NATIONAL CHENGCHI UNIVERSITY

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

# 開放銀行Open API 第二階段合規說明
# - 合規第三方服務者 (QTSP) -

**Part 2 – Conformance**

報告人：謝旻憲 (Clement) 顧問

日期：2020/04/18

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

# 聲明

- 本報告係依銀行公會與財金公司相關規範，由政治大學金融科技研究中心研讀提出之解決方案。

- 解決方案如與規範在未來應用上如有衝突之處，以主管機關的解釋為依據。

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

# 報告大綱

5. Conformance與檢驗研究
6. 輔導對象
7. 媒合方式

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

# 技術檢驗項目說明

# 國際開放銀行標準

| 地區/國家 | 資安/技術規範 | API 驗證 |
| --- | --- | --- |
| 歐盟 | 以RTS (Regulatory Technical Standards)為主<br>• 提供XS2A (Access to Account) API<br>• 強調SCA (Strong Customer Authentication)<br>• 要求採QWAC & QCSeals | 有二家驗證：<br>• Berlin Group NextGenPSD2<br>• STET |
| 英國 | 以英國Open Banking網站為主，除提供API外，<br>• 採用OIDC (Open ID Connect)為身份認證，再加FAPI (Financial API)為介接標準<br>• Functional Role含AISP, PISP, ASPSP | 採自行驗證後，呈報英國開放銀行公司確認，有四種驗證，一般統稱 UK OB：<br>1. Security Profile Conformance<br>2. Functional Conformance<br>3. Dynamic Client Registration Conformance<br>4. Customer Experience Guidelines Conformance |
| 澳洲 | 法律以CDR為主，發展CDS (Consumer Data Standards) | 目前無特定驗證機制 |

國立政治大學商學院

# 技術與資安架構示意圖

## 第二階段 open API 技術與資安規範示意圖

連線規範

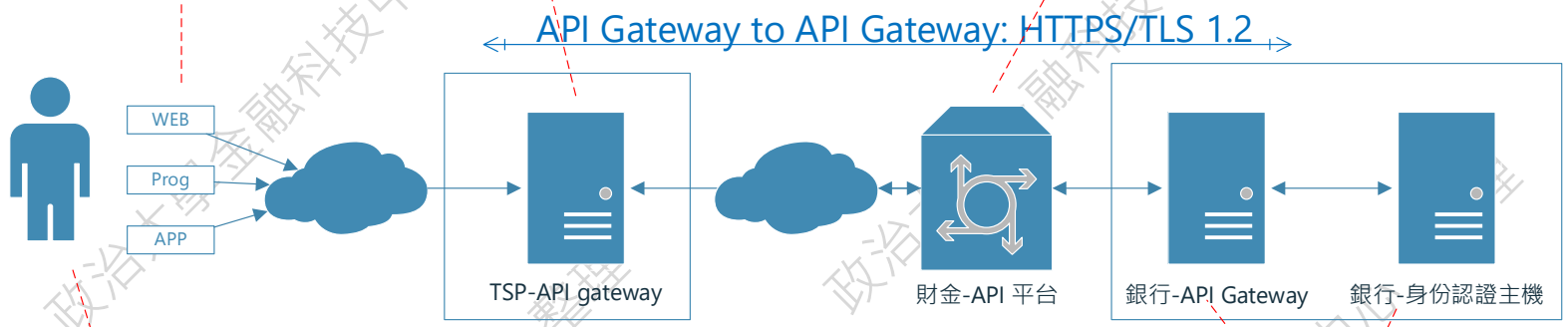
系統架構

認證規範

**第七條：程式安控**
1. 網站系統設計要求
2. 程式設計要求
3. APP設計要求

**第五條：網路類型**
**第六條：訊息加密**
*
**~~SHA/3DES/AES/RSA/ECC~~**

**第八條：財金API安規**
* REST API 規範
* WEB 安規




**第三條：使用者身份認證**
1. 電子簽章(數位簽章)
2. 存款帳戶(銀行代驗)
3. 信用帳戶(銀行代驗)
4. 電信門號(電信代驗)

**第四條：使用者帳密**
1. 電子簽章
2. OTP (簡訊不可)
3. 2FA
4. 簡單帳密

**第九條：獲取銀行資料**
1. 第一階段：API KEY
2. 第二階段：
* 認證 – 初次/再次
* 授權 – access/refresh token
3. 訊息安全性
* Token 加密/簽章
4. 使用期限

# 台灣TSP技術/資訊驗證

| 項次 | 項目 | 合規說明 |
| --- | --- | --- |
| 1 | 連線安全 | • 連線標準 TLS 1.2<br>• 比照 EU PSD2 RTS 要求，與TWCA合作提供QWCA憑證<br>• 協助銀行提供TSP憑證管理 |
| 2 | API 檢驗 | • 目前國內沒有標準，可依英國conformance certification進行相關檢驗<br>• 英國與澳洲都採用FAPI做API驗證的強度<br>• 對API進行相關API 檢驗與測試 |
| 3 | 身份驗證 | • 銀行端核定身份(核身)作業<br>• 未來會延伸為業務開辦的KYC的作業<br>• 國外目前以OIDC為主流<br>• 台灣目前會以Redirect和Decoupling Authentication為測試基準 |
| 4 | 弱點掃瞄 | • 上線程式需要通過必要弱點掃瞄驗證 |

