MITAKE 三竹資訊
www.mitake.com.tw

淺談金融與支付行動通訊應用安全

三竹資訊股份有限公司

林三衛　協理

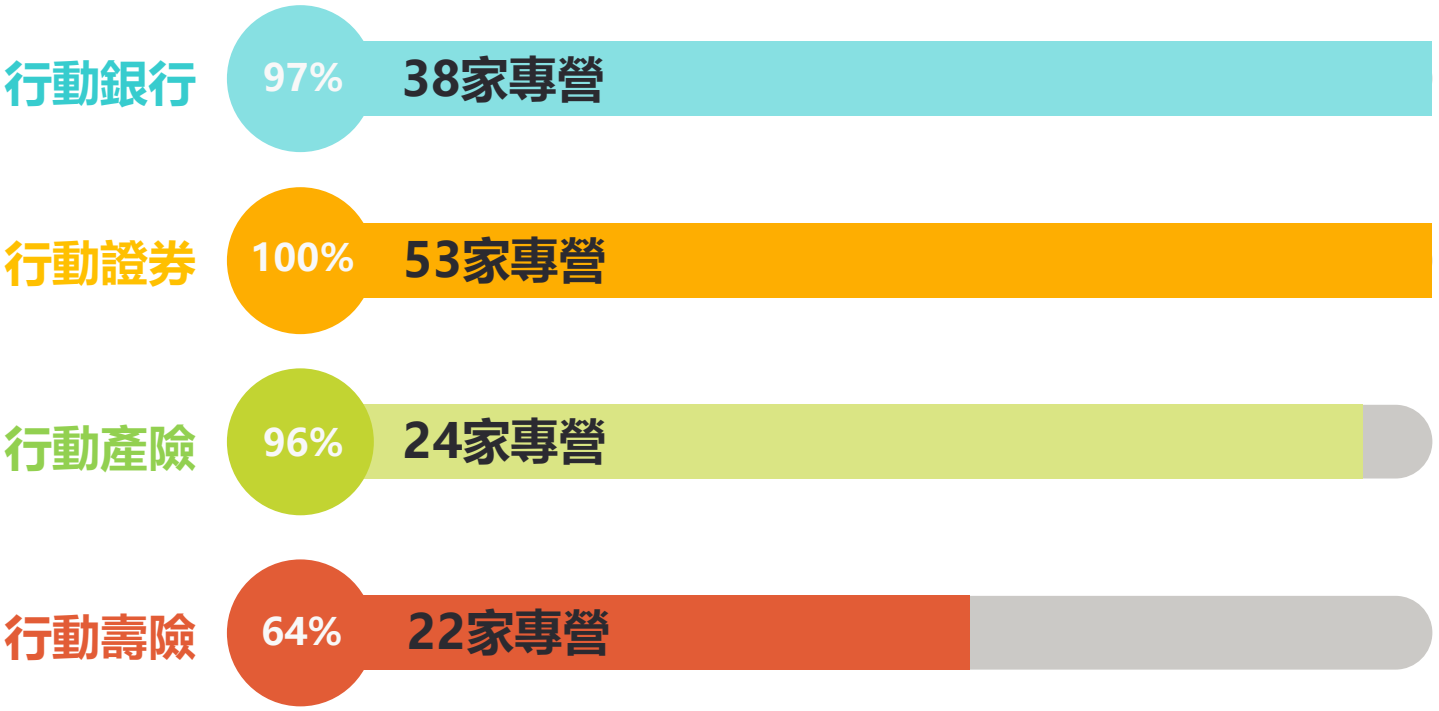
大綱

1. 國內金融與支付的行動通訊現況
2. 金融與支付交易風險定義與類型
3. 金融與支付交易的行動通訊安全
4. 金融與支付的行動通訊注意事項

Part 1

國內金融與支付的行動通訊現況

國內金融業行動通訊應用發展現況



說明：
專營：服務供應商具有獨立行動通訊應用發展。
比率：服務供應商行動通訊應用發展的飽和度。
銀行：個人財務金融行動通訊應用發展，包含中華郵政股份有限公司。
來源：三竹資訊股份有限司。
效期：2017年5月31日。

國內支付業行動通訊應用發展現況

電子票證	100%	4家專營(儲值/支付)
電子支付	100%	5家專營(儲值/支付/代付/轉帳)
第三方支付	???	4930家(代付)

