



數位服務個人化 (MyData) 資料提供者技術開發說明





壹、資料提供者申請流程

貳、服務流程

- 民眾前台服務流程說明 - 查詢個人資料
- 後台服務流程說明

參、技術說明

- 服務情境：線上申辦
- 技術規範說明 OAuth2 API
- 技術規範說明 DP-API
- 技術規範說明 DP 資料打包檔





壹、資料提供者申請流程





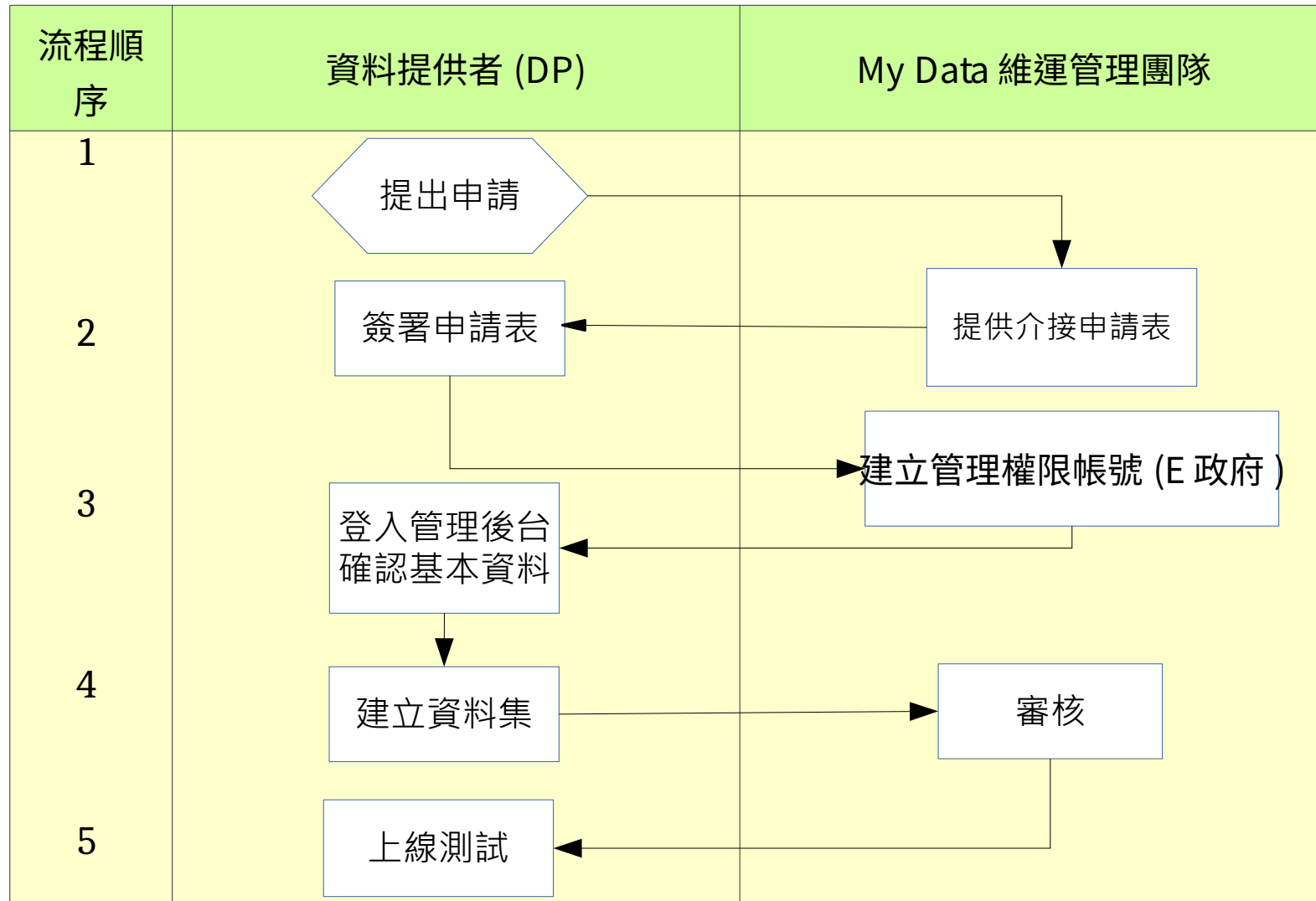
1 以電話或 E-mail 聯繫管理團隊，提出後台使用申請

2 申請機關單位與 MyData 簽署
「MyData 平臺資料提供者介接申請表」

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





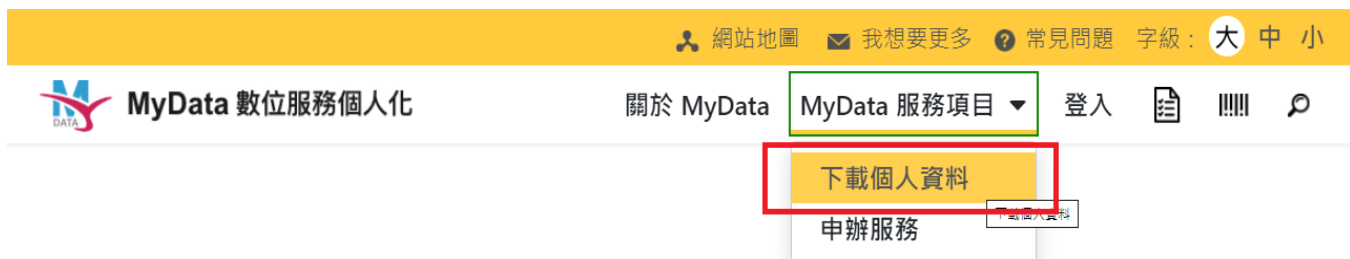
民眾前台服務流程說明

查詢個人資料

查詢個人資料服務



STEP 1 使用者從 MyData 網站點擊 `查詢個人資料`



數位服務個人化

安全・輕鬆取得個人資料

沒時間到臨櫃申辦個人資料與服務嗎？快來線上申辦 MyData 雲服務，安全、安心，省時間！

馬上申請





STEP 2 選擇資料類別

下載個人資料

我想一次下載多筆資料

從個人生活至醫療教育，提供全方位個人資訊



戶役政



勞保



地政



健保



財稅



醫療



社福



商工



金融



交通



教育



法務



其他





STEP 3 選擇項目 (以個人戶籍資料查詢 為例)


⋮ [首頁](#) > [MyData服務項目](#) > [戶政](#)

項目一覽

◎ 個人戶籍資料查詢

您可下載的資料內容

1. 個人記事
