



# 數位服務個人化 (MyData) 服務提供者技術開發說明



## 壹、服務提供者申請流程

## 貳、服務流程

- 前台服務流程說明
- 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





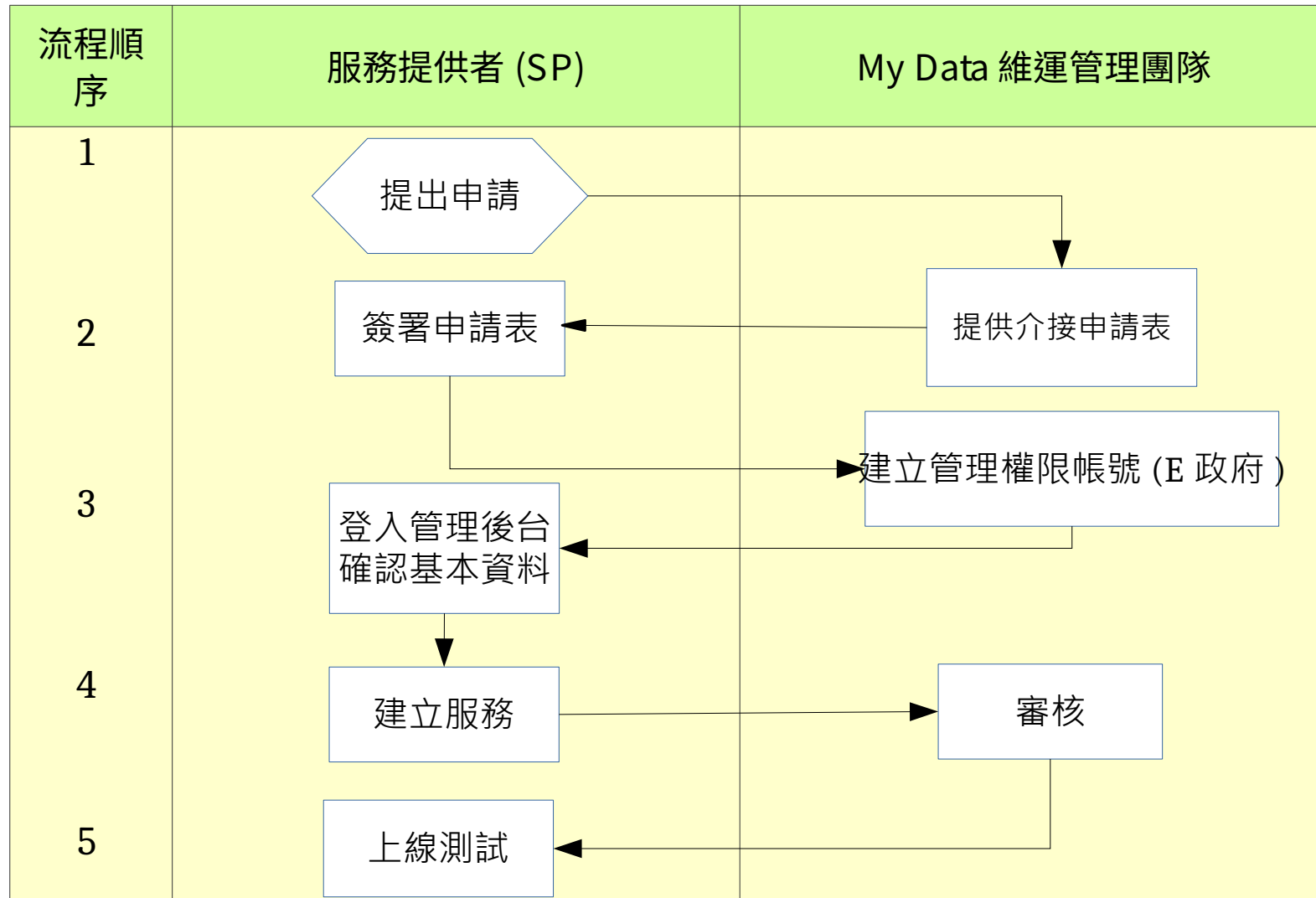
1 以電話或 E-mail 聯繫管理團隊，提出後台使用申請

2 申請機關單位與 MyData 簽署  
「MyData 平臺服務提供者介接申請表」

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資料提供者  
(DP)、服務提供者 (SP) 相關功能





## 貳、服務流程



# 前台服務流程說明



# 線上申辦服務流程



## STEP 1 使用者從服務端頁面點選服務示意圖

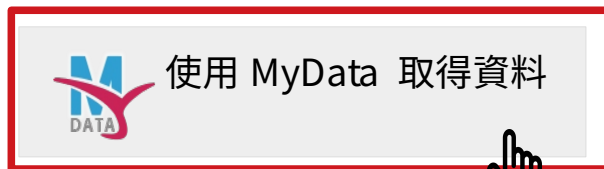


使用者輸入開戶所需基本資料：

姓名  身分證字號  ....

