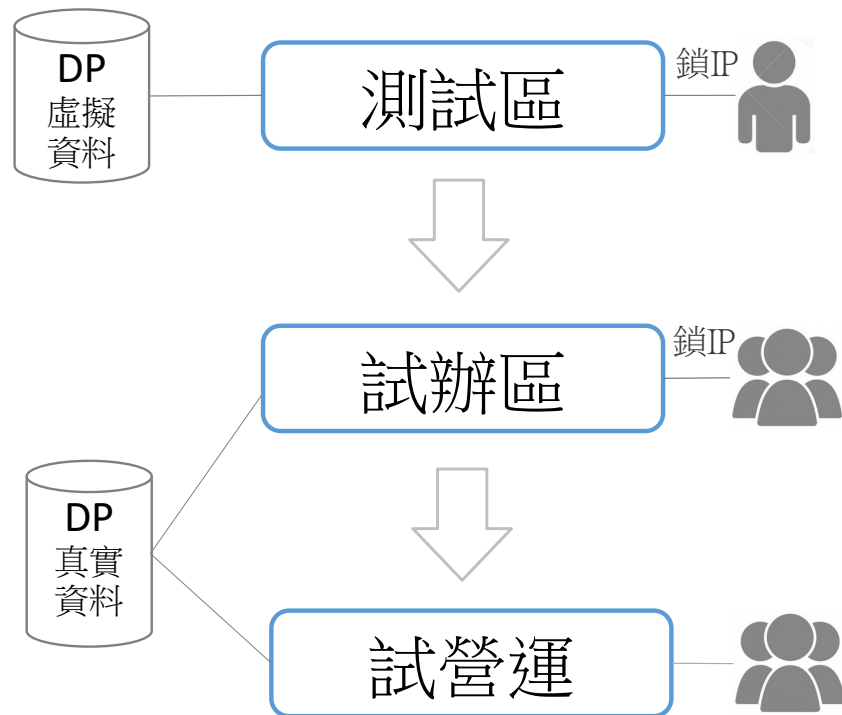
4 申請人使用帳號登入後台並確認服務內容

5 申請人開始進行服務提供者 (SP) 測試作業



服務介接申請流程說明 (2/2)

MyData 平臺



服務提供者

- 1.開發API程式
- 2.介接測試環境之虛擬資料
- 3.測試正常後API調整連結至試辦環境
(MyData鎖定SP連線網址)

-
- 1.介接試辦環境之真實資料
 - 2.辦理內部人員測試(MyData鎖定SP連線網址)
 - 3.試辦正常後API調整連結至試營運環境

-
- 1.介接試營運環境之真實資料
 - 2.提供對外民眾連線



登入管理後台確認資料

STEP 1 MyData 根據機關單位提交申請服務建立「MyData 管理後台使用權限帳號」及「服務內容」，並以電話或電子郵件告知開通。

機關單位註冊

申請日期：	106/06/01
* 機關單位名稱：	<input type="text" value="請選擇"/>
* 機關單位地址：	<input type="text" value="請輸入單位聯絡地址"/>
* 申請人姓名：	<input type="text" value="請輸入申請人之姓名(與E政府帳號同一人)"/>
* 聯絡電話：	<input type="text" value="請輸入申請人之聯絡電話號碼"/>
* 聯絡E-mail：	<input type="text" value="請輸入申請人之E-mail信箱"/>
* E政府帳號：	<input type="text" value="請輸入申請人之E帳府帳號"/>

STEP 2

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



MyData管理後台

測試區

.....

.....

登入後台

STEP 3

登入管理後台後，請先前往「帳號管理」，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 請至「服務提供者管理 / 服務列表」確認內容是否皆與申請單相同，若有不同，請與團隊聯絡進行修正作業。

編輯服務 ×

建立日期：

2018-08-01

機關(構)名稱：

國家發展委員會

承辦人姓名：

國發會管理帳號

承辦人電話：

承辦人電子郵件：

* 服務類別：

醫療照護

* 服務名稱：

e管家福利自己查

* 前端服務網址：

https://mydatadev.nat.gov.tw/emsgFrontend/welfare.jsp

* 服務目的與內容：

國發會福利自己查資料授權

* client id：

CLI.U9D4i8pmZ5

* client secret：

LQoJEvgdKug20RX3

* cbc iv：

fAzYPMzeeVC7Ln3Y

* 上傳服務同意申請書：

File not selected

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 我的個人專區 登出

MyData 數位服務個人化 試營運

關於 MyData 最新消息 資料下載 線上服務   

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

社會福利 

- ◎ 嘉義縣 - 急難救助(原馬上關懷服務) 
- ◎ 嘉義縣 - 敬老卡或愛心卡 
- ◎ 嘉義縣 - 身心障礙者及老人預防走失溫馨手鍊或項鍊 
- ◎ 嘉義縣 - 重陽節敬老禮金金融帳戶申請 
- ◎ 嘉義縣 - 長期照護線上申請 
- ◎ 桃園市 - 中醫助孕養胎調理申請 
- ◎ 桃園市 - 身心障礙者專用停車位識別證 