2. 出生地
3. 出生日期
4. 國民身分證統一編號
5. 姓名
6. 婚姻狀況
7. 戶籍地址
8. 教育程度
9. 遷入日期

我要下載 

◎ 現戶全戶戶籍資料

◎ 親屬關係資料 (範圍為父母、配偶、子女)



STEP 4 同意 MyData 服務條款，並選擇身分驗證

◎ 個人戶籍資料查詢

Step

1

同意服務條款

國家發展委員會（以下簡稱本會）配合行政院推動優質電子化政府服務，於本會e管家數位服務個人化（MyData）專區提供資料下載服務（以下簡稱本服務），期望透過本服務增進使用者瞭解個人資料運用方式。為了協助您了解本服務之功能與內容，以及保障您個人之權益，請於使用本服務前詳細閱讀以下內容，當您開始使用本服務時，即視為您已充分閱讀、瞭解與同意接受本服務條款之所有內容。

☒ 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分並取得資料：

 自然人憑證

 OTP簡訊

確認



e管家 Plus





STEP 5 進行登入、驗證

個人戶籍資料查詢

Step 同意服務條款

1

國家發展委員會（以下簡稱本會）配合行政院推動「國家發展委員會戶籍資料查詢服務」（以下簡稱本服務），期望透過本服務增進使用戶之便利，請於使用本服務前詳細閱讀以下內容，當您

☒ 我已詳實了解此服務內容，並同意上述服務條款之所有內容。

2

身份驗證

您可使用下列方式驗證您的身分：

我的E政府
WWW.GOV.TW

帳號登入

帳號

密碼

忘記帳號 忘記密碼 加入會員

登入

個人戶籍資料查詢

Step 同意服務條款

1

國家發展委員會（以下簡稱本會）配合行政院推動「國家發展委員會戶籍資料查詢服務」（以下簡稱本服務），期望透過本服務增進使用戶之便利，請於使用本服務前詳細閱讀以下內容，當您