申請線上開戶所需個人資料：

1. 個人戶籍
2. 親屬關係
3. 財產資料



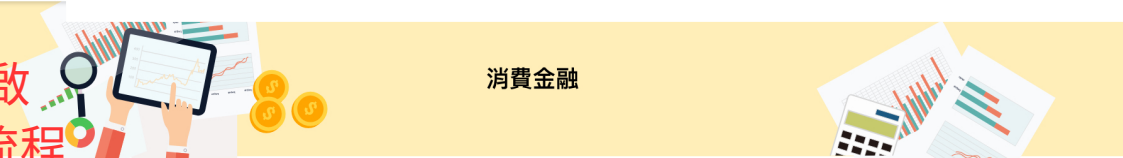




## STEP 2

( 未登入 eGOV 狀況 ) 勾選「同意」後，選擇驗證方式「自然人憑證」，點選「確認」彈跳 GSP 登入視窗

另開視窗，開啟  
MyData 申請流程



消費金融

項目一覽

◎玉山銀行線上開戶

step 同意服務條款

1. 我的生活消費：您是否總是苦無聰明的存款方式？我的民生消費服務可整合您的電子發票跟一般消費紀錄，透過您的身分驗證與線上同意授權，整合電子發票、水費、電費等個人消費資料，提供圖形化消費類別分析與每月消費趨勢分析功能，並透過APP設定儲存目標及夢想設定，讓您掌握消費方向，成為您個人理財與消費管理的最佳利器！

1. ☐ 我已詳實了解此服務內容，並同意上述服務條款

2. 身份驗證

您可使用下列方式驗證您的身份並取得資料

2. [自然人憑證](#) [健保卡](#) [H 多因子](#) [動態簡訊](#)

3. [確認](#)

3. 傳送資料

您將傳送的資料有

1.個人戶籍資料	▼
2.親屬關係資料	▼
3.財產資料	▼

您是否願意將上述個人資料提供至 玉山銀行(台北市信義區公所) 辦理 線上開戶 (新辦戶口) 使用

[拒絕](#) [確認](#)



## STEP 3

GSP 彈跳視窗：登入 -> 以您的身份繼續 -> 憑證驗證 -> 資料授權

網站地圖 聯絡我們 常見問題

My Data 數位服務個人化

關於My Data My Data服務 授權記錄 登入

消費金融

我的E政府  
WWW.GOV.TW

帳號登入

帳號

密碼

忘記帳號 忘記密碼?

登入

以 Victor Lee 的身份繼續

MyData入口網  
將收到下列資料：你的GSP會員基本資料、身分證字號、電子郵件。

查看你提供的資訊內容

確認

我的E政府  
WWW.GOV.TW

憑證驗證

請插入您的憑證並輸入PIN

PIN 請輸入PIN碼

驗證

初次使用憑證登入，請務必安裝最新版本HICOS元件方能完整支援自然人憑證之讀取及使用，安裝元件與登入問題，請詳常見問題或元件測試網頁[協助測試]

玉山銀行線上開戶要求您授予以下權限：

檢視您登入的eGov帳號及會員基本資料

您的Email  
您用來登入的Email或留在GSP的Email

您的身分證字號  
身分證字號、外來人口統一編號等

GSP會員基本資料  
留存GSP之稅號、使用者姓名、生日、性別等。

應用程式存取

個人戶籍資料  
身分證字號、出生日期、戶籍地址、婚姻狀態。

親屬關係資料  
子女數量、子女年齡。

財產資料  
個人財產資料電子稅務文件。

記住我的同意  
點選「允許」即表示您同意此服務提供方和E政府服務平臺依據各自的服務條款和隱私政策使用您的資訊。

允許 拒絕

1.個人戶籍資料

2.親屬關係資料

3.財產資料

您是否願意將上述個人資料提供至 玉山銀行(台北市信義區公所) 辦理 線上開戶 (新辦戶口) 使用

拒絕 確認



## STEP 4 經由身分驗證與授權後，使用者按「確認」傳送資料

[網站地圖](#) [聯絡我們](#) [常見問題](#)

 **My Data** 數位服務個人化

[關於My Data](#) [My Data服務](#) [授權記錄](#) [登入](#) [?](#)



### 消費金融



項目一覽

◎玉山銀行線上開戶

step

1

同意服務條款

1.我的生活消費：您是否總是苦無聰明的存款方式？我的民生消費服務可整合您的電子發票跟一般消費紀錄，透過您的身分驗證與線上同意授權，整合電子發票、水費、電費等個人消費資料，提供圖形化消費類別分析與每月消費趨勢分析功能。並透過APP設定儲存目標及夢想設定，讓您掌握消費方向，成為您個人理財與消費管理的最佳利器！

☐ 我已詳實了解此服務內容，並同意上述服務條款

2

身份驗證

您可使用下列方式驗證您的身份並取得資料

[自然人憑證](#) [健保卡](#) [多因子](#) [動態簡訊](#)

確認

3

傳送資料

您將傳送的資料有

1.個人戶籍資料

2.親屬關係資料

3.財產資料

4.