說明：
專營：服務供應商具有獨立行動通訊應用發展。
括號：服務供應商授權業務範圍。
比率：服務供應商行動通訊應用發展的飽和度。
支付：用戶藉由儲值餘額直接支付。
代付：用戶藉由第三方管道使用信用卡或簽帳卡代收代付。
轉帳：用戶甲帳號藉由儲值餘額直接轉出指定金額給用戶乙帳號。
來源：行政院經濟部商業司。
效期：2017年5月31日。

國內金融業行動通訊應用發展規範

銀行業

- 金融機構辦理電子銀行業務安全控管作業基準。
- 行動應用APP安全開發指引。

證券業(沒有專門規範，但是可以適用銀行業規範)

- 建立證券商資通安全檢查機制。
- 金融機構辦理電子銀行業務安全控管作業基準。

保險業

- 保險業經營行動投保業務自律規範。
- 保險業經營電子商務自律規範。
- 財產保險業辦理資訊安全防護自律規範。

國內支付業行動通訊應用發展規範

電子票證業

- 電子票證應用安全強度準則。

電子支付業

- 電子支付機構資訊系統標準及安全控管作業基準。

第三方支付業(沒有專門規範，但是可以適用電子支付業規範)

- 電子支付機構資訊系統標準及安全控管作業基準。

為何談論行動應用通訊發展規範？

共同性

金融業與支付業相關行動通訊發展規範具有**高度的共同性**，這些共同性即今日演講主題。

關聯性

金融業與支付業相關行動通訊發展規範與行動應用APP安全開發指引相較，前者規範彰顯**深度**，後者規範彰顯**廣度**。兩者都涉及相同的論述應用，這些論述應用即今日演講主題。

