數位服務個人化

服務提供者技術文件

V2.7

國家發展委員會
中華民國 109 年 06 月

版本修正紀錄

項次	版本	時間	修正內容	頁次
1	2.0	109/2/18	更新章節「陸、一、MyData 整合協作流程說明」之流程圖。	P7
			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。	P9
			調整章節「捌、二、(一) MyData 發出請求 – 告知 SP 準備來捉取資料檔」之內容，將 secret_key 以 AES/CBC 加密。	P19
			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。	P24
			調整章節「拾、二、Type-Valid」之內容，將請求參數增加 tx_id，並新增 TW FidO 驗證代號。	P33
			調整章節「拾、三、Txid-Status」之狀態碼。	P35
			新增章節「拾、四、交易 Log 日誌查詢」之狀態碼。	P37
			更新各 API 狀態碼，並新增「附錄、HTTP 狀態碼總表」，以方便查找。	P43
2	2.1	109/2/24	調整章節「陸、MyData 整合協作流程說明」之內容文字。	P6
			更新章節「柒、MyData 整合方式說明」子標題之文字。	P9
			更新章節「玖、三、（一）JWE 格式說明」之範例。	P24

項次	版本	時間	修正內容	頁次
			更新章節「拾壹、一、測試流程」之內容。	P41
3	2.2	109/3/30	調整章節「參、名詞定義」之說明。	P1
			調整章節「陸、MyData 整合協作方式」之內容。	P6
			調整章節「柒、二、（一）使用者在 MyData 驗證自然人憑證」，MyData 每次皆會檢查 personalId 規格的正確性。	P10
			調整章節「拾壹、二、系統環境主機及網址資訊」，新增正式機 IP。	-
4	2.3	109/4/17	調整章節「捌、二、（二）MyData 發出請求 – 告知 SP 無法給予資料檔」之說明。	P20
			新增章節「玖、MyData-API Endpoint 規格說明」之狀態碼與說明。	P22
5	2.4	109/4/27	調整章節「貳、如何成為服務提供者」之內容。	P1
			調整章節「肆、服務提供者資格申請作業」之內容。	P2
			調整章節「伍、服務提供者管理作業」之內容。	P3
			調整章節「玖、四、（二）manifest.xml 摘要檔格式說明」之內容。	P28
6	2.5	109/5/18	調整章節「捌、二、SP-API 請求及回覆規格說明(由服務提供者實作)」之內容。	P19
			調整章節「玖、四、（二）manifest.xml 摘要檔格式說明」之內容。	P28
			更新章節「拾壹、一、測試流程」之內容。	P41
			調整章節「拾壹、二、系統環境主機及網址資訊」之內容，新增試營運環境連線資訊。	-
7	2.6	109/06/15	修正客服電話	P2
			移除「拾貳、二、系統環境主機及網址資訊」之內容	-

項次	版本	時間	修正內容	頁次
			修正文件頁碼	-
8	2.7	109/06/30	新增章節「伍、二、新增服務」RSA	P4
			修正文件描述文字	-
			新增「附錄 2 工作事項檢核表」	P45

目錄

壹、目的

本文件主要描述「MyData 平臺之服務提供者」應依循之作業流程、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、實作 SP-API 開發，提供予 MyData 平臺介接

服務提供者須提供 SP-API Endpoint，MyData 平臺將於用戶同意傳輸資料後，利用此 SP-API Endpoint，將 permission_ticket 及 secret_key 傳送予服務提供者。

三、實作 MyData-API 之系統整合介接

MyData 平臺提供 MyData-API Endpoint，讓服務提供者透過此 API 取得該服務所需的用戶個人資料打包檔案。MyData-API
回應格式是 JWE，用戶個人資料打包檔案即封裝於 JWE 中。
因此服務提供者須先了解 MyData-API 及資料打包檔的相關規格與解析方式，以完成 MyData-API 的整合介接工作。

參、名詞定義

名稱	定義
OAS	國家發展委員會所發佈之「共通性應用程式介面規範（OAS）」 https://theme.ndc.gov.tw/lawout/Download.ashx?FileID=1438
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

名稱	定義
Resource Owner, RO	資料擁有者/使用者，泛指用戶或民眾
access_token	AS 核發的授權 token

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	機關單位以資料提供者介接申請表提出 MyData 註冊管理後臺使用權限申請。（聯絡資訊 Tel:02-8643-3520, E-mail: mydata@ndc.gov.tw），可至下述 Github 連結下載相關文件(https://github.com/ehousekeeper/emsg)。
2	管理團隊回覆機關單位申請需求，增加機關單位申請人之「我的 E 政府」帳號登入註冊管理後臺之權限。
3	機關單位申請人以「我的 E 政府」帳號登入註冊管理後臺並確認機關單位基本資料無誤。

機關單位申辦時須確實填寫申請表，並依介接作業試辦要點提出申請作業後，由 MyData 維運團隊依據介接申請表內容登錄帳號與服務內容建置作業。完成後，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」、「副E政府帳號」(管理後臺登入使用）。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。

