從開放API的安全問題談
開放銀行的資安挑戰

陳 恭

政大資管系教授

政大金融科技研究中心副主任

2019/09/18

Outline

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

- 開放API 簡介
- 開放API for 金融服務
- 開放API的資安與風險
- 開放銀行的資安挑戰

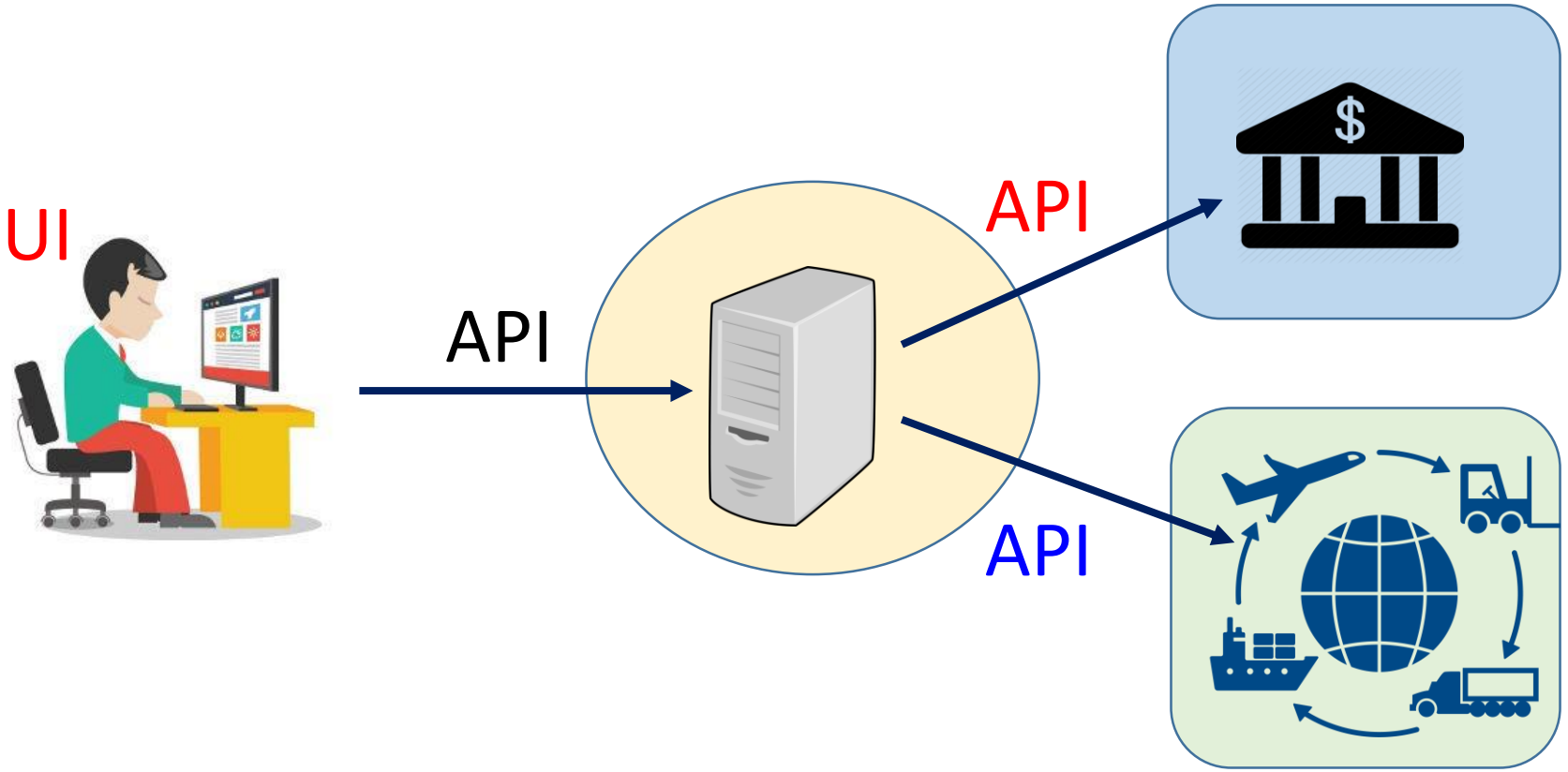
國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

