

內政部-行動自然人憑證系統 需用機關API說明會



內政部資訊中心
中華電信團隊
110年11月

議程大綱



1.機關申辦方式



2.TW FIDO既有服務仍正常運作



3.行動自然人憑證身分識別5大模式



4.API說明

議程大綱



1.機關申辦方式



2.TW FIDO既有服務仍正常運作

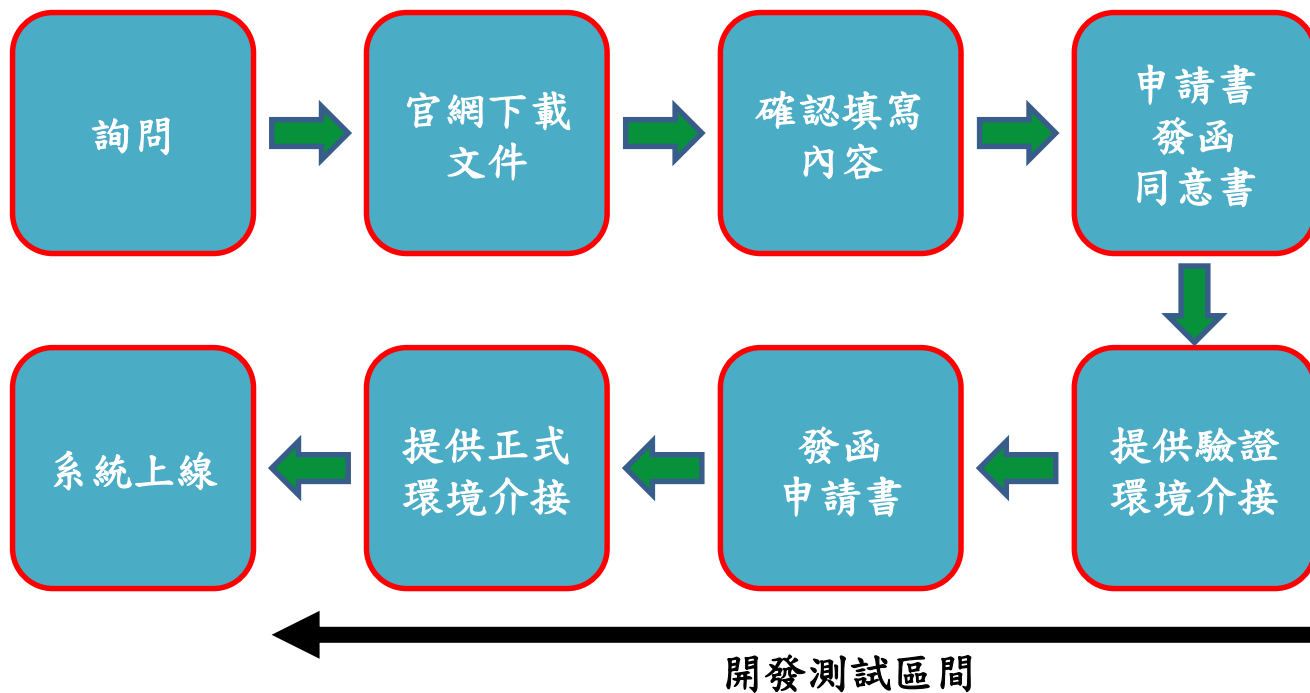


3.行動自然人憑證身分識別5大模式



4.API說明

1. 申辦流程



1.1 申辦方式

◆ 申辦資格

- 目前開放政府機關、金融、電信業者介接。

◆ 申辦流程

- 1.填寫**申請書**、**同意書**，**同意書用印**(機關用印或公司章)，申請書與同意書蓋騎縫章，檢送內政部辦理申請。
- 2.**選定驗證模式**，由內政部審核通過後提供系統介接手冊。
- 3.測試環境對接，內政部提供測試環境進行測試，需用單位可先於測試環境驗證，確認功能無誤後再切換至正式環境連線使用

◆ 注意事項

- 1.同一個單位可以申請多個系統。
- 2.一個系統提供一組系統碼，用來當作呼叫 API 的鑰匙。
- 3.若介接系統需進行壓力測試，請先告知本部及中華團隊。

議程大綱



1.機關申辦方式



2.TW FIDO既有服務仍正常運作



3.行動自然人憑證身分識別5大模式



4.API說明

2.1 TW FIDO既有服務仍正常運作(1/2)

- ◆ TW FIDO既有服務無痛移轉介面為相容於原TW FIDO行動身分識別服務之API介面，主要提供需用機關既有服務已介接TW FIDO行動身分識別服務可透過無痛移轉方式介接至行動自然人憑證服務API介面。需用機關介接TW FIDO既有服務無痛移轉介面需調整API URL，請參考「內政部行動身分識別服務介面規格」。



- ◆ 正式環境{fidoapi}:fidoapi.moi.gov.tw
- ◆ 驗證環境{fidoapi}:fidoapi-test.moi.gov.tw

2.2 TW FIDO既有服務仍正常運作(2/2)

原TW FIDO 介面編號	說明	url介面
RP-API-FWEB-01	應用系統網頁選擇認證登入時，導頁到RP Server的URL，此頁面為含有二維條碼的頁面，等待APP認證通過後再導頁回應用系統申請時本服務提供的URL。雙方的導頁皆會以chksum驗證碼的方式進行雙方主機參數驗證。	https://{fidoapi}/
RP-API-FATH-01	由應用系統發動通知RP Server，RP Server推播給APP通知使用者進行確認。	https://{fidoapi}/moili/service/v1/api/pushAuth
RP-API-FATH-02	由應用系統主機需要發動此交易，詢問使用者是否已經確認完成身分識別。	https://{fidoapi}/moili/service/v1/api/authConfirm
RP-API-FEXCH-01	由應用系統發動通知RP Server，請求提供產生QR Code需要的參數。	https://{fidoapi}/moili/service/v1/api/exPushAuth
RP-API-REG-01	提供介接單位確認使用者之註冊狀態。	https://{fidoapi}/moili/service/v1/api/regConfirm
RP-API-QUE-01	提供介接單位確認區間之身分驗證記錄統計	https://{fidoapi}/moili/service/v1/api/queryTxnByDate
RP-API-QUE-02	提供介接單位確認單一使用者之身分驗證記錄(使用者於此應用系統的登入紀錄) 逐筆列出此段期間的交易	https://{fidoapi}/moili/service/v1/api/queryTxnByUser

議程大綱



1.機關申辦方式



2.TW FIDO既有服務仍正常運作



3.行動自然人憑證身分識別5大模式



4.API說明

3. 行動自然人憑證識別程序



3.1 行動自然人憑證身分識別五大模式

◆ 需用機關識別模式-網站及行動裝置身分識別。

驗證模式	識別情境	例子
網站識別 模式	1.條碼(QR Code)模式	店家之防疫掃描
	2.推播模式	LINE訊息推播
	3.Mobile Web對App模式	
	4.網頁轉導模式	3D信用卡驗證
行動裝置 識別模式	5.App對App模式	購物網之FB帳號登入

