數位服務個人化

資料提供者技術文件

V2.5

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	109/03/30	調整章節「貳、三、完成授權驗證等相關系統整合介接」之內容，資料提供者需配合 MyData 實作授權驗證之系統整合介接。	P1
			調整章節「陸、MyData 整合協作流程說明」之內容。	P8
			調整章節「柒、授權 API Endpoint 規格說明」之內容。	P11
			新增章節「拾、交易 Log 日誌查詢」。	P27
			調整章節「拾貳、二、系統環境主機及網址資訊」之連線資訊。	-
2	2.1	109/04/17	調整章節「伍、二、資料集註冊」之內容。	P4
			調整章節「伍、三、資料集列表」之內容。	P6
			調整章節「柒、三、（二）回覆 UserInfo 請求成功」之內容。	P16
3	2.2	109/04/27	調整章節「貳、如何成為資料提供者」之內容。	P1
			調整章節「肆、資料提供者資格申請作業」之內容。	P3
			調整章節「伍、資料提供者管理作業」之內容。	P4
			於章節「柒、二、（二）Introspection 請求 － 回覆成功」新增欄位，說明申請人本次採用的身分驗證方式。	P13
4	2.3	109/05/18	調整章節「捌、二、（一）DP-API 請求」Authorization 之簡易說明。	P18
			移除原章節「捌、三、DP-API Heartbeat 機制」之內容，改以驗證資料集可下載性之機制，驗證 DP-API 的有效性與可下載性。	-

項次	版本	時間	修正內容	頁次
			新增章節「捌、三、驗證資料集可下載性之機制說明(由 MyData 實作)」之內容。	P21
			新增章節「捌、四、壓力測試機制之說明」之內容。	P21
			調整章節「玖、一、DP 資料打包檔案規格說明」之範例示意圖	P18
			新增章節「玖、一、（三）META-INFO 目錄及內含檔案說明」之內容，建議 DP 向 GCA 政府憑證管理中心申請的憑證類別為：「政府機關單位憑證非 IC 卡類」憑證。	P20
			調整章節「拾貳、一、測試流程」之內容	P32
			調整章節「拾貳、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。	-
			增加附錄工作事項檢核表	P33
5	2.4	109/06/15	修正客服電話	P3
			移除「拾貳、二、系統環境主機及網址資訊」之內容	-
			修正文件頁碼	-
6	2.5	109/06/29	新增章節「拾壹、四、提供符合資料檔解析規則說明文件之『測試資料範例檔』」之內容。	P30
			修正文件描述文字	-

目錄

壹、目的.....1

貳、如何成為資料提供者.....1

一、完成 MyData 資料提供者資格申請作業.....1
二、完成授權驗證等相關系統整合介接.....1
三、實作資料提供介面規格.....1

參、名詞定義.....2

肆、資料提供者資格申請作業.....3

伍、資料提供者管理作業.....4

一、基本資料編輯.....4
二、資料集註冊.....4
三、資料集列表.....5
四、資料集運用情形.....5
五、查詢所有資料集列表.....6

陸、**MyData** 整合協作流程說明.....7

一、MyData 整合協作流程說明.....8
二、Introspection Endpoint 與 UserInfo Endpoint 應用範圍.....9

柒、授權 **API Endpoint** 規格說明.....10

一、系統環境與 API Endpoint.....10
二、Introspection Endpoint.....10
三、UserInfo Endpoint.....13

捌、**DP-API Endpoint** 規格準則.....16

一、系統環境與條件.....16
二、DP-API 請求及回覆規格說明.....16
三、驗證 DP 資料集可下載性之機制說明(由 MyData 實作).....20
四、壓力測試之機制說明.....20

玖、**DP** 資料打包檔案規格準則.....21

一、DP 資料打包檔案規格說明.....21
二、SP 驗證 DP 資料打包完整性的方法與說明.....24

拾、交易 **Log** 日誌查詢.....26

一、 各角色勾稽必要參數說明.....26
二、 交易日誌產生時機.....26
三、 DP 請求交易日誌.....28
四、 失敗回應.....29

拾壹、**DP** 資料檔解析規則說明文件撰寫原則**.....30**
一、目的.....30
二、資料檔解析規則說明文件檔案格式及命名原則.....30
三、資料檔解析規則說明文件撰寫原則.....30
四、提供符合資料檔解析規則說明文件之「測試資料範例檔」.....30
拾貳、**DP** 與 **MyData** 測試流程說明**.....31**
一、測試流程.....31
附錄、工作事項檢核表**.....32**