開放 API 簡介

API: B2B合作的利器

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

- 商業夥伴之間資訊與流程整合與自動化



開放 API

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

Open API ⇨

- 以開放標準制定API
- 公開API規格

（HTML, REST API, JSON, …）

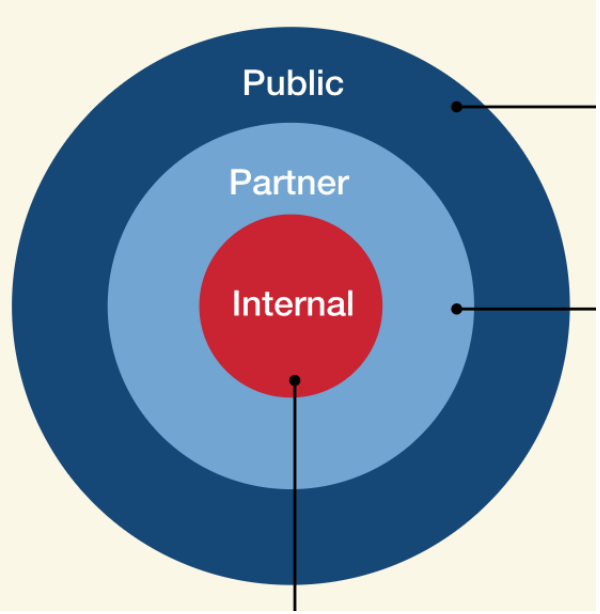
Open API 是開放，不是公開

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

Open includes Public

but

Open ≠ Public



- **認證、授權、威脅偵測、資料保密與訊息正確性，缺一不可**

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

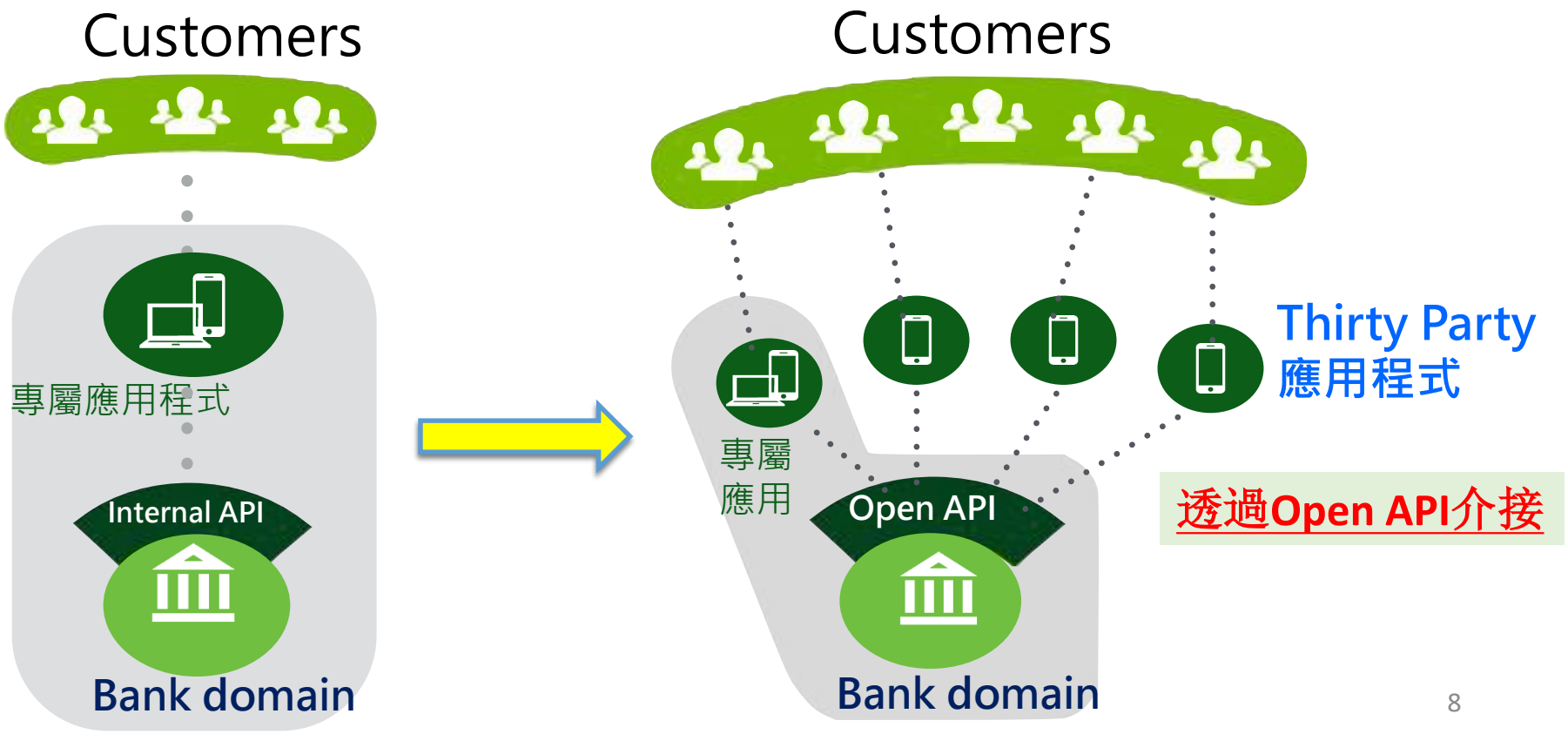
以開放API促進更多元的金融服務

開放銀行是指銀行透過與第三方服務業者(TSP, TPP)合作，以開放API方式，共享金融數據資料，也將金融數據的主導權還給消費者，使消費者可以獲得更多元的金融服務。

開放銀行世界趨勢

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

- 歐盟PSD2，英國 Open Banking，香港，新加坡，日本 ...
- 消費者，第三方服務提供者（TSP, TPP），金融機構合作共榮

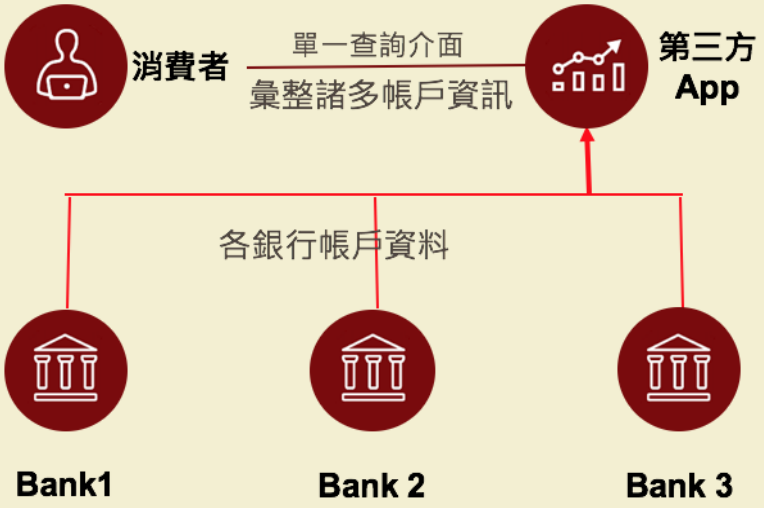


開放金融服務 場景範例

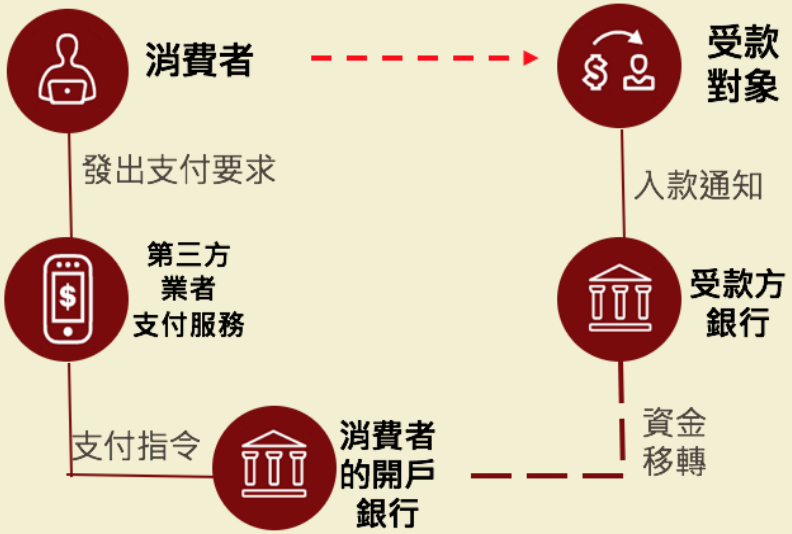
國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

- 單一介面查詢 多帳戶資料
- 第三方跨行支付服務（push payment）

第三方App提供消費者單一查詢介面



第三方App提供跨機構支付服務



Source: A.T. Kearney analysis

三階段 開放銀行API

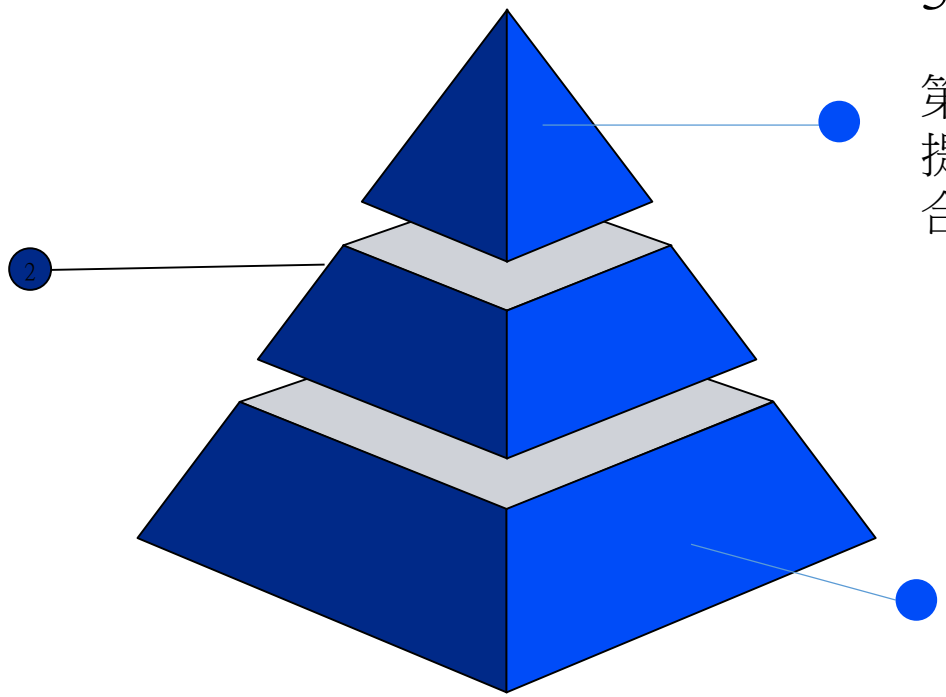
國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

