# 公司負責人及主要股東資訊查詢平臺應用程式介面規格書

版本 0.4

發佈日期 111 年 3 月 24 日

# 文件修訂紀錄

| 異動別 | 版本 | 內容說明 | 修改原因 |
|---|---|---|---|
| 新增 | 0.1 | 初版 | 初版 |
| 修改 | 0.2 | 補充 API 介面資訊 | 補充 API 驗證相關的加密資訊、代碼部份新增對應表 |
| 修改 | 0.3 | 補充 API 介面資訊 | 取得存取碼的「Request body」參數修改 |
| 修改 | 0.4 | 補充 API 介面資訊 | 新增「此筆查詢公司統編之結果」代碼、修改 API「取得存取碼」、「單筆查詢」、「查詢 ubo 資料異動日」、「查詢 ubo 資料異動日」回傳規格 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# 目 錄

# 一、目的

本文件技術標準制定之目的，主要係依據國家發展委員會於中華民國 106 年 6 月訂頒「共通性應用程式介面開放規範」辦理，訂定一致性描述方式之標準化操作方式與資料交換格式，達到可與本系統之間可程式化，以標準一致性的方式進行申報資料查詢，俾利我國持續推動數位金融科技發展。

# 二、應用範圍

本技術標準應用範圍主要以公司負責人及主要股東資訊查詢平臺 API 應用發展為主，並依「認證授權」、「公司資料查詢」等發展規劃設計。

# 三、名詞定義

為確保名詞定義一致，以下英文名稱主要參考國家發展委員會於中華民國 106 年 6 月發佈之共通性應用程式介面規範內容解釋為主。

| 英文名稱 | 中文名稱 | 定義 |
|---|---|---|
| API(Application Programming Interface) | 應用程式介面 | 為「『電腦作業系統（Operating system）』或『程式函式庫』提供給應用程式呼叫使用的程式碼」。其主要目的是讓應用程式開發人員得以呼叫一組常式功能，而無須考慮其底層的原始碼為何、或理解其內部工作機制的細節。API本身是抽象的，它僅定義了一個介面，而不涉及應用程式在實際實現過程中的具體操作。 |
| REST | 含狀態傳輸 | 全名為Representational State Transfer，是一種軟體架構設計風格。資源由URI指定，對資源的操作包括取得、創建、修改和刪除資源，這些操作正好對應HTTP協議提供之GET、POST、PUT和DELETE方法。 |
| RESTful | 含狀態傳輸的Web服務 | 是一個使用HTTP並遵循REST原則，以URL定位資源，根據HTTP內容指示操作動作與回應訊息。 |

| | | |
|---|---|---|
| JSON(JavaScript Object Notation) | - | 一種採用JavaScript物件表示法的輕量級資料交換語言，該語言以易於讓人閱讀的文字為基礎，用來傳輸由屬性值或者序列性的值組成的資料物件 |
| RESTful API | - | 是一種採用RESTful設計的Web API，其資料傳輸主要採JSON及YAML等資料格式為主。 |
| OAuth | - | 係一種開放授權標準，允許消費者授權讓第三方服務提供者存取該消費者在金融機構上所儲存的受保護資源。 |
| API Key | 應用程式介面金鑰 | 管理系統給予每個前端應用程式呼叫API之認證碼，作為身分認證用。 |

# 四、安全定義

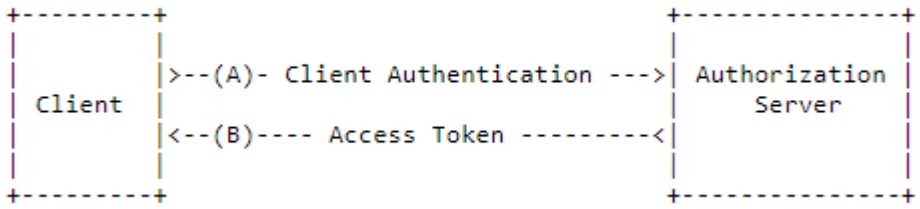
以下針對 API 應用範圍說明安全定義。

## (一)應用程式介面金鑰

1. 取存 API 時，應進行 TLS 伺服端認證（Server Authentication），且驗證伺服端憑證之正確性及有效性。
2. 集保審核完成使用單位後，將提供應用程式介面，金鑰於首次提供時可使用至當年年底,每年12月1日時,CTP 系統依註冊時設定之 API 管理者 email 寄送次年可使用之金鑰，每年之12月做為換金鑰緩衝期間，新舊金鑰皆可使用。