3.2 需用機關介接應用流程說明

◆ 網頁轉導模式：

- 透過網頁轉導方式進行認證/簽署作業。

◆ 主掃QR Code模式：

- 透過App掃描網站顯示之QR Code方式進行認證/簽署作業。

◆ App推播模式：

- 透過App訊息推播方式進行認證/簽署作業。

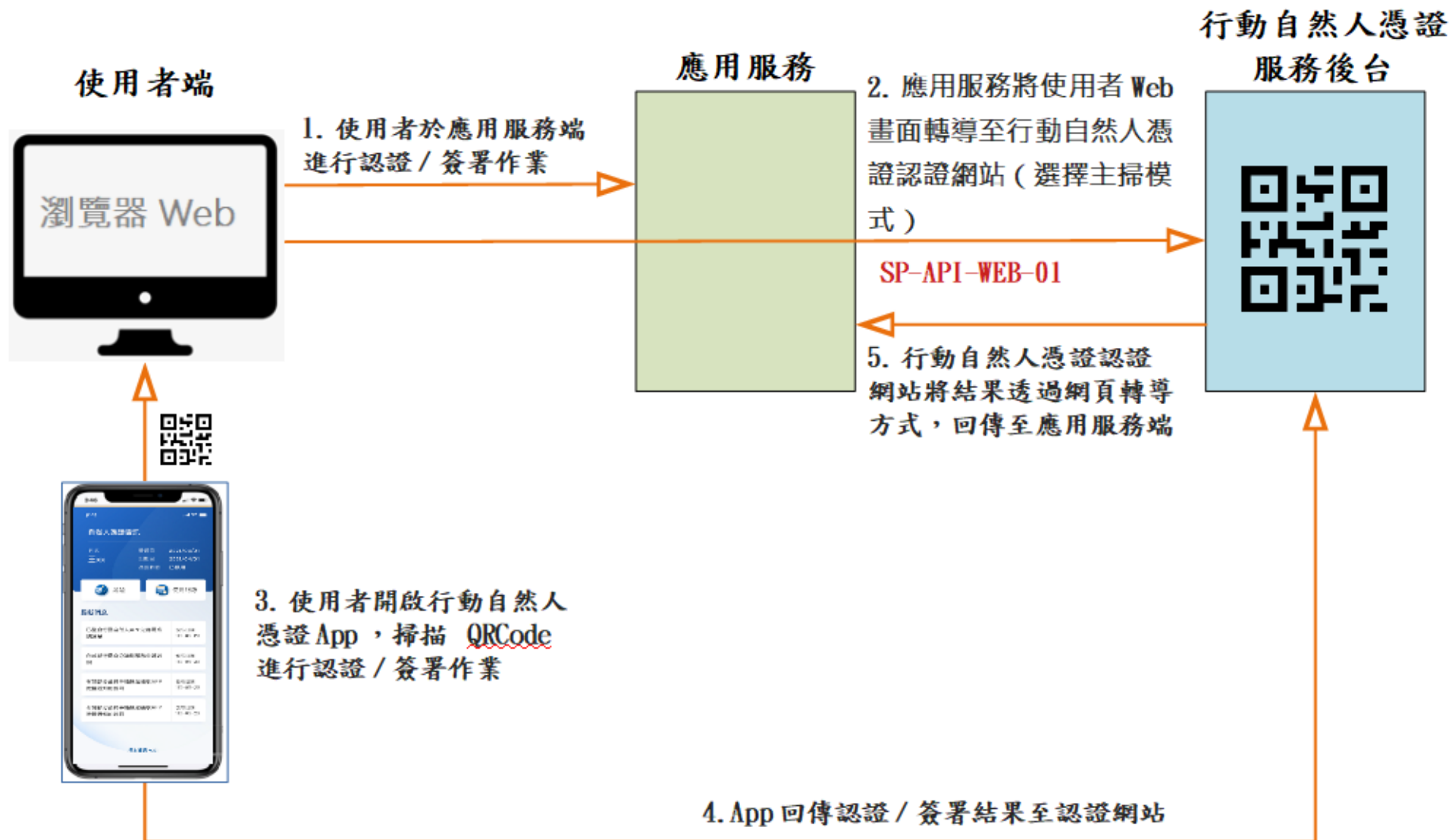
◆ Mobile Web to App模式：

- 透過 Mobile Web(手機端瀏覽器) to APP 方式進行認證/簽署作業。

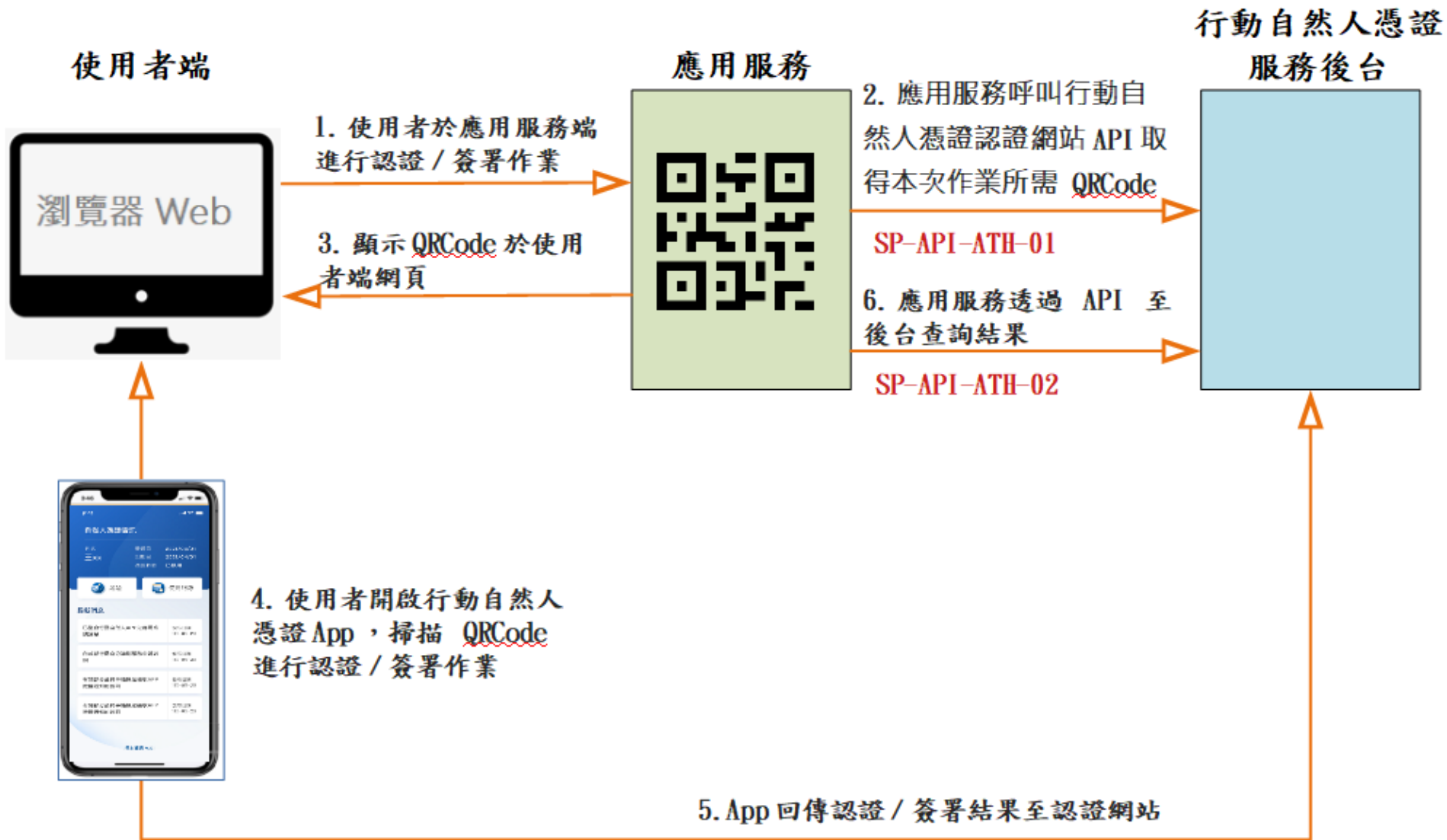
◆ App to App模式：

- 透過 App to App 方式(跨App呼叫)進行認證/簽署作業。

3.2.1 網頁轉導模式介接應用流程說明



3.2.2 QR Code模式介接應用流程說明



3.2.3 推播模式介接應用流程說明

使用者端

應用服務

行動自然人憑證
服務後台

1. 使用者於應用服務端
進行認證 / 簽署作業

2. 應用服務呼叫行動自然
人憑證認證網站 API 通知
使用者進行認證 / 簽署作業

SP-API-ATH-03

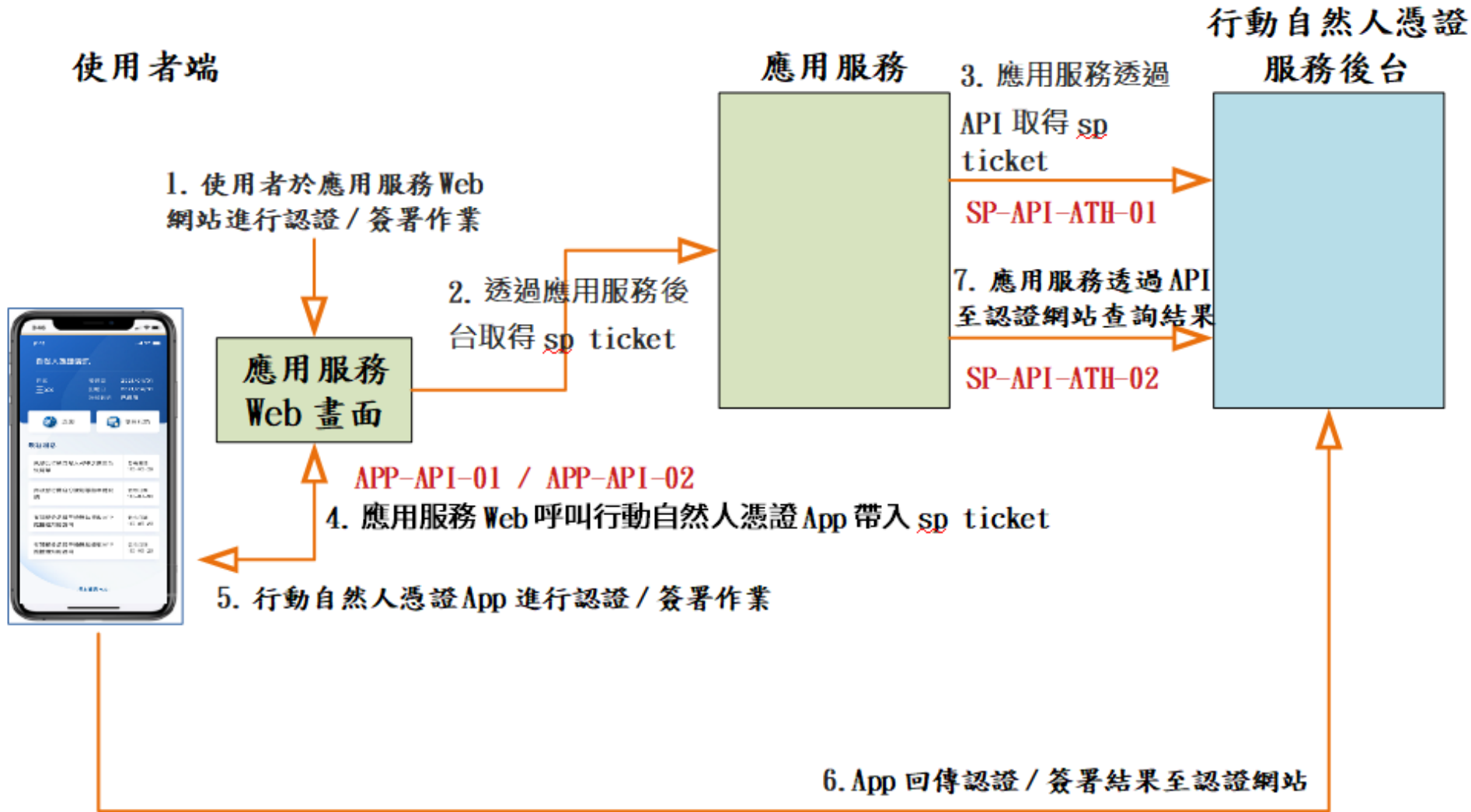
5. 應用服務透過 API 至
認證網站查詢結果

SP-API-ATH-02

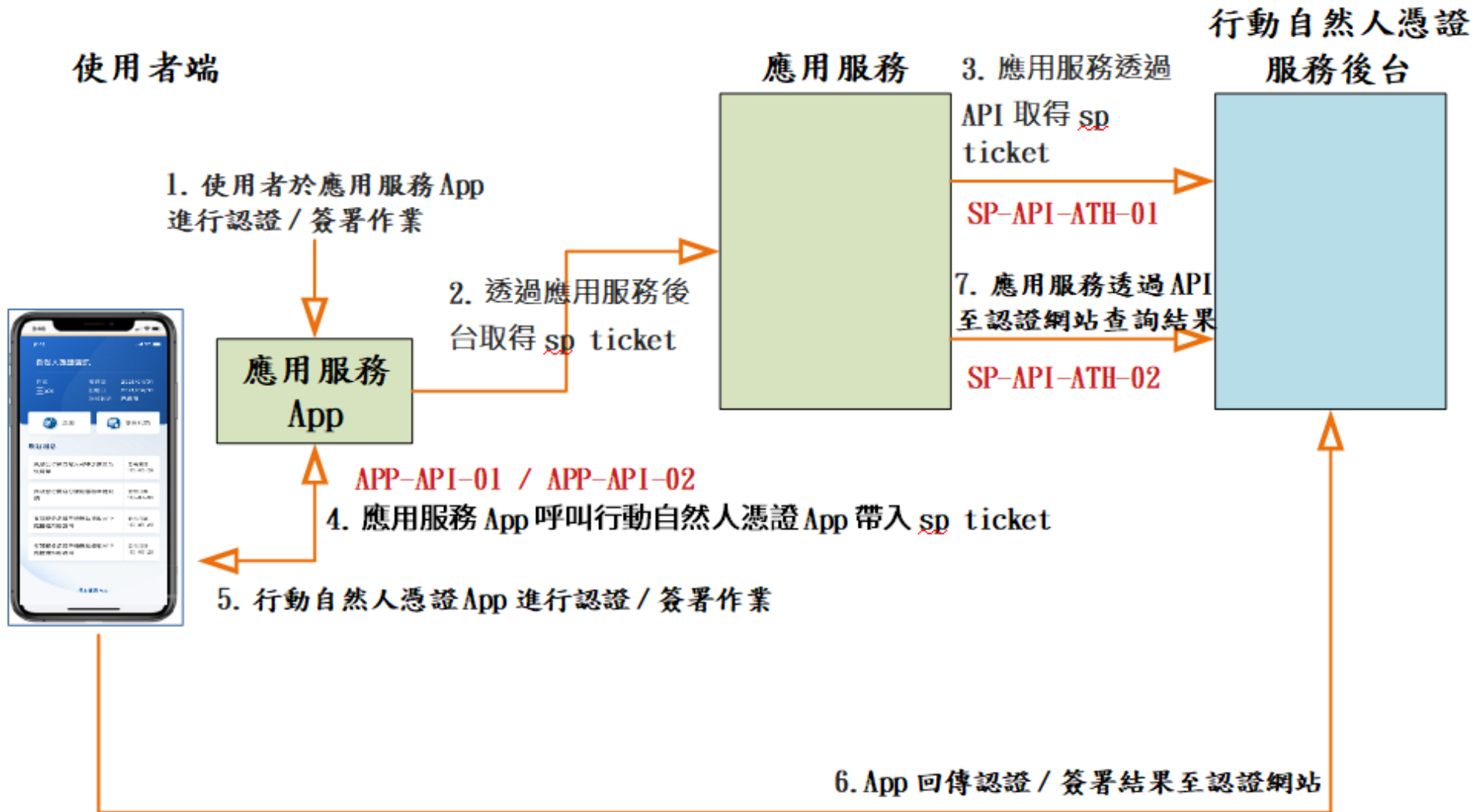
3.1 後台將認證 / 簽署請求訊息推播至使用者行動自然人憑證 App
3.2 使用者進行確認並同意後執行

4. App 回傳認證 / 簽署結果至認證網站

3.2.4 Mobile Web to APP模式介接應用流程說明



3.2.5 APP to APP模式介接應用流程說明