STEP 1 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

☒ 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 同意資料傳送

本次傳送的資料集如下：

1. 低收及中低收列冊資料



 **MyData** 成功將資料傳給「教育部國民及學前教育署」的「全國高級中等學校具中低或低收入戶資格學生於線上申請學雜費減免服務」服務後，系統將自動發通知信至您的電子信箱 [\[redacted\]](#)。如電子信箱有誤，或想變更電子信箱，請至 [個人專區](#) 進行變更，謝謝。

不同意傳送

同意傳送

STEP 5 跳轉至資料頁面，實際以申請者身分資料為主

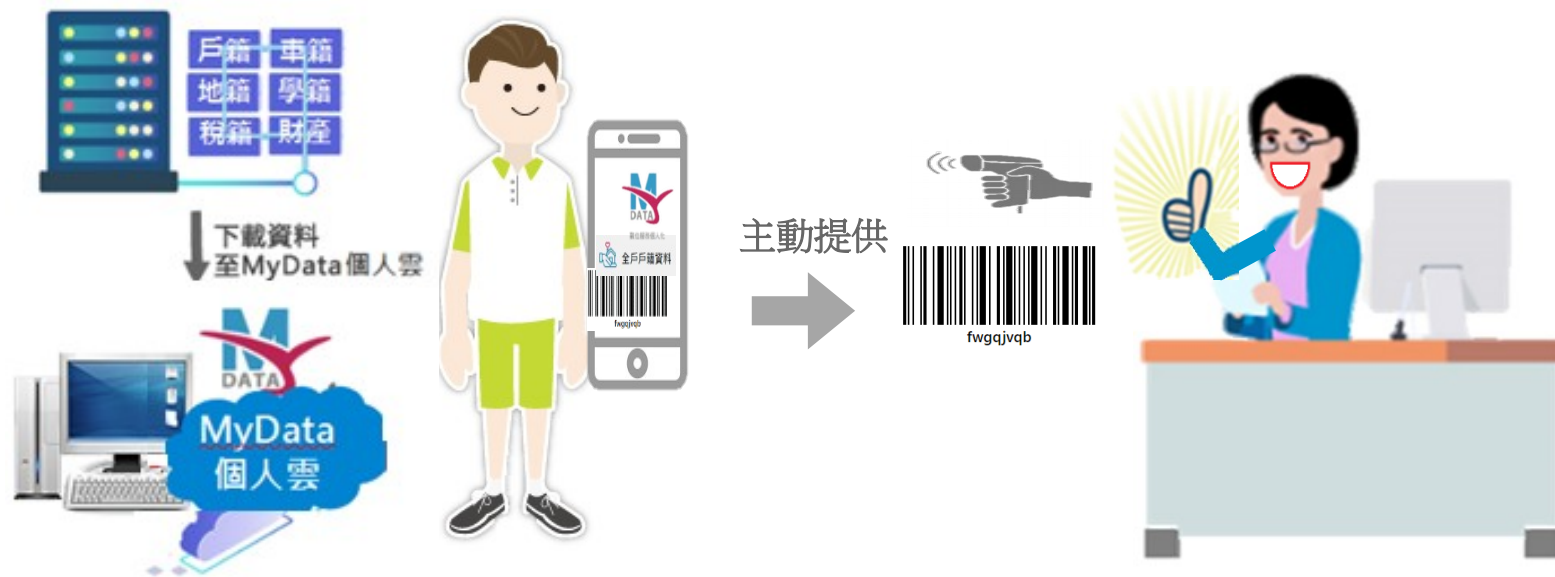


身份證字號	FOUR	姓名	
學校名稱			
有效起訖			
身份別	衛服部系統查無低收或中低收身分		
系統查不到您的低收入戶或中低收入戶資料！請您向戶籍所在地之鄉/鎮/市/區公所確認申請人的低收/中低收身分申請，是否已經報經戶籍所在地的直轄市、縣(市)主管機關審通過，並於審核通過後24小時再次使用助學補助系統申請			
因資料有誤，不送出申請			

[回到助學系統MyData申請首頁](#)

[前往國發會MyData下載紙本證明](#)