二、新增服務

步驟項次	流程內容
1	服務提供者提供「服務提供者介接申請表」。
2	維運管理團隊依據「服務提供者介接申請表」內容建立服務。
3	通知機關單位（申請人）確認服務內容是否建立正確。
4	待服務提供者依技術文件說明之介接方式完成服務介接作業。

服務內容欄位說明

欄位序號	欄位名稱	說明
1	client_id	於 MyData 後臺新增服務後，由系統產生的服務識別鍵值
2	client_secret	於 MyData 後臺新增服務後，由系統產生的密碼字串。長度固定為 16 字元，格式為英數字含大小寫。
3	使用 RSA Public Key 加密 client_secret	非必要。此欄位用以控制後臺瀏覽時是否將 client_secret 進行加密顯示。如需使用，完成申請後請登入後臺上傳憑證。 RSA 為 SP 符合 X.509 的憑證，憑證內須含公鑰，無格式或長度限定。

三、服務列表

顯示已註冊、申請中之服務項目清單，並提供關鍵字查詢與狀態顯示功能。

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
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：

陸、MyData 整合協作流程說明

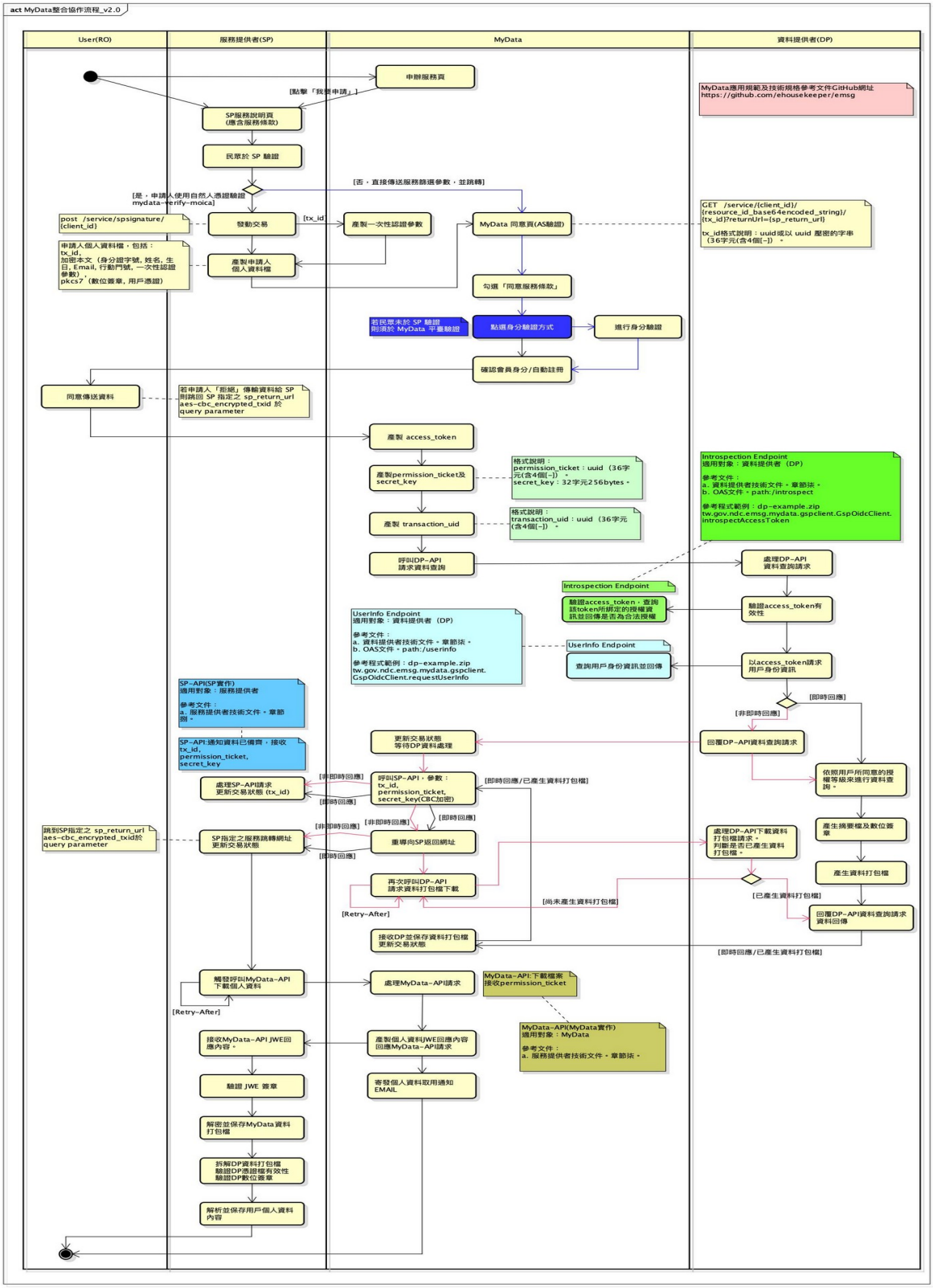
MyData 平臺提供多元身分驗證方式，包括：自然人憑證、健保卡...等；並以用戶的個人身分證字號+生日做為用戶會員的依據。

