

數位服務個人化
服務提供者技術文件

V2.1

國家發展委員會

中華民國 109 年 02 月

版本修正紀錄

項次	版本	修正內容	時間	頁次
1	2.0	更新章節「陸、一、MyData 整合協作流程說明」之流程圖。	109/2/18	P16
		調整章節「柒、MyData 整合方式說明」之內容，新增在 SP 驗證機制。新增隱性會員機制，若民眾在 MyData 使用 GSP 驗證，只須在 MyData 進行歸戶，不須註冊 GSP 會員。		P18
		調整章節「捌、二、(一) MyData 發出請求 - 告知 SP 準備來提取資料檔」之內容，將 secret_key 以 AES/CBC 加密。		P28
		調整章節「玖、三、MyData-API 的回傳格式說明」之內容，改以 JWE 回傳資料。		P32
		調整章節「拾、二、Type-Valid」之內容，將請求參數增加 tx_id，並新增 T-FidO 驗證代號。		P42
		調整章節「拾、三、Txid-Status」之狀態碼。		P44
		新增章節「拾、四、交易 Log 日誌查詢」之狀態碼。		P45
		更新各 API 狀態碼，並新增「附錄、HTTP 狀態碼總表」，以方便查找。		P50
2	2.1	調整章節「陸、MyData 整合協作流程說明」之內容文字。	109/2/24	P15
		更新章節「柒、MyData 整合方式說明」子標題之文字。		P18
		更新章節「玖、三、(一) JWE 格式說明」之範例。		P32

		更新章節「拾壹、一、測試流程」之內容。		P49
--	--	---------------------	--	-----

目錄

壹、目的.....	6
貳、如何成為服務提供者.....	6
一、完成 MyData 服務提供者資格申請作業.....	6
二、完成 MyData 線上註冊作業.....	6
三、實作 SP-API 開發，提供予 MyData 平臺介接.....	6
四、實作 MyData-API 之系統整合介接.....	6
參、名詞定義.....	6
肆、服務提供者資格申請作業.....	7
伍、服務提供者管理作業.....	8
一、基本資料編輯.....	8
二、服務註冊.....	9
三、服務管理.....	12
四、可運用的資料集.....	13
陸、MyData 整合協作流程說明.....	15
一、MyData 整合協作流程說明.....	16
二、應用範圍.....	17
柒、MyData 整合方式說明.....	18
一、服務情境示意圖.....	18
二、MyData 整合網址及參數說明.....	19
三、正常返回 SP 網址之處理方式說明.....	24
四、異常返回 SP 網址之處理方式說明.....	25
五、無法返回 SP 網址之處理方式說明.....	27
捌、SP-API Endpoint 規格說明.....	27
一、系統環境與條件.....	27
二、SP-API 請求及回覆規格說明(由服務提供者實作).....	27
玖、MyData-API Endpoint 規格說明.....	30

一、系統環境與條件.....	30
二、MyData-API 請求及回覆規格說明.....	30
三、MyData-API 的回傳格式說明.....	32
四、MyData-API 的資料打包檔規格說明.....	36
五、資料提供者的 DP 資料打包檔規格說明.....	38
六、驗證 DP 資料檔案沒有被竄改的方法說明.....	40
拾、資料查核相關網頁與 API.....	41
一、第三方身分驗證中心日誌查詢.....	41
二、Type-Valid.....	42
三、Txid-Status.....	44
四、交易 Log 日誌查詢.....	45
拾壹、SP-API 與 MyData-API 測試流程說明.....	49
一、測試流程.....	49
二、系統環境主機及網址資訊.....	50
附錄、HTTP 狀態碼.....	50

壹、目的

本文件主要描述扮演「MyData 平臺之服務提供者」時應依循的作業流程、準則及相關注意事項。

貳、如何成為服務提供者

一、完成 MyData 服務提供者資格申請作業

機關單位如欲加入 MyData 成為「服務提供者」，需先完成資格申請。內容細節請參考本文件章節「肆、服務提供者資格申請作業」。

二、完成 MyData 線上註冊作業

註冊作業包括：

- 機關單位註冊：登錄機關單位基本資料。
- 服務註冊：登錄服務資訊。

內容細節請參考本文件章節「伍、服務提供者管理作業」

三、實作 SP-API 開發，提供予 MyData 平臺介接

服務提供者必需提供 SP-API Endpoint 並登錄於 MyData 管理後台。MyData 平臺將利用此 SP-API Endpoint，於用戶同意授權後，將 permission_ticket 及 secret_key 傳送予服務提供者。

四、實作 MyData-API 之系統整合介接

MyData 平臺提供 MyData-API Endpoint 讓服務提供者可以透過此 API 取得該服務所需的用戶個人資料打包檔案。MyData 平臺的 MyData-API 的回應格式是 JWE，是將用戶個人資料打包檔案封裝於 JWE 中。因此服務提供者需了解 MyData-API 及資料打包檔的相關規格，以完成 MyData-API 的整合介接工作。

參、名詞定義

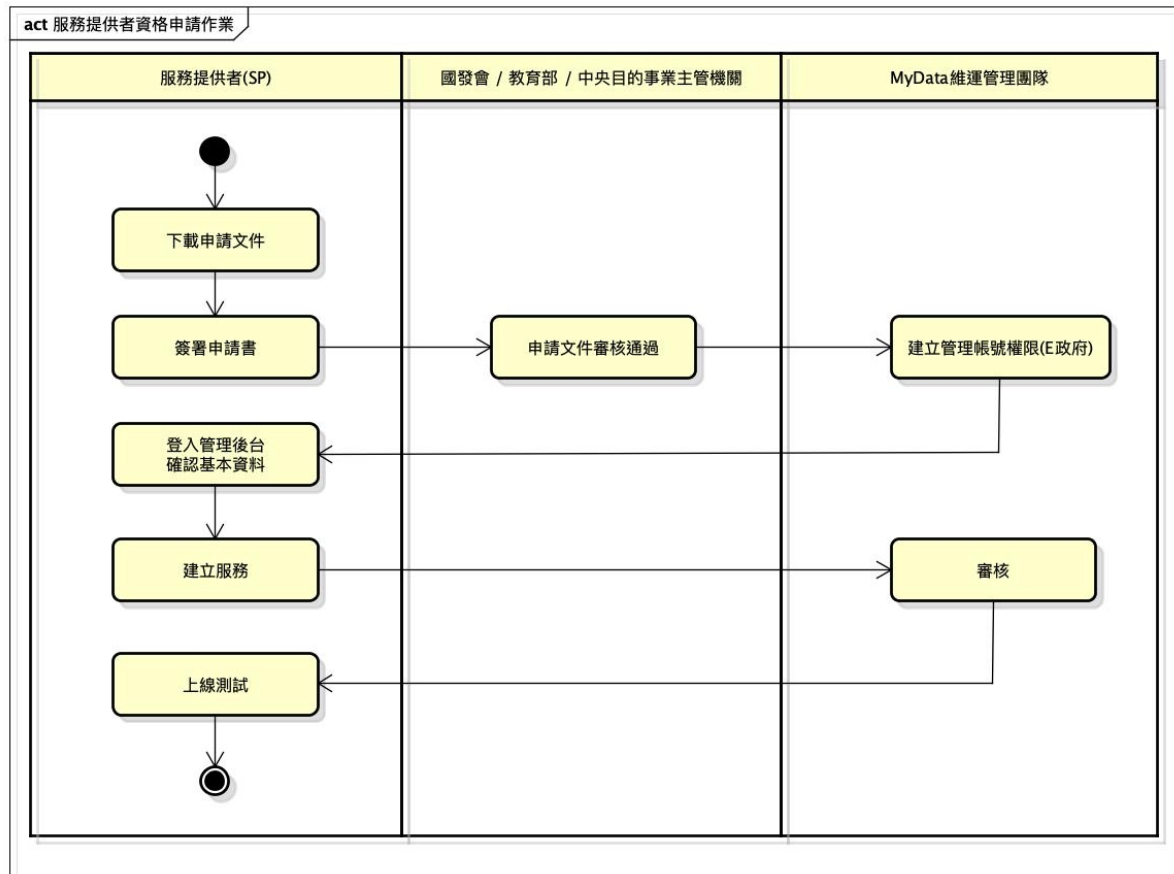
名稱	定義
OAS	共通性應用程式介面規範。
Data Provider, DP	資料提供者，存放或保管民眾個人資料之機關