臨櫃核驗服務流程說明



民眾以手機取得個人資料檔案，
至臨櫃申辦業務STEP 1~12

臨櫃機關人員取得民眾條碼，
下載民眾個人資料檔案，
進行申辦業務核驗STEP 13~16

民眾端臨櫃核驗 服務流程說明

臨櫃核驗（民眾端）服務流程說明

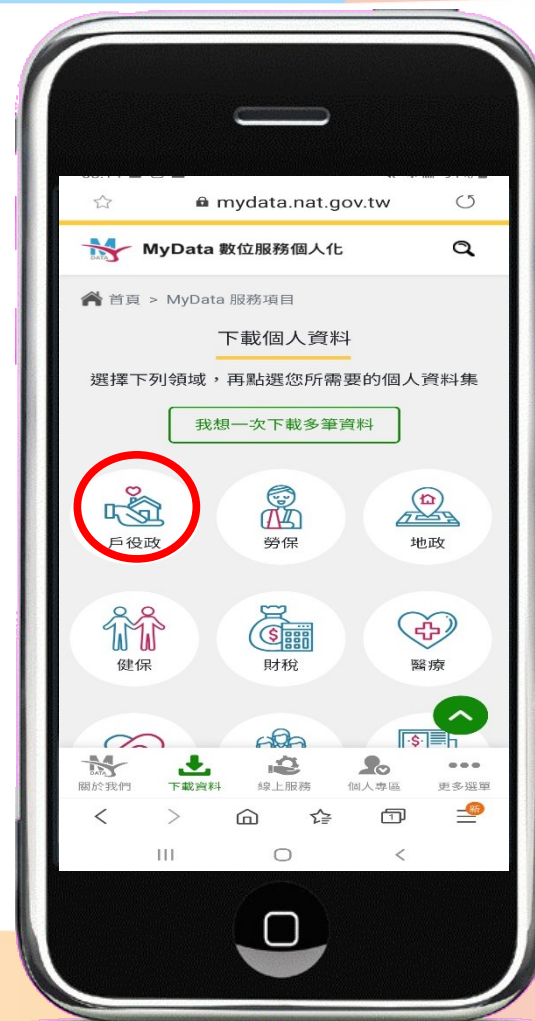
STEP 1

民眾從MyData
平臺點擊“下
載個人資料”



STEP 2

選擇資料
類別



臨櫃核驗（民眾端）服務流程說明

STEP 3

選擇項目(以戶政國民身分證影像為例)



STEP 4

點選我要下載



臨櫃核驗（民眾端）服務流程說明

STEP 5

同意
MyData服
務條款



STEP 6

輸入身分證
字號和生日



臨櫃核驗（民眾端）服務流程說明

STEP 7

並選擇身分
驗證方式
(TW FidO)



STEP 8

(TW FidO)於
工具列出現
推播訊息，
點選後進入
TW FidO APP
畫面



臨櫃核驗（民眾端）服務流程說明

STEP 9

使用生物特徵進行身分驗證(例如：指紋)



STEP 10

驗證通過



臨櫃核驗（民眾端）服務流程說明

STEP 11

資料集下載完成，選擇「前往資料條碼區」



STEP 12

取得條碼資料



機關人員臨櫃核驗 服務流程說明

臨櫃核驗（機關端）服務流程說明

STEP 13 進入機關人員臨櫃核驗頁面，輸入「資料條碼」

<https://mydata.nat.gov.tw/organ>

...


網站地圖

常見問題

字級：中

我的個人專區

登出

 MyData 數位服務個人化


試營運-機關操作區


關於 MyData


最新消息

資料下載

線上服務





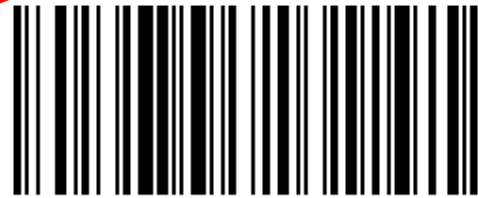


...

首頁 > 臨櫃核驗

臨櫃核驗

僅限機關人員操作使用


9cmtf2c8

Step

1

↓

請輸入資料條碼：

9cmtf2c8

下一步

臨櫃核驗（機關端）服務流程說明

STEP 14 系統將發送「驗證密碼」至民眾手機或電子郵件信箱，請民眾於 2 分鐘內提供臨櫃人員輸入至系統「驗證密碼」欄位

臨櫃核驗



資料條碼： 9cmtf2c8

下一步

輸入驗證密碼

驗證密碼已發送至當事人的電子信箱：[REDACTED]****@gmail.com，須請當事人提供驗證密碼，方能完成資料取用流程。

請於 2 分鐘內輸入驗證密碼，1分鐘後才能再次重新發送驗證密碼。(8)

驗證密碼： 19090076

確認

臨櫃核驗（機關端）服務流程說明

STEP 15 驗證通過



3

條碼取用

你可選擇下列方式使用已下載的資料檔案：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

臨櫃核驗（機關端）服務流程說明

STEP 16 資料取得



個人戶籍及相片影像資料	
統號： <input type="text"/>	
姓名： <input type="text"/>	
出生日期： <input type="text"/>	
出生地： <input type="text"/>	
領補換日期： <input type="text"/>	
身分證領補換： <input type="text"/>	
相片列印方式： <input type="text"/>	
換證機關： <input type="text"/>	
戶籍地址： <input type="text"/>	