您是否願意將上述個人資料提供至 [玉山銀行](#) (台北市信義區公所) 辦理 [線上開戶](#) (新辦戶口) 使用

[拒絕](#) [確認](#)





## STEP 1 使用者從 MyData 點選資料集下載

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：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 2 使用者到資料條碼區紀錄下條碼資料

⋮ 首頁 > MyData服務項目 > 資料條碼區

個人資料



違規資料查詢

如欲完成臨櫃申請，請將此條碼出示給臨櫃人員。

補充：為提高資料安全性，此條碼有效時間尚餘 18 分鐘。



vc9v9fh1



手動更新條碼

線上預覽檔案

轉存到我的電腦



e管家 Plus

M<sup>14</sup>  
DATA



## STEP 3 資料需求者，到資料條碼取用頁面輸入條碼



MyData 數位服務個人化

關於 MyData

MyData 服務項目 ▾

吳\*\*\*\*\* 您好 ▾



⋮ 🏠 首頁 > 資料條碼取用資料

### 資料條碼取用資料

請輸入驗證序號：

☐

我不是機器人



reCAPTCHA  
隱私權 - 條款

預覽

取資料



e管家 Plus





## STEP4 資料需求者，將資料儲存

網站地圖 我想要更多 常見問題 字級：大 中 小

MyData 數位服務個人化

關於 MyData MyData 服務項目 吳\*\*\*\*\* 您好

首頁 > 資料條碼取用資料

資料條碼取用資料

MyData 提醒

請問你要轉存資料集嗎？

取消 確定

關於 MyData

MyData 服務項目

外部連結

下載個人資料

e管家Plus

我的E政府

國家發展委員會

聯絡我們

mydata@ndc.gov.tw

APLe98PaKiAFn2....zip

全部顯示





# 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。

### 單位註冊

申請日期：

\* 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。



MyData管理後台

帳號

密碼

登入後台



e管家 Plus





## STEP 3

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

編輯單位

單位資訊

申請日期： 2018-10-23

政府機關名稱： 衛生福利部

政府機關地址： 臺北市中山區大直街123號

\* 申請人姓名： 張三

\* 聯絡電話： 02-1234-5678

\* 聯絡E-mail： abc@def.com

\* E政府帳號： my123456

副E政府帳號：

E政府帳號	姓名	電話	E-mail
請輸入E政府帳號	請輸入姓名	請輸入電話	請輸入E-mail

增加輸入列



## 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。

* 服務類別：	<input type="text" value="請選擇"/>
* 服務名稱：	<input type="text" value="請輸入服務名稱(例如：e管家福利自己查)"/>
* 服務網址：	<input type="text" value="請輸入服務網址(例如：https://mydata.nat.gov.tw/)"/>
* 服務說明：	<input type="text" value="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：	<input type="text" value="CLl.qqOjnJO4WR"/>
* 上傳服務介接申請書：	<input type="text" value="File not selected"/> 
* 需求資料集：	<input type="text" value="請選擇資料提供單位"/>
* 服務跳轉網址：	<input type="text" value="請輸入服務跳轉網址(例如：https://mydata.nat.gov.tw/MyDataResult)"/>
* SP-API：	<input type="text" value="請輸入服務SP-API(例如：https://mydata.nat.gov.tw/SP-API)"/>
* 允許連線IP：	<input type="text" value="請輸入IP(機關/企業 要連線到MyData後台及SP-API)"/> <input type="button" value="增加輸入IP欄位"/>
修改人員：	<input type="text" value="jclank1"/>

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。



單位名稱	服務類別	服務名稱	狀態
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
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
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
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 <

☒ 所有服務列表

☒ 所有資料集列表

統計數據 <

系統管理 <

登出

顯示所有  
資料集清單

顯示特定  
資料集內容

資料集名稱	SOCPE	需要的身 分驗證安 全等級	資料 機關 名稱	
	tygh.resource.prenatal.read	自然人憑證	衛生福利部 桃園醫院	查看資料集
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
高中職及特殊教育學校學生畢業資料	search	自然人憑證	教育部國民 及學前教育 署	查看資料集
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
個人資料查驗	ris_check	自然人憑證	內政部戶政 司	查看資料集
核發使用牌照稅繳納證明	etax.service.oldvab1001.owner	自然人憑證	財政部財政 資訊中心	查看資料集
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 : APLKr1C3b1ijJ