	單位。
Service Provider, SP	服務提供者，提供民眾進行個人資料之加值服務機關單位。
Authorization Server, AS	授權管理者，執行身分驗證與授權管理機制，本規範之授權管理者為本會政府服務平臺 (GSP)。
Resource Owner, RO	資料擁有者/使用者，泛指用戶或民眾。
GSP	電子化政府服務平臺
OAuth 2.0	系統授權流程規範，定義於 RFC 6749 The OAuth 2.0 Authorization Framework https://tools.ietf.org/html/rfc6749
OpenID Connect	OAuth 2.0 的補充規範，強調身分驗證流程 http://openid.net/connect/
eGov 帳號	我的 E 政府提供的會員帳號
access_token	AS 發的用戶同意授權

肆、服務提供者資格申請作業

機關單位欲成為 MyData 服務提供者角色，應先完成資格申請，步驟說明如下：

步驟項次	流程內容
1	機關單位先至 GitHub 下載申請文件(https://tinyurl.com/u2kofxj) (聯絡資訊 Tel:02-86925588#5555, E-mail:mydata@ndc.gov.tw)
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
3	管理團隊建立申請人 E 政府公務帳號後台使用權限
4	機關單位申請人以「我的 E 政府」帳號(不限於公務帳號)登入管理後台並確認機關單位基本資料無誤後，使用服務提供者管理功能項目。
5	機關單位成為服務提供者，使用相關功能註冊服務。



機關單位以電話（號碼）、電子郵件（信箱）聯繫 MyData 維運團隊申辦註冊管理後台機關帳號，並於申辦時提供「機關單位名稱」及「機關單位地址」、「申請人姓名」、「聯絡電話」、「電子郵件信箱」與申請人之「我的 E 政府註冊帳號」，由 MyData 維運人員協助完成帳號註冊作業。完成機關單位註冊後，MyData 維運人員將透過註冊時機關單位提供之「聯絡電話」及「電子郵件信箱」通知機關單位聯絡人。

伍、服務提供者管理作業

一、基本資料編輯

機關單位登入管理平臺後，點選「機關單位管理」功能項目，可自行編輯機關單位基本資料，包含「聯絡人姓名」、「聯絡電話」、「聯絡 E-

mail」、「E 政府帳號」（管理後台登入使用）、「副 E 政府帳號」。於此功能頁面中，可瀏覽目前機關單位已建立之資料集與加值服務項目。

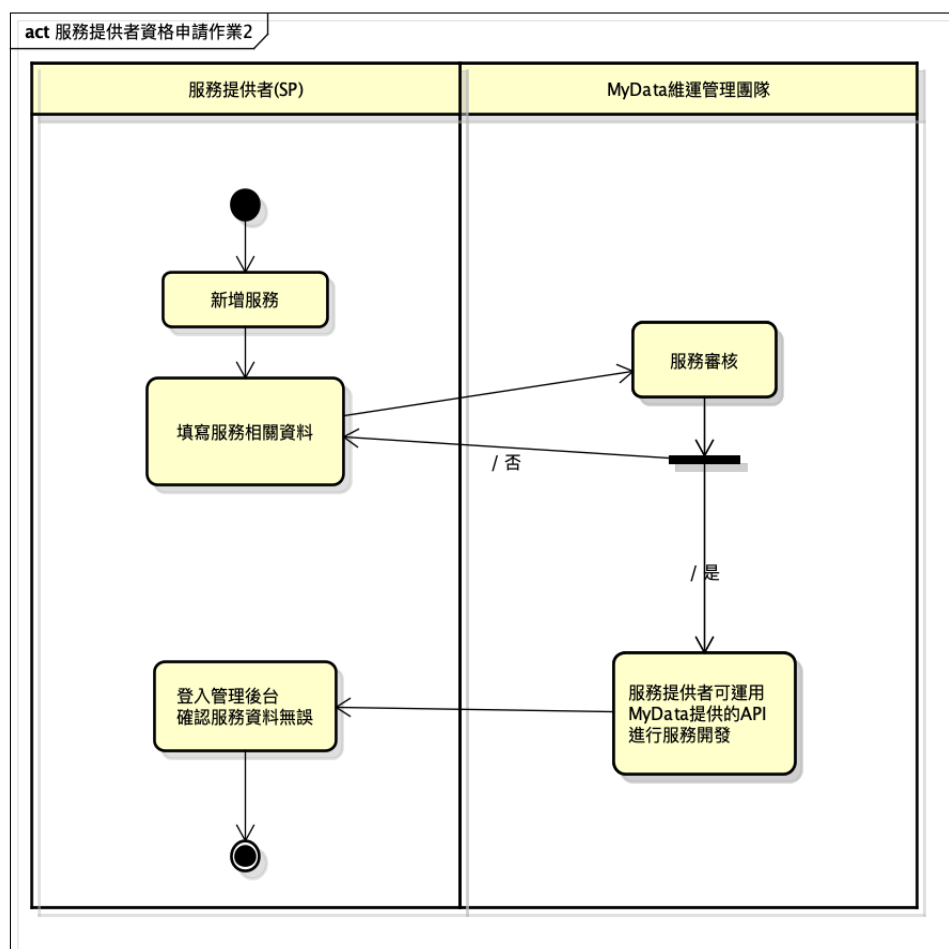
單位資訊				
申請日期：		2018-02-26		
機關單位名稱：		國家發展委員會		
機關單位地址：		臺北市中正區貴陽路3號		
* 申請人姓名：		<input type="text" value="國發會管理帳號"/>		
* 聯絡電話：		<input type="text" value="02-21927111"/>		
* 聯絡E-mail：		<input type="text" value="mydata@ndc.gov.tw"/>		
* E政府帳號：		<input type="text" value="wederlin"/>		
修改人員：		dream4825		
修改時間：		2018-02-26 00:00:00		
SP項目				
序次	建立日期	服務類別	服務名稱	狀態
1	2018-08-01	民生消費	e管家Plus個人資料運用服務	啟用
2	2019-04-23	社會福利	https://msg.nat.gov.tw	審查中
3	2019-04-23	社會福利	服務名稱4	審查中
4	2019-04-23	社會福利	服務名稱2	審查中
5	2019-04-23	社會福利	服務名稱	下架
DP項目				
序次	建立日期	資料類別	資料名稱	狀態
				<input type="button" value="取消"/> <input type="button" value="儲存"/>