3.3 需用機關介接測試方式說明

◆ 測試環境申請：

- 需用機關應用服務評估所需採用之識別模式(五種模式)。
- 向內政部申請應用服務介接測試，並填妥與交付【行動自然人憑證服務申請書】與【使用規定同意書】。
- 內政部審查通過後，開通防火牆等網路設定，並提供應用服務窗口介接測試所需相關資料：
 - 行動自然人憑證服務介面規格(含介面與流程說明)
 - 應用服務介接所需 API Key
 - 測試區行動自然人憑證認證網站網址或App (Android、iOS)
- 測試人員透過自然人憑證IC卡至認證網站執行App註冊綁定作業。
- 透過介面規格內API與流程說明及參考範例，即可進行所需認證模式介接測試。
 - 行動自然人憑證認證網站後台，提供 Restful API方式供介接(除轉導模式外)。
 - 應用服務應開通與內政部測試環境防火牆，並確認連線正常。
 - 若遇到測試異常，請提供所接收到之錯誤訊息。

3.4 防火牆 – 正式環境/驗證環境

發送端	發送端 IP	接收端	接收端 IP/Domain	接收端port
應用系統	發動API的政府 單位IP	行動自然人憑證系統 (正式環境)	https://fidoapi.moi.gov.tw	443

發送端	發送端 IP	接收端	接收端 IP/Domain	接收端port
應用系統	發動API的政府 單位IP	行動自然人憑證系統 (驗證環境)	https://fidoapi-test.moi.gov.tw	443

議程大綱



1.機關申辦方式



2.TW FIDO既有服務仍正常運作



3.行動自然人憑證身分識別5大模式



4.API說明

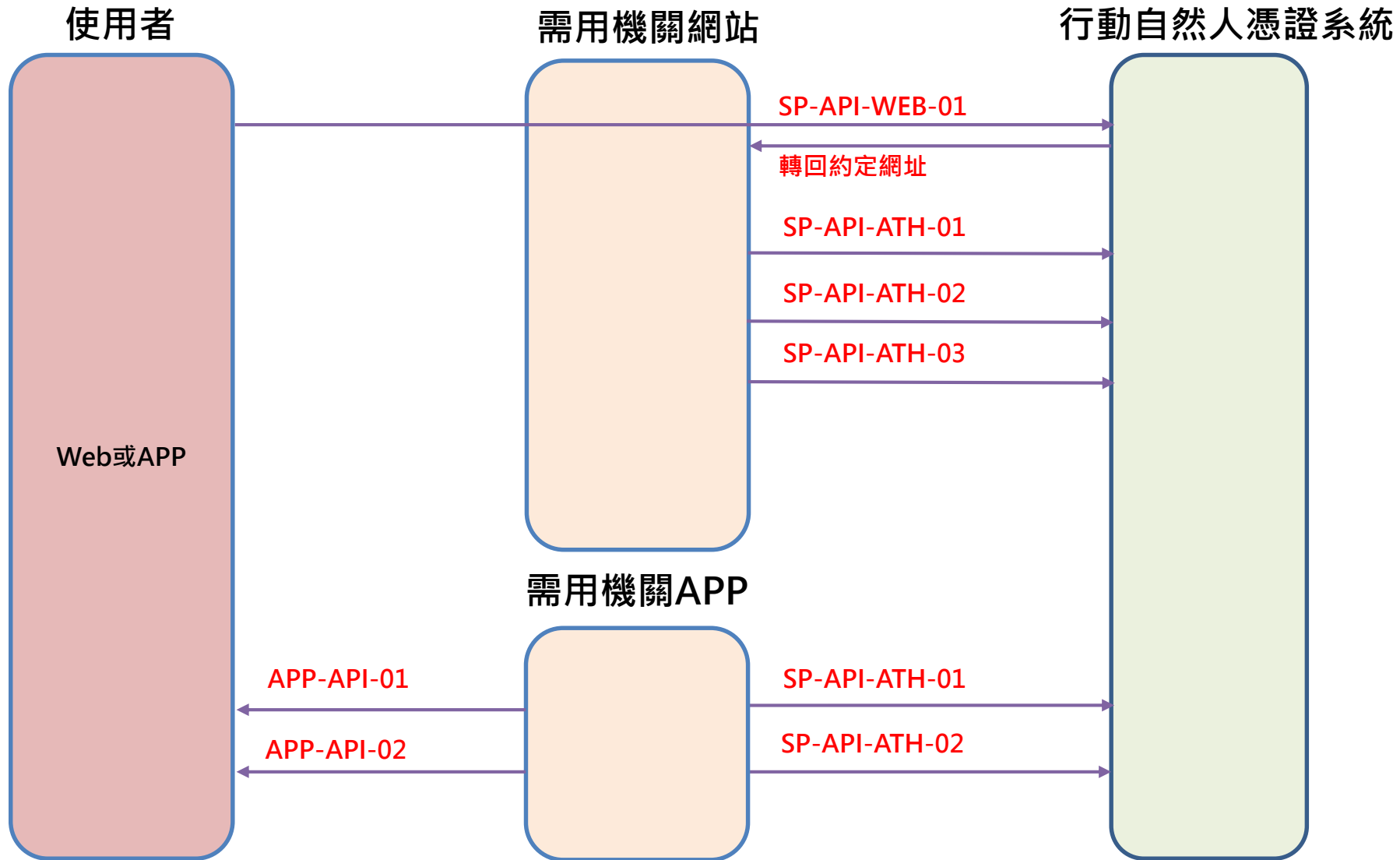
4. 行動自然人憑證服務介面清單(1/2)