3.支付交易資訊

第三階段：Payment API
提供支付相關交易的整合服務。

2.帳戶資訊

第二階段：
Account API
提供客戶帳戶相關資訊的查詢



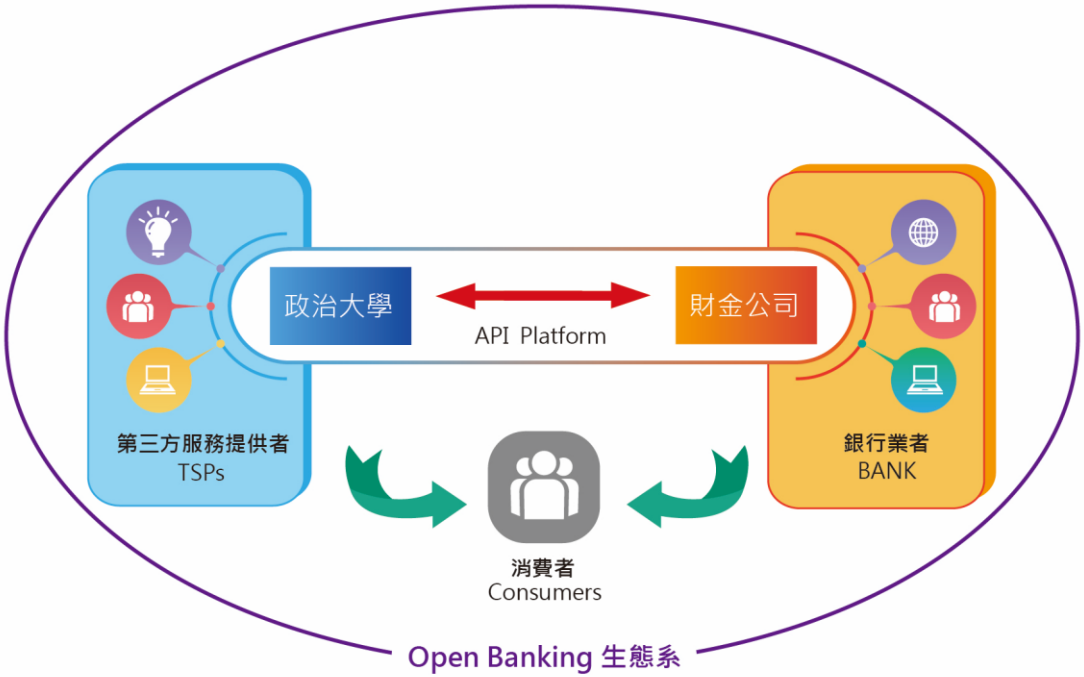
1.產品公開資訊

第一階段：Product API
提供唯讀的銀行產品與服務相關資訊。

財金公司 開放API平台

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

- 銀行業與財金公司於今年初成立「開放 API 研究暨發展委員會」
- 為推動Open API平台，財金公司選擇“政大金融科技研究中心”，協助第三服務業者進入開放銀行生態系，做API沙盒測試。



國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

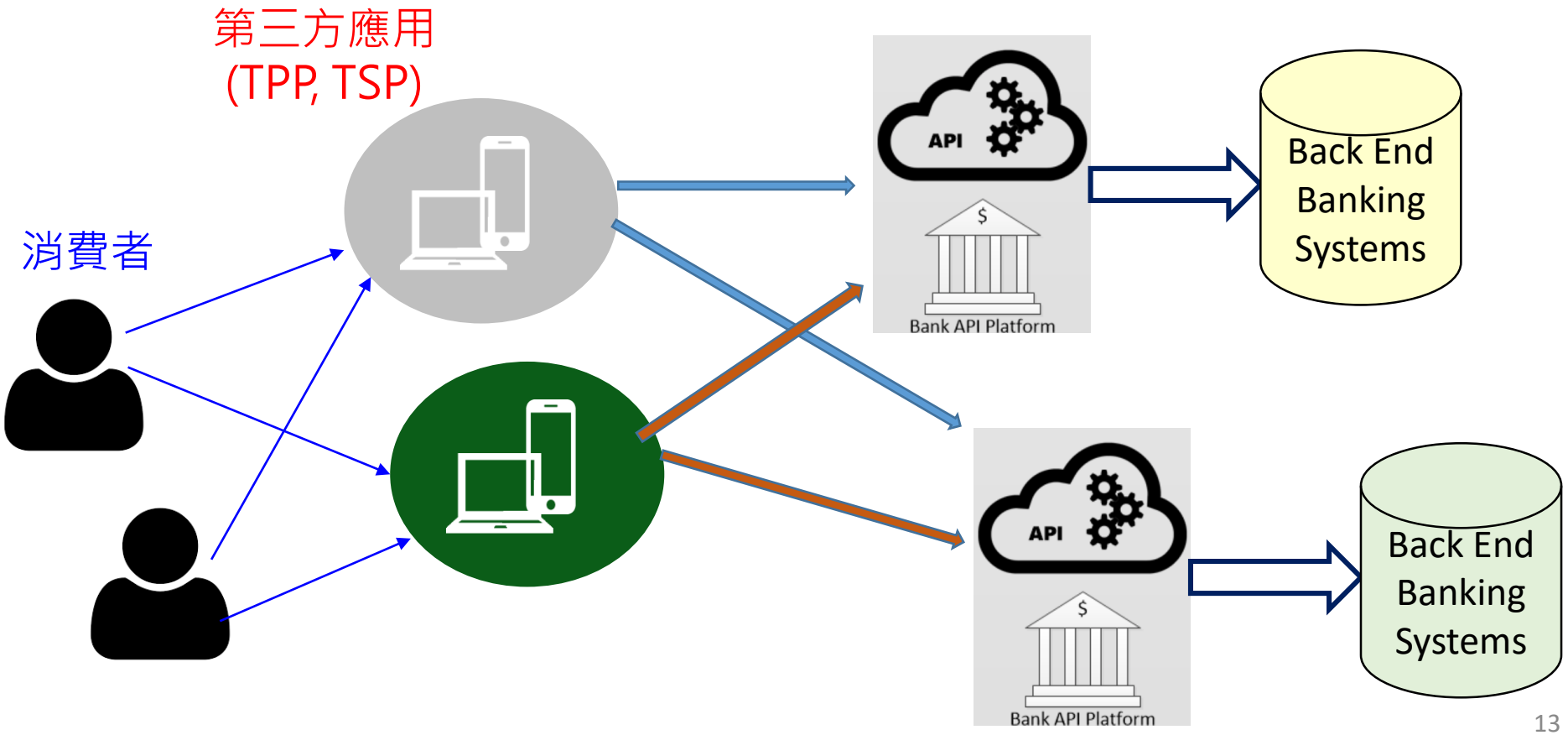
開放 API 資安議題

- 所有網路應用程式的資安都必須考量
- 本次聚焦於Open Banking API

開放銀行資安：身份辨識與權限控管

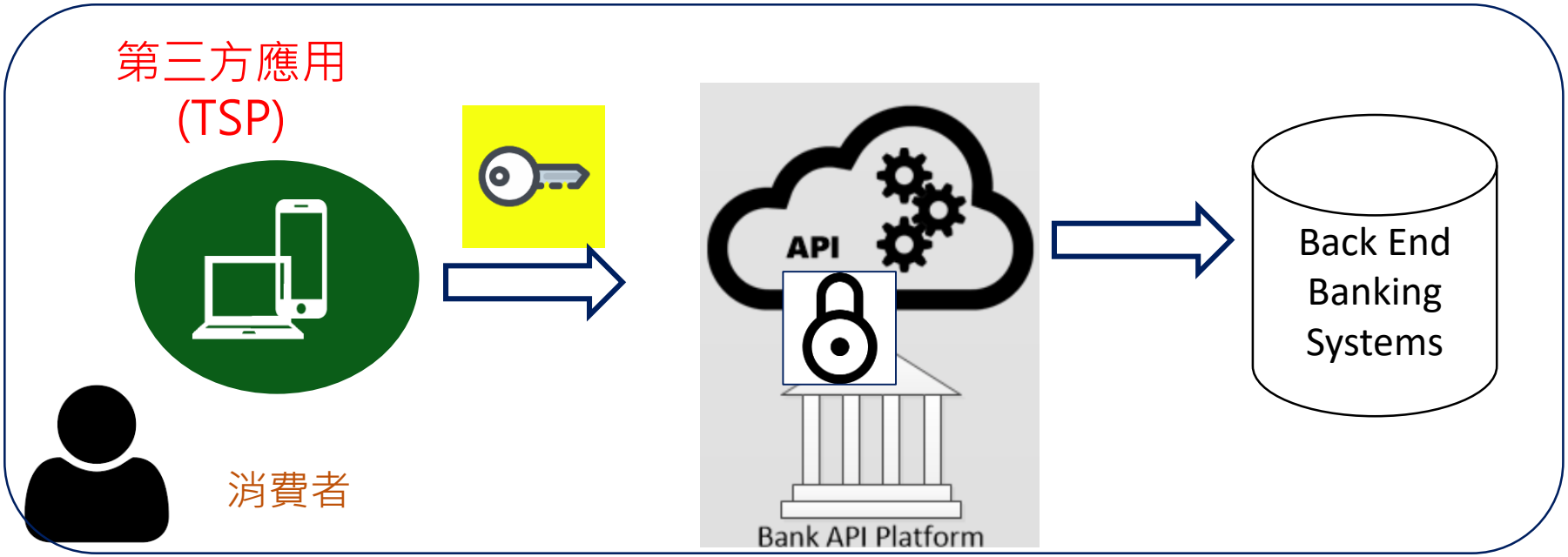
國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