機關單位登入管理平臺後，點選「服務提供者管理」功能項目，若尚未同意「服務提供者合作契約」內容，需先同意契約內容成為服務提供者身分後，即可開通服務提供者相關功能使用權限（服務新增、編輯與管理功能）。

二、服務註冊

步驟項次	流程內容
1	服務提供者使用 MyData 管理後台「新增服務」功能。
2	完成新增服務頁面中相關欄位內容，並提交審核。
3	經維運管理團隊確認相關內容符合 MyData 規範後，通知服務單位（申請人）審核通過。若審核未通過，將回覆服務單位（申請人）修正建議，服務單位依修正建議調整後可重新提交審核申請。
4	依 MyData 之技術規範完成 SP-API 開發實作及 MyData-API 整合介接工作。

新增服務	
基本資料欄位	申請日期、單位名稱、申請人姓名、聯絡電話、聯絡電子郵件信箱、服務類別、服務名稱、服務說明、client_id，上傳服務同意申請書，需求資料集、服務跳轉網址、SP-API 網址，允許連線 IP。
選填欄位	
功能動作	選擇資料集、上傳服務同意申請書、取消、送審。



編輯服務

✕

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
* 服務網址：	請輸入服務名稱
* 服務說明：	請輸入該服務簡單之說明文字
* client id：	CLi.bhkGfVPpB
* 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 加入資料欄位
* 服務跳轉網址：	服務跳轉網址
* SP-API：	請輸入服務SP-API
* 允許連線IP：	輸入IP 增加輸入IP欄位
修改人員：	wederlin

取消
送審

欄位介面示意：

欄位序號	欄位名稱	說明
1	client_id	註冊新服務時，MyData 系統會產生用以識別服務的唯一的識別值 client_id。當 SP 網站重導向至 MyData 整合網址時，須帶入 client_id 於 path parameter 中。
2	允許連線 IP	允許連線 IP 的設定用於 SP 呼叫 MyData-API 時，MyData 系統用以過濾請求來源。允許連線 IP 可以設定多筆。

三、服務管理

顯示已註冊、申請中之服務項目清單，並提供關鍵字查詢與新增、修改、刪除功能。已送審或上架之服務無法修改服務內容，服務狀態為啟用者應先完成下架申請流程。

修改服務	
基本資料欄位	申請日期、單位名稱、申請人姓名、聯絡電話、聯絡電子郵件信箱、服務類別、服務名稱、服務說明、client_id、client_secret、上傳服務同意申請書、需求資料集、服務跳轉網址、SP-API 網址，允許連線IP。
選填欄位	
功能動作	選擇資料集、上傳服務同意申請書、取消、送審、下架申請。

欄位介面示意：

編輯服務 ×

建立日期：

2018-08-01

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：

金融消費

* 服務名稱：

e管家Plus個人資料運用服務

* 服務網址：

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

* 服務說明：

國發會民生消費資料授權

* client id：

CLIU9D4iBpmZ6

* client secret：

LQoJEvgdKug20RX4

* 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 加入資料欄位
 內政部戶政司
 個人戶籍資料查詢 ✕ 親屬關係資料 ✕
 財政部財政資訊中心電子發票組
 手機條碼載具內所持有發票清單 ✕ 手機條碼載具內所持有單一發票消費明細 ✕

* 服務跳轉網址：

* SP-API：

* 允許連線IP：
 增加輸入IP欄位

修改人員： admin
 修改時間： 2019-05-16 09:48:39

下架申請 取消 送審

欄位序號	欄位名稱	說明
1	client_secret	SP 於 MyData 後台服務註冊完成後，MyData 平台才會產製此密碼字串。長度固定為 16 字元，格式為英數字含大小寫。

四、可運用的資料集

服務提供者檢視 MyData 已註冊資料提供者與資料集清單時，可使用「查詢列表／所有資料集列表」功能項目，將以清單顯示資料提供者與相對應資料集名稱，並提供依資料提供者篩選資料及 API 識別值、資料集名稱關鍵字搜尋功能。

欄位序號	欄位名稱	說明
1	resource_id	系統自動建立之識別碼
2	資料集名稱	資料提供者註冊之資料集名稱
3	SCOPE	OAuth2 資源 SCOPE 值
4	需要的身分驗證安全等級	資料集要求的授權身分驗證等級
5	資料提供機關單位名稱	資料提供者名稱

欄位介面示意：

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

所有資料集列表

搜尋:

項次	resource_id	資料集名稱	SOCPE
----	-------------	-------	-------

陸、MyData 整合協作流程說明

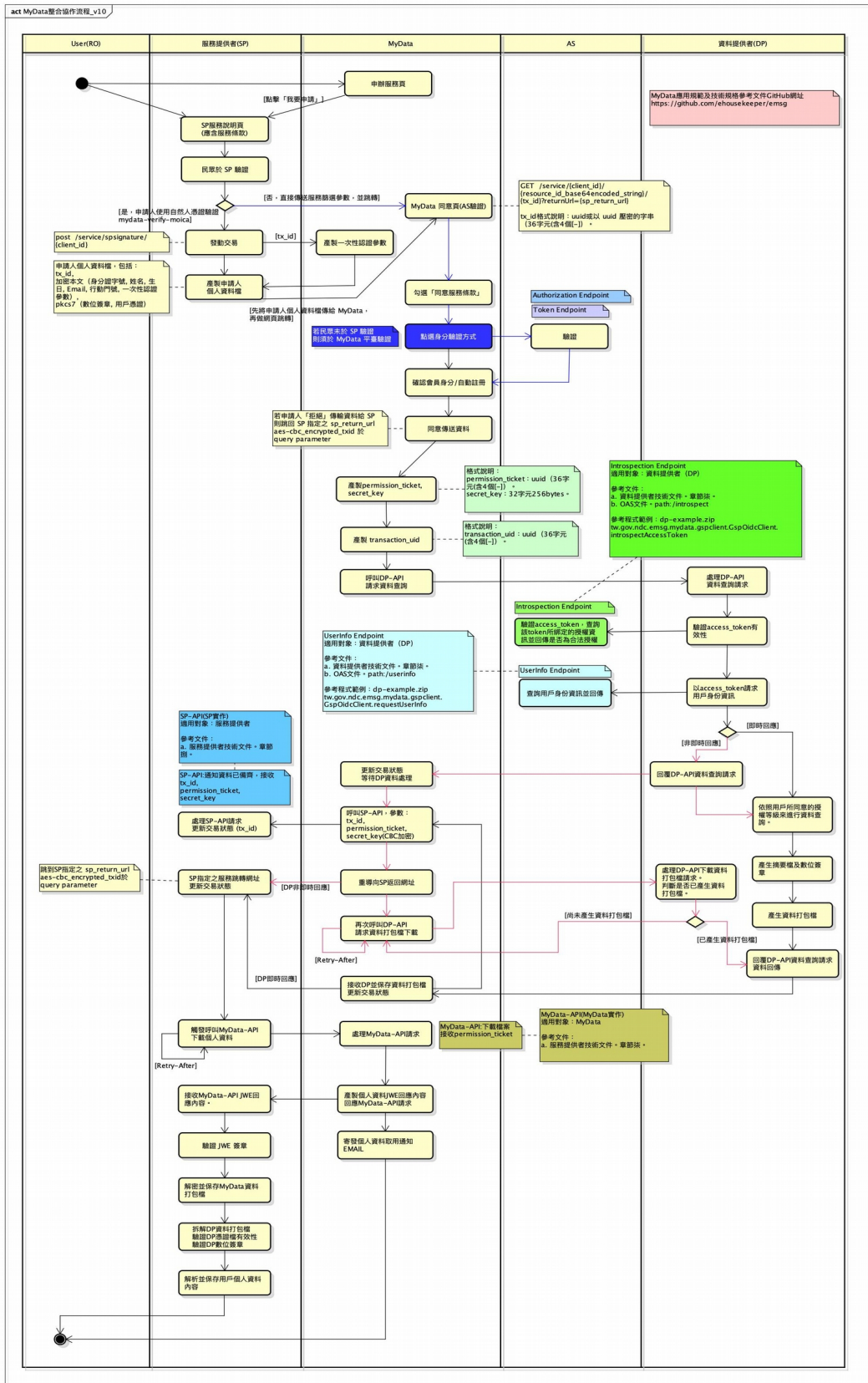
MyData 平臺的身分驗證及授權機制，採整合介接 GSP 所提供的驗證方式，民眾用戶使用個人身分證字號及生日進行驗證登入，且需同意授權 MyData 平臺向資料提供者取得用戶自己的個人資料。MyData 平臺則會將代表該用戶已同意授權的憑據 `access_token` 傳遞給資料提供者，讓資料提供者可依此向 GSP OAuth2 授權主機發出請求，以檢核用戶是否已同意授權及取得用戶資訊。