那裡可以取得完善的行動通訊發展規範？

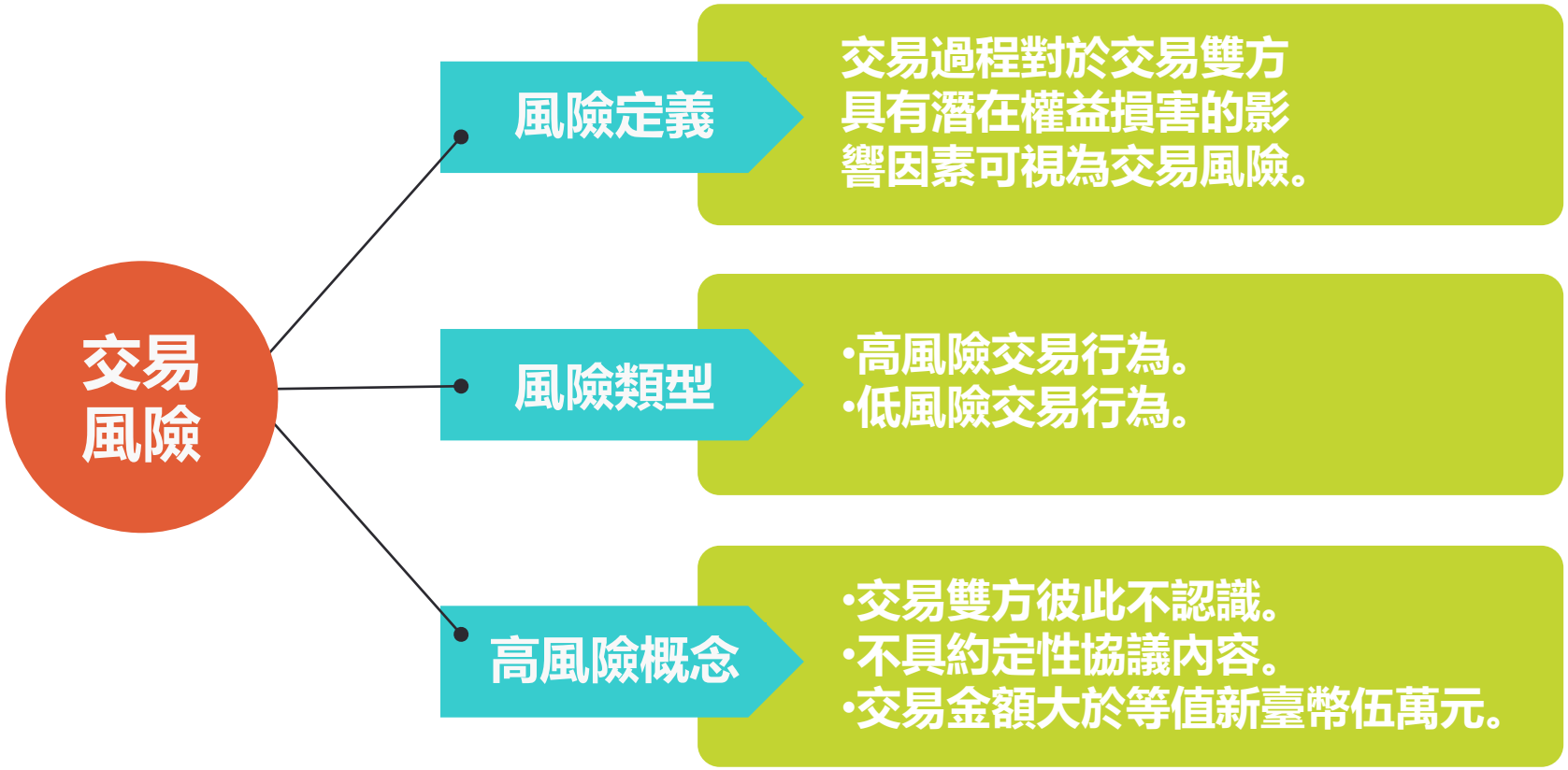
下列四個管道是在實務上推薦給讀者：

1. 行政院經濟部工業局
2. 行政院金融監督管理委員會
3. National Institute of Standards and Technology
4. Open Web Application Security Project

Part 2

金融與支付交易風險定義與類型

何謂金融與支付交易風險？



說明：
交易雙方：買方是您自己；賣方可以是金融業者、支付業者或實體商店。
通訊安全：行動通訊應用發展規範中的通訊安全是建構在交易雙方立場。

檢視國內支付業服務管理規範

交易模式	主管機關	授權範圍	服務資本	交易限制
電子票證	金管會	儲值 支付	新臺幣三億	1.單筆支付新臺幣 3,000 元 2.單筆儲值新臺幣 10,000 元
電子支付	金管會	儲值 支付 代付 轉帳	新臺幣五億	1.單筆儲值新臺幣 50,000 元 2.單筆支付新臺幣 50,000 元 3.單筆代付新臺幣 50,000 元 4.單筆轉帳新臺幣 50,000 元
第三方支付	經濟部	代付	新臺幣一億	1.單筆代付新臺幣 50,000 元

註：支付是指用戶藉由儲值餘額直接支付；代付是指用戶藉由第三方管道使用信用卡或簽帳卡代收代付。

低風險交易行為行動通訊安全原則

下列前四項為低風險交易行為的行動通訊安全原則：

1	行動通訊是否在交易過程規劃敏感資料的保護？
2	行動通訊是否在交易過程確保交易資料完整性？
3	行動通訊是否在交易過程辨識交易對象的合法？
4	行動通訊是否在交易過程控制交易資料唯一性？
5	行動通訊是否交易過程無法否認傳送交易請求？
6	行動通訊是否交易過程無法否認接收交易結果？

Part 3

金融與支付交易的行動通訊安全
低風險交易行為

行動通訊的隱密性

原則定義

- 行動通訊資料應該避免遭受被截取或被窺竊，致使洩漏資料內容導致交易雙方權益損害。

實務觀念

- 現有工業標準中的網路傳輸層安全協議具有一定程度的安全性。
- 現有安全性架構之下規劃對敏感資料進一步保護實為必要之舉。

建議方案

- 實務上先定義敏感資料範圍屬於交易雙方基本資料與交易資料。
- 實務上建議採用加密方法對敏感資料實做加密(AES/RSA/ECC)。
- 對稱式加密方法需注意加密演算程序與公鑰生成程序必須分開。
- 對稱式加密方法需切記公鑰生成程序盡量以動態演算生成公鑰。
- 選定複數個屬性配置一定的商業規則，演算一組有效的加密公鑰。若將時戳或裝置識別加入演算，生成結果將具有唯一性。