- 銀行端需辨識使用者（消費者）外，**也要辨識第三方的應用程式並控管權限**



第一階段公開產品資訊

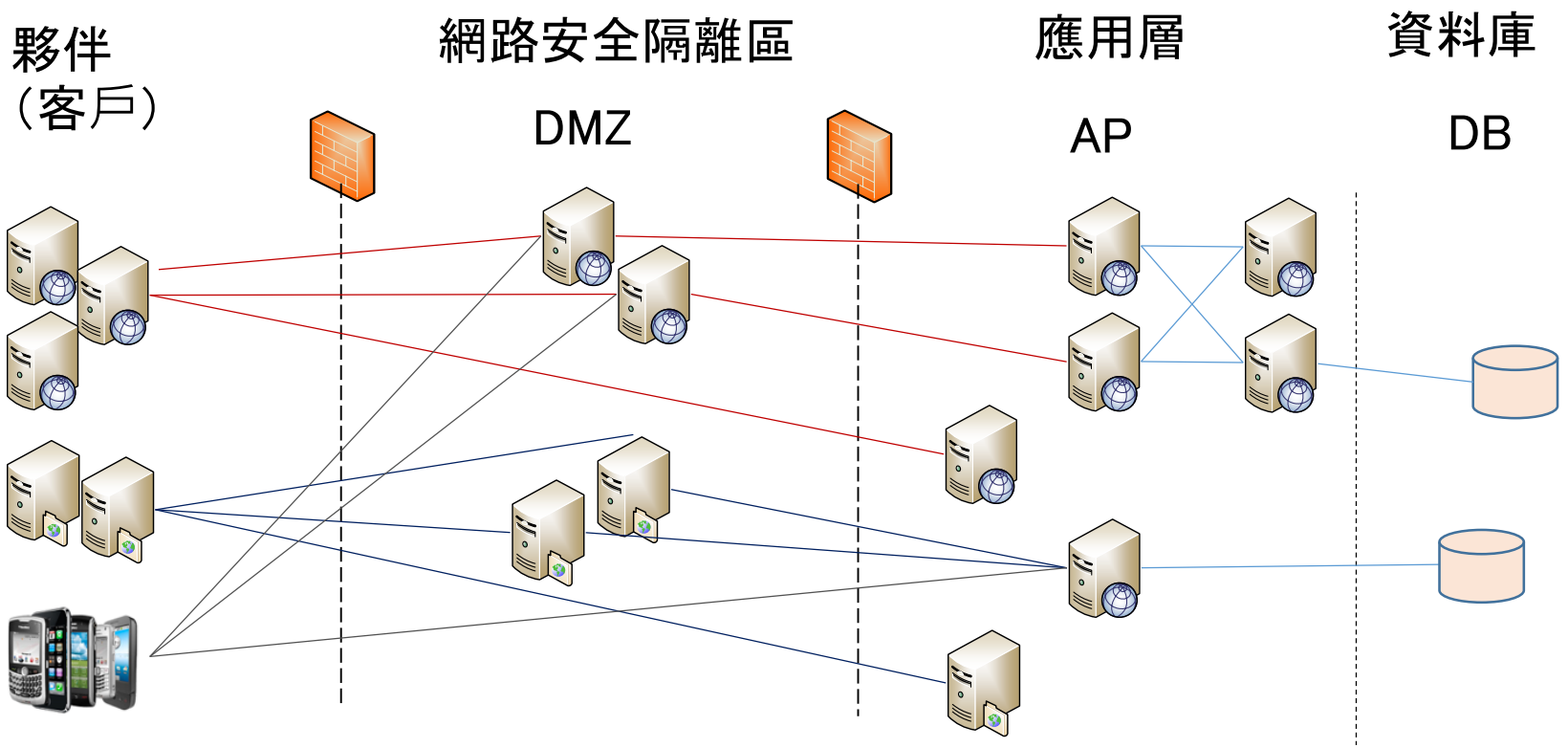
- 第一階段公開產品資訊，無消費者辨識與認證議題
- 第三方服務業者事先註冊。
- 所有第三方應用程式經審核後，
  以API Key辨識身份（認證，類似應用程式的密碼）



企業API架構與治理

國立政治大學商學院 金融科技研究中心
FinTech Research Center College of Commerce, National Chengchi University

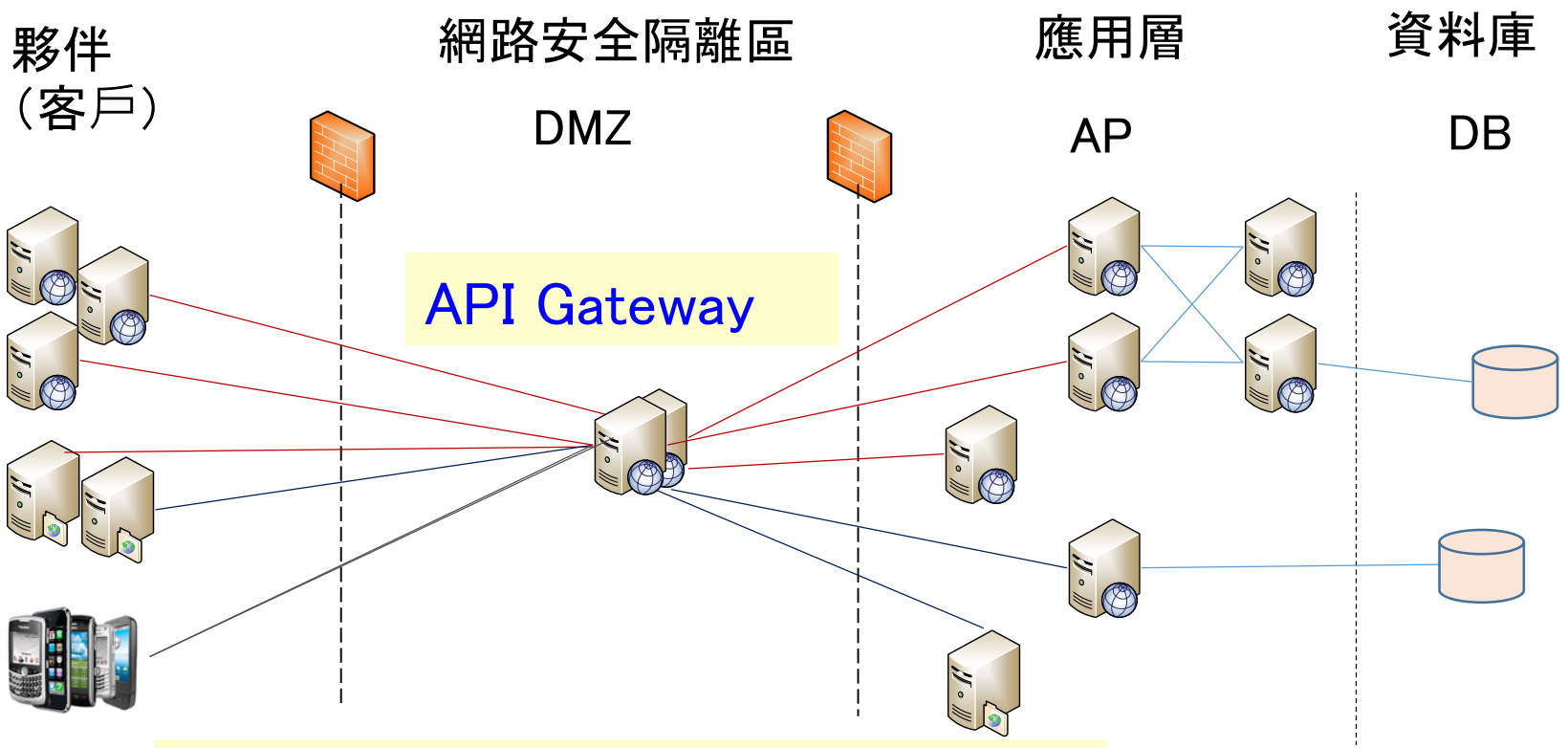
安全、認證、授權、Logging、轉換、Caching、流量控管、交易記錄...等課題？