GSP OAuth2 授權主機之身分驗證及授權機制符合 OpenID Connect (OIDC) 規範。OIDC 是基於 RFC 6749 The OAuth 2.0 Authorization Framework 標準之上的一種 OAuth 2.0 協議。它使客戶端可以根據授權服務器執行的身分驗證來驗證最終用戶的身分，及以可互操作和 REST 的方式獲取有關最終用戶的基本配置文件信息。

本文件主要對象為提供資料提供者參考，為避免混淆，僅著重描述服務提供者何時請求呼叫以下 API：

- SP-API
- MyData-API

一、MyData 整合協作流程說明



註：流程說明圖檔案可至下述 Github 連結下載、瀏覽。

<https://github.com/ehousekeeper/emsg/blob/master/MyData> 服務說明、應用規範與技術文件/MyData 整合協作流程_v10.jpg

二、應用範圍

（一）規範資料集下載通知格式

服務提供者應實作資料集下載通知 API(SP-API)，此 API 為 MyData 通知有使用者允許下載的資料集打包壓縮 zip 檔，給予 permission_ticket 和 secret_key，以 permission_ticket 下載資料，並以 secret_key 解密資料檔案及驗證 JWE 簽章，內容細節請參考本文件章節「捌、SP-API Endpoint 規格說明」。

（二）資料集下載

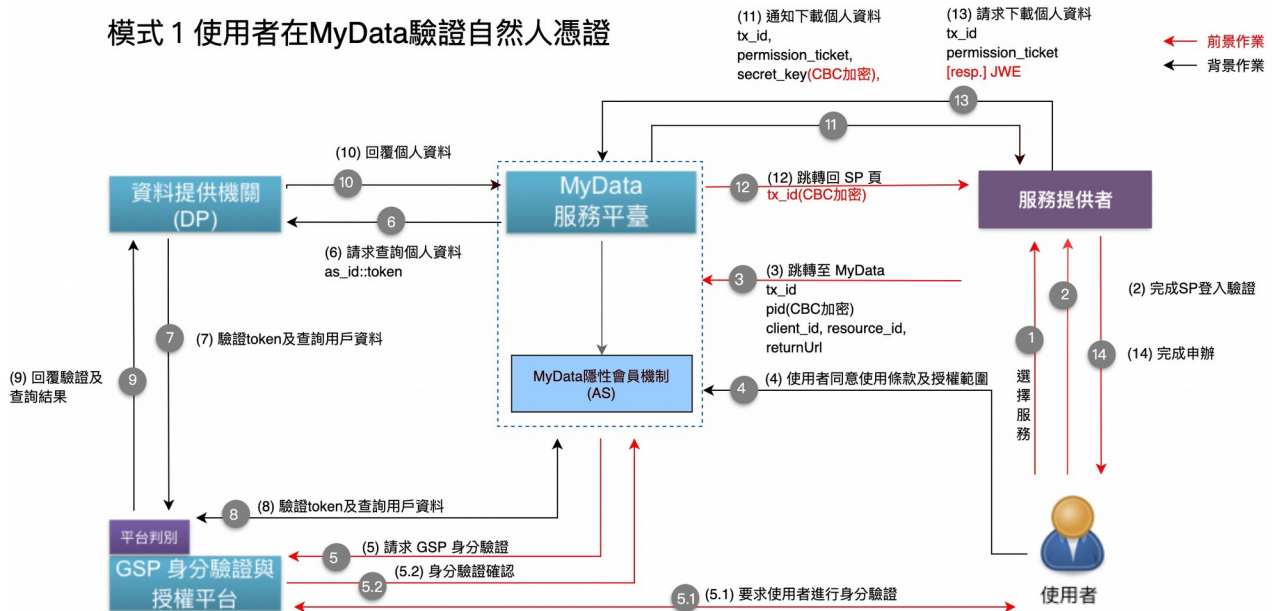
服務提供者取得用戶同意授權的資料集檔案。內容細節請參考本文件章節「玖、MyData-API Endpoint 規格說明」。