壹、目的

本文件目的主要描述「資料提供者」於實作「MyData 平臺之資料提供者」時應依循的作業流程、準則、技術規格及相關注意事項。

貳、如何成為資料提供者

一、完成 MyData 資料提供者資格申請作業

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

二、完成授權驗證等相關系統整合介接

資料提供者需配合 MyData 實作授權驗證之系統整合介接。相關之 Endpoint 規格，請參考章節「柒、授權驗證 API Endpoint 規格說明」。

三、實作資料提供介面規格

資料提供者應保有彈性並定義資料提供介面規格，但於發展實作資料提供介面規格時，應參考並依循國發會發佈之「共通性應用程式介面規範（OAS）」所提及之要點實作，使 API 具有共通性之特性，為擴大政府資訊服務效益。

資料提供介面規格準則，請參考本文件章節「捌、DP-API Endpoint 規格準則」及「玖、DP 資料打包檔案規格準則」。

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

肆、資料提供者資格申請作業

機關單位欲使用 MyData 機制成為資料提供者角色，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	維運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建立。
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與資料集內容無誤。

機關單位申辦時須確實填寫，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資料集建置作業。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、資料提供者管理作業

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、資料集註冊

步驟項次	流程內容
1	資料提供者提供「資料提供者介接申請表」。
2	維運團隊依據「資料提供者介接申請表」內容建立資料集。
3	通知機關單位（申請人）確認資料集內容是否建立正確。
4	待資料提供者依技術文件說明之介接方式完成資料介接作業。

資料集內容欄位說明

欄位序號	欄位名稱	說明
1	resource_id	註冊新資料集時，MyData 系統會產生用以識別服務的唯一的識別值 resource_id。
2	resource_secret	DP 於 MyData 後臺服務註冊完成後，MyData 平臺才會產製此密碼字串。

三、資料集列表

顯示已註冊、申請中之資料資源項目清單，並提供關鍵字查詢與狀態顯示功能。

如示意圖：

四、資料集運用情形

資料提供者需檢視各啟用之資料集現行運用之情形時，可使用「被運用資料集」功能項目，將以清單顯示介接資料集之服務提供者與相對應服務名稱，並提供依資料集名稱篩選及服務提供者、註冊服務關鍵字搜尋功能。