資料集名稱 : 親屬關係資料 (範圍為父母、配偶、子女) 查詢

需要的身分驗證安全  
等級 : OTP

資料提供者 : 內政部戶政司

資料集欄位 :

- 出生日期
- 國民身分證統一編號
- 姓名
- 子女出生日期
- 子女國民身分證統一編號
- 子女姓名
- 母出生日期
- 母國民身分證統一編號
- 母姓名
- 父出生日期
- 父國民身分證統一編號
- 父姓名
- 配偶出生日期
- 配偶國民身分證統一編號
- 配偶姓名
- 養母出生日期
- 養母國民身分證統一編號
- 養母姓名
- 養父出生日期
- 養父國民身分證統一編號
- 養父姓名

# 測試環境網址與技術參考文件



- 後臺測試機登入網址：  
<https://mydatadev.nat.gov.tw/mydata-backend>
- 前臺測試機網址：  
<https://mydatadev.nat.gov.tw/mydata>
- MyData 應用規範、技術文件與範例程式下載路徑：  
<https://github.com/ehousekeeper/emsg>

Branch: master ▾ New pull request Find file Clone or download ▾

ehousekeeper Update README.md Latest commit 4305b70 Dec 11, 2019

MyData介接資料檔案規格書	Delete 05-MyData介接內政部地政司_個人名下地籍資料檔案規格書.pdf	Dec 11, 2019
MyData應用規範與技術文件		
MyData範例程式	Add files via upload	Dec 11, 2019
e管家相關技術文件	Add files via upload	Mar 23, 2018
LICENSE	no message	Dec 28, 2017
README.md	Update README.md	Dec 11, 2019