企業API架構與治理

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

導入API Gateway/Manager

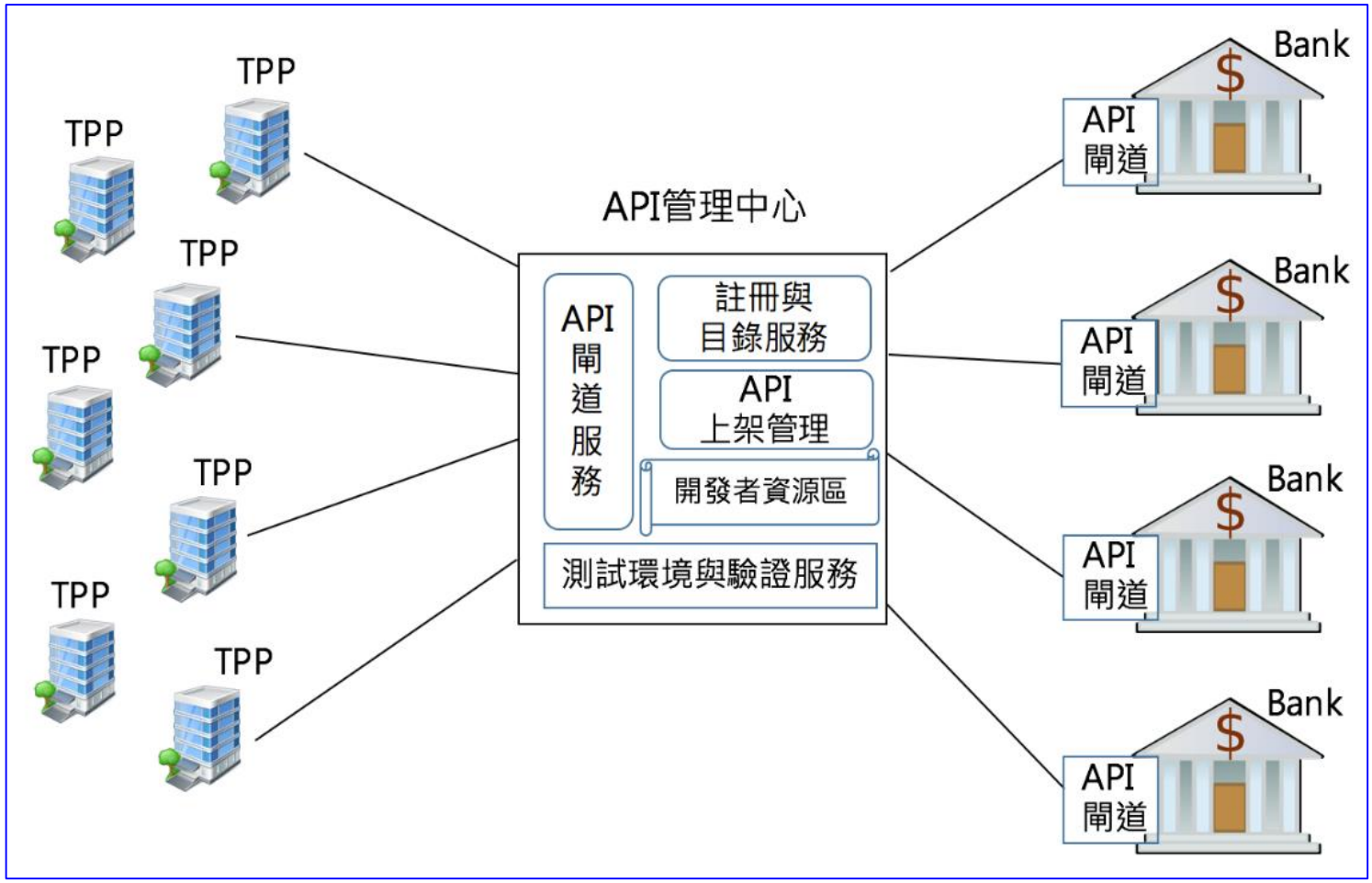


執行安全、認證、授權、Logging、轉換、Caching、流量控管、交易記錄

銀行共同之API 管理中心

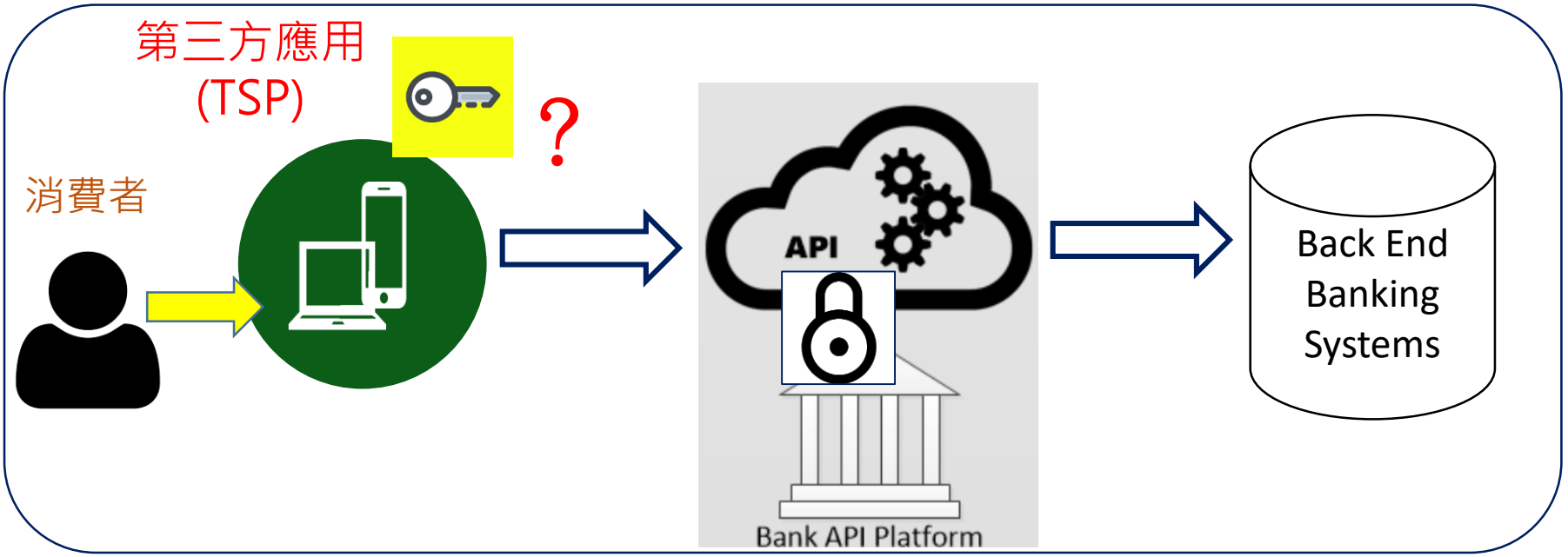
國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

- TPP/TSP集中註冊與認證



第二、三階段客戶資訊

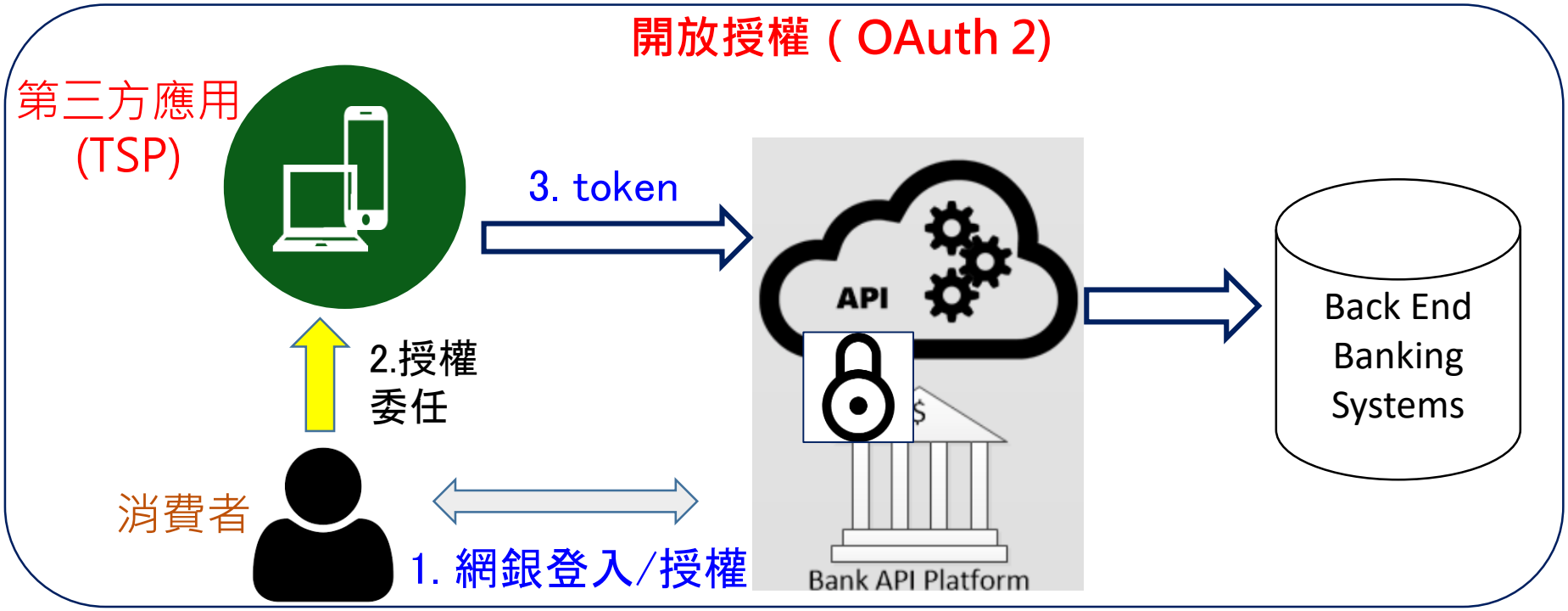
- 涉及消費者帳戶與交易資訊，不能只辨識第三方程式
- 也不能將 消費者的帳號與密碼 交給第三方！