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

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	查看資料集
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	查看資料集
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	查看資料集
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	查看資料集
5	API.fS9bsX4web	個人資料查驗	ris_check	自然人憑證	內政部戶政 司	查看資料集
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	查看資料集
7	API.KvyRZSc5K	地籍及實價資料	MoiLandReadMyData	自然人憑證	內政部地政 司	查看資料集

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 :

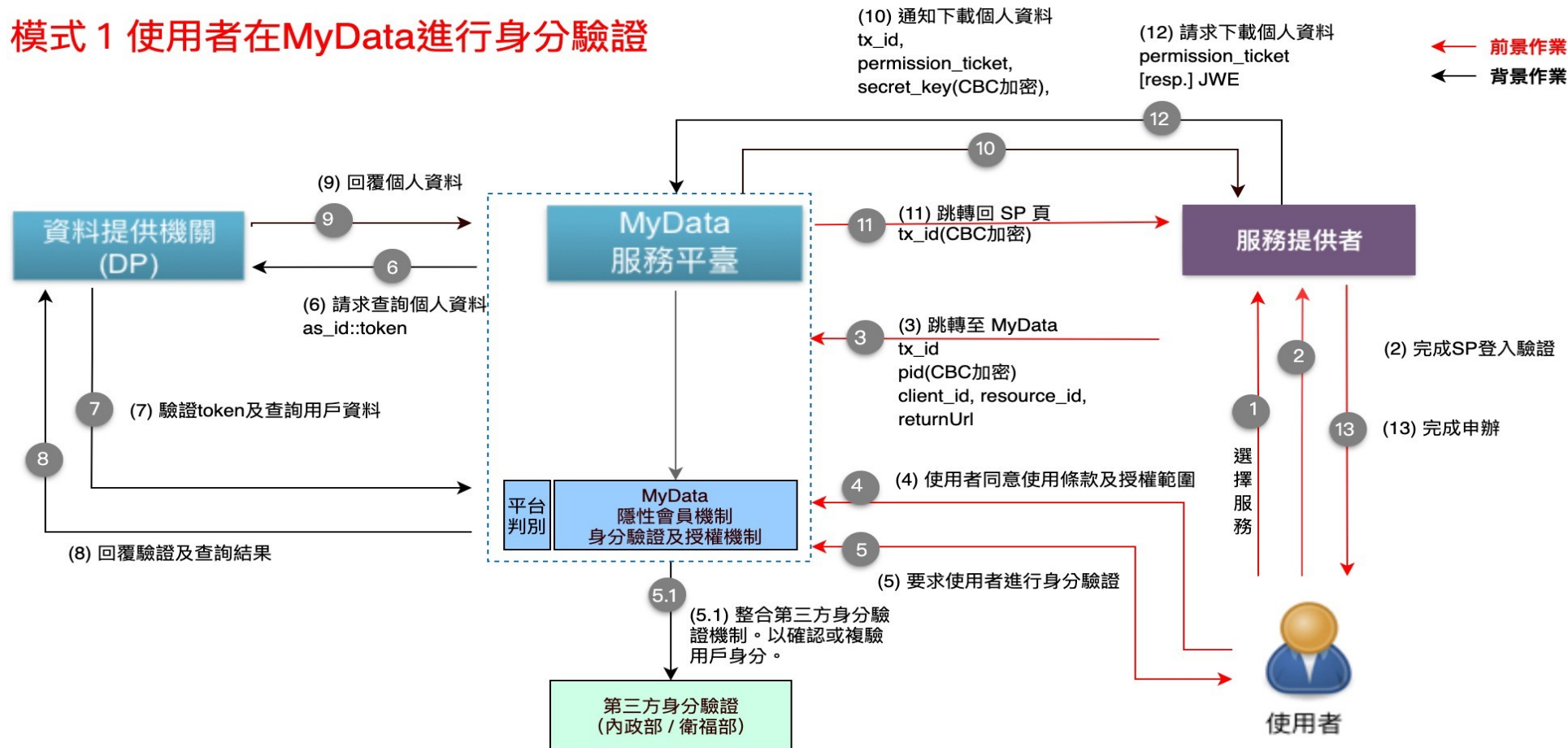
- 個人記事
- 出生地
- 出生日期
- 國民身分證統一編號
- 姓名
- 婚姻狀況
- 戶籍地址
- 教育程度
- 遷入日期