# 參、技術規範說明

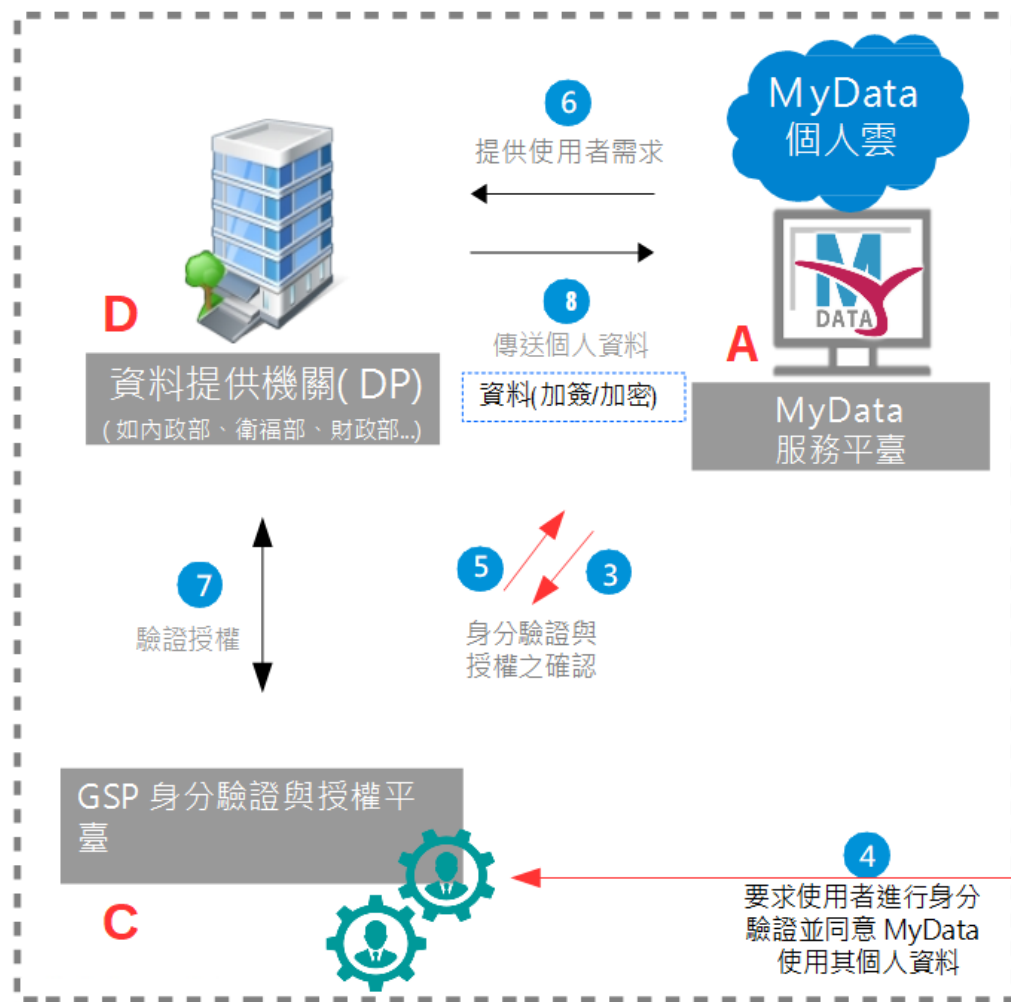
## MyData整合網址及參數說明

# MyData 服務情境：線上申辦



使用者將個人資料儲存於MyData個人資料暫存空間

使用者至機關進行業務申辦



連結至 MyData

服務申辦頁 tx\_id

pid(AES/CBC 加密)

2

9  
A 呼叫 SP 雙向憑證  
API x-api-key

tx\_id,  
permission\_ticket,  
secret\_key

10

重導向回 E 網頁  
tx\_id

11

E 呼叫 MyData 雙  
向憑證 API · 取得  
B 的個人資料  
permission\_ticket  
資料(AES/CBC 加密)



服務提供者  
(SP) 線上服  
務系統

1  
選擇所  
需服務

12  
完成線上申辦

使用者



← : 前端網頁流程

← : 後端系統流程

網路通道皆走 https 加密傳  
輸 · 步驟 6,9,11 以白名單鎖定

# MyData 整合網址及參數說明

## Step 2 : 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}

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。

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。如不檢核，則輸入 A99999999 即可。

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。

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

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

Step 10. (1)：重導向回服務提供者網頁，帶回 tx\_id

GET {sp\_return\_url}?tx\_id={tx\_id}

HTTP/1.1 TLS 1.2

OR

GET {sp\_return\_url}?tx\_id={tx\_id}&{sp\_param\_key}={sp\_param\_value}

HTTP/1.1 TLS 1.2

tx\_id：SP 核發的交易識別值。

格式為 version 4 UUID，長度共 36 字元的字符串。

{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

## Step 10. (2) : 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={tx\_id} HTTP/1.1

HTTP/1.1 TLS 1.2

OR

GET {sp\_return\_url}?code={code}&tx\_id={tx\_id}&{sp\_param\_key}={sp\_param\_value}

HTTP/1.1 TLS 1.2

狀態碼	說明
400	無法順利解析 SP 帶入的 Path Parameter 。
401	無效的 client_id 或 resource_id 。
403	sp_return_url 與 MyData 管理後台登錄值不相符。
404	SP 所請求的 resource_id 不在該 SP 服務申請的 DP 資料集項目中。
409	身分衝突。使用者查詢 pid 參數，與登入者身分不符，或帶入 pid 參數格式不符合身分證規格。
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，無法順利傳遞 DP 資料檔案。