## (二)開放授權(OAuth 2.0)

OAuth 2.0 是用於授權的行業標準協議。在本案 API 技術標準範圍中，將採用客戶端模式(Client Credentials) 作為使用者身份認證與授權機制。該機制目前已發展至 2.0，有關該技術標準及應用說明可參考 RFC 6749。(https://tools.ietf.org/html/rfc6749)，本系統採客戶端模式(Client Credentials)流程及定義如下：




1. 代理存取端(Client)：客戶端向授權伺服器提出授權請求並提交存取代碼給資源伺服器藉以存取客戶端授權之資源。
2. 授權伺服器(Authorization Server)：負責對客戶端進行身分確認並在客戶端完成認證後賦與授權，核發存取碼給客戶端。
3. 存取代碼(Access Token)：為一定期間使用的代碼，可限制或中止第三方應用程式存取資源。由授權伺服器產生。

# 五、概要設計

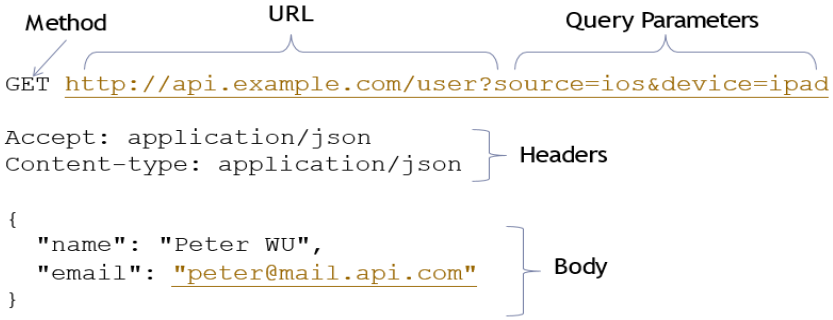
## (一) API 設計方式

採 RESTful 風格 API，資料欄位定義採 JSON 格式 UTF-8 字元編碼(參考 RFC 7158)。

## (二) API 設計結構

### 1. HTTP Url

此為 API 訊息處理接受的網址，同時也是 Request 的處理資源。




### 2. HTTP Header

#### (1)認證授權

API 訊息 Request/Response Success/Response Error 均需使用此 HTTP Header 資料結構作為訊息識別。

| Field Name | Field Description | Field Format | Memo |
|---|---|---|---|
| X-UserId | Client 使用者代號 | String | pcclient 填入使用者代號, 一般呼叫填入管理者之代號 |

| | | | |
|---|---|---|---|
| X-InstId | Client 單位代碼 | String | 填入單位代碼 |
| X-TxnInitDateTime | 交易發起日期時間 | String (ISO UTC+0) yyyy-MM-dd'T'HH:mm:ss.SSS'Z' | 時間戳 2020-08-27T05:56:33.919Z |

(2)一般資料類型

API 訊息 Request/Response Success/Response Error 均需使用此 HTTP Header 資料結構作為訊息識別。

| Field Name | Field Description | Field Format | Memo |
|---|---|---|---|
| X-UserId | Client 使用者代號 | String | pcclient 填入使用者代號, 一般呼叫填入管理者之代號 |
| X-InstId | Client 單位代碼 | String | 填入單位代碼 |
| X-TxnInitDateTime | 交易發起日期時間 | String (ISO UTC+0) yyyy-MM-dd'T'HH:mm:ss.SSS'Z' | 時間戳 2020-08-27T05:56:33.919Z |
| Authorization | Access Token | String | 使用時應將存取代碼(Access Token)放置此欄位，內容值為先放置"Bearer"固定字串，再放置一空格及存取代碼(Access Token)。 |

3. HTTP Request 資料結構

HTTP Request 由四個項目組成，分別說明如下：

| URL | Method | Header | Body |
|---|---|---|---|

(1)URL

請參閱 HTTP URL。

(2)Method

為標準的 HTTP Method，可為 GET(查詢)、POST(新增/更新)等指示方法。

(3)Request Header

請參閱 HTTP Header。

(4)Request Body 架構

Request Body 於 HTTP GET Method 時無需放置資料；HTTP POST Method 則用於放置查詢參數或上傳內容。

內容依據 Header Content-Type 有所不同

當 Content-Type: application/json 時, 範例：

```
{
  "rpt_year": "2020",
  "rpt_num": "001",
}
```