☒ 我已詳實了解此服務內容，並同意上述服務條款之所有內容。

2

身份驗證

您可使用下列方式驗證您的身分並取得資料：

我的E政府
WWW.GOV.TW

自然人憑證驗證

請插入您的自然人憑證，並輸入PIN碼：

待驗證證號: [F12742****]

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]

現戶全戶戶籍資料

親屬關係資料（範圍為父母、配偶、子女）





STEP 6 取得資料 (可線上預覽、下載、臨櫃申辦條碼)

2

身分驗證

您可以選用下列其中一種方式驗證身分取得資料：



自然人憑證



OTP簡訊

確認

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





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

<https://mydata.nat.gov.tw/mydata-backend/signin>



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，**同時也可新增副帳號**。

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：

* 聯絡電話：

* 聯絡E-mail：

* E政府帳號：

副E政府帳號：

E政府帳號	姓名	電話	E-mail
<input type="text" value="請輸入E政府帳號"/>	<input type="text" value="請輸入姓名"/>	<input type="text" value="請輸入電話"/>	<input type="text" value="請輸入E-mail"/>

增加輸入列



STEP 4

請先前往「資料提供者管理／資料集列表」功能，點擊新增資料集，開始進行資料集註冊。





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。

資料集基本資料

* 資料集類別：請選擇

* 資料集名稱：請輸入資料集名稱

* 資料集說明：請輸入該資料集簡單之說明文字

* 授權取用資料安全等級：
☐ 自然人憑證 ☐ OTP ☐ 健保卡 ☐ 多因子 ☐ E政府帳號
☐ 工商憑證(*可提供公司行號或法人資料再行勾選)

* 資料更新時間： 天

* 資料預計下載時間：
☒ 即時 ☐ 非即時

下載內容簡述：請輸入文件下載內容簡述（一般民眾瀏覽使用）

資料集欄位

項次	*欄位名稱(以中文說明)	備註	
1			✖
			+

資料集存取範圍

項次	*SCOPE值	資料集名稱	
1			✖
			+

前台查詢參數

項次	*鍵值(OAS檔輸入欄位鍵值)	*欄位名稱(包括中文說明與範例)	
1			✖
			+

* resource id：APLr8t2w41ynI

* 介接API文件：
(符合OAS規範)

* 檔案規格書：



STEP 6

送審之服務，經 MyData 管理團隊審核完成即上架至 MyData
`所有資料集列表`，表示資料提供者可開始提供資料。



所有資料集列表				
搜尋: <input type="text"/>				
項次	resource_id	資料集名稱	SOCPE	需要的身分驗證安全等級
1	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	自然人憑證或工商憑證
2	tygh.resource.prenatal	產前檢查紀錄	tygh.resource.prenatal.read	自然人憑證或工商憑證
3	API.UbwT0ojLZ1	高級中等學校學生畢業資料	search	自然人憑證或工商憑證



測試流程



項次	工作項目	備註
1	機關單位依資料集註冊之內容，開發功能。	
2	若機關單位測試環境進行介接測試時，須通過防火牆設定者請先告知，雙方團隊先行完成相關設定。	
3	機關單位 Introspection Endpoint 測試。	
4	機關單位 UserInfo Endpoint 測試。	
5	機關單位功能開發完成，與 MyData 團隊進行資料請求、傳輸功能測試。 (DP-API Endpoint 測試)	
6	於測試環境驗證機關單位「Heartbeat」功能。	
7	機關單位正式環境移轉。若機關單位正式環境進行介接時，須通過防火牆設定者請先告知，雙方團隊先行完成相關設定。	
8	MyData 團隊於機關單位正式環境進行資料請求、傳輸功能測試。 (DP-API Endpoint 測試)	
9	於正式環境驗證機關單位「Heartbeat」功能。	
10	正式介接完成，於正式上線前 MyData 團隊將主動通知合作機關服務上線日期。	

正式環境網址與技術參考文件



- 後臺正式機登入網址：
<https://mydata.nat.gov.tw/mydata-backend>
- 前臺正式機網址：
<https://mydata.nat.gov.tw>
- 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 ▾