MyData 平臺經民眾同意並完成身分驗證後，得向資料提供者請求用戶自己的個人資料。

本文件主要對象為提供服務提供者參考，故僅著重描述服務提供者應如何呼叫以下 API：

- SP-API：通知並傳遞交易用之交易鍵值與金鑰
- MyData-API：取得用戶個人資料檔

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_V2.0.jpg

二、SP-API 與 MyData API 應用範圍

（一）SP-API：通知並傳遞交易用之交易鍵值與金鑰

當用戶完成身分驗證，並點擊「同意傳送」資料給 SP 時，MyData 會以 SP-API 告知 SP 需等候多久才能取得檔案，並同時將 permission_ticket 和 secret_key 提供給 SP；SP 須以 permission_ticket 取用資料，並以 secret_key 解密資料檔案及驗證 JWE 簽章。

請參閱章節「捌、SP-API Endpoint 規格說明」與「玖、MyData-API Endpoint 規格說明」。

（二）MyData-API：取得用戶個人資料檔

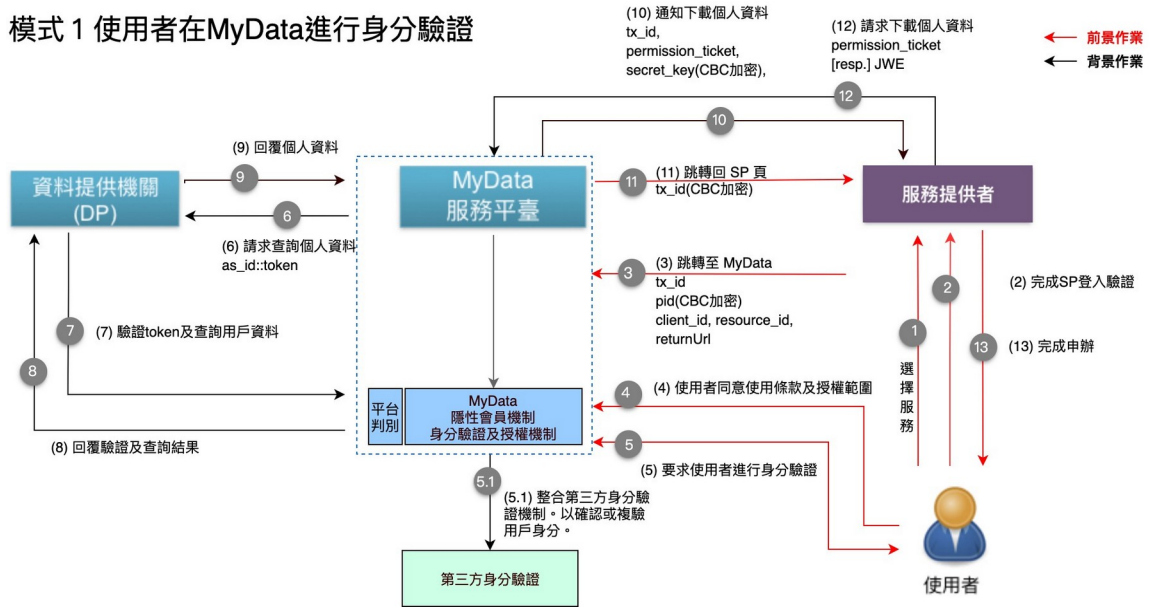
SP 於指定的等待時間後，透過 MyData-API 取得個人資料檔，並進行相關驗簽、與解密動作。