當 Content-Type: application/x-www-form-urlencoded 時, 範例：
grant_type=client_credentials

4. HTTP Response 資料結構

HTTP Response 由三個項目組成，分別說明如下：

| Status Code | Header | Body |
|---|---|---|

(1)Response Status Code

常用 Status Code 支援範圍說明如下：

| Status Code | Status Description | 處理說明 |
|---|---|---|
| 200 | OK | API 處理成功，訊息格式請參閱 Response Body[1] |
| 400 | Bad Request | 業務應用檢核錯誤，訊息格式請參閱 Response Body[2] |
| 401 | Unauthorized | 未認證的請求，如 API Key 錯誤 |
| 403 | Forbidden | 未授權的訪問，如存取路徑未授權 |
| 404 | Not Found | 無法找到存取路徑 |
| 500 | Internal Server Error | API 內部程式無法處理 |
| 503 | Service Unavailable | 伺服器目前無法處理請求 |

其他 04xx、05xx 等 Status Code 請依運用狀況參閱 RFC 2616。

(2)Response Header

請參閱 HTTP Header。

(3)Response Body

Response Body 訊息會以 JSON 為回傳格式，回應成功及回應錯誤之訊息格式說明如下。

[1].HTTP Status Code：200 -(Success)

API 回應成功之訊息區塊格式如下：

```
{
  "repBody": {
    …
  },
}
```

■ repBody

API 回應訊息主要資料區塊。

範例：

```
{
  "repBody": {
    "dataName": [dataObject1,dataObject2,…]
  },
}
```

[2].HTTP Status Code：400－(Error)

API 回應錯誤之訊息設計可容納多個錯誤訊息以陣列形式包裝格式如下：

```
{
"errors": [
  {
    "code": "string",
    "message": "string"
  }
]
}
```

■ code

自訂錯誤代碼。

■ message

自訂錯誤描述。

## (三) JWE 資料加解密

JSON Web Encryption(JWE)係用於解決訊息隱密性的安全機制，申報相關 API 將採用 JWE 作為資料隱密性安全機制。

JWE 使用 JSON 資料結構表示加密內容並且使用 base64url 編碼，本技術採用是 JWE Compact Serialization 作為傳輸時的資料格式，有關該技術標準及應用說明可參考 RFC 7516 (https://tools.ietf.org/html/rfc7516)。

1. 金鑰說明

(1)本文加密金鑰(Content-Encrypt Key：CEK)

【本文加密金鑰】係用於確保 API 訊息資料於傳輸過程中之隱密性，相關演算法詳參 JWA(RFC7518：JSON Web Algorithms) 5.1。

2. API 訊息區塊

| 加密前-API 訊息（context） |
| --- |
| { "repBody": { … }, } |
| 加密後-API 訊息（jwe-enveloped）」 |
| eyJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiZGlyIn0..ZrdIM9bMRppo_on9TGNP6Q.Gi5aQllknZG89rQKzV-dlrLYn_oQg3uIh2-LEY5FjFUIFZPKJ9em0JsixZhDY80opgxtSTjJ2u5RVHoHsN9QUk0rb_AopiAhGBZiy3NBd5g.zvwB4ugalL9ERAvUoBVOlw |

3. API 訊息欄位(加密後)

在 JWE Compact Serialization 中使用”.”符號作為分隔符號共有 5 個區段,各區段表示內容為:

(1)Protected Header：描述本文加密演算法資訊

- ✓ JWE 支援加密演算法資訊，詳參 JWA(RFC7518：JSON Web Algorithms) 5.1。
- ✓ 如採用 A128CBC-HS256，此欄位值為{"enc":"A128CBC-HS256"}，A128CBC-HS256 表示採用 AES_128_CBC_HMAC_SHA_256 authenticated encryption algorithm。其中 AES_128_CBC 表示本文加密演算法，HMAC_SHA_256 表示本文簽章演算法，詳參 JWA 5.2.3。
- ✓ 須採 BASE64URL 編碼。