五、查詢所有資料集列表

提供查詢已上線資料集與服務清單

陸、MyData 整合協作流程說明

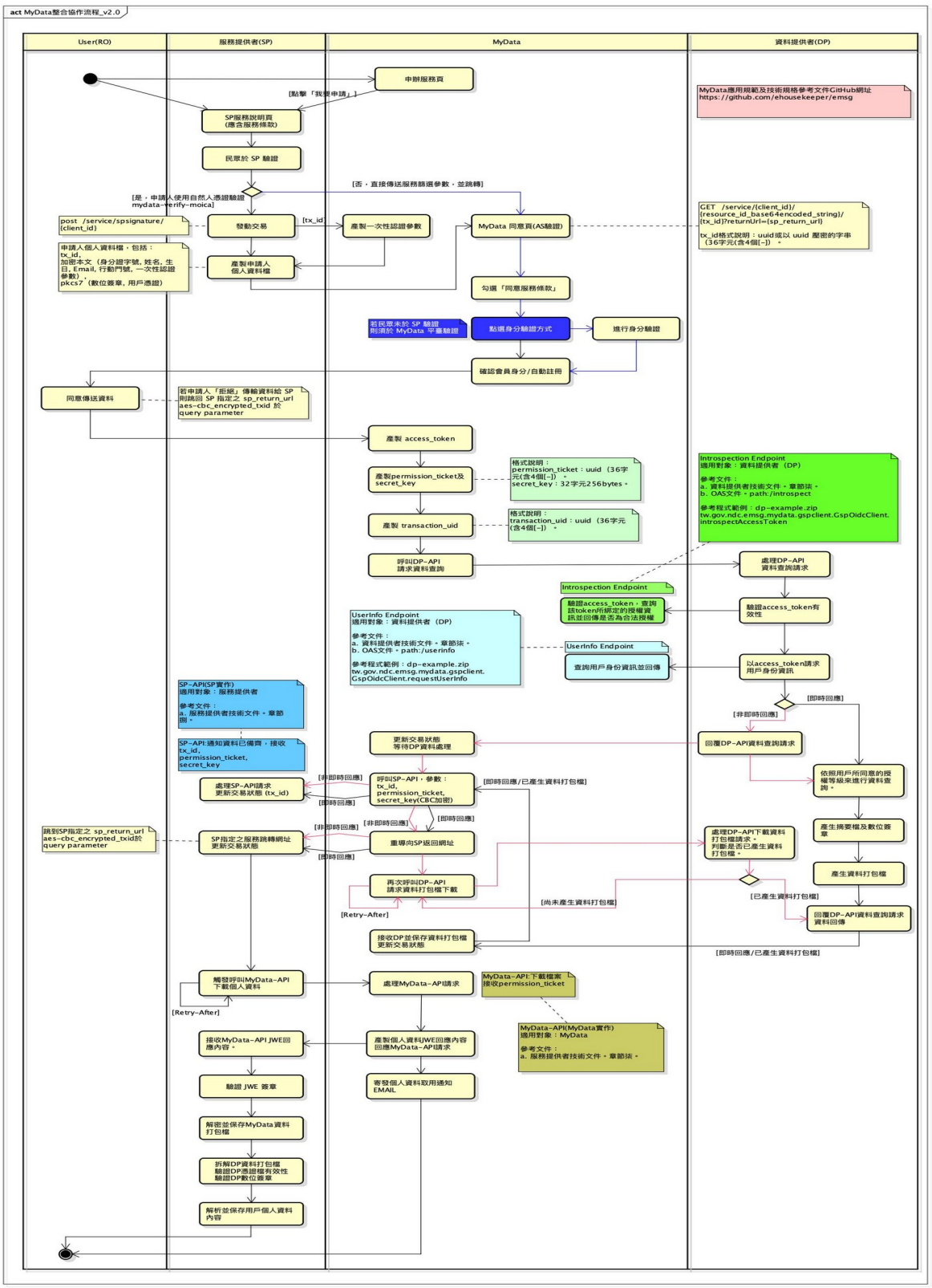
MyData 平臺提供多元身分驗證方式，包括：自然人憑證、健保卡...等，並以用戶的個人身分證字號+生日做為用戶會員的依據。

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。同時，MyData 平臺會將用戶同意後產生的 access_token 傳遞給資料提供者，資料提供者再分別透過 Introspection Endpoint, UserInfo Endpoint 向 MyData 平臺發出驗證與確認身分之請求，以檢核請求之合法及有效性。

本文件主要對象為提供資料提供者參考，故僅描述資料提供者應如何呼叫以下 API：

- Introspection Endpoint：檢核用戶同意的有效性
- UserInfo Endpoint：取得用戶資訊

一、MyData 整合協作流程說明



【註】流程說明圖檔案可至 **Github** 連結下載。

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、Introspection Endpoint 與 UserInfo Endpoint 應用範圍

(一) Introspection Endpoint ：檢核用戶同意的有效性

當 MyData 平臺向資料提供者發出請求時，會一併傳遞代表用戶同意憑據的 access_token 給資料提供者，資料提供者須向 MyData 平台以 Introspection Endpoint 檢核該 access_token 是否有效，才得以啟動本次交易。

access_token 前方皆會有站台的前綴詞(mydata::)，範例如下：
mydata::fd05257048b303d2bad3cc4aa6313290eb80654e554054ea8e2fc88ff516b15d

詳情請參閱章節「柒、二、Introspection Endpoint」。

(二) UserInfo Endpoint：取得用戶資訊

當資料提供者已經確認 access_token 為合法有效後，即可呼叫 UserInfo Endpoint 來取得用戶資訊。取得用戶資訊的主要目的是為了識別用戶身分，資料提供者應以身分證字號與生日做為識別用戶的主要依據。