請參閱章節「玖、MyData-API Endpoint 規格說明」。

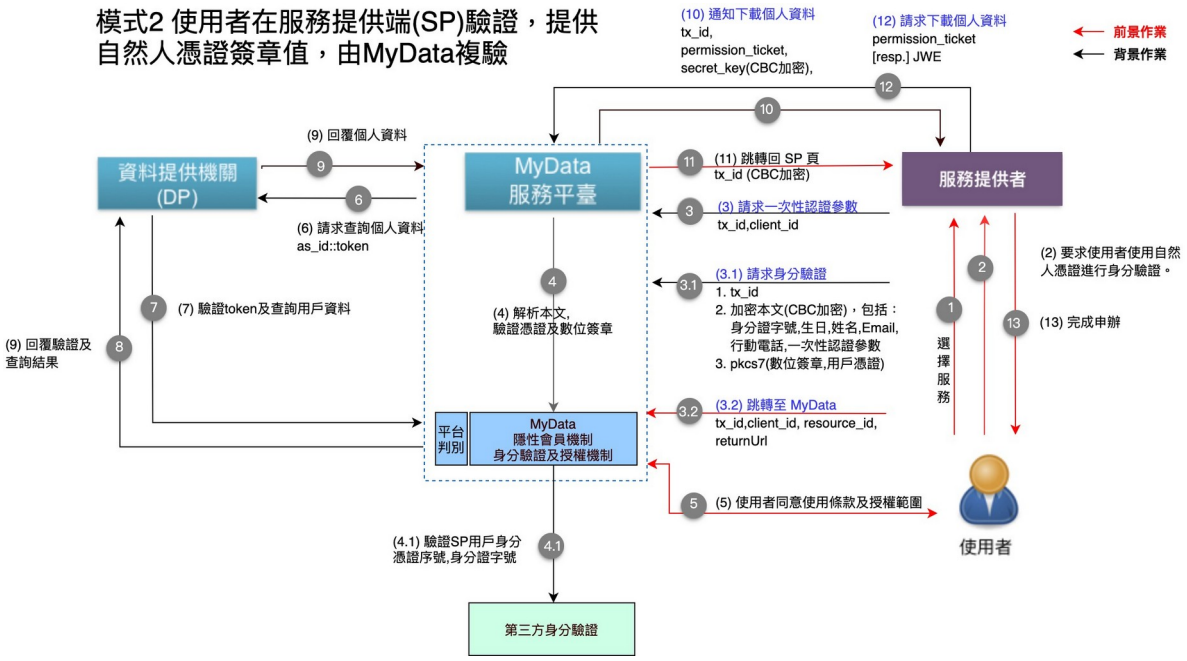
柒、MyData 整合方式說明

一、服務情境示意圖

（一）使用者在 MyData 進行身分驗證



（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



二、MyData 整合網址及參數說明

（一）使用者在 MyData 驗證自然人憑證

在上述服務情境示意圖中的步驟 3，用戶從 SP 網站導向 MyData 平臺的同意頁時，在整合網址列，會出現下列參數：

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
```

參數/欄位說明：

參數/欄位	說明
client_id	於 MyData 後臺新增服務後，由系統產生的服務識別鍵值
resource_id_base64encoded_string	resource_id 為系統自動建立之識別碼 resource_id_base64encoded_string 則是將 resource_id 以 base64Encode 編碼後的結果 如果 SP 服務需多個資料集，可以:符號分隔各別的資料集識別碼，示意如下： Base64Encode({resource_id1}:{resource_id2}) MyData 系統會檢核 SP 所請求的資料集，是否符合 SP 申請服務時，介接申請單上所載明的資料集項目
tx_id	由 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）

參數/欄位	說明
sp_return_url	由 SP 指定的，用戶從 MyData 點選「同意傳送」後，重導至 SP 網站完成服務的指定網址 此參數值必須以 UrlEncode 編碼處理過，並須與後臺登錄的服務跳轉網址一致 MyData 系統僅會判斷 url path 是否相同， 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，以便 SP 進行後續處理
personalId	personalId 為將用戶身分證字號以 AES/CBC/PKCS5PADDING 演算法加密後的值 AES 加密的金鑰，為 SP 的 client_secret 合併 2 次（長度 256bit）的字串 如：client_secret 為 ToRcIGDx6hLHOdJX 則金鑰為 ToRcIGDx6hLHOdJXToRcIGDx6hLHOdJX CBC 加密向量值，請登入後臺查看該服務之「cbc iv」欄位，如：q9qiPmVm2eFKWt79 若用戶身分證字號為 A123456789，加密並以 Base64 編碼後為 PmGYdTqUqoBChg/fZT6UuQ==

參數/欄位	說明
	MyData 每次皆會檢查 pid 是否符合上述規格

（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/欄位說明：

參數/欄位	說明
client_id	於 MyData 後臺新增服務後，由系統產生的服務識別鍵值
tx_id	由 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）
salt	由 MyData 產生的一次性認證參數，

參數/欄位	說明
	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/欄位說明：

參數/欄位	說明
client_id	於 MyData 後臺新增服務後，由系統產生的服務識別鍵值
tx_id	由 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 用戶資料將原為 json 的本文，以 AES/CBC 加密後的字串 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”: ${電子信箱}, “mobile”: ${手機號碼}, “salt“: ${salt}

參數/欄位	說明
	} 上述欄位中，姓名、電子信箱與手機號碼為非必填，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. 使用 ${base64_encoded_aescbc-encrypted-data} 當作加密資料所產製的數位簽章，其中，簽章演算法為 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/欄位說明：

參數	說明
client_id	於 MyData 後臺新增服務後，由系統產生的服務識別鍵值
resource_id_base64encoded_string	resource_id 為系統自動建立之識別碼 resource_id_base64encoded_string 則是將 resource_id 以 base64Encode 編碼後的結果 如果 SP 服務需多個資料集，可以:符

參數	說明