(2)Encrypted Key：描述本文加密金鑰資訊

- ✓ 加密內容加密密鑰值。某些算法此欄位值指定為空的 8 位位組序列。
- ✓ 須採 BASE64URL 編碼。

(3)iv：Initialization Vector

- ✓ 加密本文所採用演算法所需之初始參數，通常為亂數。
- ✓ 須採 BASE64URL 編碼。

(4)ciphertext：加密密文

- ✓ 須採 BASE64URL 編碼。

(5)tag：JWE Authentication Tag

- ✓ 用來代表本文資料完整性的加密驗證值。
- ✓ 須採 BASE64URL 編碼。

4. API 訊息加密程序

以下加密程序係以本文加密演算法 A128CBC-HS256 做說明，如採 A128GCM 方式，則應依演算法於步驟(2)、(5)、(6)調整合適作法，詳參 JWE(RFC7516：JSON Web Encryption)附錄 A。

(1)確認本文加密演算法

產生「加密演算法資訊（JWE Protected Header)」，並以 Base64URL 編碼為 protected。如本文加密演算法採{"enc":"A128CBC-HS256","alg","dir"}，則 Base64URL 編碼後為 eyJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiZGlyIn0。

➔

"eyJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiZGlyIn0"

(2)產生【本文加密金鑰】

產生 256 Bits 亂數，如本文加密演算法採 A128CBC-HS256，亂數前 128 Bits 為 HMAC Key，後 128 Bits 為 ENC Key。

(3)產生 IV 值

亂數產生一個 128 Bits Initial Vector。

➔

"iv":"ZrdIM9bMRppo_on9TGNP6Q"

(4)本文加密

將「API 訊息區塊」組成「訊息加密明文（clear-text)」，如本文加密採 A128CBC-HS256 運算法進行加密，產生「密文」。

➔

"ciphertext":"Gi5aQllknZG89rQKzV-dlrLYn_oQg3uIh2-LEY5FjFUIFZPKJ9em0JsixZhDY80opgxtSTjJ2u5RVHoHsN9QUk0rb_AopiAhGBZiy3NBd5g"

(5)產生 tag 值

將步驟(1)產生的 protected 以 ASCII 編碼，並產出 aad(Additional

Authenticated Data)值,計算aad長度產生一組8個Bytes的aad Length,例如 aad 長度為 51 個 Bytes(408 Bits),則產生的 aad Length 為 0x0000000000000198。

組合 aad、Initial Vector、「密文」、aad Length,如 aad || Initial Vector || context-ciphered || aad Length,如本文加密採 A128CBC-HS256 運算法,則使用 HMAC-SHA256 演算法,以步驟 2 產生的 HMAC Key 對上述組合資料進行運算,取得 HMAC 值,並取前 128 Bits 為「加密驗證值」。

➔

"tag":"zvwB4ugalL9ERAvUoBVOlw"

(6)產出 JWE Compact Serialization 加密訊息

➔

eyJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiYWxnIjoiZGlyIn0..ZrdIM9bMRppo_on9TGNP6Q.Gi5aQllknZG89rQKzV-dlrLYn_oQg3uIh2-LEY5FjFUIFZPKJ9em0JsixZhDY80opgxtSTjJ2u5RVHoHsN9QUk0rb_AopiAhGBZiy3NBd5g.zvwB4ugalL9ERAvUoBVOlw

# 六、訊息規格

## (一)訊息規格清單

| 種類編號 | 開放 API 功能種類 | 項目編號 | 開放 API 功能應用項目 |
|---|---|---|---|
| 1 | 認證授權 | 1-1 | 取得存取碼 |
| | | 1-2 | 檢查存取碼 |
| | | 1-3 | 撤銷存取碼 |
| 2 | 單筆資料查詢 | 2-1 | 單筆查詢 |
| 3 | 累積筆數查詢 | 3-1 | 查詢使用量 |
| 4 | 公司申報資料異動日查詢 | 4-1 | 查詢 ubo 資料異動日 |
| 5 | 批次資料查詢 | 5-1 | 批次查詢 |
| | | 5-2 | 批次處理狀態查詢 |
| | | 5-3 | 取消批次查詢 |
| | | 5-4 | 批次查詢結果下載 |