參、技術規範說明

MyData整合網址及參數說明

線上服務情境：模式 1（由 MyData 驗證）

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。

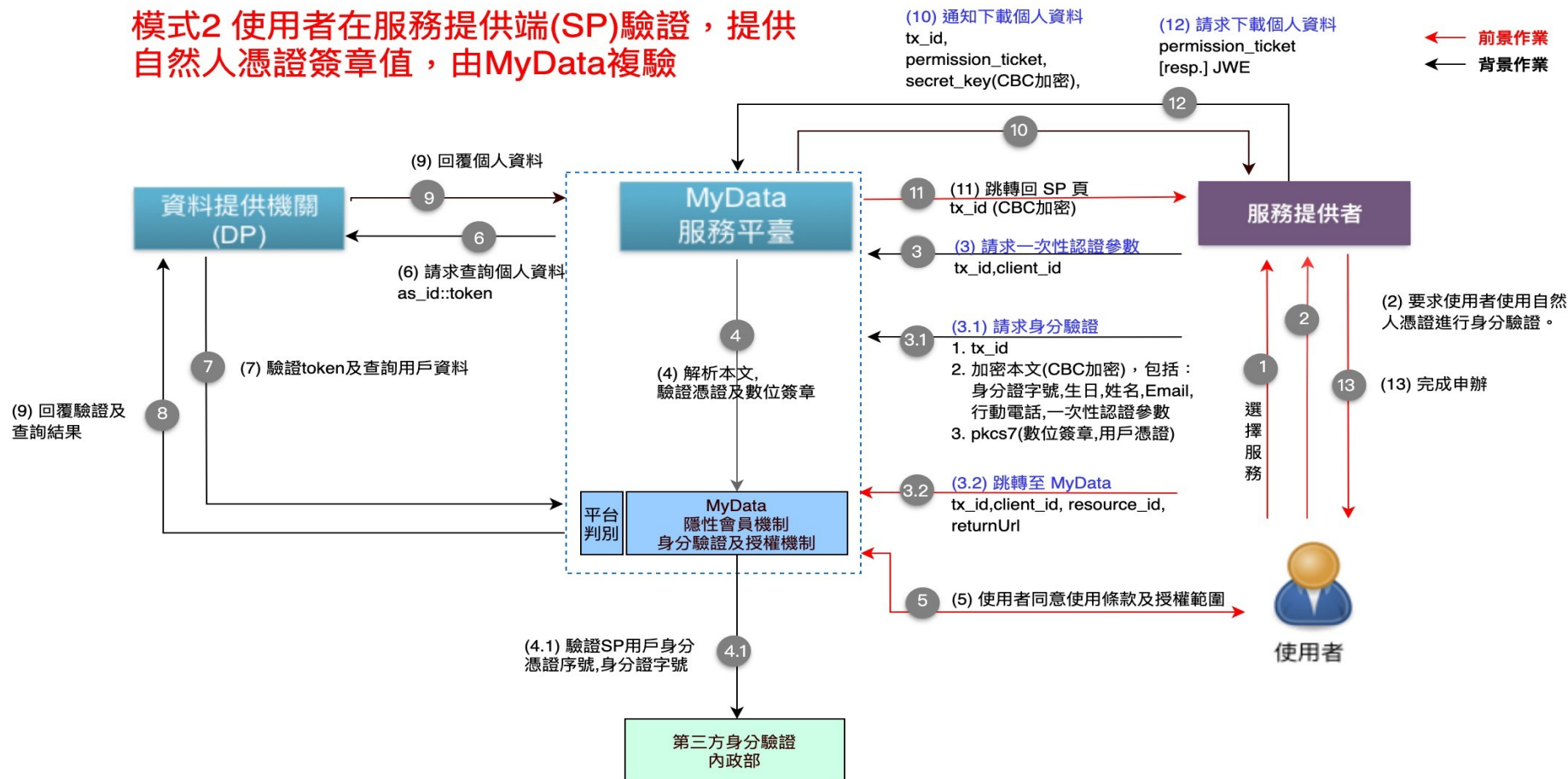
須以 UrlEncode 編碼處理過。

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。

線上服務情境：模式 2(由 SP 驗證自然人憑證)