	號分隔各別的資料集識別碼，示意如下： Base64Encode({resource_id1}:{resource_id2}) MyData 系統會檢核 SP 所請求的資料集，是否符合 SP 申請服務時，介接申請單上所載明的資料集項目
tx_id	由 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	由 SP 指定的，用戶從 MyData 點選「同意傳送」後，重導至 SP 網站完成服務的指定網址 此參數值必須以 UrlEncode 編碼處理過，並須與後臺登錄的服務跳轉網址一致 MyData 系統僅會判斷 url path 是否相同， 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，以便 SP 進行系統後續處理

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	由 SP 指定的，用戶從 MyData 點選「同意傳送」後，重導至 SP 網站完成服務的指定網址 此參數值必須以 UrlEncode 編碼處理過，並須與後臺登錄的服務跳轉網址一致 MyData 系統僅會判斷 url path 是否相同， 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，以便 SP 進行系統後續處理
code	HTTP 狀態碼
aes-cbc_encrypted_txid	由 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） aes-cbc_encrypted_txid 為 以 AES/CBC/PKCS5PADDING 算法進行加密後的字串

參數	說明
	加密的金鑰為 client_secret 合併 2 次為長度 256bit 字串 加密向量值，請登入後臺查看該服務之「cbc iv」欄位
sp_param_key	此為 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/欄位說明如下：

參數	說明
sp_return_url	由 SP 指定的，用戶從 MyData 點選「同意傳送」後，重導至 SP 網站完成服務的指定網址 此參數值必須以 UrlEncode 編碼處理過，並須與後臺登錄的服務跳轉網址一致 MyData 系統僅會判斷 url path 是否相同， 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，以便 SP 進行系統後續處理

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」。 • 【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、SP 所請求的 resoruce_id 不屬於 MyData 管理後臺中所登錄的設定、未完成身分驗證或身分驗證失敗、無法順利解密 • 【403】拒絕存取、參數（tx_id 或 client_id）不存在 • 【404】sp_return_url 不符合 MyData 管理後臺中所登錄的設定 • 【408】交易逾時 ◦ 從 SP 跳轉至 MyData 超過 20 分鐘未完成交易，則視為交易逾時。此時，MyData 前臺頁面會顯示需要「重新申辦」 的提醒，若民眾點擊「重新申辦」，則 MyData 會於跳轉回 sp_return_utl 時回傳此狀態碼 ◦ 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 與用戶於 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

參數	說明
aes-cbc_encrypted_txid	由 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） aes-cbc_encrypted_txid 為 以 AES/CBC/PKCS5PADDING 算法進行加密後的字串 加密的金鑰為 client_secret 合併 2 次為長度 256bit 字串 加密向量值，請登入後臺查看該服務之「cbc iv」欄位
sp_param_key	此為 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 無法於 20 分鐘內返回 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)

當用戶完成身分驗證，並點擊「同意傳送」資料給 SP 時，MyData 會以 SP-API 告知 SP 需等候多久才能取得檔案，並會同時將 permission_ticket 和 secret_key 提供給 SP；SP 可以 permission_ticket 下載資料，並以 secret_key 解密資料檔案及驗證 JWE 簽章。

（一）MyData 發出請求 – 通知 SP 可以準備取得資料檔

如 MyData 第一次發出請求後未收到 SP 回應，將等待 15 秒後重發第二次。第二次等待 15 秒後，如仍無回應，將視為失敗。

格式說明：