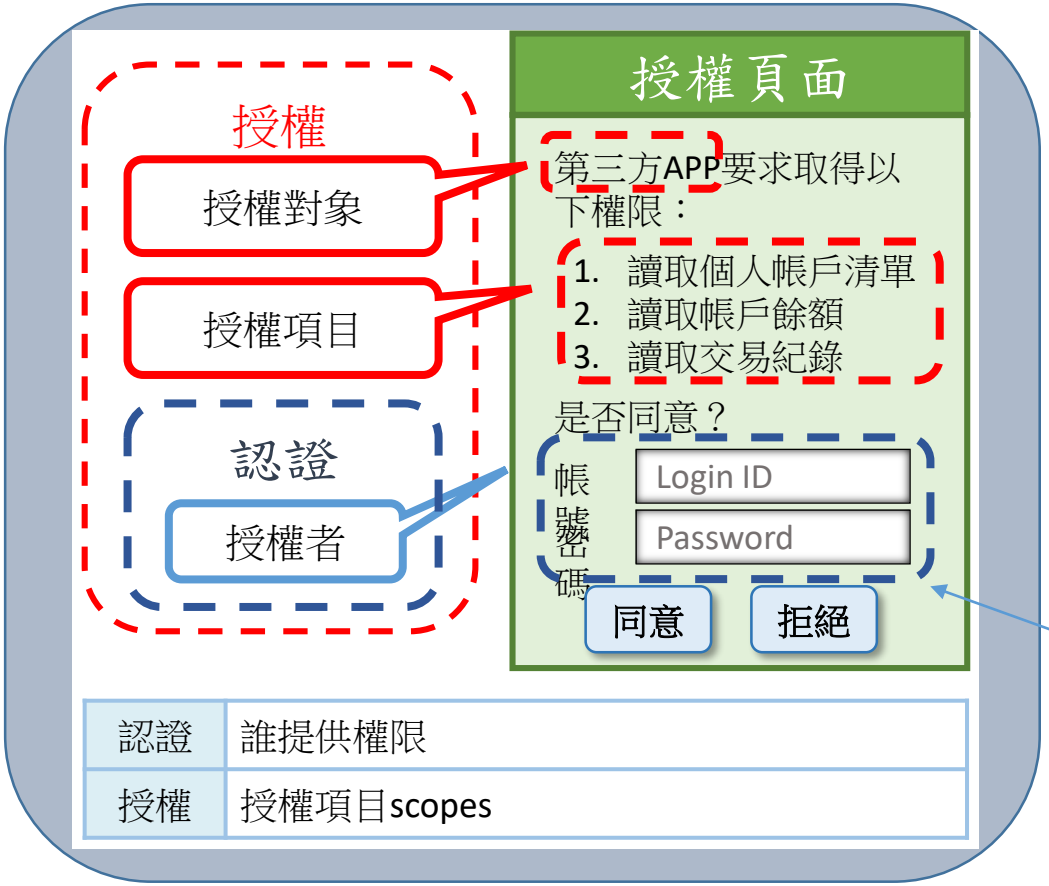
授權委任TSP存取客戶資料

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

- 消費者在原網銀執行帳密登入並授權第三方
- 第三方程式以授權之 Token(通行證)存取銀行API
- Token限制API存取範圍與時間，隨時可撤銷



OAuth2 授權委任存取



第三方程式
要求以下權限：

1. 讀取個人帳戶清單
2. 讀取帳戶餘額
3. 讀取交易紀錄

原網銀隻帳號密碼

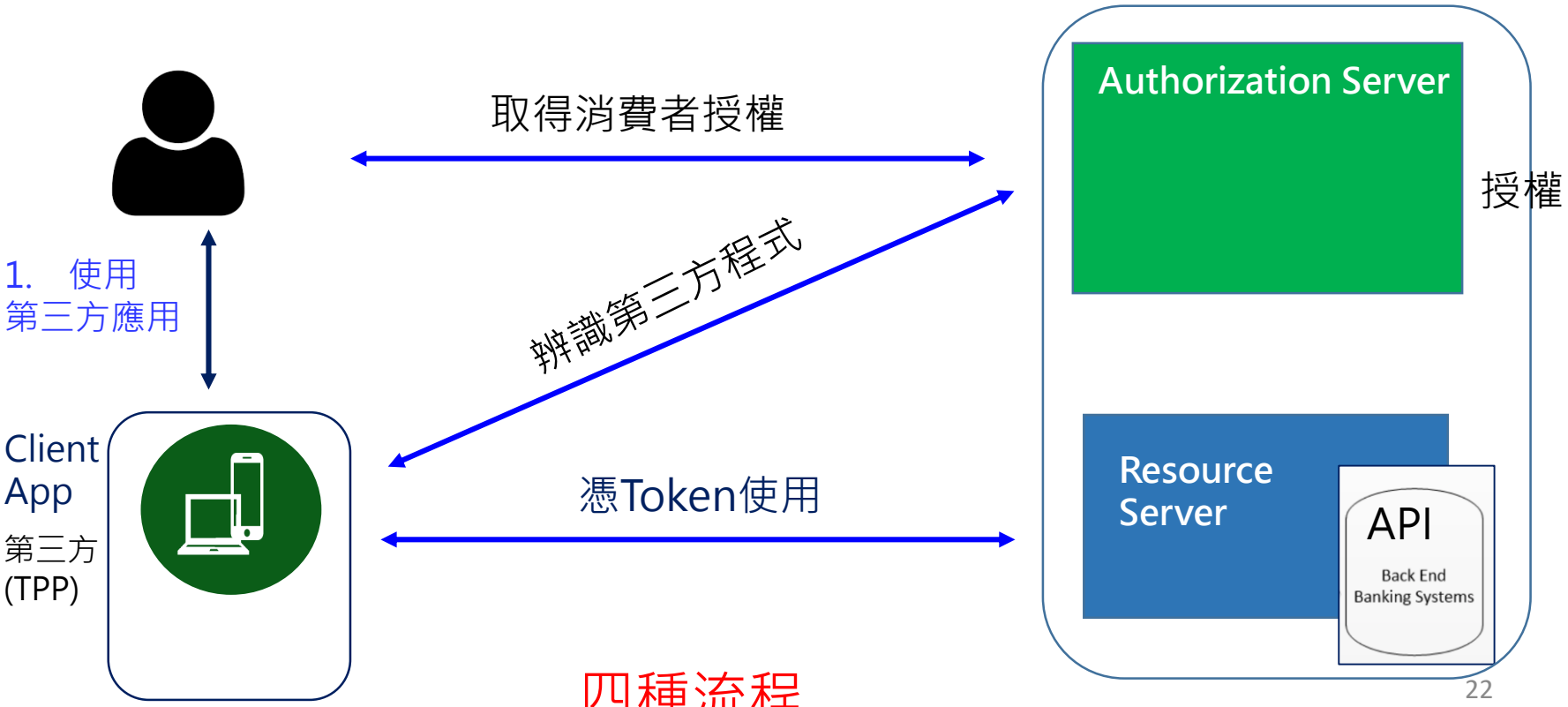
國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

API的風險與防護

開放銀行第二，第三階段的資安挑戰

OAuth 2.0委任存取管理

- 角色分工：AS授權，RS資源（API）管理
  Resource owner消費者
- AS辨識第三方程式(Client)與取得消費者授權第三方
- RS管制資源存取，第三方(Client)憑Token使用