- ◆ 正式環境{fidoapi}:fidoapi.moi.gov.tw
- ◆ 驗證環境{fidoapi}:fidoapi-test.moi.gov.tw

介面編號	說明	url介面
SP-API-WEB-01	網頁轉導模式介面	https://{weburl}/fidoRedirect
SP-API-ATH-01	請求 SP ticket(主掃, APP2APP, MWeb2APP)	https://{fidoapi}/moise/sp/getSpTicket
SP-API-ATH-02	查詢認證/簽署結果	https://{fidoapi}/moise/sp/getAthOrSignResult
SP-API-ATH-03	請求認證/簽署推播	https://{fidoapi}/moise/sp/requestAthOrSignPush
SP-API-LF-01	確認使用者裝置綁定狀態	https://{fidoapi}/moise/sp/checkDeviceStatus

介面編號	說明	url介面
APP-API-01	當第三方服務需透過「自然人憑證APP」進行簽章功能時使用。	請參閱下方說明。
APP-API-02	當第三方服務需透過「自然人憑證APP」進行認證功能時使用。	請參閱下方說明。

4. 行動自然人憑證服務介面清單(2/2)



4.1.1 SP-API-WEB-01：網頁轉導模式介面

介面編號	SP-API-WEB-01							
中文名稱	網頁轉導模式介面							
英文名稱	fidoRedirect							
介面方式	WEB UI							
通訊協定	HTTP POST							
URL	https://{fidoweb}/fidoRedirect/web							
功能描述	提供需用機關系統網頁轉導 UI							
使用限制	需帶 SP 服務識別代碼、SP 驗證碼、hint							
使用範例	需用機關以網頁轉導進行簽章、驗證功能							
呼叫系統名稱	需用機關系統網站							
被呼叫系統名稱	行動自然人憑證服務網站							
輸入 POST Form 參數								
編號	中文名稱	英文名稱	型別	長度	必要欄位	傳輸類別	次數	備註
1	交易序號	transaction_id	String		Y	Request	1	請參考三、 (一) transaction_id 格式說明
2	操作代碼	op_code	String		Y	Request	1	認證/簽章 值域：{ATH, SIGN}
3	SP 服務識別代碼	sp_service_id	String		Y	Request	1	
4	SP 驗證碼	sp_checksum	String		Y	Request	1	請參考三、 (三) sp_checksum 格式說明及 計算方式 ● Payload： transaction_id

請參考三、
(一)
[transaction_id](#)
格式說明

認證/簽章
值域：{ATH,
SIGN}

請參考三、
(三)
[sp_checksum](#)
格式說明及
計算方式

● Payload：
[transaction_id](#)

							+sp_service_id+op_code+hint+sign_data
5	提示訊息	hint	String		Y	Request	1
6	簽章資訊	sign_data	String			Request	0, 1
回傳 callback 參數							
編號	中文名稱	英文名稱	型別	長度	必要欄位	傳輸類別	次數
1	交易序號	transaction_id	String		Y	Response	1
2	錯誤代碼	error_code	String		Y	Response	1
3	身份證號	id_num	String		Y	Response	1
4	簽章結果	signed_response	String			Response	0, 1
5	Server 端驗證碼	idp_checksum	String		Y	Response	1

PKCS#7 格式
僅適用於簽
章模式

請參考三、
(四)
[idp_checksum](#)
格式說明及
驗證方式

● Payload：
[transaction_id](#)
+ [error_code](#)
+ [id_num](#) + [signed_response](#)

範例

輸入參數範例

POST https://{weburl}/fidoRedirect/web

Form data

4.1.2 SP-API-WEB-01 : 範例

範例

輸入參數範例

POST https://{weburl}/fidoRedirect/web

Form data

op_code=SIGN

sign_data=待簽資料

hint=簽章提示訊息

transaction_id=TD1635246114704

sp_service_id=7b2c7f94-9f7b-481a-89a8-56b883dea695

sp_checksum=09fc41e5ed1b3bed6e09e000b0ed0d8056717e429dd70c846cd006e8a26b383691eb51e82693f4692ef111cb2afc724cde6c4b25a90bb231528c3b987bce1d7a587510888d73eb55e37d3d8d200a6eb65db5d4da4d7343dfcc27942

回傳參數範例

POST https://{callback_url}

Form data

transaction_id=TD1635246114704

error_code=0

id_num=A123456789

signed_response=EROEJROWERJOREWORJEWOREORJEOR

idp_checksum=1af56063d5f182ae67443133d2d81b24bb76d29399d9a03f1004290368dc575bbab68b77f220e9d8545b5549f9584f843bcb12cfd4a22aef7debe124fd91849b707eefdb5e40980bc38c539205a0de58ac07dd52452c23870fbf721a

4.2.1 SP-API-ATH-01：請求 SP ticket (輸入)

介面編號：SP-API-ATH-01

類型：Rest API

功能：請求 SP ticket

介面名稱：getSpTicket

URL：HTTP POST <https://{fidoapi}/moise/sp/getSpTicket>

Header 參數：

- Content-Type: [APPLICATION/json](#)

傳入參數：

- JSON 格式，定義如下：

欄位名稱	型態	必要欄位	說明
transaction_id	String	V	交易序號
sp_service_id	String	V	SP 服務識別代碼
sp_checksum	String	V	SP 驗證碼 ● 格式： AES_GCM_HEX(SHA256_HEX(Payload)) ● Payload： transaction_id+sp_service_id+id_num+op_code+op_mode+hint+sign_data 計算方式請參考資料格式設計之 sp_checksum
id_num	String	V	身分證號
op_code	String(Enum)	V	認證/簽署 值域：{ATH, SIGN}
op_mode	String(Enum)	V	主動式掃描/APP-to-APP/Mobile Web to APP 值域：{I-SCAN, APP2APP, MWEB2APP}

hint	String	V	提示訊息
sign_info	JSON	C	簽章資訊

- [sign_info](#) 欄位，定義如下：

欄位名稱	型態	必要欄位	說明
sign_data	String	V	待簽資料

4.2.2 SP-API-ATH-01：請求 SP ticket (輸出)

回傳參數：↵

- JSON 格式，定義如下：↵

欄位名稱↵	型態↵	必要欄位↵	說明↵
<u>error code</u> ↵	String↵	V↵	錯誤代碼↵
<u>error message</u> ↵	String↵	V↵	錯誤訊息↵
<u>result</u> ↵	JSON↵	C↵	回應資訊之集合↵

↵

- result 欄位，定義如下：↵

欄位名稱↵	型態↵	必要欄位↵	說明↵
<u>sp ticket</u> ↵	String↵	V↵	欄位請參考資料格式設計之 sp ticket ↵
<u>idp checksum</u> ↵	String↵	V↵	Server 端驗證碼↵ ↵ ● 格式：↵ 同 <u>sp checksum</u> ↵ ↵ ● Payload：↵ <u>transaction id</u> + <u>error code</u> + <u>sp ticket</u> ↵ ↵ 計算方式請參考資料格式設計 之 idp checksum ↵

↵

4.2.3 SP-API-ATH-01：範例

範例：↵

輸入參數↵

```
{↵
  "transaction_id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",↵
  "sp_service_id": "7b2c7f94-9f7b-481a-89a8-56b883dea695",↵

  "sp_checksum": "1241c87f32fbe9effec8ac9206e89e066b751f4dec9bb126e93dd
b67dbad10e8abc69206b84b64660675d90a8e1ff887057f42dbfceb3f49167c4e
9ca1481359ffb76efdcabd7649ffa045805a87f1e834ef41f6427646e9bffc5",↵
  "id_num": "A123456789",↵
  "op_code": "SIGN",↵
  "op_mode": "I-SCAN",↵
  "hint": "待簽署資料",↵
  "sign_info": {↵

  "sign_data": "DOC_DIGEST_JLDKJFLKDSJFLDSLFLJSDLFLSKDFJLSFJLS
FJLDSKFJLKSDFJLSFJLKDSFJLKSDFFSFSDFSDFFSDFSFF"↵
}↵
}↵
```