# SP-API





# SP-API 請求及回覆規格說明

Step 9. (1) : 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

Step 9. (2) : 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

## Step 11 : 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/json

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/json

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

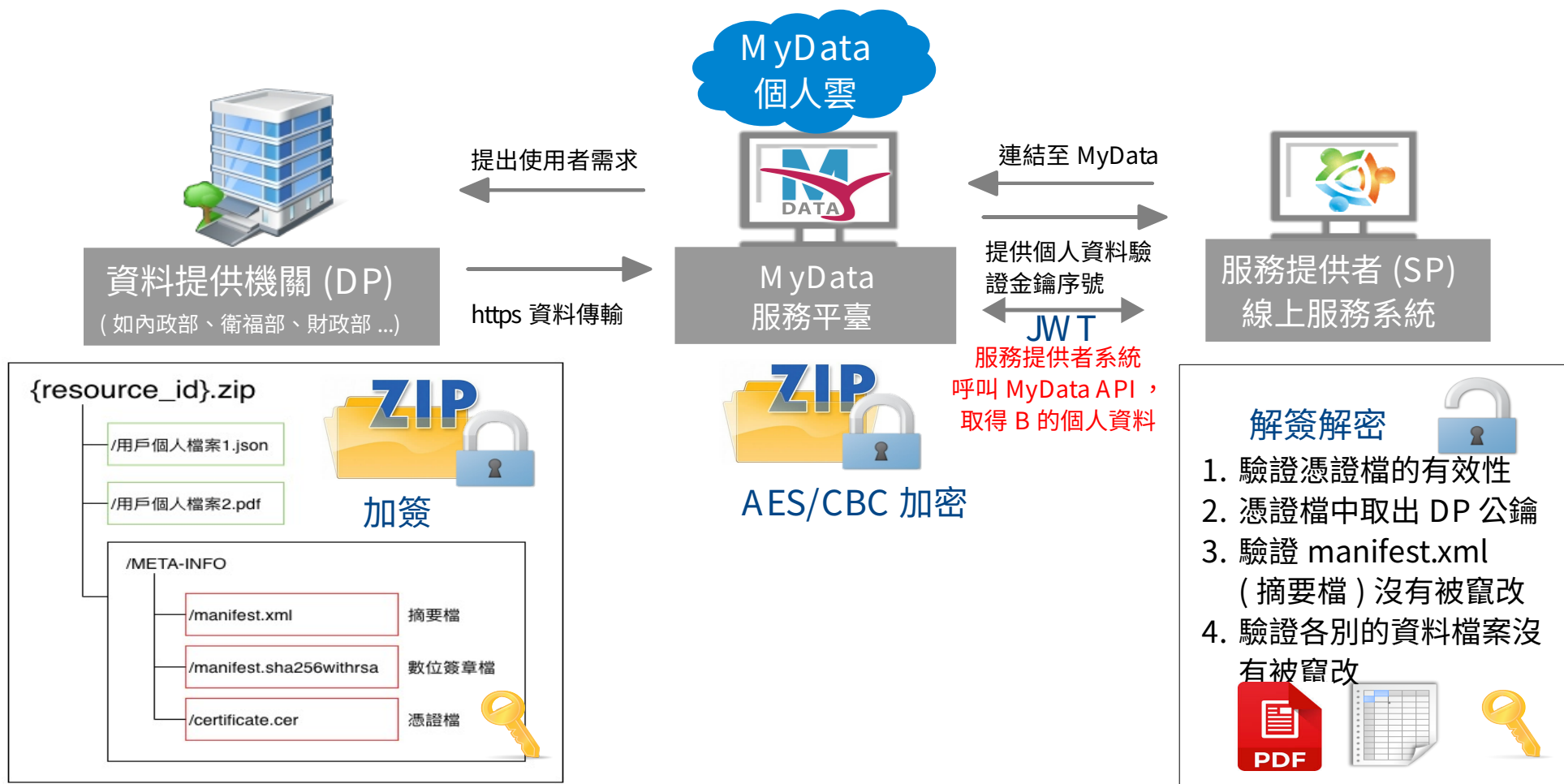
401：未完成身分驗證或身分驗證失敗。

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。

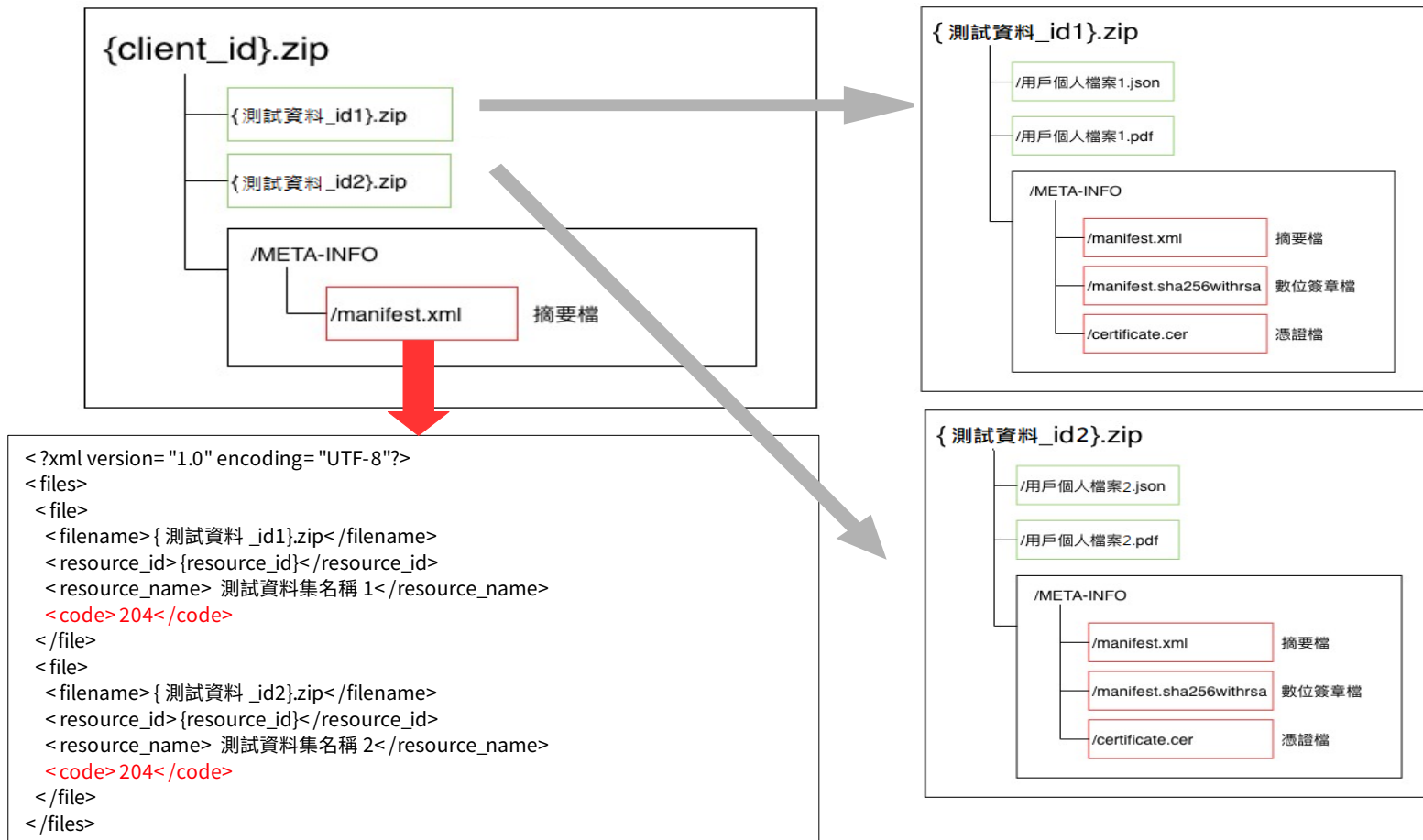
# 資料傳輸過程

## 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。





# MyData資料結構與驗簽





# MyData-API, JWT 內容說明



JWT 將三種資訊以 . 符號串接組合為一個字符串 => `header.payload.signature`

`eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9`

`.ewogICJjb2RlljogIjAiLAogICJmaWxlbmFtZSI6ICJhYmMuemlwliwKICAiZGF0YSI6ICJhcHBsaWNhdGlvbi96aXA7ZGF0YTpYc2RmYXNDU0ZEU0FERkFTVmN4diIKfQ==`

`.dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk`

header 及 payload 原為 JSON 內容，並以 Base64Encoder 編碼後置入 JWT。  