詳情請參閱章節「柒、三、UserInfo Endpoint」。

柒、授權 API Endpoint 規格說明

一、系統環境與 API Endpoint

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

二、Introspection Endpoint

Introspection Endpoint 的主要功能是讓資料提供者檢核 access_token 的合法及有效性之用。

（一）Introspection 請求

Introspection Endpoint 支援 HTTP POST 呼叫，參數的傳遞方式為 application/x-www-form-urlencoded，同時需以 HTTP Basic authentication 方式帶入身分驗證資訊。

請求網址示意：

```
POST /connect/introspect
HTTP/1.1 TLS 1.2
Content-Type: application/x-www-form-urlencoded
Authorization:Basic {credential}

token={access_token}
```

參數/欄位說明：

參數/欄位	說明
credential	credential 為 Base64encode { resource_id:resource_secret} 後的字符串 Base64encode 的範例結果如下： Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
access_token	代表用戶同意憑據之 token

（二）Introspection 請求成功

MyData 回覆內容示意如下：

```
HTTP/1.1 TLS 1.2 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache

{
  "active": "true",
  "verification":"CER"
}
```

參數/欄位說明：回應欄位數目未來可能因需求而增加，接收時請考量擴充性。

參數/欄位	說明
active	必要。說明 access_token 當前的活動狀態 true：有效 false： 無效
verification	CER：自然人憑證 FIC：晶片金融卡

參數/欄位	說明
	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）Introspection 請求失敗

MyData 回覆內容示意如下：

```
HTTP/1.1 TLS 1.2 400 Bad Request
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache

{
  "error": "invalid_request"
}
```

http header：

參數/欄位	說明
Content-Type	application/json
Cache-Control	no-store
Pragma	no-cache

參數/欄位說明：

參數/欄位	說明
error	必要。提供錯誤代碼 invalid_request：缺少必要參數。 invalid_client：client 身分驗證失敗。 invalid_grant：非合法授權或已過期。 unauthorized_client：未授權的 client。

參數/欄位	說明
error_description	非必要。描述錯誤原因
error_uri	非必要。描述發生錯誤的頁面網址

三、UserInfo Endpoint

UserInfo Endpoint 的主要功能是讓資料提供者識別用戶身分；資料提供者應以身分證字號與生日做為識別用戶的主要依據。

（一）UserInfo 請求

規範使用 HTTP GET 方法進行請求，並採用 Bearer token 進行身分驗證。

請求網址示意：

```
GET /connect/userinfo
HTTP/1.1 TLS 1.2
Authorization: Bearer {access_token}
```

http header：

參數/欄位	說明
access_token	代表用戶同意憑據之 token。

參數/欄位	說明
sub	必要。用來代表帳戶的唯一識別值
uid	必要。身分證字號
birthdate	必要。生日，格式為 YYYY-MM-DD 八碼
uid_verified	非必要。身分證字號是否已驗證
gender	非必要。性別 male/female
cn	非必要。中文姓名
email	非必要。電子郵件
account	必要。MyData 會員帳號

（三）UserInfo 請求失敗

MyData 回覆內容示意如下：

```
HTTP/1.1 TLS 1.2 401 Unauthorized
WWW-Authenticate: error="invalid_token",
error_description="The access token expired"
```

參數/欄位說明：

參數/欄位	說明
error	必要，提供錯誤代碼 invalid_request： 缺少必要參數、提供了不支援的參數、提供了錯誤的參數值、同樣的參數出現多次、使用一種以上的方法來出示 access_token（如：放在 header 裡又放在 form 裡）、或是其他無法解讀 request 的情況。 invalid_token： access_token 過期、授權無效、無法解讀、

參數/欄位	說明
	或其他 access_token 不合法的情況。
error_description	非必要，描述錯誤原因

捌、DP-API Endpoint 規格準則

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、DP-API 請求及回覆規格說明

（一）DP-API 請求（由 MyData 發動請求）

請求網址示意：

```
POST /mydata-dp/{resource}
HTTP/1.1 TLS 1.2
Content-Type: {content_type}
Authorization: Bearer {access_token}
transaction_uid: {transaction_uuidv4_string}
{custom_param1_key}: {custom_param1_value}
{custom_param2_key}: {custom_param2_value}
```