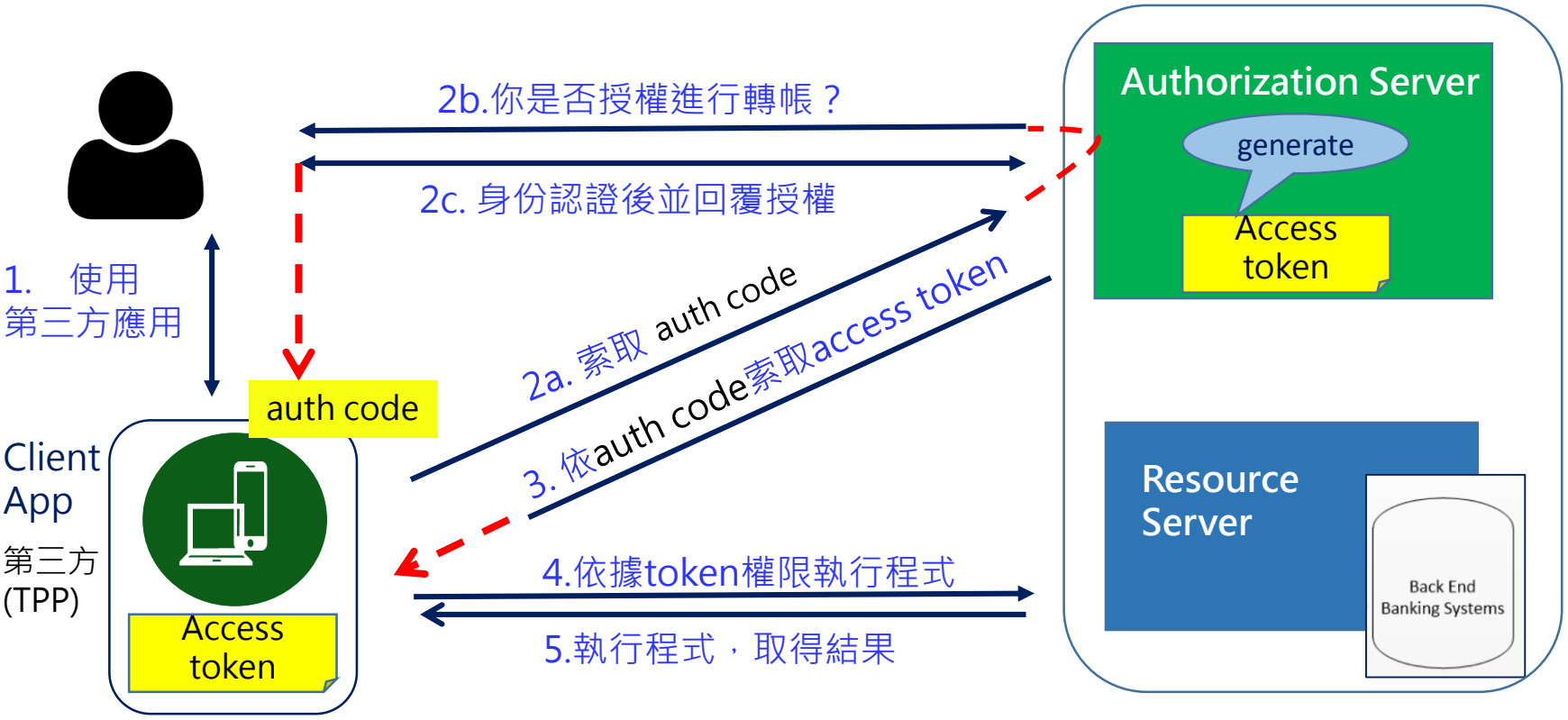
四種流程

OAuth 2.0委任存取管理

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

- AS辨識第三方程式與取得消費者授權第三方
  → Auth code for 第三方程式
- 第三方以auth code換取access token
- RS管制資源存取，第三方憑Token使用

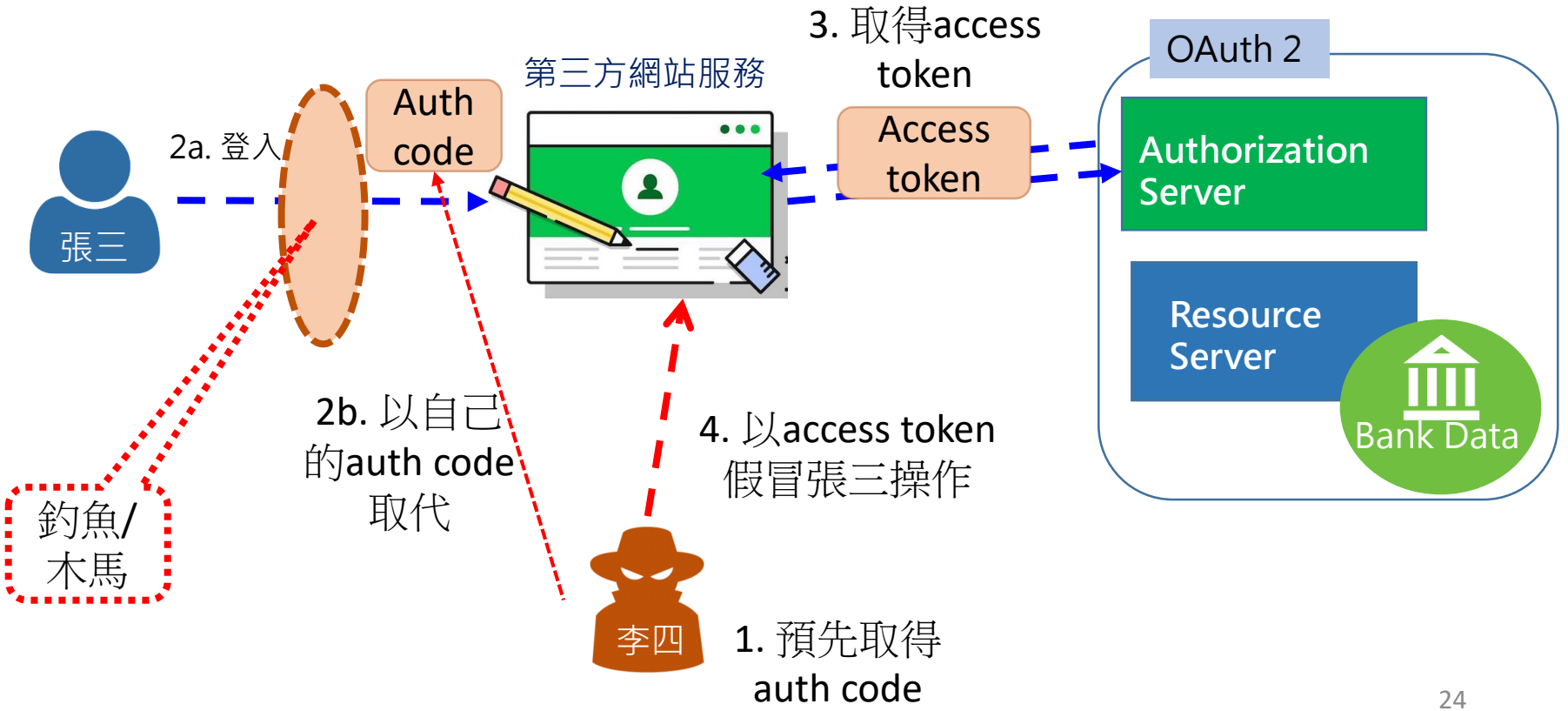
Authorization Code Grant流程



委任存取攻擊：移花接木

- 一般使用者：張三 (沒有任何張三的auth code & access token)
- 惡意攻擊者：李四(取得張三資料或存款)