輸出參數↵

```
{↵
  "result": {↵
    "sp_ticket":
"eyJ0cmFuc2FjdGlvb19pZCI6IjA0NmI2YzdmLTBib0GETNDNiOS1iMzVkLT
Y0ODllNmRhZWU5MSIsIm9wX2NvZGU0iJTSUdOIiwib3BfbW9kZSI6Ikkt
tU0NBtIiIsInNwX3NlcnZpY2VfaWQiOiI3YjJjN2Y5NC05ZjdiLTQ4MWEtO
DlhOC01NmI4ODNkZWE2OTUiLCJzcF90aWNrZXRFaWQiOiI3NzE2NWM
1OS1iYjA3LTRjODYtYTMxYS0wZWY4ZjNlOGU0ZGEiLCJzcF9uYW1lIjo
i5qih5pOs5ris6Kmm5qmf6ZecIiwic2lnbl9kb2MiOiJET0NfREIHRVNUX0pM
REtKRkxLRfNKRkxU0xGSINETEZKTFNLRZKTFNGSkxTRkpMRfNL
RkpMS1NERkpMU0ZKTEtEU0ZKTEtTREZEU0ZTREZTREZEU0ZEU0ZG
IiwiaGludCI6IuW-heewvee9suizh-
aWmSIslmV4cGlyYXRpb25fdGltZSI6IjE2Mjk0ODAyNjYwMDAiLCJoYXN
oZWRFaWRfbnVtIjojVWY4Z3BYSlQ5X0R1T3B2XzZhcUdvaFFjY1dzdlZV
c3I5a0tkOVE1VGpCTSJ9.NVDdk5DXwfDhtgy2KrQRCbw10F2Xfji6_vUUY1
ff9FM",↵
    "idp_checksum":
"1af56063d5f182ae67443133d2d81b24bb76d29399d9a03f1004290368dc575b
bab68b77f220e9d8545b5549f9584f843bcb12cfd4a22aef7debe124fd91849b707
eefdb5e40980bc38c539205a0de58ac07dd52452c23870fbf721a "↵
  },↵
  "error_message": "SUCCESS",↵
  "error_code": "0"↵
}↵
```

4.3.1 SP-API-ATH-02：查詢認證/簽署結果

類型：Rest API

功能：查詢認證/簽署結果

介面名稱：getAthOrSignResult

URL：HTTP POST https://{fidoapi}/moise/sp/getAthOrSignResult

Header 參數：

- Content-Type: Application/json

傳入參數：

- JSON 格式，定義如下：

欄位名稱	型態	必要欄位	說明
<u>transaction id</u>	String	V	交易序號
<u>sp service id</u>	String	V	SP 服務識別代碼
<u>sp checksum</u>	String	V	SP 驗證碼 ● 格式： <u>AES_GCM_HEX(SHA256_HEX(Payload))</u> ● Payload： <u>transaction id+sp service id+sp ticket id</u> 計算方式請參考資料格式設計之 <u>sp checksum</u>
<u>sp ticket id</u>	String	V	SP Ticket 內含之查詢代碼

回傳參數：

- JSON 格式，定義如下：

欄位名稱	型態	必要欄位	說明
<u>error code</u>	String	V	錯誤代碼
<u>error message</u>	String	V	錯誤訊息
<u>result</u>	JSON	C	回應資訊之集合

- result 欄位，定義如下：

欄位名稱	型態	必要欄位	說明
<u>hashed id num</u>	String	V	身分證號 Hash 值
<u>signed response</u>	String	C	PKCS#7格式(請參考PKI SDK 介面規格) 僅適用於簽署模式
<u>idp checksum</u>	String	V	Server 端驗證碼 ● 格式： 同 <u>sp checksum</u> ● Payload： <u>transaction id+ error code+ hashed id num+signed response</u> 計算方式請參考資料格式設計之 <u>idp checksum</u>

4.3.2 SP-API-ATH-02：範例

範例：←

輸入參數←

```
{←
  "transaction_id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",←
  "sp_service_id": "7b2c7f94-9f7b-481a-89a8-56b883dea695",←

  "sp_checksum": "1241c87f32fbe9effec8ac9206e89e066b751f4dec9bb126e93dd
b67dbad10e8abc69206b84b64660675d90a8e1ff887057f42dbfbceb3f49167c4e
9ca1481359ffbf76efdcabd7649ffa045805a87f1e834ef41f6427646e9bffc5",←
  "sp_ticket_id": "901070aa-0650-4480-99e3-fd5573a3e0b9"←
}←
```

←

輸出參數←

```
{←
  "result": {←
    "signed response": "EROEJROWERJOREWORJEWOREORJEOR",←
    "idp_checksum":
"1af56063d5f182ae67443133d2d81b24bb76d29399d9a03f1004290368dc575b
bab68b77f220e9d8545b5549f9584f843bcb12cfd4a22aef7debe124fd91849b707
eefdb5e40980bc38c539205a0de58ac07dd52452c23870fbf721a"←
  },←
  "error_message": "SUCCESS",←
  "error_code": "0"←
}←
```

4.4.1 SP-API-ATH-03：請求認證/簽署推播(輸入)

介面編號：SP-API-ATH-03

類型：Rest API

功能：請求認證/簽署推播

介面名稱：requestAthOrSignPush

URL：HTTP POST https://{fidoapi}/moise/sp/requestAthOrSignPush

Header 參數：

- Content-Type: Application/json

傳入參數：

- JSON 格式，定義如下：

欄位名稱	型態	必要欄位	說明
transaction id	String	V	交易序號
sp service id	String	V	SP 服務識別代碼
sp checksum	String	V	SP 驗證碼 ● 格式： AES_GCM_HEX(SHA256_HEX(Payload)) ● Payload： transaction id+sp service id+id_num+ device user def desc +op code+hint+sign_data 計算方式請參考資料格式設計之 sp_checksum
id num	String	V	身分證號
device user def desc	String	C	使用者自定義之裝置描述
op code	String(Enum)	V	認證/簽署 值域：{ATH, SIGN}
hint	String	V	提示訊息
sign info	JSON	C	簽章資訊

- sign info 欄位，定義如下：

欄位名稱	型態	必要欄位	說明
sign_data	String	V	待簽資料

4.4.2 SP-API-ATH-03：請求認證/簽署推播(輸出)

回傳參數：

- JSON 格式，定義如下：

欄位名稱	型態	必要欄位	說明
<u>error code</u>	String	V	錯誤代碼
<u>error message</u>	String	V	錯誤訊息
<u>result</u>	JSON	V	回應資訊之集合

- result 欄位，定義如下：

欄位名稱	型態	必要欄位	說明
<u>sp ticket</u>	String	V	欄位請參考資料格式設計之 sp ticket
<u>idp checksum</u>	String	V	Server 端驗證碼 ● 格式： 同 <u>sp checksum</u> ● Payload： <u>transaction id</u> + <u>error code</u> + <u>sp ticket</u> 計算方式請參考資料格式設計之 idp checksum

4.4.3 SP-API-ATH-03：範例

範例：↵

輸入參數↵

```
{↵  
  "transaction_id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",↵  
  "sp_service_id": "7b2c7f94-9f7b-481a-89a8-56b883dea695",↵  
  
  "sp_checksum": "1241c87f32fbe9effec8ac9206e89e066b751f4dec9bb126e93dd  
b67dbad10e8abc69206b84b64660675d90a8e1ff887057f42dbfbceb3f49167c4e  
9ca1481359ffbf76efdcabd7649ffa045805a87f1e834ef41f6427646e9bffc5",↵  
  "id_num": "Z111222333",↵  
  "op_code": "SIGN",↵  
  "hint": "待簽署資料",↵  
  "sign_info": {↵  
  
  "sign_data": "DOC_DIGEST_JLDKJFLKDSJFLDSLFIJSDLFIJLSKDFJLSFJLS  
FJLDSKFJLKSDFJLSFJLKDSFJLKSDFSFSDFSDFSDFSFF",↵  
  }↵  
}↵
```

```
AwliwiaGFzaGVkX2lkX251bSI6InMzQXQzcWtYZ3hlaU5VMWR6Z2pkbm  
5lZUhXVE81Q3FfUDgzT3JrQXo5UGMifQ.suoSD-  
odntrHNxEbgmm68gnB1vecryazryTIGkqxSKY",↵  
  "idp_checksum":  
  "1af56063d5f182ae67443133d2d81b24bb76d29399d9a03f1004290368dc575b  
bab68b77f220e9d8545b5549f9584f843bcb12cfd4a22aef7debe124fd91849b707  
eefdb5e40980bc38c539205a0de58ac07dd52452c23870fbf721a",↵  
  },↵  
  "error_message": "SUCCESS",↵  
  "error_code": "0"↵  
}↵
```