```
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}
}
```

參數/欄位說明：

參數/欄位	說明
tx_id	由 SP 核發的交易識別值

參數/欄位	說明
	tx_id 格式為 version 4 UUID（36 字元，含 4 個 - 符號）
permission_ticket	由 MyData 核發，代表該次用戶同意的交易鍵值 permission_ticket 格式為 version 4 UUID 字符串，有效時間最長 8 小時，單次有效、不重覆
secret_key	產製 JWE 簽章時使用，僅該次交易有效的金鑰 MyData 會以 AES/CBC/PKCS5PADDING 演算法加密後傳給 SP 加密的金鑰為 client_secret 合併 2 次為長度 256bit, 64bytes 字串 加密向量值，請登入後臺查看該服務之「cbc iv」欄位 解密後的 secret_key 為隨機產生的英數字含大小寫的字符串，長度為 256bit, 32bytes.

（二）MyData 發出請求 - 告知 SP 無法給予資料檔

```
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}
  ]
}
```

參數/欄位說明：

參數/欄位	說明
tx_id	由 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	由 MyData 核發，代表該次用戶同意的交易鍵值 permission_ticket 格式為 version 4 UUID 字符串，有效時間最長 8 小時，單次有效、不重覆
unable_to_deliver	若 MyData 向 DP 發出請求失敗，則 MyData 視為該筆交易失敗，並以陣列的方式回傳此內容 若該次交易 SP 請求 3 個資料集，但其中 1 個無法傳遞時，此欄位值僅會載明無法傳遞的資料集 resource_id 如: unable_to_deliver: [{resource_id1}]

（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 /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	由 MyData 核發，代表該次用戶同意的交易鍵值 permission_ticket 格式為 version 4 UUID 字符串，有效時間最長 8 小時，單次有效、不重覆

（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。 • 從 SP 跳轉至 MyData 超過 20 分鐘未完成交易，則視為交易逾時。此時，MyData 前臺頁面會顯示需要「重新申辦」 的提醒，若民眾點擊「重新申辦」，則 MyData 會於跳轉回

	sp_return_utl 時回傳此狀態碼 • permissoin_ticket 最長效期為 8 小時
504	SP 請求資料集之系統發生異常，無法傳送資料集。

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：

eyJhbGciOiJBMjU2S1ciLCJlbmMiOiJBMjU2Q0JDLUhTNTEyIn0
.
1-mJQI42l08E3mz6Zac4OlHsNDXxz7g6DoAmJqayHmmEVIUIiNhLMYS5kjWAKPl7LrsFZ0pmdFVqfC77688Mdfni0Xgu4PST
.
SHR6R1k3ZzFoTHk1Ymw5Ug
.
LMz7XIhl2p6FPQwXfHAhb0yZ7YjgjPsLXzR6J96Lxzc-z0G3dR5P5_MB_NBQmumD7exefh2GpXjCvwkI277CD5htL7XzJodZLIqOwp1Ymhg
.
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到 IV 值，是否與 MyData 管理後臺中取得的 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。

（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：