柒、MyData 整合方式說明

一、服務情境示意圖

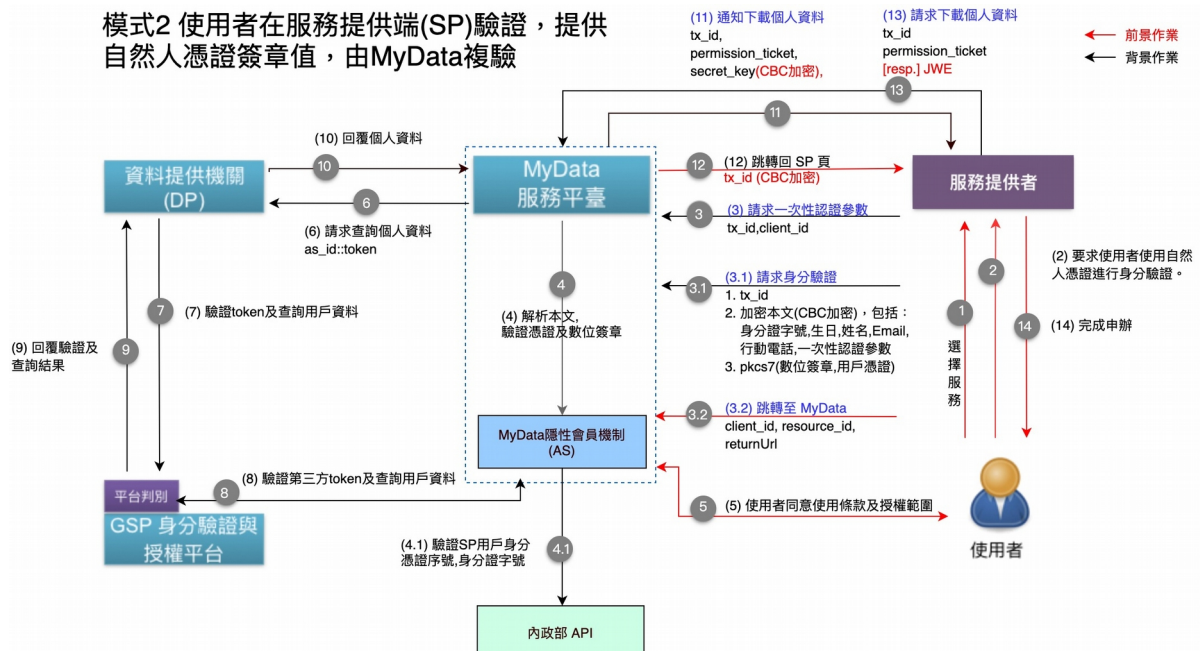
(一) 使用者在 MyData 驗證自然人憑證

模式 1 使用者在 MyData 驗證自然人憑證



(二) 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

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



二、MyData 整合網址及參數說明

(一) 使用者在 MyData 驗證自然人憑證

上述服務情境示意圖中步驟 2，由 SP 網站導向 MyData 整合網址時以 Path Parameter 帶入所需參數，若由 MyData 驗證則走此路徑，示意如下：

網址路徑：

```
GET /service/{client_id}/{resource_id_base64encoded_string}/{tx_id}?
returnUrl={sp_return_url}&pid={personalId}
HTTP/1.1 TLS 1.2
```

MyData 主機及網址資訊請參考章節「拾壹、二、系統環境主機及網址資訊」。

參數說明如下：

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。
resource_id_base64encoded_string	Base64Encode 編碼後的 DP 資料集識別值。若需多個 DP 資料集可以:符號分隔各別的資料集識別值。 示意如下： Base64Encode({resource_id1}:{resource_id2})
tx_id	SP 核發的交易識別值。 tx_id 格式為 version 4 UUID (36 字元，含 4 個 - 符號)。
sp_return_url	SP 載明，令 MyData 處理完身分認證及同意授權後，重導向回到 SP 網站的網址。 同時 SP 也須將這個返回網址登錄於 MyData 管理後臺中。MyData 會依據

	<p>管理後台中的返回網址設定來判斷此參數值是否合法。</p> <p>MyData 的判斷原則為只判斷 url path 是否相同，但不會判斷 request parameter 是否完全相同。因此 SP 可視實際需要附加其它的 request parameter，MyData 將不會移除任何 SP 原本附加的 request parameter，以方便 SP 系統後續處理。</p> <p>此參數值必須以 UriEncode 編碼處理過。</p>
personalId	<p>將用戶身分證字號以 AES/CBC/PKCS5PADDING 演算法進行加密。</p> <p>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。</p> <p>例如 client_secret 為 ToRcIGDx6hLHOdJX 則金鑰為 ToRcIGDx6hLHOdJXToRcIGDx6hLHOdJX。</p> <p>另外 CBC 加密向量值，請使用後台服務編輯頁「CBC IV」值為準，例如 q9qiPmVm2eFKWt79。</p> <p>例如用戶身分證字號為 A123456789，加密並以 Base64 編碼後為 PmGYdTqUqoBChg/fZT6UuQ==</p> <p>系統開發與測試期間，如不進行檢查，則請統一代入 A999999999 進行加密資料，待上線後皆需帶入申請人 pid，以供 MyData 進行上述比對動</p>

	作。
--	----

當 SP 令瀏覽器導向至上述 MyData 整合網址後，MyData 以 `client_id` 識別 SP 為誰，以 `resource_id_base64encoded_string` 識別 SP 欲請求的 DP 資料集有那些。

MyData 系統會檢核 SP 所請求的 DP 資料集，是否符合 SP 申請服務時所載明的 DP 資料集項目。

(二) 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

上述服務情境示意圖中步驟 3 和 3.1，由 SP 網站導向 MyData 整合網址時以 Path Parameter 帶入所需參數，示意如下：

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}
}
```

參數	說明
<code>client_id</code>	SP 於 MyData 管理後台新增服務後所得的 <code>client</code> 識別值。
<code>tx_id</code> SP 核發的交易識別值。	SP 核發的交易識別值。 <code>tx_id</code> 格式為 version 4 UUID (36 字元，含 4 個 - 符號)。

salt	MyData 產生的一次性認證參數，有效期限 15 秒。
------	------------------------------

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}
}
```

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。
tx_id	SP 核發的交易識別值。 tx_id 格式為 version 4 UUID (36 字元，含 4 個 - 符號)。
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： <pre>{ "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} }</pre>

	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。
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。

步驟 3.2 跳轉至 MyData

由 SP 網站導向 MyData 整合服務網址

GET /service/spsignature/{client_id}/{resource_id_base64encoded_string}/{tx_id}?
returnUrl={sp_return_url}
HTTP/1.1 TLS 1.2

參數	說明
clent_id	SP 於 MyData 管理後台新增服務後所得的 client 識別值。
resource_id_base64encoded_string	Base64Encode 編碼後的 DP 資料集識別值。若需多個 DP 資料集可以:符號分隔各別的資料集識別值。 示意如下： Base64Encode({resource_id1}:{resource_id2})
tx_id	SP 核發的交易識別值。 tx_id 格式為 version 4 UUID (36 字元，含 4 個 - 符號)。
sp_return_url	SP 載明，令 MyData 處理完身分認證

	<p>及同意授權後，重導向回到 SP 網站的網址。</p> <p>同時 SP 也須將這個返回網址登錄於 MyData 管理後台中。MyData 會依據管理後台中的返回網址設定來判斷此參數值是否合法。</p> <p>MyData 的判斷原則為只判斷 url path 是否相同，但不會判斷 request parameter 是否完全相同。因此 SP 可視實際需要附加其它的 request parameter，MyData 將不會移除任何 SP 原本附加的 request parameter，以方便 SP 系統後續處理。</p> <p>此參數值必須以 UriEncode 編碼處理過。</p>
--	---

三、正常返回 SP 網址之處理方式說明

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

當 MyData 處理完成 SP 請求後，會重導向回到 SP 指定的返回網址，並將 SP 核發的 tx_id 值以 query parameter 的方式夾帶於返回網址參數中，以利 SP 識別交易。

參數說明如下：

參數	說明
sp_return_url	SP 載明，令 MyData 處理完身分認證及同意授權

	<p>後，重導向回到 SP 網站的網址。</p> <p>同時 SP 也須將這個返回網址登錄於 MyData 管理後台中。MyData 會依據管理後台中的返回網址設定來判斷此參數值是否合法。</p> <p>MyData 的判斷原則為只判斷 url path 是否相同，但不會判斷 request parameter 是否完全相同。因此 SP 可視實際需要附加其它的 request parameter，MyData 將不會移除任何 SP 原本附加的 request parameter，以方便 SP 系統後續處理。</p> <p>sp_return_url 必須以 UriEncode 編碼處理過。</p>
code	HTTP 狀態碼。
aes-cbc_encrypted_txid	<p>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。</p> <p>加密向量值，請使用後台服務編輯頁「CBC IV」值為準。</p>
sp_param_key	用於示意表示 SP 原本附加的參數，MyData 將原值返回。