參數/欄位說明：

參數/欄位	說明
resource	用來識別資料集的字符串，由 DP 定義
content_type	依據請求的 content_type 回應該格式的檔案，並於 filename 中註明檔案名稱 application/zip 代表回覆「資料打包 zip 檔」
Authorization	宣告 Client 身分資訊，請參考 RFC-7617, 6750
access_token	代表用戶同意憑據之 token
transaction_uid	格式為 UUID v4 且不重複的交易鍵值。 有效期始於第一次發動 DP-API 請求，直至取得 DP 回覆資料檔、或 DP 回覆請求失敗、或查無資料後終止
custom_param1_key	自訂欄位，非必要。

參數/欄位	說明
custom_param2_key	用戶必須於前臺輸入的查詢參數欄位名稱（如：carNo） 若需多個查詢參數，則分別帶入，不限於 2 個。
custom_param1_value custom_param2_value	自訂欄位，非必要。 用戶必須於前臺輸入的查詢參數內容（如：1234-QQ） 若需多個自訂參數，則分別帶入，不限於 2 個 每多一組自訂參數即帶入一組 key: value。 如：carNo:1234-QQ

經用戶身分驗證與同意後，MyData 已透過 Userinfo 將使用者的身分資訊提供給 DP 查詢資料。因此如有需要額外資訊，建議多利用現行 Userinfo 已有之資訊，減少用戶額外輸入查詢欄位。

若用戶調閱資料時，有必須輸入前臺查詢參數的需求，DP 須將相關資訊備註於「資料提供者介接申請表」與 OAS 文件中。此欄位於 MyData 前臺呈現時為必填，無法提供用戶選填。

MyData 將依照 OAS 文件之內容，以 POST 呼叫 DP-API，以避免查詢條件值洩漏。

(二) DP-API 請求成功：

1. 資料準備完成，DP 可即時回傳資料

   依據請求的 content_type 回應該格式的檔案。filename 中註明檔案名稱。

   ```
   HTTP/1.1 TLS 1.2 200 OK
   Content-Type: {content_type}
   Content-Disposition: attachment; filename={filename}
   Content-Transfer-Encoding: binary
   Accept-Ranges: bytes
   ```

參數/欄位說明：

參數/欄位	說明
content_type	依據請求的 content_type 回應該格式的檔案，並於 filename 中註明檔案名稱 application/zip 代表回覆「資料打包 zip 檔」
filename	檔案名稱
HTTP 狀態碼	200：請求成功 204：請求成功，此資料集屬證明類資料集，DP 查查無證明資料，因此無法提供資料檔 206：超過資料集下載上限

2. 資料需較長準備時間，DP 非即時回傳資料

   若 DP-API 需較長時間準備資料，而不能即時回傳資料，則以 HTTP 429 回應，並告知等候時間。

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

參數/欄位說明：

參數/欄位	說明
content_type	依據請求的 content_type 回應該格式的檔案，並於 filename 中註明檔案名稱 application/zip 代表回覆「資料打包 zip 檔」
delay_seconds	下次發動請求前需等待的秒數。

3. 查無用戶資料

此回應方式與有資料的情形相同，差別在於查無資料的檔案內會顯示查無資料相關說明文字。

HTTP/1.1 TLS 1.2 200 OK
Content-Type: {content_type}
Content-Disposition: attachment; filename={filename}
Content-Transfer-Encoding: binary
Accept-Ranges: bytes

參數/欄位說明：

參數/欄位	說明
content_type	依據請求的 content_type 回應該格式的檔案，並於 filename 中註明檔案名稱 application/zip 代表回覆「資料打包 zip 檔」
filename	檔案名稱

DP 仍須正常回覆 PDF 與 JSON 檔，並於 PDF 內文標明「查無資料」。JSON 檔內容備註如下：
{“code”：“204”,” text”:” 查無資料” }

一、 DP-API 請求失敗

DP 以 HTTP 狀態碼來表示回覆請求失敗的狀況。

HTTP/1.1 TLS 1.2 401 Unauthorized
Content-Type: application/json

HTTP 狀態碼	說明
400	缺少必要參數或參數驗證失敗。
401	access_token 檢核失敗。
403	拒絕存取。
504	無法完成傳送個人資料檔案。