```
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，參數/欄位說明如下：

參數/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

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的完整性的數位簽章檔，及為了方便服務提供者進行驗簽的憑證檔。

由於用戶線上申請服務提供者服務所需的資料集，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 平臺會先將來自不同資料提供者的資料檔案，打包成一個壓縮檔(zip)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，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：

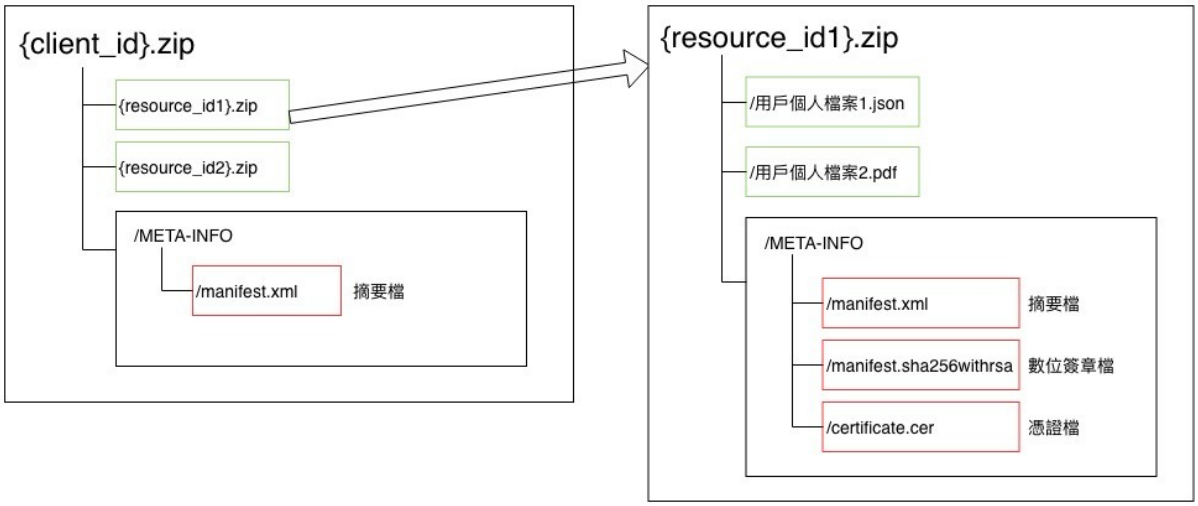
1. DP 資料打包檔格式需為壓縮檔(zip)。
2. zip 檔的檔名為 {resource_id}.zip。resource_id 是變數，代表資料集的識別代碼，可從 MyData 後臺取得。
3. zip 檔中可以包含多種格式之個人資料檔案，依資料提供者規範需包含的檔案用途、數量、檔名、副檔名等。
4. 數位簽章置於 META-INFO 子目錄，且包括下列檔案：
   - manifest.xml 摘要檔
   - manifest.sha256withrsa 數位簽章檔
   - ertificate.cer 憑證檔

（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>
 <file>
  <filename>{resource_id3}.zip</filename>
  <resource_id>{resource_id}</resource_id>
  <resource_name> 資料集中文名稱3</resource_name>
  <code>403</code>
 </file>
</files>
```

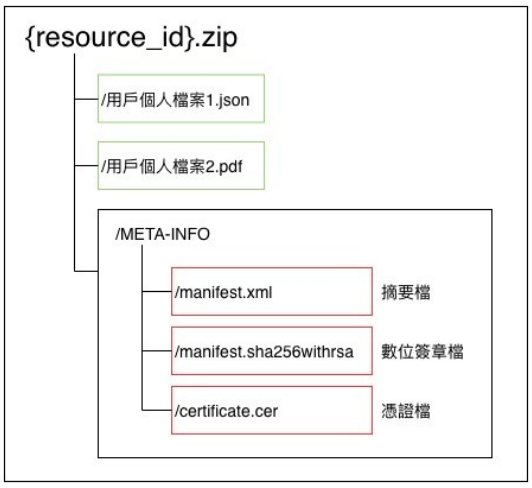
參數	說明
filename	MyData 收到下載資料集檔案名稱。
resource_id	MyData 收到下載資料集識別代碼。
resource_name	MyData 收到下載資料集中文名稱。
code	描述檔案處理狀態。 【200】正常 【204】查無使用者資料(封裝內無檔案) 【403】資料集下載失敗 補充說明： 若有部分資料集下載失敗，MyData 將視為整筆交易失敗，故不會傳輸任何資料集。

（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

（一）DP 資料打包檔案目錄結構示意如下：



（二）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/
zCCAuegAwIBAgIJAMhtYm3fde9AMA0GCSqGSIb3DQEBCwUAMIGVMQswCQY
D
-----END CERTIFICATE-----
```