輸出參數↵

```
{↵  
  "result": {↵  
    "sp_ticket":  
    "eyJ0cmFuc2FjdGlvb9pZCI6IjA0NmI2YzdmLTBiOGEtNDNiOS1iMzVkLT  
Y0ODIlNmRhZWU5MSIsIm9wX2NvZGUiOiJTSUd0Iiwib3BfbW9kZSI6IlB  
VU0giLCJzcF9zZXJ2aWNlX2lkIjojN2IyYzdmOTQtOWY3Yi00ODFhLTg5Y  
TgtNTZiODgzZGVhNjk1Iiwic3BfdGJja2V0X2lkIjojZDc2NzNiNmQtNDk1Yi  
00MWUzLTk0ZDktYjlyYzBiMTg4MjE2Iiwic3BfbmFtZSI6IuaooeaTrOa4rOip  
puapn-  
mXnCIsInNpZ25fZG9jIjojRE9DX0RJROVTVF9KTERLSkZMS0RTSkZMRf  
NMRkpTRExGSkxTS0RGSKxTRkpMU0ZKTERTS0ZKTETREZKTFNGSKx  
LRFNGSKxLU0RGRFNGU0RGU0RGRFNGRFRNGRiIsImhpbmQiOiIvOlxns  
L3nvbLos4fmlpkiLCJleHBpcmF0aW9uX3RpbWUiOiIjNjE5NDgwMzgwMD
```


4.5.1 SP-API-LF-01：確認使用者裝置綁定狀態

介面編號：SP-API-LF-01

類型：Rest API

功能：確認使用者裝置綁定狀態

介面名稱：checkDeviceStatus

URL：HTTP POST https://{fidoapi}/moise/sp/checkDeviceStatus

Header 參數：

- Content-Type: APPLICATION/json

傳入參數：

- JSON 格式，定義如下：

欄位名稱	型態	必要欄位	說明
<u>transaction id</u>	String	V	交易序號
<u>sp service id</u>	String	V	SP 服務識別代碼
<u>sp checksum</u>	String	V	SP 驗證碼 <ul style="list-style-type: none">格式： <u>AES_GCM_HEX(SHA256_HEX(Payload))</u>Payload： <u>transaction id+sp service id+id_num</u> 計算方式請參考資料格式設計之 <u>sp_checksum</u>
<u>id_num</u>	String	V	身分證號

回傳參數：

- JSON 格式，定義如下：

欄位名稱	型態	必要欄位	說明
<u>error code</u>	String	V	錯誤代碼
<u>error message</u>	String	V	錯誤訊息
<u>result</u>	JSON	V	回應資訊之集合

- result 欄位，定義如下：

欄位名稱	型態	必要欄位	說明
<u>is fido</u>	String(Enum)	V	持有可用 FIDO 之裝置 值域：{Y, N}
<u>is mcert sign</u>	String(Enum)	V	持有可用憑證（簽章用途）之裝置 值域：{Y, N}
<u>idp checksum</u>	String	V	Server 端驗證碼 <ul style="list-style-type: none">格式： 同 <u>sp_checksum</u>Payload： <u>transaction id+ error code + is fido + is mcert sign</u> 計算方式請參考資料格式設計之 <u>idp_checksum</u>

4.5.2 SP-API-LF-01：範例

範例：↵

輸入參數↵

```
{↵  
  "transaction_id": "046b6c7f-0b8a-43b9-b35d-6489e6daee91",↵  
  "sp_service_id": "7b2c7f94-9f7b-481a-89a8-56b883dea695",↵  
  
  "sp_checksum": "1241c87f32fbe9effec8ac9206e89e066b751f4dec9bb126e93dd  
b67dbad10e8abc69206b84b64660675d90a8e1ff887057f42dbfbceb3f49167c4e  
9ca1481359ffbf76efdcabd7649ffa045805a87f1e834ef41f6427646e9bffc5",↵  
  "id_num": "A123456789"↵  
}
```

輸出參數↵

```
{↵  
  "result": {↵  
    "debug":  
    "2a0daff4d93f08d638c47de8698cc28687674c41c9e72e94f538659aa45a5865",↵  
    "is_fido": "N",↵  
    "is_mcert_sign": "N",↵  
    "idp_checksum":  
    "9df5e83e74b79adc4c3b567b312a7c82a6f46e15433093c03df1f2cde41c1285a1  
0667728c9bee5ec735c79a28d03cf8d0cd8b4887f5deeb9d5495869f2cb62f48ff0  
ddaa0a392652f23d8c8efa4899f095dd630521af18fa525fdfa"↵  
  },↵  
  "error_message": "SUCCESS",↵  
  "error_code": "0"↵  
}
```

備註：↵

4.6 資料格式說明：transaction_id

transaction id↵

格式：「UUID version 4」or「其他識別符號」↵

範例：046b6c7f-0b8a-43b9-b35d-6489e6daee91↵

備註：視情況可串接時間戳記等字串，惟 transaction id 總長度不大於100字元(暫定)↵

4.8.1 資料格式說明：sp_checksum

sp checksum↵

格式說明：←

AES GCM HEX(SHA256 HEX(Payload))⁴

[1] 產生 Payload \leftarrow

欄位範例(詳情請參考 SP-API-XX 各介面)←

```
transaction id+sp service id+id num+op code+op mode+hint+sign data+  
-----
```

內容範例←

046b6c7f-0b8a-43b9-b35d-6489e6daee917b2c7f94-9f7b-481a-89a8-

56b883dea695A987654321SIGNI-SCAN待簽署資料

DOC_DIGEST_JLDKJFLKDSJFLDSLFLJSLKDFJLSFJLSFJLDSK
FJLSKDFJLSFJLKDSFJLKSDSFDSDSFDSDSFDSDSFF

[2] 產生 SHA256 HEX(Payload) (==> sha256HexPayload)←

整個Payload字串 `getBytes(UTF-8)` 轉換後，進行 SHA256 運算產生 byte array，轉換為 Hex string 顯示

```
MessageDigest digest = MessageDigest.getInstance("SHA-256");  
final byte[] passwordBytes = base.getBytes("UTF-8");  
final byte[] salt = "".getBytes("UTF-8");  
final byte[] all = ArrayUtils.addAll(passwordBytes, salt);  
byte[] hash = digest.digest(all);  
return convertBinaryToHexString(hash);
```

[3] 產生 Random IV \leftarrow

```
int GCM_IV_LENGTH = 12;
byte[] iv = new byte[GCM_IV_LENGTH];
(new SecureRandom()).nextBytes(iv);
```

[4] 進行 AES GCM 加密←

```
int TAG_LENGTH = 128;←
```

```
GCMPParameterSpec ivSpec = new
GCMPParameterSpec(TAG_LENGTH, iv);
```

```
Cipher c = Cipher.getInstance(AES/GCM/NoPadding);  
c.init(Cipher.ENCRYPT_MODE, new SecretKeySpec(AesKeyInBytes,  
"AES"), ivSpec);
```

```
byte[] cipherVal = c.doFinal(sha256HexPayload.getBytes());
```

[5] 串接[3][4], Random IV+ (AES GCM(Payload)) \leftarrow

```
byte[] result = new byte[iv.length + cipherVal.length];  
System.arraycopy(iv, 0, result, 0, iv.length);  
// iv 放前面12 byte  
System.arraycopy(cipherVal, 0, result, iv.length, cipherVal.length);  
// (AES GCM(Payload))放後面的 byte
```

[6] 最後再 HEX([5]) 轉換為 Hex string，即 sp_checksum

4.8.2 資料格式說明：sp_checksum(範例)

備註1：提供各步驟驗證範例↵

↵

AesKeyBase64:↵

y5e6LfXmB9v43kA3qm2KnjW4bXiHWPu08Igp4xzi6U↵

↵

Payload:↵

046b6c7f-0b8a-43b9-b35d-6489e6daee917b2c7f94-9f7b-481a-89a8-

56b883dea695A987654321SIGNI-SCAN 待 簽 署 資 料

DOC_DIGEST_JLDKJFLKDSJFLDSLFLJSDLFJLSKDFJLSFJLSFJLDS

KFJLKSDFLJLSFJLKSDFLKSDFLSDFSDFLSDFSDFSFF↵

↵

[2] 產生 SHA256_HEX(Payload)↵

c703cd8e41913805e3e8644eeb42d18aa841645b028a16e491e91c4b9c406
b4e↵

↵

[3] 產生 Random IV↵

1241c87f32fbe9effec8ac92↵

↵

[4] 進行 AES_GCM 加密↵

06e89e066b751f4dec9bb126e93ddb67dbad10e8abc69206b84b64660675d
90a8e1ff887057f42dbfbceb3f49167c4e9ca1481359ffbf76efdcabd7649ffa
045805a87f1e834ef41f6427646e9bffc5↵

↵

[5] 串接[3][4]，Random IV+ (AES_GCM(Payload))，Hex後得到[6]↵

1241c87f32fbe9effec8ac9206e89e066b751f4dec9bb126e93ddb67dbad10e
8abc69206b84b64660675d90a8e1ff887057f42dbfbceb3f49167c4e9ca148
1359ffbf76efdcabd7649ffa045805a87f1e834ef41f6427646e9bffc5↵

↵

4.9.1 資料格式說明：idp_checksum

idp_checksum

格式說明：

AES_GCM_HEX(SHA256_HEX(Payload))

[1] 產生 Payload

欄位範例(詳情請參考 SP-API-XX 各介面)

transaction id + error code + has active fido + has active mcert sign

內容範例

e75bddcb-ef16-4700-9ef9-f584e9871f910YY

[2] 產生 SHA256_HEX(Payload)