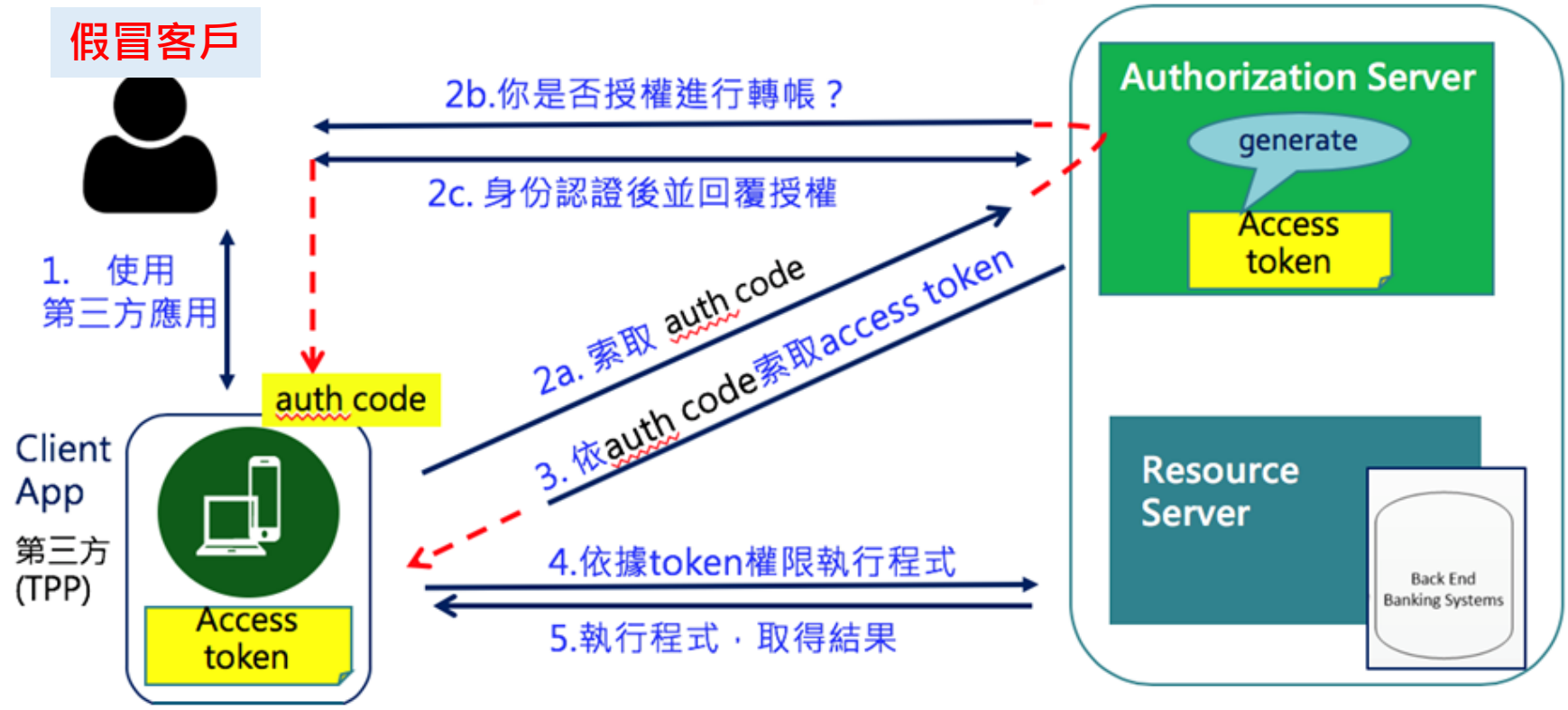
  李四的auth code配上張三的access token



強客戶辨識（SCA）

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

- OAuth2 以授權為主軸
- 第三方程式也可能遭 惡意攻擊，或 因假客戶而是受害
- Strong Customer Authentication避免 假客戶攻擊

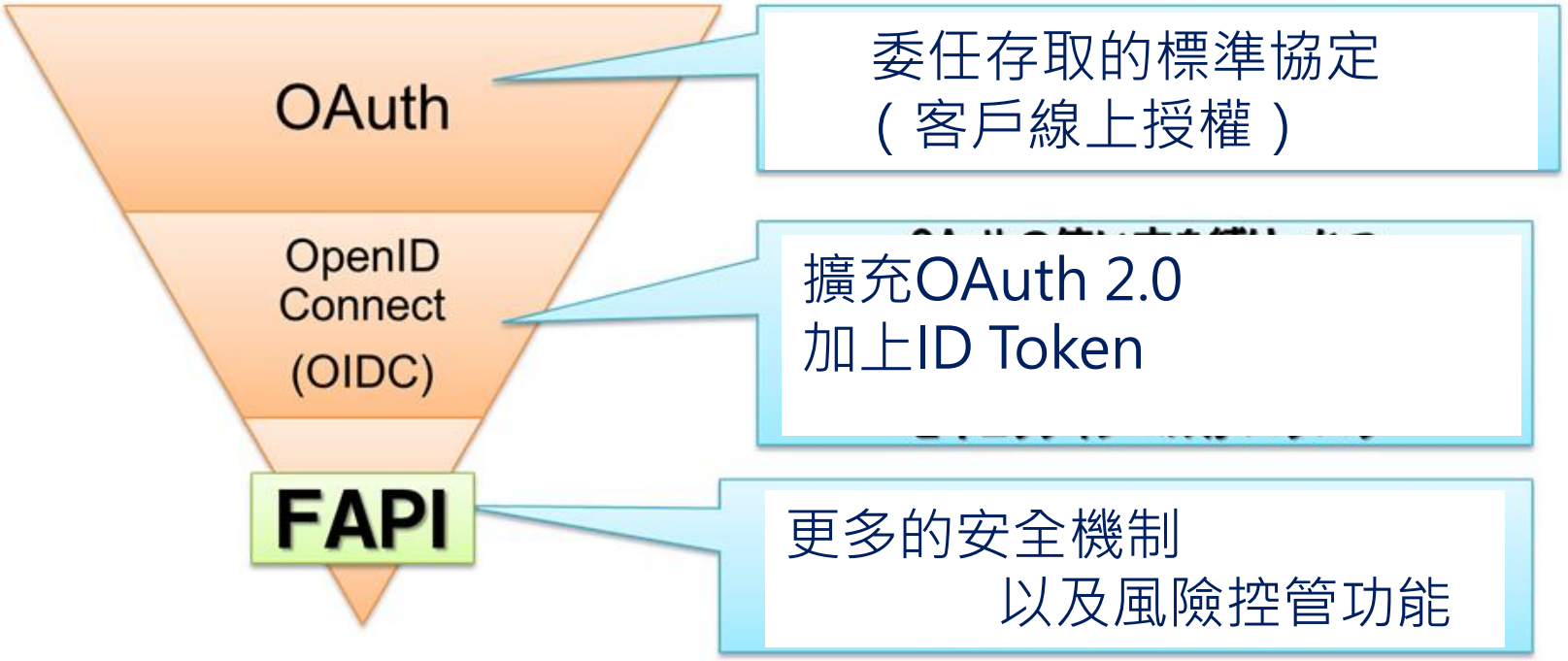


Open API資安國際標準

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

- 線上交易前如何辨識身份
- 移花接木式的攻擊
- 預防 詐欺支付交易！

- OAuth 2.0
- OpenID Connect (OIDC)
- FAPI (Financial-Grade API)



OIDC委任存取管理

- 客戶認證後資訊存入ID Token，第三方可檢視

ID Token using JWT

國立政治大學商學院 金融科技研究中心 FinTech Research Center College of Commerce, National Chengchi University

- JSON Web Token (JWT)
- JWS/JWE: 數位簽章與加密

```
{
 "iss": "http://server.example.com",
 "sub": "248289761001",
 "aud": "s6BhdRkqt3",
 "nonce": "n-0S6_WzA2Mj",
 "exp": 1311281970,  到期時間
 "iat": 1311280970,  發放時間
 "name": "Jane Doe",
 "given_name": "Jane",
 "family_name": "Doe",
 "gender": "female",
 "birthdate": "0000-10-31",
 "email": "janedoe@example.com",
 "picture": "http://example.com/janedoe/me.jpg"
}
```

個資

結語：開放銀行的資安挑戰

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

- Open API 安全防護需要多面向考量
  - API Keys，API gateway
  - 第三方程式註冊與認證，惡意程式防護
  - 客戶端消費者辨識
  - 詐欺交易偵測
  - …
- API的安全標準：從OAuth 2, OIDC 到FAPI
  - 網路層認證，應用層認證，資料加密，資料檢驗
- 銀行端開放API的測試
- 第三方程式的合規測試與資安防護
- 客戶資料的保護
- …

The End

國立政治大學商學院
金融科技研究中心
FinTech Research Center
College of Commerce, National Chengchi University

Thanks

謝謝聆聽

政大資管系教授兼金融科技中心副主任
陳　恭 博士 chenk@nccu.edu.tw