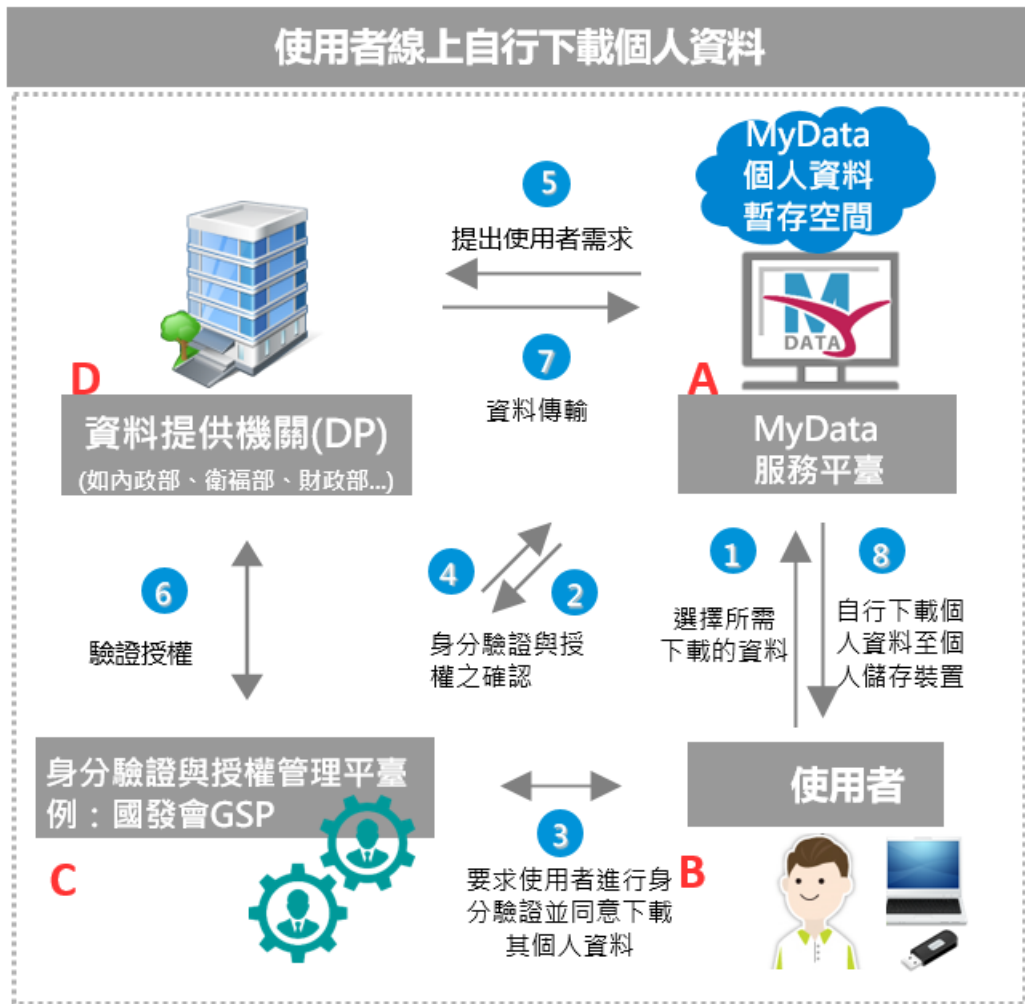
ehousekeeper Update README.md Latest commit 4305b70 Dec 11, 2019

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、技術說明

服務情境：資料下載





技術規範說明

OAuth2 API



Step6 : Introspection Endpoint



使用目的： DP 向 GSP 授權主機檢核 access_token 的有效性。

請求網址示意：

```
POST /v1/connect/introspect HTTP/1.1
Host: login.cp.gov.tw
Content-Type: application/x-www-form-urlencoded
Authorization: Basic {credential}

token={access_token}
```

credential 的組成方式： `Base64Encode({resource_id}:{resource_secret})`

resource_id：MyData 核發的資料集的識別值，於 MyData 管理後台取得。

resource_secret：MyData 核發的資料集密鑰，於 MyData 管理後台取得。

將 resource_id 及 resource_secret 以：符號串接後的字符串，以 Base64Encoder 編碼演算所得即為 credential 參數值。



Step6 : Introspection Endpoint



GSP 回覆請求成功：

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

```
{
  "nbf": "",
  "exp": "",
  "iss": "",
  "aud": "",
  "client_id": "",
  "sub": "",
  "auth_time": "",
  "scope": "{scope}",
  "active": true|false
}
```