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

步驟 11

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

步驟 11

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

206 : 超過 DP 資料集當日請求之上限

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

步驟 12

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 TLS 1.2 200 OK

Content-Type: application/json

SP 回覆請求失敗

HTTP/1.1 TLS 1.2 403 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

步驟 12

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

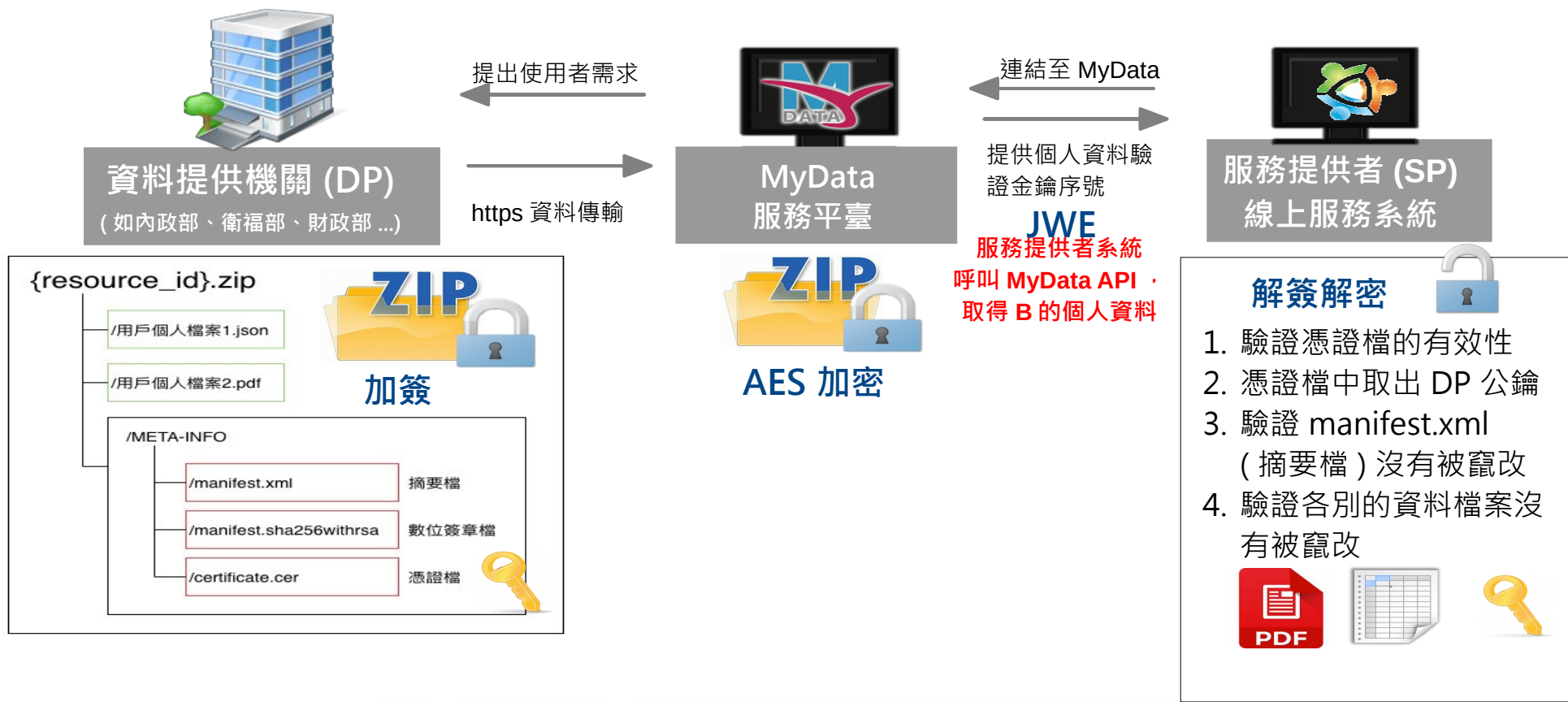
302 : 未加入白名單。 400 : 參數不正確，或缺少必要參數。

401 : 權限錯誤。 403 : 拒絕存取。

408 : 交易逾時。 504 : SP 異常，無法傳送資料集。

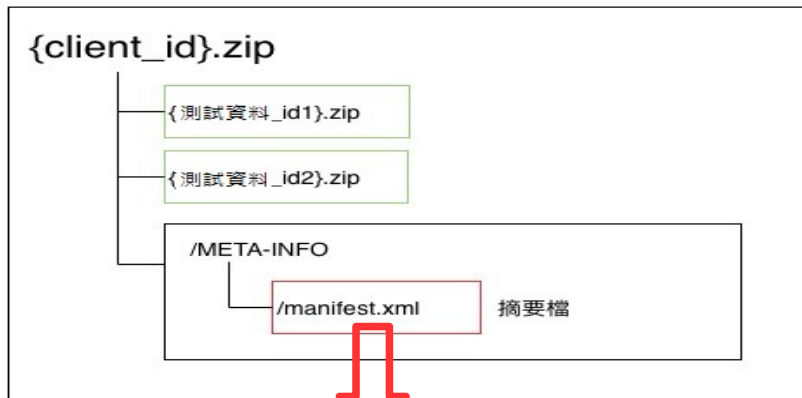
資料傳輸過程

安全的資料傳輸過程：資料加簽與加密

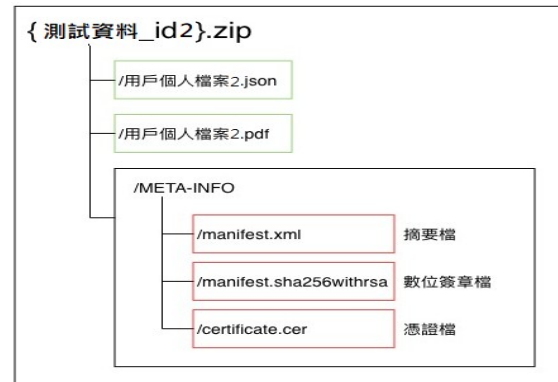
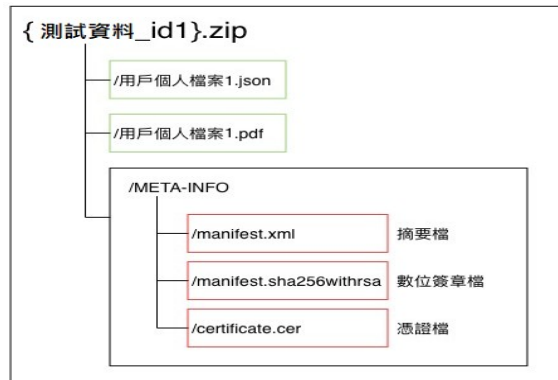