三、驗證 DP 資料集可下載性之機制說明(由 MyData 實作)

為維護服務品質並驗證資料集的可下載性，MyData 將定時（如：每 30 分鐘）以系統自動產生之合法 access_token，身分證字號為 A999999999，透過 DP-API 發送下載請求，以確保可正常下載資料集。若有需輸入「查詢參數」之資料集，DP 須提供此機制專用的測試參數。

當 MyData 運行可下載性機制時，若 DP 回應 200（交易成功）或 400（參數格式或內容不正確，或是缺少必要參數）皆視為可下載性成功。

若 MyData 發現資料集無法正常下載，將由系統自動發信通知資料提供者及有使用此 DP 資料集的服務提供者，並於 MyData 前臺顯示資料集無法使用等內容。

為能確保資料提供者與服務提供者之負責人員可順利收到系統信件，請將 MyData 客服信箱 mydata@ndc.gov.tw 加入收信白名單，如負責人員信箱有變更，亦請通知維運團隊。

四、壓力測試之機制說明

DP-API 於 MyData 平臺正式上線前，MyData 會對該 DP-API 進行壓力測試，壓力測試標準以及執行方式，經 MyData 維運團隊與 DP 相關負責人員協議後擬定。

壓力測試的對象是 DP-API 的正式機環境，壓力測試時 MyData 將以系統自動產生之合法 access_token，身分證字號為 A999999999，進行呼叫 DP-API，DP-API 則應如實的完成 MyData 介接請求並回傳「查無資料」的資料集打包檔。

玖、DP 資料打包檔案規格準則

一、DP 資料打包檔案規格說明

為了使 MyData 的應用更加廣泛，資料檔至少應包含之內容如下：

- 機器可讀的 JSON 格式。
- 易於人讀的 PDF 格式，並以民眾身分證字號加密。
- META-INFO 子目錄與數位簽章、憑證檔：保證資料完整性，並可供服務提供者進行驗簽。

其中，PDF 檔之內容須符合正式文件之規範(含查無資料之資料檔)，至少應包含：資料提供者之機關 LOGO、單位名稱、浮水印、提供資料單位名稱、產製時間等可證明文件出處之標誌，以示該機關提供文件之公正性，示意如下圖：

為了簡化 MyData 平臺與資料提供者之間傳遞資料的機制，MyData 平臺規範資料提供者須將同一個資料集的多種格式之檔案(如 JSON 與 PDF)打包成一個壓縮檔(zip)後，再傳遞給 MyData 平臺。

(一) DP 資料打包檔案規格要點如下：

1. DP 資料打包檔格式需為壓縮檔(zip)，為利 MyData 平臺提供線上預覽功能，此壓縮檔請勿設定密碼。

2. zip 檔的檔名為 {resource_id}.zip。resource_id 是變數，為此資料集的識別代碼，可從 MyData 後臺取得。

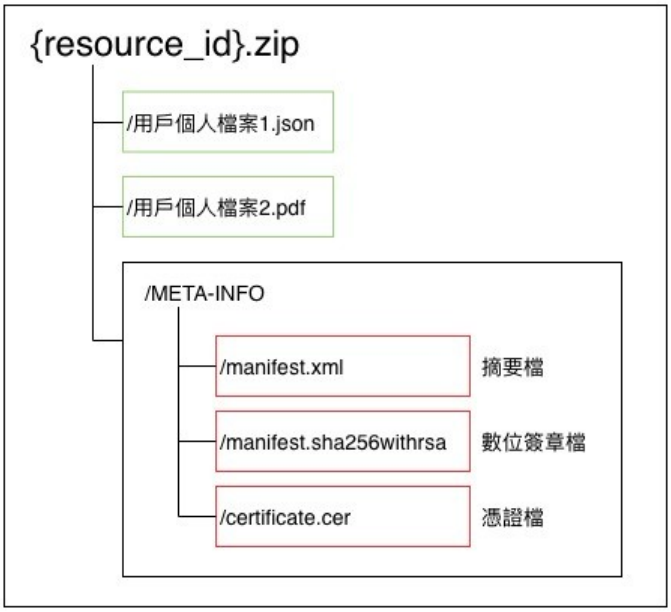
   【註】該 zip 檔的存放與傳送，皆應以不同交易(transation_uid)為依據，以確保正確性。