六、驗證 DP 資料檔案的完整性的方法說明

（一）驗證憑證檔的有效性

服務提供者得向簽發憑證的 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

SP 須從 DP 夾帶的憑證檔（PEM 格式）中取出 DP 公鑰，作爲後續驗證數位簽章檔案 manifest.sha256withrsa 之用。

（三）驗證 manifest.xml 的完整性

manifest.xml 檔案中載明了各別資料檔案的數位指紋（摘要值）。因此 SP 須先驗證 manifest.xml 檔中所載明的摘要值的完整性，並以 DP 的公鑰對 manifest.sha256withrsa 進行驗簽。

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 為完整。

（四）驗證各別的資料檔案的完整性

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為完整。

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	於 MyData 後臺新增服務後，由系統產生的服務識別鍵值
as_id	第三方身分驗證中心
token	由第三方身分驗證中心核發的 access_token AES 加密的金鑰為 SP 的 client_secret 合併 2 次為長度 256bit 的字串 將 access_token 以 AES/CBC/PKCS5PADDING 演算法進行加密，其中，CBC 加密向量值，請登入後臺查看該服務之「cbc iv」欄位

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/欄位說明：

參數/欄位	說明
tx_id	由 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）驗證憑證檔的有效性

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

body:
{"verification":"CER"}
```

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 NHI：健保卡 FCS：軟體金融憑證 PII：雙證件

（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，若用戶點擊「重新申辦」，則 MyData 會跳轉回 sp_return_url 時回傳此狀態碼。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	由 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」。 • 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。
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

由 DP、MyData、SP 分別實作的交易勾稽機制。

說明如下：

(一) 各角色勾稽必要參數說明如下：

1. DP：transaction_uid, resource_id, 事件代碼, 日誌產生時間, 請求來源 IP。
2. MyData ：transaction_uid, client_id, resource_id, tx_id, 事件代碼, 身分證字號/統一編號, 日誌產生時間, 請求來源 IP。
3. SP：client_id, resource_id, tx_id, 事件代碼, 身分證字號/統一編號, 日誌產生時間, 請求來源 IP。

(二) 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	

#	事件代碼	事件時機	DP	MyData	SP
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

（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": [ “” , “” ],
}

responeBody:
{
  "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	於 MyData 後臺新增服務後，由系統產生的服務識別鍵值
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	由 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,

參數	說明
	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

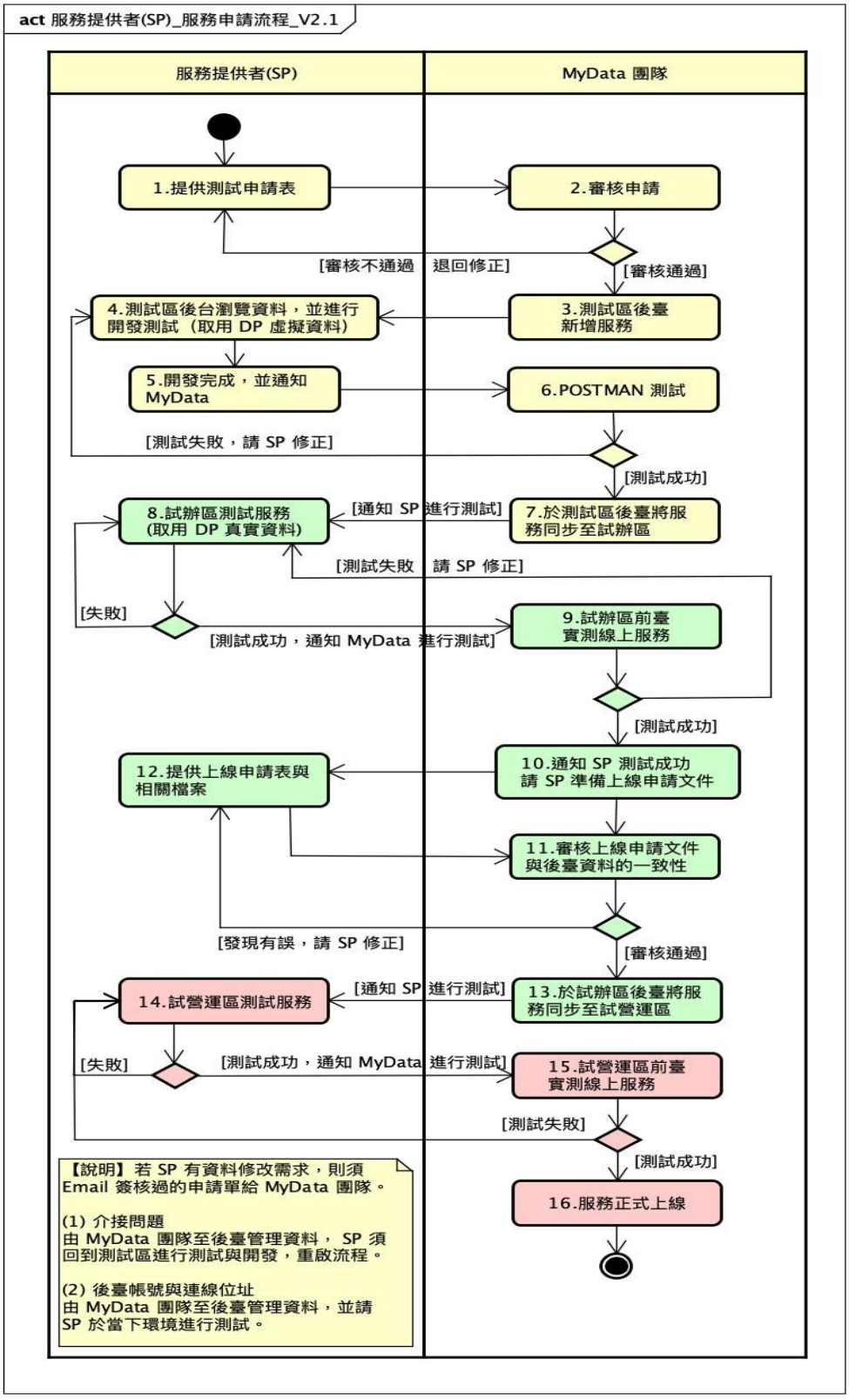
SP 需完成申請流程才能進行測試，申請方式請參考章節「肆、服務提供者資格申請作業」。

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。

如需將服務自測試區移轉至試辦區，請提供前端服務介面與測試流程說明文件，待維運團隊測試無誤，將協助移轉試辦區，並通知 SP 續行內部試營運作業。

測試或試辦期結束，系統將自動關閉測試連線，如需延長測試或試辦，請重新申請。

試辦完畢，如欲更新試營運區，亦須重新填寫申請單，提出上線需求，營運團隊將協助資料移轉正式環境後，通知 SP 確認。


act 服務提供者(SP)_服務申請流程_V2.1
服務提供者(SP)
MyData 團隊
1.提供測試申請表
2.審核申請
[審核不通過 退回修正]
[審核通過]
4.測試區後台瀏覽資料，並進行開發測試（取用 DP 虛擬資料）
3.測試區後臺新增服務
5.開發完成，並通知 MyData
6.POSTMAN 測試
[測試失敗，請 SP 修正]
[測試成功]
8.試辦區測試服務(取用 DP 真實資料)
[通知 SP 進行測試]
7.於測試區後臺將服務同步至試辦區
[測試失敗 請 SP 修正]
[失敗]
[測試成功，通知 MyData 進行測試]
9.試辦區前臺實測線上服務
[測試成功]
12.提供上線申請表與相關檔案
10.通知 SP 測試成功請 SP 準備上線申請文件
11.審核上線申請文件與後臺資料的一致性
[發現有誤，請 SP 修正]
[審核通過]
14.試營運區測試服務
[通知 SP 進行測試]
13.於試辦區後臺將服務同步至試營運區
[失敗]
[測試成功，通知 MyData 進行測試]
15.試營運區前臺實測線上服務
[測試失敗]
[測試成功]
16.服務正式上線
【說明】若 SP 有資料修改需求，則須 Email 簽核過的申請單給 MyData 團隊。
(1) 介接問題
由 MyData 團隊至後臺管理資料， SP 須回到測試區進行測試與開發，重啟流程。
(2) 後臺帳號與連線位址
由 MyData 團隊至後臺管理資料，並請 SP 於當下環境進行測試。

附錄 1 、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
206	超過 DP 資料集當日請求之上限
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 resoruce_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{resource_id}
404	• 無效的路徑 • sp_return_url 不符合 MyData 管理後臺中所登錄的設定
408	交易逾時或交易未完成，可能原因如下： • 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，若民眾點擊「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

HTTP 狀態碼	說明
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

附錄 2 、工作事項檢核表

項次	工作項目
1	填寫服務提供者介接申請表
2	MyData 整合協作流程可正常運行與跳轉
3	透過 SP-API 取得 permission_ticket 與 secret_key
4	透過 MyData-API 取得個人資料檔
5	解密個人資料檔
6	於 SP 服務頁加上以 MyData 取用資料之按鈕
7	提供測試成功流程佐證資料
8	完成交易 Log 日誌查詢 API 之實作與開發