行動通訊的完整性

原則定義

- 行動通訊資料應該避免遭受竄改，致使通訊資料內容不正確。
- 行動通訊資料若已遭受竄改時，該筆交易資料必須視為無效。

實務觀念

- 假設交易雙方執行新臺幣1000元的交易行為，您如何確保最後的交易結果為新臺幣1000元？

建議方案

- 實務上建議採用訊息押碼函數或訊息雜湊函數(MAC/SHA)。
- 用戶端提交資料實做訊息押碼或訊息雜湊，致使資料生成不可逆。
- 伺服端接收資料重新實做訊息押碼或訊息雜湊，再比對演算結果。
- 訊息押碼或訊息雜湊演算過程也可以配置初始值向量或公鑰協定。

行動通訊來源辨識

原則定義

- 行動通訊提交交易資料時，不得以冒名方式傳送交易資料。
- 伺服端必須具有一定的交易檢核機制辨識來源的交易對象。

實務觀念

- 任何一個交易請求來源，伺服端是否都無條件執行該命令？
- 交易雙方在交易的過程中是否可能允許不知道對象是誰嗎？

建議方案

- 實務上建議設計一套用戶身分暨用戶裝置交易授權碼(TAC)。
- 單純使用用戶身分檢核者，建議不要使用單一屬性作為檢核條件。
- 選定複數個屬性配置一定的商業規則，演算一組可以有效辨識的用戶身分或用戶身分暨用戶裝置交易授權碼，由伺服端驗證合法性。

行動通訊不可重複

原則定義

- 行動通訊提交交易資料時，同一筆資料同時不得重複交易。
- 伺服端必須具有一定的交易檢核機制控制交易的不可重複。

實務觀念

- 設想交易雙方執行一筆交易，用戶端重複提交兩次交易怎麼辦？
- 設想交易雙方執行一筆交易，同一筆交易產生兩個結果怎麼辦？

建議方案

- 實務上建議用戶端實做防止在短時間之內用戶重複提交交易資料。
- 用戶端提交交易資料時，實做遮照或千分之一秒內拒絕重複提交。
- 伺服端對交易雙方每一筆交易資料需配置交易唯一的序號與時戳。

Part 4

金融與支付的行動通訊注意事項

1.應用程式最小權限管理

注意事項

•行動通訊應該針對應用程式檢視服務所需最小權限，並設定應用程式設計介面存取過程的授權管理。

潛在影響

•服務存取授權一旦管理不當，有心人士即可任意調用資料。

實務對策

•藉由屬性表適當地設定應用程式服務的開啟或關閉。
•若您的產品沒有使用電話簿，發行時請關閉電話簿。
•若您的產品沒有使用行事曆，發行時請關閉行事曆。

2.行動通訊落地資料保護

注意事項

•行動通訊若有必要儲存敏感資料於用戶端，應該採取加密或亂碼相關資料保護措施。

潛在影響

•資料存取授權一旦管理不當，有心人士即可任意調用資料。
•資料若保護不夠完善，不當取得資料即可直接檢視或使用。

實務對策

•請先檢視落地資料量的規模。
•若資料量大，建議採用具有保護措施的小型資料庫來儲存。
•若資料量小，建議採用加密方法對落地資料執行保護措施。
•加密過程若涉及公鑰生成程序，請參照行動通訊的隱密性。
•請適當管理存取資料的權限。
•請勿使用訊息押碼函數或訊息雜湊函式保護資料。

3.應用程式的原始碼掃描

注意事項

•行動通訊**建議**應該針對應用程式的原始碼執行弱點掃描。

潛在影響

•應用程式處理程序存在弱點或漏洞的風險性。

實務對策

•本項對策可能涉及委託掃描或採購掃描工具**成本**。

•建議針對掃描報告高度或中度弱點問題實行除錯。

4.行動裝置遭受破解提醒

注意事項

•行動通訊在啟動應用程式時，若擬似偵測到行動裝置遭受破解，應該盡量提醒用戶注意可能潛在的風險。

潛在影響

•凡是已破解的行動裝置，行動裝置被置入木馬的風險性較大。

實務對策

•本項對策納入服務供應商免責聲明(權益損害訴訟對賣方有利)。
•提醒用戶可用畫面或對話方塊執行。
•使用網路上已公開的偵測方式執行。

5.應用程式蓄意竄改防護

注意事項

•行動通訊應用程式為了保障原生程式碼的完整性，建議應該避免未經授權的竄改或更新。

潛在影響

•應用程式可能存在被惡意複製使用的風險。
•處理程序可能存在被解譯的風險，尤其是Java中介格式位元碼。

實務對策

•本項對策可能涉及採購封裝工具成本。
•應用程式在編譯時，可以採用原生程式碼混碼保護措施。
•應用程式初始化時，IPA可以驗證Code Sign Bundle ID一致性；APK可以驗證Code Sign KeyStore Hash Value一致性。
•完善的原生程式碼防止竄改規劃仍然具有暴露於反組譯的風險當中，建議將應用程式藉由專業的封裝工具執行封裝。