測試資料檔案結構

- 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>200</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>200</code>
  </file>
</files>
```





MyData資料結構與驗簽

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`

`eyJhbGciOiJIbmJU2S1ciLCJlbmMiOiJBMjU2Q0JDLUhTNT`

`1-mJQI42l08E3mz6Zac4OIHsNDXxz7g6DoAmJqayHm`

`SHR6R1k3ZzFoTHk1Ymw5Ug`

`LMz7XIhl2p6FPQwXfHAhb0yZ7YjgjPsLXzR6J96Lxzc-z0G3dR5P5_MB_NBQmumD7exefh2GpXjCwkl277CD5htL7XzJodZLlqOwp1Ymhg`

`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"  
}
```

(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`

`eyJhbGciOiJIbMjU2S1ciLCJlbmMiOiBMbmJU2Q0JDLUhtNTNTEyIn0`

`1-mJQI42l08E3mz6Zac4OIHsNDXxz7g6DoAmJqayHmmeVIUliNhLMYS5kjWAKPI7LrsFZ0pmdFVqfC77688Mdfni0Xgu4PST`

`SHR6R1k3ZzFoTHk1Ymw5Ug`

`LMz7Xlhl2p6FPQwXfHAhb0yZ7YjgjPsLXzR6J96Lxzc-z0G3dR5P5_MB_NBQmumD7exefh2GpXjCvwkl277CD5htL7XzJodZLIqOwp1Ymhg`