整個Payload字串 getBytes(UTF-8) 轉換後，進行 SHA256 運算產生 byte array，轉換為 Hex string 顯示

MessageDigest digest = MessageDigest.getInstance("SHA-256");

final byte[] passwordBytes = base.getBytes("UTF-8");

final byte[] salt = "".getBytes("UTF-8");

final byte[] all = ArrayUtils.addAll(passwordBytes, salt);

byte[] hash = digest.digest(all);

return convertBinaryToHexString(hash);

[3] 拆解 Random IV

int GCM_IV_LENGTH = 12;

byte[] cipherVal =
CryptoHelper.convertHexStringToBinary(idpChecksum);
byte[] iv = Arrays.copyOfRange(cipherVal, 0, GCM_IV_LENGTH);

[4] 進行 AES_GCM 解密

int TAG_LENGTH = 128;

GCMParameterSpec ivSpec = new
GCMParameterSpec(TAG_LENGTH, iv);

Cipher c = Cipher.getInstance(CIPHER_AES_GCM);

c.init(Cipher.DECRYPT_MODE, new SecretKeySpec(AesKeyInBytes,
"AES"), ivSpec);

byte[] plainVal = c.doFinal(cipherVal, GCM_IV_LENGTH,
idpChecksum.length - GCM_IV_LENGTH);

plainHexString = new String(plainVal);

[5] 比對[2]與[4]結果是否一致

if(SHA256_HEX(Payload).equals(plainHexString))

true;

else

false;

4.9.2 資料格式說明：idp_checksum(範例)

備註1：提供各步驟驗證範例↵

↵

AesKeyBase64:↵

y5e6LfXmB9v43kA3qm2KnjW4bXiHWPu08Igp4xzi6U↵

↵

Payload:↵

e75bddcb-ef16-4700-9ef9-f584e9871f910YY↵

↵

idpChecksum:↵

947e3cedec310d6fcd213bbfbe63aa5d92c0c7a93ab3f587396c5faf048d649

fa9b41d3b04769e304817ee50746170a293f7f2c01546f0d13a3949c2fd24f

9deea9ed195d3b37e53b9dca6269a7a99e38ab62588942bfa4f71f040da↵

↵

[2] 產生 SHA256 HEX(Payload)↵

97275f15f4e0bcbb82500c75815dd6f62206d27e8e8b86663ad8ce1fb70353
35↵

↵

[3] 拆解 Random IV↵

947e3cedec310d6fcd213bbf↵

↵

[4] 進行 AES_GCM 解密↵

97275f15f4e0bcbb82500c75815dd6f62206d27e8e8b86663ad8ce1fb70353
35↵

↵

[5] 比對[2]與[4]結果是否一致↵

true↵

4.10.1 APP-API-01：簽章功能

介面編號	APP-API-01
中文名稱	簽章功能
英文名稱	verifySign
介面方式	URLScheme
通訊協定	mobilemoica
URL	mobilemoica://moica.moi.gov.tw/w2a/verifySign?token=&sp_ticket=&rtn_url=&rtn_val=
功能描述	當需用機關服務系統需透過「自然人憑證 App」進行簽章功能時使用。
使用限制	需帶入合法身分證號、SP 服務識別代碼、SP 驗證碼
使用範例	需用機關服務系統透過「自然人憑證 App」進行簽章
呼叫系統名稱	需用機關服務系統
被呼叫系統名稱	行動自然人憑證 APP

輸入參數								
編號	中文名稱	英文名稱	型別	長度	必要欄位	傳輸類別	次數	備註
1	SP 票據	sp_ticket	String		Y	Request	1	請參考三、(二)sp_ticket 格式說明
2	回應網址	rtn_url	String		Y	Request	1	Base64(rtn_url)，自然人憑證 App 執行完成簽章功能時，透過此參數值將結果進行回傳。
3	回應資訊	rtn_val	String		Y	Request	1	Base64(rtn_val)，第三方服務需由「自然人憑證 App」再回傳的參數值，如：

輸出參數								
編號	中文名稱	英文名稱	型別	長度	必要欄位	傳輸類別	次數	備註
1	SP 票據	sp_ticket	String		Y	Response	1	請參考三、(二)sp_ticket 格式說明
2	回應網址	rtn_url	String		Y	Response	1	Base64(rtn_url)，自然人憑證 App 執行完成簽章功能時，透過此參數值將結果進行回傳。
3	回應資訊	rtn_val	String		Y	Response	1	Base64(rtn_val)，第三方服務需由「自然人憑證 App」再回傳的參數值，如：sessionId、token 等。
4	錯誤代碼	error_code	String		Y	Response	1	
5	錯誤訊息	error_message	String		Y	Response	1	

4.10.2 APP-API-01：範例

範例

輸入參數範例

mobilemoica://moica.moi.gov.tw/w2a/verifySign?token=&sp_ticket=&rt_n_url=
=aHR0cHM6Ly9tb21jYS5tb2kuZ292LnR3L3N1cnZpY2Vz&rt_n_val=c2Vzc21vbklkPW1Yb
kNjc0luTnBaMjVmWkc5aklqb21SRT1EWDBSS1Iw

輸出參數範例

https://moica.moi.gov.tw/services?sp_ticket=eyJ0cmFuc2FjdGlvb19pZCI6ImE
zYTJmZWMOlWRhZDQ0LTJiMjQ0OTMyNSk0WE0YjczZDI5MzciLCJvcF9jb2R1IjojU01HTi
IsIm9wX21vZGUioiJJLVNDQU4iLCJzcF9zZXJ2aWN1X21kIjojN2IyYzdmOTQtOWY3Yi000
DFhLTg5YTgtNTZiODgzZGVhbjklIiwic3BfdG1ja2V0X21kIjojMGZiNzMwNmItYjNhNC00
Nm1lLTg3YTgtNTgzYzg4ODJhMGlxIiwic3BfbmFtZSI6IuaooeaTr0a4r0ippuapn-
mXnClSlnNpZ25fZG9jIjojRE9DX0RJR0VTVF9KTERLSkZMS0RTSkZMRFNMRkpTRExGSkxTS
0RGSkxTRkpMU0ZKTERTS0ZKTEtTREZKTFNGSkxLRFNGSkxLU0RGRFNGU0RGU0RGRFNGRFG
RiIsImhpbmQioiImgqjmmK_lkKbmraPlnKjlmJfoqabnmbvlhaXlhaflmL_pg6jos4foqIr
mlbT1kIjIhaXljbPntrIiLCJleHBpcnF0aW9uX3RpbWUiOiIxNjI2MzczNDY2MDAwIiwiaG
FzaGVkX21kX251bSI6ImNtQ2NwSXdcVkc4ZEHqYVBWbWJCT0FBWGx2OF1vdDN3dzIxX1g3U
FFEblUifQ.n4hlol7waCR1MQ1ly0ASIDaMA1psnKoQ_h-
9zfCeaFs&rt_n_val=c2Vzc21vbklkPW1YbkNjc0luTnBaMjVmWkc5aklqb21SRT1EWDBSS1
Iw&error_code=ok&error_message=

4.11.1 APP-API-02：認證功能

介面編號	APP-API-02
中文名稱	認證功能
英文名稱	authenticate
介面方式	URLScheme
通訊協定	mobilemoica
URL	mobilemoica://moica.moi.gov.tw/w2a/authenticate?token=&sp_ticket=&rtn_url=&rtn_val=
功能描述	當需用機關服務系統需透過「自然人憑證 App」進行認證功能時使用。
使用限制	需帶入合法身分證號、SP 服務識別代碼、SP 驗證碼
使用範例	需用機關服務系統透過「自然人憑證 App」進行認證
呼叫系統名稱	需用機關服務系統
被呼叫系統名稱	行動自然人憑證 APP

輸入參數							
編號	中文名稱	英文名稱	型別	長度	必要欄位	傳輸類別	次數
1	SP 票據	sp_ticket	String		Y	Request	1
2	回應網址	rtn_url	String		Y	Request	1
3	回應資訊	rtn_val	String		Y	Request	1

輸出參數							
編號	中文名稱	英文名稱	型別	長度	必要欄位	傳輸類別	次數
1	SP 票據	sp_ticket	String		Y	Response	1
2	回應網址	rtn_url	String		Y	Response	1
3	回應資訊	rtn_val	String		Y	Response	1
4	錯誤代碼	error_code	String		Y	Response	1
5	錯誤訊息	error_message	String		Y	Response	1

token 等。

請參考三、
(二)
sp_ticket 格式說明

Base64(rtn_url)，自然人憑證 App 執行完成簽章功能時，透過此參數值將結果進行回傳。

Base64(rtn_val)，第三方服務需由「自然人憑證 App」再回傳的參數值，如：sessionId、token 等。

4.11.2 APP-API-02：範例

範例

輸入參數範例

mobilemoica://moica.moi.gov.tw/w2a/authenticate?token=&sp_ticket=&rtn_url=aHR0cHM6Ly9tb21jYS5tb2kuZ292LnR3L3N1cnZpY2Vz&rtn_val=c2Vzc2lvbklkPW1YbkNjc0luTnBaMjVmWkc5aklqb21SRT1EWDBSS1Iw