signature 則用於驗證 header.payload 的內容是否被竄改。

## 編碼前的 header 示意

```
{  
  "alg": "HS256"  
  "typ": "JWT"  
}
```

## 編碼前的 payload 示意

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

## Signature 產製方式示意

`HMACSHA256(base64Encode(header) + "." + base64Encode(payload), "secret_key")`





MyData 以 [secret\\_key](#) 做為產製 JWT signature 的密鑰。  
secret\_key 已於 MyData 呼叫請求 [SP-API](#) 時傳遞給 SP。

SP 驗證 signature 的步驟：

1. 自 JWT 中擷取 header 的字符串，並以 Base64Decoder 解碼。
2. 自 alg 值 HS256，得知 MyData 所使用的演算法是 [HMAC-SHA256](#)。
3. 自 JWT 中擷取 header.payload 的字符串。
4. 以 [HMAC-SHA256](#) 演算法及 [secret\\_key](#)，對 header.payload 進行演算。
5. 演算後所得值如符合 JWT signature 值，即代表 JWT 未被竄改。

[alg](#) 值為 HS256 為固定值，目前 MyData 不會動態改變演算法。



# SP 解譯 MyData-API JWT 內容的方法



MyData 傳遞的資料內容，放置於 JWT payload 中。  
以 Base64Decoder 解譯 payload 。

```
{  
  filename: "{service_id}.zip",  
  data: "application/zip;data:{binary_base64encoded_string}"  
}
```

filename：載明資料打包檔的檔名。格式為壓縮 zip 檔，預設以服務識別代碼為檔名。  
data：載明資料打包檔的內容。格式為 Base64 編碼後的字符串。