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. 將數位簽章置於 META-INFO 子目錄，且 META-INFO 子目錄中，共包括下列檔案：

   - manifest.xml 摘要檔
   - manifest.sha256withrsa 數位簽章檔
   - ertificate.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。

- **manifest.xml**：

manifest.xml 內，載明各資料檔案以 SHA256 演算法演算出的數位指紋（摘要值）。

內容格式示意如下：

```
<?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>
```

- **manifest.sha256withrsa：**

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

建議 DP 使用長度至少 2048bits 的私鑰，並向 GCA 政府憑證管理中心申請可支援 SHA256 的「政府機關單位憑證非 IC 卡類」憑證。

- **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-----
```

二、SP 驗證 DP 資料打包完整性的方法與說明

(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、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

(一) DP：transaction_uid, resource_id, 事件代碼, 日誌產生時間, 請求來源 IP。

(二) 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。

(三) 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

#	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

三、 DP 請求交易日誌

POST /log/dp
HTTP/1.1 TLS 1.2
Content-Type: application/json

requestBody:
```
{
  ""resource_id": "API.xxxxxxxx",
  "stime": "yyyy-mm-dd",
  "etime": "yyyy-mm-dd",
  "transaction_uid": [ “” , “” ],
  "event": [ “” , “” ],
}
```

responeBody:
```
{
  ""resource_id": "API.xxxxxxxx",
  “data” : [
     {
        "transaction_uid":"",