輸出參數範例

https://moica.moi.gov.tw/services?sp_ticket=eyJ0cmFuc2FjdGlvb19pZCI6ImEzYTJmZWMOlWRhZDQ0LTJiMjQ0OTMyNSk0WE0YjczZDI5MzciLCJvcF9jb2R1IjoIU01HTiIsIm9wX21vZGU0iJJLVNDQU4iLCJzcF9zZXJ2aWN1X21kIjoIN2IyYzdmOTQtOWY3Yi00ODFhLTg5YTgtNTZiODgzZGVhbjk1Iiwic3BfdG1ja2V0X21kIjoIMGZiNzMwNmItYjNhNC00Nm1lLTg3YTgtNTgzYzg4ODJhMGlxIiwic3BfbmFtZSI6IuaooeaTrOa4r0ippuapn-mXnClSInNpZ25fZG9jIjoIRE9DX0RJR0VTVF9KTERLSkZMS0RTSkZMRFNMRkpTRExGSkxTS0RGSkxTRkpMU0ZKTERTS0ZKTEtTREZKTFNGSkxLRFNGSkxLU0RGRFNGU0RGU0RGRFNGRFNGRiIsImhpbmQ0i0iLmgqjmmK_lkKbmraPlnKjlmJfoqabnmbvlhaXlhafmlL_pg6jos4foqlrm1bT1kIj1haX1j6PntrIiLCJleHBpcmF0aW9uX3RpbWUiOiIxNjI2MzczNDY2MDAwIiwiaGFzaGVkX21kX251bSI6ImNtQ2NwSXdcVkc4ZElhYVYwNFJCT0FBWGx2OF1vdDN3dzIxX1g3UFEFb1UifQ.n4h1o17waCR1MQ11y0ASIDaMA1psnKoQ_h-9zfCeaFs&rtn_val=c2Vzc2lvbklkPW1YbkNjc0luTnBaMjVmWkc5aklqb21SRT1EWDBSS1Iw&error_code=ok&error_message=

4.12 錯誤訊息與問題排除清單(1/4)

錯誤代碼為：介面編號||'|系統錯誤代碼

範例：SP-API-ATH-01-INV_SP_CHECKSUM

系統錯誤代碼	詳細敘述	處理建議
DB_CONN_ERR	資料庫連線失敗	[1021]系統維護中，請稍後再試。
DB_SQL_EXP	資料庫操作失敗	[1022]系統維護中，請稍後再試。
DB_ROOLBACK	資料庫批次操作失敗，已回復到操作前狀態	[1023]系統維護中，請稍後再試。
DB_CLOSE_ERR	資料庫連線關閉失敗	[1024]系統維護中，請稍後再試。
DB_JNDI_ERR	資料庫設定錯誤	[1025]系統維護中，請稍後再試。
OTP_EXPIRED	OTP 認證碼逾期	[1031]驗證碼逾時，請重新再試一次。
OTP_IDNUM_MISMATCH	身分證字號與 OTP 比對不符合	[1032]驗證碼與身分證號不符，請重新再試一次。
OTP_NF	找不到 OTP	[1033]未取得驗證碼，請按照流程重新再試一次。
OTP_DBSQL	OTP 查詢時發生 DB 錯誤	[1034]驗證碼與身分證號不符，請重新再試一次。
IDNUM_USERPROF_NF	身分證字號未找到對應之使用者資訊 操作人員身分為新用戶或者過去完成註銷之用戶	[1051]您尚未註冊綁定裝置，請先綁定裝置並申請行動自然人憑證。
IDNUM_USERPROF_DBSQL	身分證字號查詢使用者資訊時發生 DB 錯誤	[1052]查詢使用者資訊不成功，請洽客服人員處理。
IDNUM_DEVPROF_NF	身分證字號未找到對應之裝置資訊	[1053]您尚未註冊綁定裝置，請先綁定裝置並申請行動自然人憑證。
IDNUM_DEVPROF_DBSQL	身分證字號查詢裝置資訊時發生 DB 錯誤	[1054]查詢使用者資訊不成功，請洽客服人員處理。

4.12 錯誤訊息與問題排除清單(2/4)

DEVID_DEVPROF_NF	Device_id 未找到對應之裝置資訊	[1061]查詢裝置資訊不成功，請至行動自然人憑證官方網站確認該裝置名稱是否一致。
DEVID_DEVPROF_DBSQL	Device_id 查詢裝置資訊時發生 DB 錯誤	[1062]查詢裝置資訊不成功，請洽客服人員處理。
DEV_DESC_MISMATCH	未找到對應之自訂裝置名稱	[1063]查詢裝置資訊不成功，請至行動自然人憑證官方網站確認該裝置名稱是否一致。
DEVID_SPTKT_MISMATCH	Device_id 與 sp ticket 中對應之身份證字號雜湊值不符合	[1064]裝置資訊驗證不成功，請確定使用合法裝置進行認證/簽章。
USERPROF_INS_ERR	使用者資訊 DB 資料表寫入失敗	[1071]系統維護中，請稍後再試。
DEVPROF_INS_ERR	裝置資訊 DB 資料表寫入失敗	[1072]系統維護中，請稍後再試。
SPTKT_INS_ERR	Sp ticket DB 資料表寫入失敗	[1073]系統維護中，請稍後再試。
TXNLOG_INS_ERR	認證簽署紀錄 DB 資料表寫入失敗	[1074]系統維護中，請稍後再試。
PS_CONNECT_404	推播模組 PS 回應 404	[3002]系統維護中，請稍後再試。
PS_CONNECT_500	推播模組 PS 回應 500	[3003]系統維護中，請稍後再試。
PS_JSON_FMT_ERR	推播模組 PS 回應非 JSON 格式內容	[3004]系統維護中，請稍後再試。
PS_JSON_TYPE_ERR	推播模組 PS 回應 JSON 中部份型態不符合	[3005]系統維護中，請稍後再試。
PS_JSON_MISS_KEY	推播模組 PS 回應 JSON 中缺少必要欄位	[3006]系統維護中，請稍後再試。
PS_CONNECT_IOEXC	推播模組 PS 連線失敗	[3007]系統維護中，請稍後再試。
PS_1001	訊息推播模組 JSON 參數輸入錯誤	[3008]系統維護中，請稍後再試。
PS_5000	訊息推播模組 <u>push_data</u> JSON 解析錯誤	[3009]系統維護中，請稍後再試。

4.12 錯誤訊息與問題排除清單(3/4)

PS_FCM_UNKNOWN	未知的錯誤，通常是伺服器問題	[3101]系統維護中，請稍後再試。
PS_FCM_ABORTED	推播中止，推播過程發生衝突	[3102]系統維護中，請稍後再試。
PS_FCM_ALREADY_EXISTS	資源已重複存在，無法建立推播資源	[3103]系統維護中，請稍後再試。
PS_FCM_CANCELLED	推播操作已取消	[3104]系統維護中，請稍後再試。
PS_FCM_CONFLICT	資源讀寫衝突	[3105]系統維護中，請稍後再試。
PS_FCM_DATA_LOSS	資料遺失或資料毀損、接收不完全	[3106]系統維護中，請稍後再試。
PS_FCM_DEADLINE_EXCEEDED	推播逾時	[3107]系統維護中，請稍後再試。
PS_FCM_FAILED_PRECONDITION	推播失敗，請檢查系統程式完整性	[3108]系統維護中，請稍後再試。
PS_FCM_INTERNAL	推播系統內部發生錯誤	[3109]系統維護中，請稍後再試。
PS_FCM_INVALID_ARGUMENT	參數錯誤	[3110]系統維護中，請稍後再試。
PS_FCM_NOT_FOUND	找不到推播資源，可能來源端位置為黑名單	[3111]系統維護中，請稍後再試。
PS_FCM_OUT_OF_RANGE	超出推播範圍	[3112]系統維護中，請稍後再試。
PS_FCM_PERMISSION_DENIED	API 無存取權限或尚未啟用	[3113]系統維護中，請稍後再試。
PS_FCM_RESOURCE_EXHAUSTED	推播資源忙碌中，超出系統負荷範圍	[3114]系統維護中，請稍後再試。
PS_FCM_UNAUTHENTICATED	未認證的名稱	[3115]系統維護中，請稍後再試。
PS_FCM_UNAVAILABLE	資源目前無法存取	[3116]系統維護中，請稍後再試。
PM_INV_NF	缺少參數或者格式不正確	[5002]簽章不成功，請洽客服人員處理。
PM_SIGDATA_ERR	APP 端簽章內容格式不正確	[5003]簽章不成功，請洽客服人員處理。

4.12 錯誤訊息與問題排除清單(4/4)

PM_INV_SG↵	APP 端簽章驗證失敗↵	[5004]驗證不成功，請確認憑證有效性。↵
↵	↵	↵
SPTKT_PLD_FT_ERR↵	Sp_ticket 格式錯誤↵	[9002]資料格式有誤，請洽該應用服務之管理員。↵
SPTKT_DIG_FT_ERR↵	Sp_ticket 簽章驗證失敗↵	[9003]資料驗證不成功，請洽該應用服務之管理員。↵
INV_SP_CHECKSUM↵	SP CHECKSUM 檢驗失敗↵	[9004]資料驗證不成功，請洽該應用服務之管理員。↵
TGT_INV↵	無效的操作對象代碼↵	[9005]資料驗證不成功，請洽該應用服務之管理員。↵
PM_IDN_FT_ERR↵	身份證字號格式錯誤↵	[9006]身分證號格式錯誤，請確認輸入資訊。↵
SPTKTID_TXNLOG_NF↵	查無使用者認證/簽署結果↵	[9007] 使用者認證/簽署作業尚未完成，請稍後再試。↵

問題與討論