以 Base64Decoder 解譯 {binary\_base64encoded\_string} 內容。

以 secret\_key 為密鑰，以 AES/CBC/PKCS5Padding 解密，CBC 加密向量值，請使用後台服務編輯頁「CBC IV」值為準。

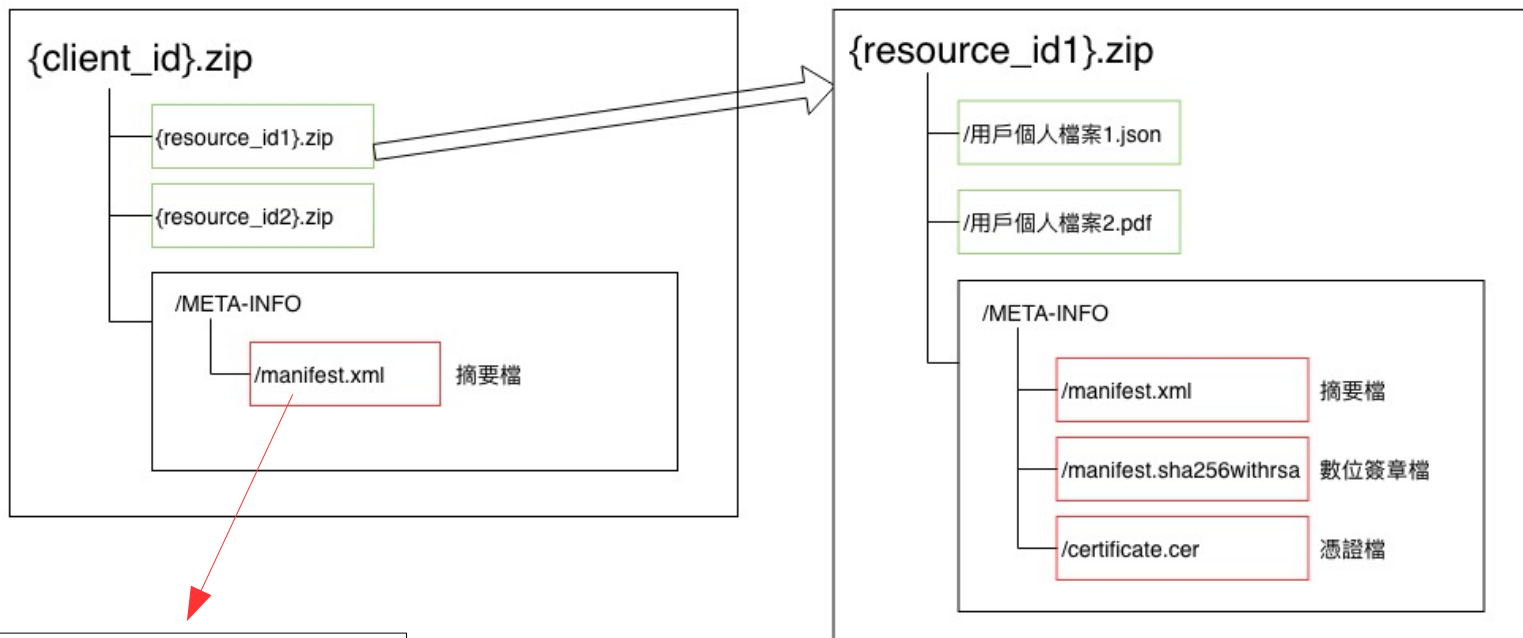
將解密後的 binary 儲存為 filename 載明的檔案名稱。  
此檔案即為 MyData 個人資料打包檔。



# 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>
```

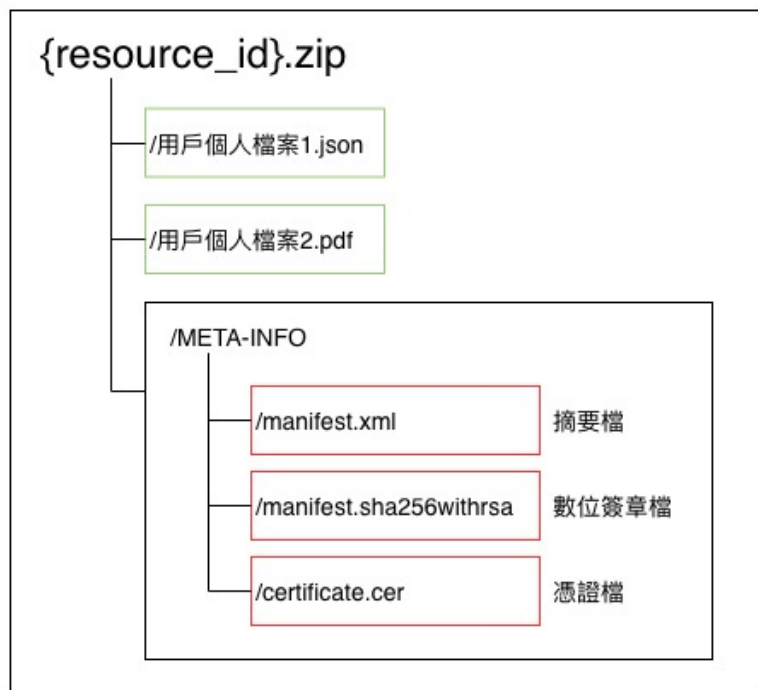
參數	說明
code	檔案處理狀態， 200：正常 204：查無使用者資料（封裝內無檔案）



# 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。





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





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
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 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

參數	說明
code	429 : MyData 資料準備中 200 : MyData 資料已準備完成 201 : SP 已取用資料
text	429 : MyData 資料準備中 200 : 資料已準備完成 201 : SP 已取用資料
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 tx_id 無效 (無效情況可能為連線未建立，或該 tx_id 的 permission_ticket 已超過效期)。



簡報完畢  
敬請指教