DP 判斷 access_token 是否有效的方法：

1. 判斷 active 值是否為 true 。 true 代表 access_token 有效，反之為 false 。
2. 依據 scope 值來判斷用戶是否同意授權。資料集的 scope 值，由 DP 於 MyData 管理後台中設定。



Step6 : Introspection Endpoint



GSP 回覆請求失敗：

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

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

GSP 以 HTTP 400 代表回覆請求失敗。



Step6 : UserInfo Endpoint



使用目的： DP 向 GSP 授權主機查詢用戶基本資訊。

請求網址示意：

```
GET /v1/connect/userinfo HTTP/1.1  
Host: login.cp.gov.tw  
Authorization: Bearer {access_token}
```

access_token：由 GSP 授權主機核發，於用戶同意授權後產生。



Step6 : UserInfo Endpoint



GSP 回覆請求成功：

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

{
  "sub": "GSP USER ID",
  "cn": " 王小明 ",
  "uid": " 身分證字號 ",
  "uid_verified": "true|false 身分證字號是否已綁定 eGov 帳號",
  "birthdate": "1973/07/14",
  "gender": "M|F 性別",
  "email": "janedoe@example.com",
  "account": "eGov 帳號"
}
```

DP 識別用戶身分的方法：以用戶身分證字號 (uid) 來判斷使用者身份。



Step6 : UserInfo Endpoint



GSP 回覆請求失敗：

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

GSP 以 HTTP 401 回覆請失敗。





技術規範說明

DP-API



Step7 : DP-API 請求及回覆規格說明



使用目的： MyData 向 DP 請求取得用戶個人資料。

```
POST /mydata-dp/{resource} HTTP/1.1
Host: xxx.xxx.xxx.xx
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}
```

參數說明：

resource：用來識別資料集的字符串。DP 於 MyData 管理後台登錄 DP-API URL。

content_type：application/zip 代表 MyData 請求 DP 回覆「DP 資料打包檔」。

access_token：GSP 核發，代表用戶同意授權的識別值。

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。

交易鍵值有效期為，始自第一次發動 DPAPI 請求後，到 MyData 取得 DP 回覆資料檔後或 DP 回覆請求失敗或查無資料後止。格式為 UUID v4 字符串。

custom_param1_key：用戶填入的自訂參數鍵。

custom_param1_value：用戶填入的自訂參數值。



Step7 : DP-API 請求及回覆規格說明



DP 回覆請求成功 – 即時回應

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

若 DP 回覆請求時，已可將資料檔案回傳，則令 MyData 以檔案下載的方式取得。
在 HTTP header 上註明 content_type 及 filename。

DP 回覆請求成功 – 等候處理

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

若 DP 尚須時間準備資料檔案。可先回覆 HTTP 429 並於告知須等候處理的時間。
delay_seconds：藉此告知 MyData 下次發動請求前需等待的秒數。



Step7 : DP-API 請求及回覆規格說明



DP 回覆查無資料

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

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

依據請 `pdf` 設計格式與標準應如正常回復 `pdf` 檔並於內文標明「查無資料」； `json` 檔內容請請回覆：

```
{ "code": 204, "text": "查無資料" }
```



Step7 : DP-API 請求及回覆規格說明



DP 回覆請求失敗

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

401 : access_token 檢核失敗。

403 : 拒絕存取。

504 : 無法完成傳送資料檔案。



Step7 : DP-API Heartbeat 機制



目的：MyData 藉此確認 DP-API 仍有效存在。

MyData 發出 heartbeat 請求：