6.應用程式近端場域通訊

注意事項

•行動通訊採用近端場域通訊(NFC)技術執行交易資料傳送之前，應該經由用戶人工確認該筆交易資料。

潛在影響

•無法防止傳送一筆未經確認交易。
•傳送交易的動作可能容易被模擬。

實務對策

•任何涉及交易程序必定提供交易確認步驟。
•初始化應用程式交易功能時，請於交易結果的前一個步驟提供畫面或對話方塊提醒用戶。
•本項注意事項可以擴充於QR Code交易確認應用。

7.加密公鑰白箱作業生成

注意事項

•行動通訊應用程式若在用戶端儲存且加密敏感資料時，加密所需要的公鑰與方法建議藉由白箱作業。

潛在影響

•加密金鑰存在被竊取的風險性。

實務對策

•白箱作業是指將應用程式中的加密公鑰資訊得以充分隱藏，目的是降低加密演算程序遭攻擊的機率。

•有關公鑰白箱作業請參照行動通訊的隱密性。

8.應用程式除錯日誌管理

注意事項

•行動通訊應用程式發行正式版本時，應該關閉或移除除錯日誌，或避免儲存敏感資料於未經加密的日誌儲存區。

潛在影響

•應用程式執行時期效能變差。
•明確地違反個人資料保護法。

實務對策

•iOS應用程式可以藉由發行日誌自訂旗標管理
•iOS應用程式也可以藉由NSLog函數關閉除錯日誌。
•Android應用程式可以藉由發行日誌自訂旗標管理。

9.行動通訊個資授權管理

注意事項

•行動通訊首次啟動應用程式時，應該明確告知用戶資料蒐集、處理、利用與用戶得以要求刪除資料的權利。

潛在影響

•明確地違反個人資料保護法。

實務對策

•本項對策納入服務供應商免責聲明(權益損害訴訟對賣方有利)。

•提醒用戶可用合約、畫面或對話方塊執行。

10.行動通訊憑證認證管理(1/2)

注意事項

•有效的伺服端SSL憑證認證管理可以防止行動通訊期間中間人蓄意的攻擊。行動通訊應用程式是否使用憑證約定性認證管理，並確保連線的伺服端為應用程式開發者所指定的通訊對象？

潛在影響

•暴露於行動通訊期間中間人蓄意攻擊的風險性。

實務對策

•應用程式採用預先載入SSL憑證公鑰，並在應用程式與伺服端交握程序之後，驗證預先載入公鑰是否與伺服端公鑰相同。
•上開對策在用戶端應用需要規劃SSL憑證公鑰的生命週期管理。
•伺服端預先生成一對RSA公鑰與私鑰，公鑰預先載入用戶端。
•用戶端在初始化時，判斷連線網域相對應的SSL憑證公鑰是否已經過期或判斷行動通訊期間是否造成應用程式與伺服端交握失敗。

10.行動通訊憑證認證管理(2/2)

注意事項

•有效的伺服端SSL憑證認證管理可以防止行動通訊期間中間人蓄意的攻擊。行動通訊應用程式是否使用憑證約定性認證管理，並確保連線的伺服端為應用程式開發者所指定的通訊對象？

潛在影響

•暴露於行動通訊期間中間人蓄意攻擊的風險性。

實務對策

•上開結果若為過期或失敗，應用程式觸發更新SSL憑證公鑰介面。
•應用程式調用更新SSL憑證公鑰介面時，請求命令以RSA公鑰執行加密，伺服端接收請求命令之後再以私鑰執行解密。
•若伺服端解密正確，伺服端把新版SSL憑證公鑰藉由RSA私鑰簽章回傳給用戶端，用戶端藉由RSA公鑰驗證簽章是否正確。
•若用戶端驗證伺服端私鑰簽章正確，用戶端更新新版SSL憑證公鑰。

MITAKE 三竹資訊
www.mitake.com.tw

感謝您的聆聽　歡迎您的指教

三竹資訊股份有限公司

林三衛　協理