四、異常返回 SP 網址之處理方式說明

當 MyData 無法處理或拒絕處理來自 SP 的請求，或發現參數檢核失敗時，MyData 會將異常狀態碼，以 code 參數附加於 sp_return_url 網址上重導向回 SP 網站，以利 SP 後續處理作業。

網址示意如下：

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

參數	說明
sp_return_url	<p>SP 載明，令 MyData 處理完身分認證及同意授權後，重導向回到 SP 網站的網址。</p> <p>同時 SP 也須將這個返回網址登錄於 MyData 管理後台中。MyData 會依據管理後台中的返回網址設定來判斷此參數值是否合法。</p> <p>MyData 的判斷原則為只判斷 url path 是否相同，但不會判斷 request parameter 是否完全相同。因此 SP 可視實際需要附加其它的 request parameter，MyData 將不會移除任何 SP 原本附加的 request parameter，以方便 SP 系統後續處理。</p> <p>sp_return_url 必須以 UriEncode 編碼處理過。</p>
code	<p>HTTP 狀態碼，完整狀態碼與說明可參考「附錄、HTTP 狀態碼」。</p> <ul style="list-style-type: none"> • 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。

	<ul style="list-style-type: none"> • 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。
aes-cbc_encrypted_txid	<p>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。</p> <p>加密向量值，請使用後台服務編輯頁「CBC IV」值為準。</p>
sp_param_key	用於示意表示 SP 原本附加的參數，MyData 將原值返回。

五、無法返回 SP 網址之處理方式說明

若因網路問題或其它不可控因素，導致 MyData 無法令瀏覽器於 SP 跳轉至 MyData 的 20 分鐘內順利返回 SP 網址時，SP 須視該交易為無效交易。

捌、SP-API Endpoint 規格說明

一、系統環境與條件

API endpoint 以 RESTful Service 方式提供介面，且皆基於 TLS v1.2 以上提供加密傳輸管道。

二、SP-API 請求及回覆規格說明(由服務提供者實作)

服務提供者必須實作 API，以接收 MyData 平臺傳送來的，使用者於平臺授權資料的加密鍵值。以利後續服務端抓取資料及將資料解密使用。

(一) MyData 發出請求 - 告知 SP 準備來提取資料檔

如 MyData 第一次發出請求後未收到 SP 回應，將等待 1 分鐘後重發第二次。如仍無回應，將等待 5 分鐘後重發第三次。如仍無回應，

將等待 15 分鐘後重發第四次。如第四次仍無回應，則視為失敗。

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: {aes-cbc_encrypted_secret_key}
}
```

欄位說明：

欄位	說明
tx_id	SP 核發的交易識別值。 tx_id 格式為 version 4 UUID (36 字元，含 4 個 - 符號)。
permission_ticket	MyData 核發，代表該次用戶同意授權的交易識別碼。 格式為 version 4 UUID 字符串。 單次有效且唯一不重覆。 有效時間最長 8 小時。
secret_key	只於該次交易有效的金鑰。隨機產生的英數字含大小寫的字符串，長度為 256bit, 32bytes。 產製 JWE 簽章時使用的金鑰。 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。

(二) MyData 發出請求 - 告知 SP 無法給予資料檔

欄位說明：

欄位	說明
tx_id	SP 核發的交易識別值。 tx_id 格式為 version 4 UUID (36 字元，含 4 個 - 符號)。
permission_ticket	MyData 核發，代表該次用戶同意授權的交易識別碼。 格式為 version 4 UUID 字符串。 單次有效且唯一不重覆。 有效時間最長 8 小時。
unable_to_deliver	MyData 已確認無法取得的 DP 資料集。 例：若該次交易 SP 請求的 DP 資料集共有 3 個，但只有其中 1 個已確定無法傳遞時，此欄位值只會載明已確定無法傳遞的 DP 資料集識別值共 1 個，但仍會以陣列的方式表述。

當 SP 請求的 DP 資料集中有任何一個資料集無法順利傳遞時，MyData 即視為該筆交易為失敗。

當以下情況發生時，MyData 將無順利傳遞 DP 資料集予 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 發出請求失敗。

(三) SP 回覆請求成功

HTTP/1.1 TLS 1.2 200 OK

Content-Type: application/json

(四) 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。

HTTP 狀態碼	說明
403	拒絕存取。

完整狀態碼與說明可參考「附錄、HTTP 狀態碼」。

玖、MyData-API Endpoint 規格說明

一、系統環境與條件

API endpoint 以 RESTful Service 方式提供介面，且皆基於 TLS v1.2 以上提供加密傳輸管道。

MyData 主機及網址資訊請參考章節「拾壹、二、系統環境主機及網址資訊」。

二、MyData-API 請求及回覆規格說明

(一) SP 發出請求

網址路徑：

GET /v1/service/data
HTTP/1.1 TLS 1.2
Content-Type: application/json
permission_ticket: {permission_ticket}

參數說明：

參數	說明
permission_ticket	代表該次用戶同意授權的交易識別碼。 格式為 version 4 UUID 字符串。

	單次有效且唯一不重覆。 有效時間最長 8 小時。
--	-----------------------------

(二) MyData 回覆請求成功 - 即時回應

HTTP/1.1 TLS 1.2 200 OK
Content-Type: application/jwe

請求回覆內容格式為 JWE，請參考章節「玖、三、MyData-API 的回傳格式與加簽機制說明」。

(三) MyData 回覆請求成功 - 等候處理

HTTP/1.1 TLS 1.2 429 Too Many Requests
Content-Type: application/jwe
Retry-After: {delay_seconds}

若 MyData-API 不能即時回應請求，則以 HTTP 429 回應。

參數說明：

參數	說明
delay_seconds	下次發動請求前需等待的秒數。

(四) MyData 回覆請求失敗

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

HTTP 狀態碼	說明
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 (permission_ticket) 不存在。

408	交易逾時。若跳轉至 MyData 超過 20 分鐘未完成交易，則視為 交易逾時，MyData 前臺頁面會顯示需要「重新申辦」的提醒，若民眾「重新申辦」，則回傳此狀態碼。 • permissoin_ticket 最長效期為 8 小時。
504	SP 請求的 DP 資料集之系統異常，無法傳送 DP 資料集。

完整狀態碼與說明可參考「附錄、HTTP 狀態碼」。

三、MyData-API 的回傳格式說明

MyData-API 的回傳格式為 JWE (JSON Web Encryption)，規範為 RFC7516 (<https://tools.ietf.org/html/rfc7516>)，序列化方式採用 JWE Compact Serialization，封裝內容加密金鑰 (Content Encryption Key, CEK) 使用 A256KW (AES Key Wrap using 256-bit key) 演算法，加密內容使用 A256CBC-HS512 (AES_256_CBC_HMAC_SHA_512) 演算法，說明如下。

(一) JWE 格式說明

JWE 格式為

「header.encrypted_key.initialization_vector.ciphertext.authentication_tag」，五段資料以「.」隔開，每段資料皆以 Base64Url 編碼處理，範例如下：