         "ctime":"yyyy-MM-dd hh24:MI:SS",
        "event":"",
        "ip":"",
    }
  ]
}
```

參數/欄位說明：

參數/欄位	說明
resource_id	資料集鍵值。
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。
transaction_uid	交易鍵值。用於讓 DP 方便識別資料查詢請求為同一次交易。
event	事件代碼。非必填。

參數/欄位	說明
	第三層過濾條件，查詢結果會滿足 stime, etime, transaction_uid, event 的條件交集結果。
ip	該事件的請求來源 IP。

四、 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（resource_id）不存在。

拾壹、DP 資料檔解析規則說明文件撰寫原則

一、目的

為了令 **SP** 能順利解析 **DP** 所提供的資料檔內容，針對機器可讀的文件格式，請 **DP** 提供明確的解析規則並提供範例資料檔，以利 **SP** 運用。

二、資料檔解析規則說明文件檔案格式及命名原則

格式採用 **PDF** 並將資料檔解析規則命名為「**XXX_MyData** 介接資料檔案規格書**.**pdf」。另外關於資料範例部分，請依照資料檔實際格式提供範例檔案，如：example.json。

三、資料檔解析規則說明文件撰寫原則

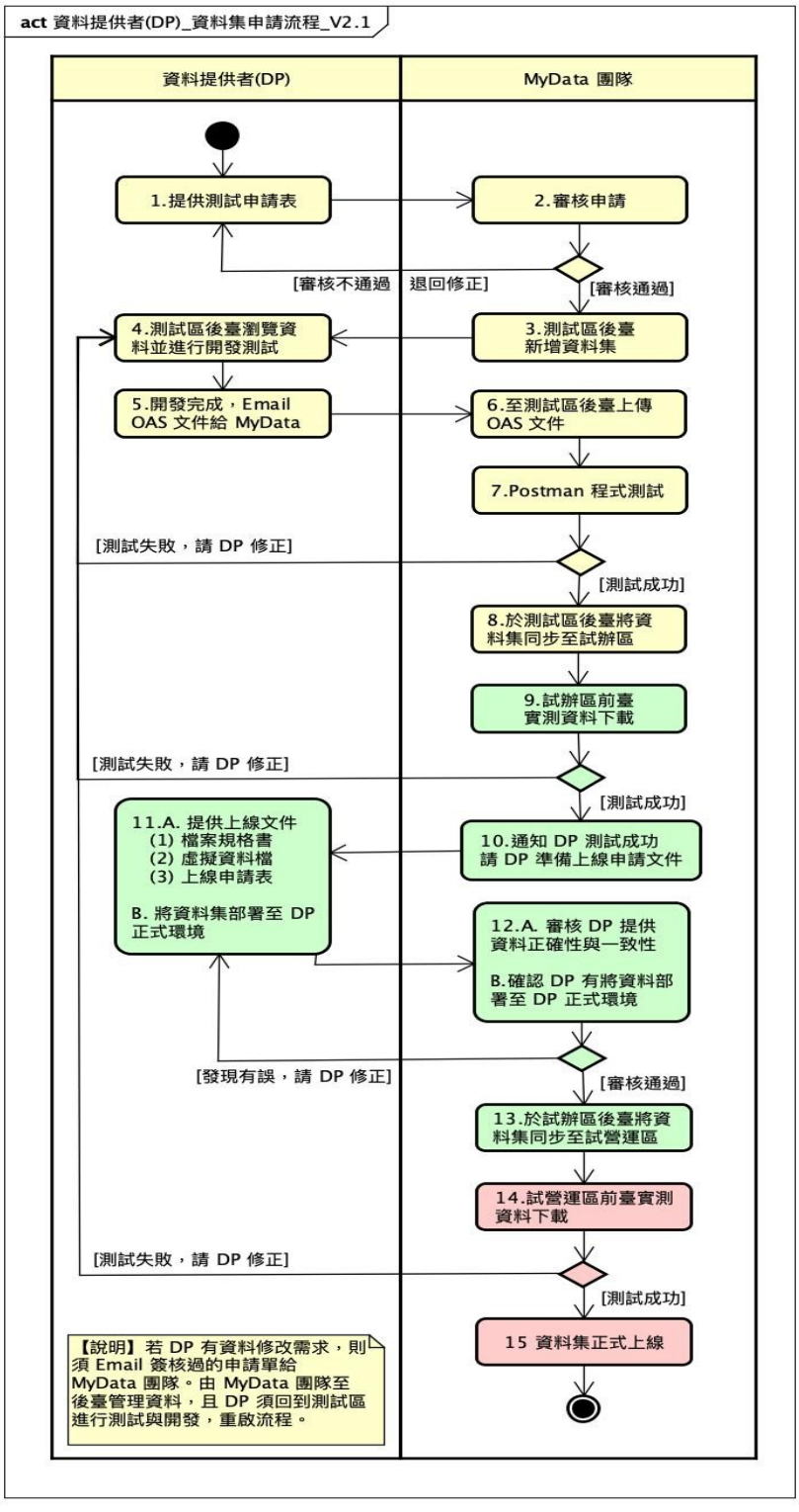
文件格式請參考「MyData 介接資料檔案規格書(範例).odt」，下載網址如下：
https://github.com/ehousekeeper/emsg/blob/master/MyData 應用規範與技術文件**/MyData** 介接資料檔案規格書**(**範例**).odt**。

四、提供符合資料檔解析規則說明文件之「測試資料範例檔」

DP 所提供之範例檔之格式、命名規則、資料欄位、資料格式皆須與真實資料之格式為主，惟資料欄位的值以虛擬資料示意之。其中，測試資料檔的 PDF，統一以「A999999999」作為開啟密碼。

拾貳、DP 與 MyData 測試流程說明

一、測試流程



附錄、工作事項檢核表

項次	工作項目
1	填寫資料提供者介接申請表
2	可正常呼叫 Introspection API
3	可正常呼叫 Userinfo API
4	提供 OAS 介接文件
5	提供 PDF & JSON(機器可讀)兩種檔案格式，其中 PDF 須加入機關名稱、機關 logo、浮水印、產製時間，並以使用者身分證字號加密
6	上項之檔案須用機關憑證進行簽章，並打包為壓縮檔(zip 格式)
7	提供測試資料範例檔（PDF 以 A999999999 作為檔案開啟密碼）
8	提供檔案規格書
9	完成交易 Log 日誌查詢 API 之實作與開發
10	提供可下載性檢驗機制之測試參數值(如有需要)
11	將客服信箱 mydata@ndc.gov.tw 加入收信白名單