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

# 輔導目標


| 項目 | 目的 | 作法 |
|---|---|---|
| 教育訓練 | 協助TSP了解與銀行合作上必要的法令與技術規範 | • 提供商模、法令、技術、檢驗等四類課程，協助TSP降低與銀行合作門檻 |
| ISO認證 | TSP在輔導期間必須取得由銀行認可的第三方資安認證，由符合未來上線的法遵要求。 | • 由政大協同第三方輔導與認證單位一起協助TSP。<br>• 未來TSP稽核可以銀行認的第三方單位執行。 |
| 測試檢驗 | 建立銀行間共用交換資料格式，並公開讓銀行與TSP使用。<br><br>建立標準測試項目，加速TSP與銀行測試速度與效率。 | • 與SI廠商合作<br>• 建立測試標準項目<br>• 建立標準版API templates<br>• 開發資料驗證小工具<br>• 開發API測試小工具<br>• 與SI合作進行API平台測試 |

* 可參考政大開放銀行網站有關以上資訊

五月中第二場說明會釋出

# 政大合作的資訊服務/系統整合廠商






| 華威數位/IBM API-C | 叡揚 Axway | 昕力 DigiRunner (TSMP) | 精誠 MuleSoft | 果核數位 (資安掃瞄) |
|---|---|---|---|---|



* 以上為簽MOU合作之資訊廠商，其它開源API平台(如RedHat, WSO2) 由委外廠商負責測試

# 政大與資訊廠商合作模式

合作方式：政大與系統整合廠商簽定MOU

合作目的：在協助互助建立開放銀行API介接各項標準

合作範圍：

- 協助規劃銀行端作業流程，如核身作業、OAuth驗證流程
- 協助提供TSP端API所需資料規格
- 共同建立開放銀行測試平台
- 協助有關TSP與銀行端測試相關作業
- 以及，其它有助於開放銀行以及Open API推動相關事宜

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

# 政大輔導對象與合作廠商

# 目前政大合作的TSP

## TSP類群

| 金融科技公司 | 電信公司 | 三方支付* | 其它金融公司 |
| --- | --- | --- | --- |

麻布記帳 MONEYBOOK

CW MONEY

遠傳FET

twMP

CRIF Together to the next level

安心比 iCompare

ipromise 愛承諾金融網

Money101

橘子支付 GAMA PAY

TDCC

聰明貸款

anue 鉅亨

SYSTEX 精誠資訊

好好投資 HowInvest



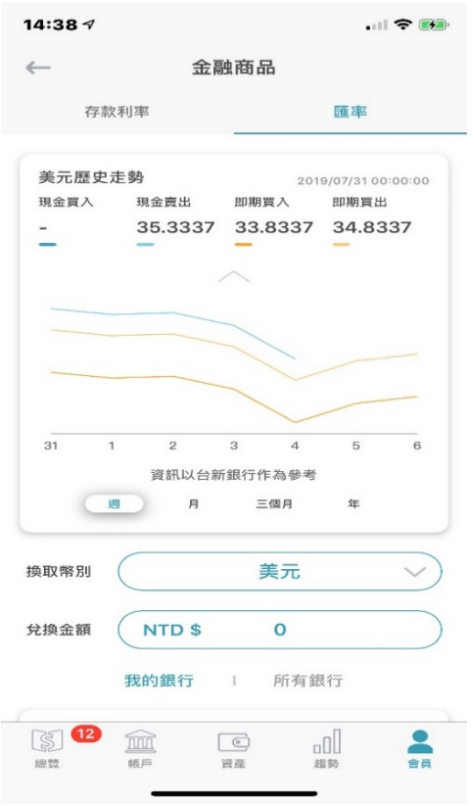
* 三方支付視第三階段提供，目前洽談合作輔導中

# 政大媒合/合作方式

- 由政大提供輔導名單和測試情境
- 協助銀行現行TSP符合第二階段的合規
- 透過政大找尋銀行想要的TSP合作廠商
- 由政大協助銀行做試辦POC
- 由政大提供API介接測試人力

# 合作方式一：現有TSP分段介接

- 策略：挑選未來要合作的TSP分階段介接
- 進行方式：
  1. 先介接第一階段，提供現行雙率資訊
  2. 設計提供信用卡行銷資訊
  3. 待輔導成功後，再接第二階段API
- 適用TSP：CWMoeny、鉅亨網、iPromise …
- 適用情境：帳戶整合、信用卡行銷



# 合作方式二：POC

- 策略：引進國外TSP
- 進行方式：
  1. 三方簽訂MOU
  2. 進行POC
  3. 驗證相關情境
- 適用TSP ：CRIF
  - ✓英國開放銀行TSP
- 適用情境：信用評等

# 合作方式三：試辦

- 策略：挑選未來要合作的TSP分階段介接
- 進行方式：
  1. MOBILE ID代驗
  2. 提供數位帳號整合—例：活存 / 定存
  3. 提供TSP端eKYC和線上申辦業務
- 適用TSP：遠傳電信 (Friday 57)
- 適用情境：定額存款、跨業行銷

# 小結與未來計劃

- 開放銀行在台灣仍持續發展，今年度**政大輔導以”合規“為主**，確保銀行與TSP合作時可以確保TSP達到規範上的各項要求
- 政大目前有**開發TSP輔導網站**，會將TSP各項合規項目與輔導進度放置至網站中，供銀行與TSP使用
- 今年度會展開TSP治理相關研究與POC，重點在透過API做資料交換時，如何達到可追蹤、可信賴及可控制
- 參考英國發展開放銀行進程，今年度會往更全面性**”開放金融“**前進

# 敬請指教


政治大学
NATIONAL CHENGCHI UNIVERSITY


FTRC
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