```

eyJhbGciOiJBbmJU2S1ciLCJlbmMiOiJBbmJU2Q0JDLUhTNTEyIn0
.
1-
mJQl42l08E3mz6Zac4OlHsNDXxz7g6DoAmJqayHmmeVIUliN hLMYS5kjWAKPl7L
rsFZ0pmdFVqfC77688Mdfni0Xgu4PST
.
SHR6R1k3ZzFoTHk1Ymw5Ug
.
LMz7XIhl2p6FPQwXfHAhb0yZ7YjgjPsLXzR6J96Lxzc-
z0G3dR5P5_MB_NBQmumD7exefh2GpXjCvwl277CD5htL7XzJbdZLIqOwp1Ymh
g
.
C7iWNo6BVCpamm3KlpuPxJYgCkcCh1QcTc8BzDKD3Sw

```

註：為方便閱讀，本文件以分段如上述，開發人員測試時，須移除跳行符號。

此範例所使用的參數為

```
secret_key = dgFpgO7FhNF15UJsOB1xmCjwwWw3SO6D
```

```
IV = HtzGY7g1hLy5bl9R
```

(1) header

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

Base64Url 編碼前的 header 示意如下：

```

{
  "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。

(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:XsdfasCSFD SADFASVcxv"
}
```

(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。

(二) 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);

```

(三) 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。

(四) 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 lvParameterSpec(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。

(五) 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>

四、MyData-API 的資料打包檔規格說明

由於服務提供者一次請求的用戶個人資料可能來自於多個不同的資料提供者，為了簡化 MyData 平臺與服務提供者之間傳遞資料的機制，MyData 平臺希望將來自於多個不同的資料提供者的資料檔案，打包成為一個壓縮 zip 檔案後再傳遞給服務提供者，因此 MyData 平臺規範了資料提供者檔案的打包規則，也同時規範了資料提供者檔案的打包規則，藉此達成讓服務提供者有一致性的檔案處理規則及做法。

(一) MyData 資料打包檔規格要點如下：

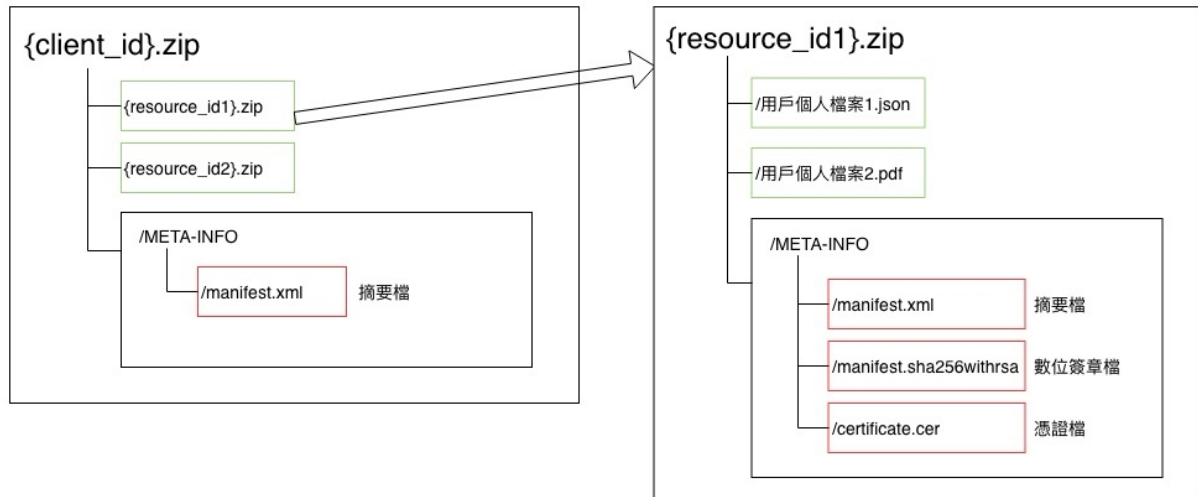
1. MyData 資料打包檔格式為壓縮 zip 檔。
2. zip 檔的檔名為 {client_id}.zip。client_id 是變數，代表服務的識別代碼。
3. zip 檔中包含來自各資料提供者的資料打包檔，檔案格式為壓縮 zip 檔，檔名為 {resource_id}.zip，resource_id 是變數，代表資料集的識別代碼。
4. zip 檔中包含 META-INFO 的子目錄。
5. META-INFO 目錄中，包含 manifest.xml 摘要檔。

(二) manifest.xml 摘要檔格式說明如下：

```
<?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 1</resource_name>
    <code>200</code>
  </file>
  <file>
    <filename>{resource_id2}.zip</filename>
    <resource_id>{resource_id}</resource_id>
    <resource_name> 資料集中文名稱 2</resource_name>
    <code>204</code>
  </file>
</files>
```

參數	說明
filename	MyData 收到下載資料集檔案名稱。
resource_id	MyData 收到下載資料集鍵值。
resource_name	MyData 收到下載資料集中文名稱。
code	檔案處理狀態。 200：正常 204：查無使用者資料(封裝內無檔案)

(三) MyData 資料打包檔目錄結構示意如下



五、資料提供者的 **DP** 資料打包檔規格說明

為了使 MyData 的應用更加廣泛，同一份資料可能提供多種格式，包括機器可讀的格式，如：json, csv, xml 等，以及易於人讀的格式，如：以申請人身分證字號加密的 pdf 等。此外也包括了保證資料未經竄改的數位簽章檔，及為了方便服務提供者進行驗簽的憑證檔。

為了簡化 MyData 平臺與資料提供者(DP)之間傳遞資料的機制，MyData 平臺希望資料提供者可以將同一份資料的多個檔案打包成為一個壓縮 zip 檔案後再傳遞給 MyData 平臺，因此 MyData 平臺規範了用戶個人資料檔案的打包規則，同時也使服務提供者在處理來自不同資料提供者的檔案時，可以有一致性的處理規則及做法。

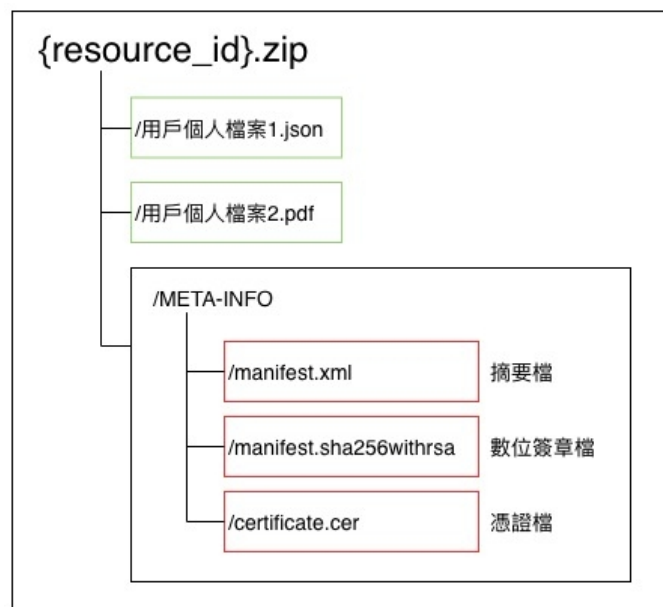
(一) DP 資料打包檔案規格要點如下：

1. DP 資料打包檔格式為壓縮 zip 檔。
2. zip 檔的檔名非限定但建議為 {resource_id}.zip。resource_id 是變數，代表資料集的識別代碼。
3. zip 檔中可能包含多個個人資料檔案，依資料提供者規範需包含的檔案用途、數量、檔名、副檔名等。
4. 如提供數位簽章，則包含於 META-INFO 子目錄。