`C7iWN06BVCpamm3KlpuPxJYgCkcCh1QcTc8BzDKD3Sw`

(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：

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

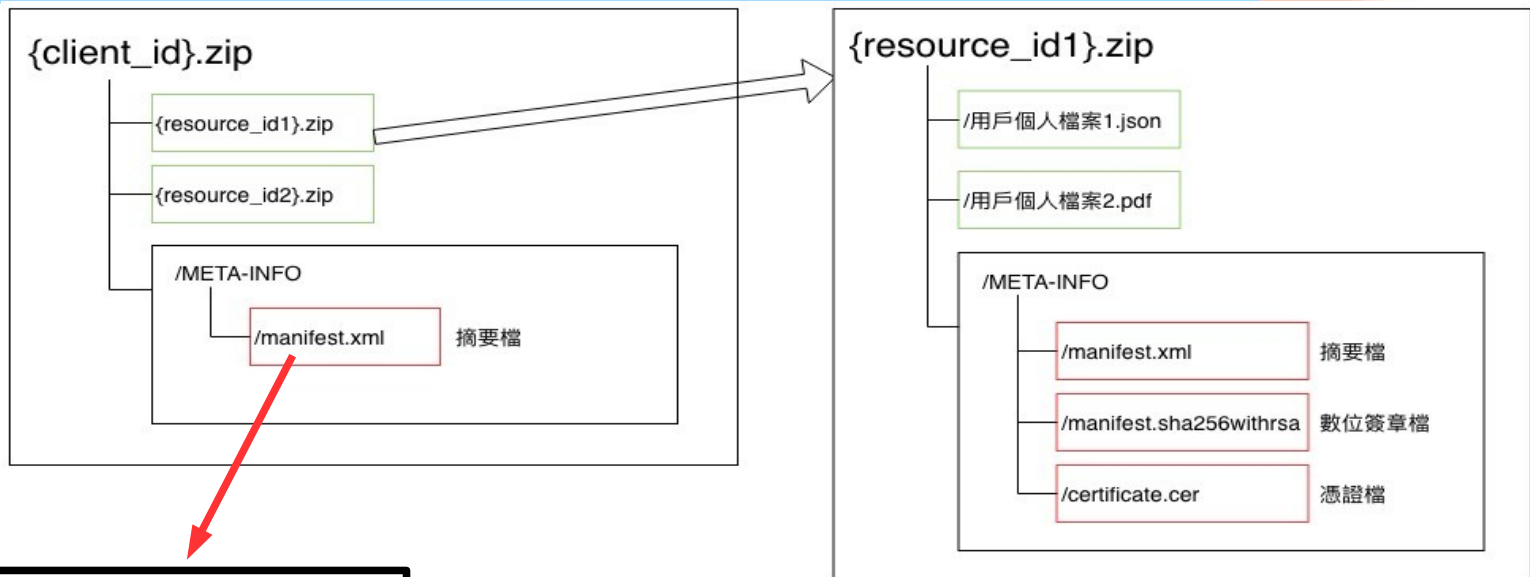
內容解密成功後，可得到一個 JSON 格式的資料內容，欄位說明如下：

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：

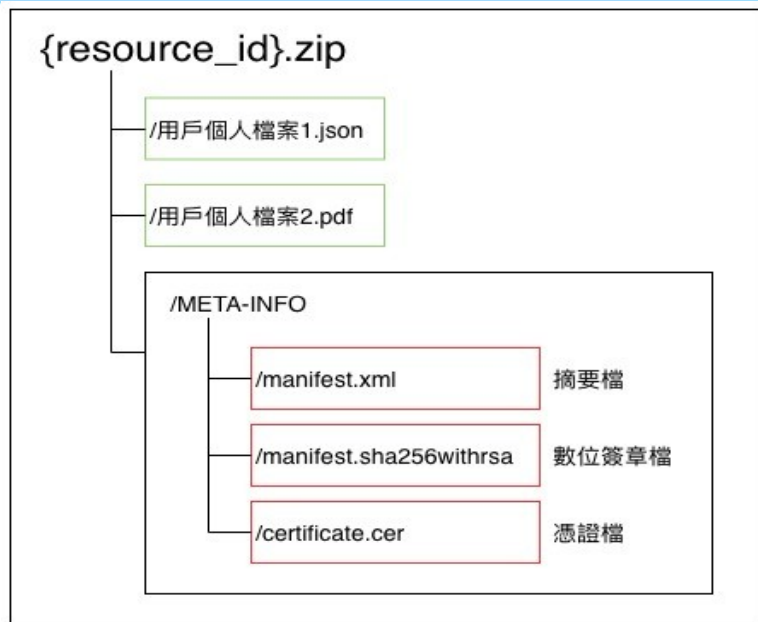


```
<?xml version=" 1.0" encoding=" UTF-8" >
<files>
<file>
  <filename>{resource_id1}.zip</filename>
  <resource_id>{resource_id}</resource_id>
  <resource_name> 資料集中文名稱 </resource_name>
  <code>200</code>
</file>
</files>
```

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/1.1 TLS 1.2 403 Forbidden

Content-Type: application/json

HTTP 狀態碼	說明
400	參數不正確或缺少必要參數。
401	權限錯誤。
403	拒絕存取。
408	交易逾時。

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：雙證件

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。

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 (1/4)

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，如下頁（同技術文件之說明）。

交易 Log 日誌查詢 (2/4)

交易日誌產生時機

#	事件代碼	事件時機	DP	MyData	SP
1	110	民眾在 SP 做自然人憑證驗證			V
2	120	SP 請求一次性驗證參數		V	V
3	130	將壓縮加密過的民眾的個人資料與簽章憑證傳給 MyData		V	V
4	140	SP 跳轉至 MyData 同意頁		V	V
5	150	MyData 向內政部 API 驗民眾憑證與數位簽章		V	
6	160	MyData 呼叫 ICS API		V	
7	170	MyData 呼叫生日 API		V	
8	180	民眾於 MyData 頁面完成身分驗證		V	
9	190	自動註冊帳號		V	
10	200	發送手機認證簡訊		V	
11	210	完成手機認證		V	
12	220	發送 email 認證信		V	

#	事件代碼	事件時機	DP	MyData	SP
13	230	完成 email 認證		V	
14	240	民眾同意傳輸資料給 SP		V	
15	250	MyData 請求 DP 資料集	V	V	
16	260	DP 呼叫 Introspection API	V	V	
17	270	DP 呼叫 UserInfo API	V	V	
18	280	MyData 取得 DP 資料集	V	V	
19	290	MyData 呼叫 SP-API 通知取資料		V	V
20	300	MyData 跳轉回 SP		V	V
21	310	SP 呼叫 MyData-API 取個人資料		V	V
22	320	民眾臨櫃申辦，MyData 發送資料條碼驗證碼給民眾		V	
23	330	臨櫃人員輸入資料條碼驗證碼		V	
24	340	MyData 發送資料取用通知簡訊/信（轉存、服務應用、條碼取用）		V	
25	350	MyData 刪除個人資料檔案		V	
26	360	SP 刪除個人資料檔案			V

交易 Log 日誌查詢 (3/4)

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 (4/4)

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 : 拒絕存取，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>

參考附件

數位服務個人化 (MyData) 多元身分驗證方式

預計於109年底加入晶片金融卡、硬體金融憑證、軟體金融憑證等身分驗證方式。



數位服務個人化 (MyData) 多元身分驗證方式

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 (TW FidO) ，須使用自然人憑證綁定
3	健保卡、軟體金融憑證
4	雙證件驗證 (身分證字號 + 健保卡號 + 戶號或身分證換補證日期)