```
GET /mydata-dp/{resource}?heartbeat=true HTTP/1.1  
Host: xxx.xxx.xxx.xx  
Content-Type: application/json
```

請 DP 於 DP-API 定義參數 **heartbeat** 代表不須處理資料。
直接回覆請求，以告知 MyData 此 DP-API 的狀態。

200：回覆 HTTP 200 代表 DP-API 狀態健康。

其它：回覆非 200 時，MyData 即視為 DP-API 狀態異常。
發生連線逾時的情況時，也視為 DP-API 狀態異常。



技術規範說明

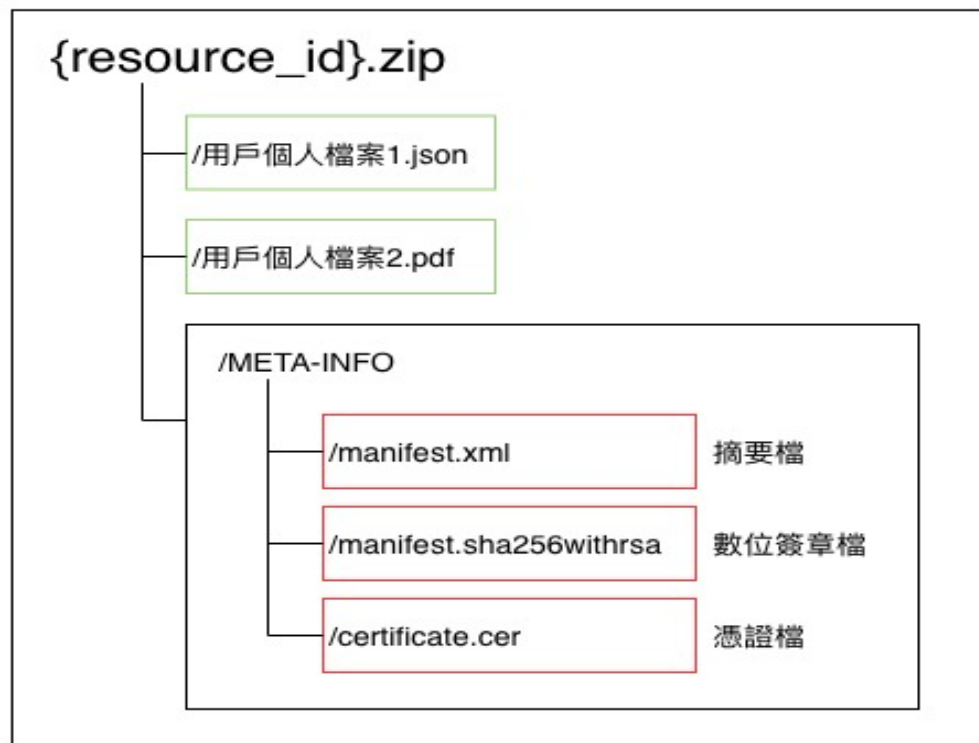
DP資料打包檔



DP 資料打包檔，結構及內容物說明



DP 資料打包檔，
檔案結構示意：



一個 DP 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。

**** 如果 DP 沒有產製數位簽章檔案就沒有 META-INFO 子目錄。**



DP 資料打包檔，結構及內容物說明



DP 個人資料檔格式，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，並須以民眾身分證字號加密 PDF 檔。）。

DP 個人資料檔內容的**解析規則**，DP 須提供檔案規格文件供 SP 使用。



產生 manifest.xml 摘要檔的方法



manifest.xml 摘要檔，內容格式示意：

```
<?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>
```

摘要檔的產生方法：

1. 以 SHA256 演算法計算各別資料檔案的摘要值（數位指紋）。
2. 如上述 XML 規格，將資料檔的檔名及摘要值載明於 filename, digest TAG 中。
3. 摘要檔檔案名稱請固定使用 manifest.xml 並保存於 META-INFO 子目錄。





以 **SHA256withRSA** 針對 manifest.xml 演算後產生的二進位內容。
保存檔案名稱固定使用 manifest.sha256withrsa

SHA256withRSA 演算過程說明：

1. 以 SHA256 演算法，計算 manifest.xml 的摘要值（數位指紋）。
2. 以 DP 的私鑰對摘要值進行加密演算後，將結果保存為檔名 manifest.sha256withrsa。
3. 此檔案即為 manifest.xml 的數位簽章檔。以副檔名 sha256withras 示意演算方法為 SHA256withRSA。

建議 DP 可以向 GCA 政府憑證管理中心申請「**政府機關單位憑證非 IC 卡類**」。

建議 DP 的私鑰長度至少為 2048 bits。

certificate.cer 憑證檔，規範以 **PEM** 格式提供給 SP 於驗簽時使用。

若 DP 由 CA 所取得的憑證檔為 DER 格式，須請 DP 將之轉換為 PEM 格式後提供。

同一 DP 可使用同一憑證作為簽章

註：只須提供憑證資訊，切不可包含私鑰資訊。





簡報完畢
敬請指教