5. 承上，META-INFO 子目錄中包含檔案：

- manifest.xml 摘要檔
- manifest.sha256withrsa 數位簽章檔
- certificate.cer 憑證檔

(二) DP 資料打包檔案目錄結構示意如下：



(三) META-INFO 目錄及內含檔案說明：

META-INFO 目錄下放置摘要檔、數位簽章檔及憑證檔。若 DP 沒有產製數位簽章，則不會產生 META-INFO 子目錄。

manifest.xml：

針對各別的資料檔案，以 SHA256 演算法，演算出的數位指紋（摘要值）後載明於 manifest.xml 檔案中。

內容格式示意如下：

manifest.sha256withrsa :

```
<?xml version="1.0" encoding="UTF-8"?>
<files>
  <file>
    <filename> 用戶個人資料檔案 1.json</filename>
    <digest> {digest value}</digest>
  </file>
  <file>
    <filename> 用戶個人資料檔案 2.pdf</filename>
    <digest> {digest value}</digest>
  </file>
</files>
```

以 SHA256 演算出 manifest.xml 的數位指紋後，以 DP 的 RSA 私鑰進行加密演算後所得的二進位內容，以副檔名 sha256withrsa 來示意所使用的演算機制為 SHA256withRSA。

certificate.cer :

憑證檔。PEM 格式的憑證資訊。PEM 格式的檔案是 ASCII (base64) 檔案，內容包含前置及後置文字，如下示意：

```
-----BEGIN CERTIFICATE-----
MIID/
zCCAuegAwIBAgIJAMhtYm3fde9AMA0GCSqGSIb3DQEBCwUAMIGVMQswCQYD
-----END CERTIFICATE-----
```

六、驗證 DP 資料檔案沒有被竄改的方法說明**(一) 驗證憑證檔的有效性**

服務提供者可向簽發憑證的 CA 驗證憑證有效性。原則上會建議 DP 向 GCA 政府憑證管理中心來申請數位簽章用的憑證。

GCA 支援兩種驗證憑證有效性的方法，包括：CRL 及 OCSP。

（二）憑證檔中取出 DP 公鑰

DP 夾帶的憑證檔為 PEM 格式，SP 須從憑證檔中取出 DP 公鑰，用於後續驗證數位簽章檔案 manifest.sha256withrsa。

（三）驗證 manifest.xml 沒有被竄改

manifest.xml 檔案中載明了各別資料檔案的數位指紋（摘要值）。因此先驗證 manifest.xml 沒有被竄改，即代表 manifest.xml 檔中所載明的摘要值沒有被竄改。

manifest.sha256withrsa 是針對 manifest.xml 所做出來的數位簽章檔，SP 須以 DP 的公鑰對 manifest.sha256withrsa 進行解密後，可得到正確的 manifest.xml 的摘要值。

SP 對 manifest.xml 進行 SHA256 演算後，比較前後兩者摘要值是否相符，若相符則代表 manifest.xml 沒有被竄改。

（四）驗證各別的資料檔案沒有被竄改

SP 讀取 manifest.xml 內容後，得到各別資料檔案的正確的摘要值，再針對各別資料檔進行 SHA256 演算後，比較前後兩者摘要值是否相符，若相符則代表該資料檔案沒有被竄改。

拾、資料查核相關網頁與 API

一、第三方身分驗證中心日誌查詢

流程：民眾 → SP 服務網頁 → 透過 TWID 登入驗證 → 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	<p>第三方身分驗證中心核發的 access_token</p> <p>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。</p> <p>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。</p>

二、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}

tx_id: {tx_id}

參數說明：

參數	說明
tx_id	<p>SP 核發的交易識別值。</p> <p>tx_id 格式為 version 4 UUID (36 字元，含 4 個 - 符號)。</p>

(二) 驗證憑證檔的有效性

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：T-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

(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。拒絕存取。參數 (tx_id 或 permission_ticket) 不存在。
408	交易逾時。若跳轉至 MyData 超過 20 分鐘未完成交易，則視為 交易逾時，MyData 前臺頁面會顯示需要「重新申辦」的提醒，若民眾「重新申辦」，則回傳此狀態碼。permissoin_ticket 最長效期為 8 小時。

完整狀態碼與說明可參考「附錄、HTTP 狀態碼」。

三、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}
```

參數說明：

參數	說明
tx_id	SP 核發的交易識別值。 tx_id 格式為 version 4 UUID (36 字元，含 4 個 - 符號)。

（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}"}
```

參數	說明
code	HTTP 狀態碼，完整狀態碼與說明可參考「附錄、HTTP 狀態碼」。 <ul style="list-style-type: none"> 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

	<p>下載失敗[API.xxxxxxx]。</p> <ul style="list-style-type: none"> • 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。
text	顯示 code 的說明。

(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。

完整狀態碼與說明可參考「附錄、HTTP 狀態碼」。

四、交易 Log 日誌查詢

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，說明如下。

#	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	
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		V	V

		資料			
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

(一) SP 請求交易日誌

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：

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。

(二) 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。

完整狀態碼與說明可參考「附錄、HTTP 狀態碼」。

拾壹、SP-API 與 MyData-API 測試流程說明

一、測試流程

SP 需完成申請流程才能進行測試，申請方式請參考章節「肆、服務提供者資格申請作業」。

SP 服務測試流程同本文件所註明流程，唯操作路徑在測試機後臺。當 SP 通過申請並完成 SP-API 開發，即可在測試環境取得 MyData 提供的測試用資料，並進行身分驗證、資料實作相關解密、解簽流程測試。

其中，測試環境虛擬資料集的 PDF 開啟密碼固定為 A999999999。

二、系統環境主機及網址資訊

提供主機及網址資訊如下，以利 SP 進行防火牆設定及測試工作。

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 MyData-API 網址	https://mydata.nat.gov.tw/service/data
正式機後臺登入網址	https://mydata.nat.gov.tw/mydata-backend
正式機前臺首頁網址	https://mydata.nat.gov.tw
測試機 IP	117.56.91.143
測試機 MyData-API 網址	https://mydatadev.nat.gov.tw/mydata/service/data
測試機後臺登入網址	https://mydatadev.nat.gov.tw/mydata-backend
測試機前臺首頁網址	https://mydatadev.nat.gov.tw/mydata

附錄、HTTP 狀態碼

為方便查找，將通用狀態碼列於此處，若有狀態碼有特殊涵義，將直接補充於該 API 章節。

HTTP 狀態碼	說明
200	執行成功。資料準備完成。
201	SP 已取用資料。
205	User 不同意傳送資料給 SP。
400	參數格式或內容不正確，或是缺少必要參數。 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, client_id, permission_ticket 或 salt) 不存在。 部分資料集下載失敗[API.xxxxxxx]。
404	無效的路徑。 sp_return_url 不符合 MyData 管理後台中所登錄的設定。
408	交易逾時或交易未完成，可能原因如下： <ul style="list-style-type: none"> • 一次性認證參數(salt)的有效期限為 15 秒。 • SP 請求一次性認證參數至跳轉到 MyData 限時 600 秒。 • 若跳轉至 MyData 超過 20 分鐘未完成交易，則視為交易逾時，MyData 前臺頁面會顯示需要「重新申辦」的提醒，若民眾「重新申辦」，則回傳此狀態碼。 • permissoin_ticket 最長效期為 8 小時。
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。
429	MyData 資料準備中
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。