各 API 存取方式、欄位輸出入格式請參閱附件 CTP_API_OAS_v1.0.json，此附件以 OpenAPI Specification 標準撰寫，可以使用符合標準之程式開啟本文件，或至「https://editor.swagger.io/」亦可將此檔案開啟。

## (二)訊息規格設計

1. 欄位名稱如說明為additionalProp*,表示該欄位名稱係由自訂Key/Value所組成，key 為鍵值，需為字串型態；value 為對應值，可為任意型態的內容，例如：object、object array、string、string array 等型態，以查詢報表狀態 API 為例，欄位型態裡可知其回應 forms 型態為 array，內容說明為"…可含任意數量的 additionalProp*"，接著參考其下方additionalProp*的型態欄位，可知對應值為字串型態，故可知回應內文

為自訂多筆字串型態的 Key/Value 組合。

2. 有關資料欄位定義採 JSON 格式設計並以 Key/Value 組合為主，故除特定資料欄位格式長度有定義外，其餘資料欄位之格式長度無特別限制。
3. 資料欄位內容無值時，應採下列處理方式，不可回應空值(NULL)。

(1)該 Key 對資料內容為字串型態時，回應空字串，例如："" 。

(2)該 Key 對資料內容為 JSON 物件型態時，回應空物件，例如：{}。

(3)該 Key 對資料內容為陣列型態時，回應空陣列，例如：[]。

# 七、代碼對應表

## (一)證件種類代碼

| 代碼 | 代碼中文名稱 |
|---|---|
| 1 | 身分證 |
| 2 | 外僑居留證 |
| 3 | 華僑身分證明 |
| 4 | 身分證照號碼 |
| 5 | 統一編號 |
| 6 | 機關代碼 |
| 7 | 護照號碼 |
| 8 | 其他 |

## (二)職稱代碼

| 代碼 | 代碼中文名稱 |
|---|---|
| 01 | 董事長 |
| 02 | 副董事長 |
| 03 | 常務董事 |
| 04 | 董事 |
| 05 | 監察人 |
| 06 | 獨立董事 |
| 09 | 經理人 |
| 11 | 執行業務股東 |
| 12 | 代表公司股東 |
| 14 | 股東 |
| 16 | 重整人或重整監督人 |
| 18 | 臨時管理人 |
| 23 | 臨時監察人 |
| 48 | 超過 10%股東 |
| 90 | 其他負責人 |

## (三)發行類型(可能傳空值)

| 代碼 | 代碼中文名稱 |
|---|---|
| 1 | 上市 |
| 2 | 上櫃 |
| 3 | 興櫃 |
| 4 | 公發 |
| 5 | 轉非公發 |

## (四)理由代碼

| 代碼 | 代碼中文名稱 |
|---|---|
| 01 | 與客戶建立業務關係 |
| 02 | 進行臨時性交易 |
| 03 | 發現疑似洗錢或資恐交易 |
| 04 | 對於過去所取得客戶身分資料之真實性或妥適性有所懷疑 |
| 05 | 為客戶買賣不動產 |
| 06 | 為客戶管理金錢、證券或其他資產 |
| 07 | 為客戶管理銀行、儲蓄或證券帳戶 |
| 08 | 提供公司設立、營運或管理服務 |
| 09 | 辦理法人或法律協議之設立、營運或管理以及買賣事業體 |
| 10 | 擔任法人之名義代表人 |
| 11 | 擔任或安排他人擔任公司董事或秘書、合夥人或在其他法人組織之類似職位 |
| 12 | 提供公司、合夥或其他型態商業經註冊之辦公室、營業地址、居住所、通訊或管理地址 |
| 13 | 擔任或安排他人擔任信託或其他類似契約性質之受託人或其他相同角色 |
| 14 | 擔任或安排他人擔任實質持股股東 |
| 15 | 從事辦理客戶不動產買賣交易 |
| 16 | 既有客戶定期審查 |
| 99 | 其他：請輸入查詢目的 |

## (五)此筆公司申報狀態

| 代碼 | 代碼中文名稱 |
|---|---|
| 00 | 正常 |
| 01 | 無申報資料 |
| 02 | 無須申報 |
| 03 | 資料不符 |
| 04 | 已解散 |
| 05 | (興櫃)尚未申報 |
| 06 | 外國公司 |
| 99 | 系統發生不預期錯誤 |