Testing Laboratory
0263

中華電信
Chunghwa Telecom

行動應用App資安檢測服務說明

中華電信研究院

董元昕

Refresh your life

大綱

實驗室簡介
- 實驗室認證
- 檢測能量
- 人員資格

檢測項目
- MAS標章
- 檢測項目

申請流程
- 檢測流程
- 檢測申請
- 測試報告

中華電信資安團隊(1/2)

- **中華電信資安團隊得獎紀錄與驗證成果**
  - 2016年台銀資安服務共同供應契約評鑑結果最頂尖之資安公司，SOC監控、資安健診服務、弱點掃描服務、滲透測試服務與社交工程郵件服務。
  - 2014年第八屆(ISC)2亞太區資訊安全領導成就表彰計畫獲選ISLA「資訊安全從業人員」獎項
  - 取得多項認證，ISO27001、BS10012、ISO 20000、CSA STAR LV2、TAF 17025
  - 自營通用憑證管理中心通過國際公認的WebTrust for CA雙項認證
- **資安團隊及組織規模**
  - **服務團隊：**資安監控服務、資安檢測服務、產品研發與管理、身分安全認證服務約 **120人**
  - **研發團隊：**研究院負責資安技術研究及服務支援人力約 **130人**
- **資安團隊專業證照**
  - 具備各領域資安技術與管理、資訊、網路等相關證照共計**311張**，含檢測、IT管理、系統、網路、開發、專案管理

中華電信資安團隊(2/2)

❖ 外部服務實績

- **弱點掃描與滲透測試服務**
  - 130家客戶，**平均每個網站有17個漏洞**
- **ISP端資安代管服務(MSSP)服務(含IPS/DDoS/內容過濾)**
  - 超過20,000家客戶，**平均每日阻擋逾43萬次攻擊**
- **SOC代建與代管服務**
  - 超過30個專案　，**每日平均分析6.6億筆記錄，發現78件資安異常事件**

❖ 內部維運能量

- **眾多設備維運管理**：終端電腦約3萬多部，主機近1萬部
  - 主機安全管理、網路存取管理、資安設備管理、弱點掃描、滲透測試、資安監控及處理...等
- **台灣最大ISP業者**：擁有最多台灣在地即時資安情資

中華電信研究院測試中心(1/3)

- 中華電信研究院是中華電信所屬的研發機構，國內知名的ICT系統開發廠商，擁有經驗豐富APP開發工程師。
- 多年來致力於資訊安全的推廣，除了檢測服務的提供外，資訊安全的教育訓練更是主要業務之一。
- 專業測試實驗室，通過CMMI Level 3認證，TAF認證之ISO/IEC 17025實驗室，取得工業局行動應用APP基本資安認證實驗室、資安鑑識實驗室、NCC資通訊設備安全檢測實驗室，有完整軟硬體測試能量，及經驗豐富的測試工程師。
  - http://www.chttl.com.tw/test/

CMMI LEVEL 3 certified

TAF Testing Laboratory 0263

NCC

BSMI

中華電信研究院測試中心(2/3)

中華電信 Chunghwa Telecom

厚實的安全系統開發訓練經驗，包含完整的系統生命週期SSDLC。

全方位的軟體品質驗證技術(ISO/IEC 25010 軟體品質模型)

設計 → 開發 → 測試

軟體品質

品質軟體開發		品質軟體檢測	
安全系統設計原則	安全系統開發方法	自動化檢測工具	滲透測試方法

中華電信研究院測試中心(3/3)

- 測試中心有完整的APP檢測能量，包含完善的硬體設備資源，與充足的檢測軟體，藉此提供最「精確」、「完整」的檢測結果，確保您的APP能夠符合工業局行動應用APP基本資安認證規範。

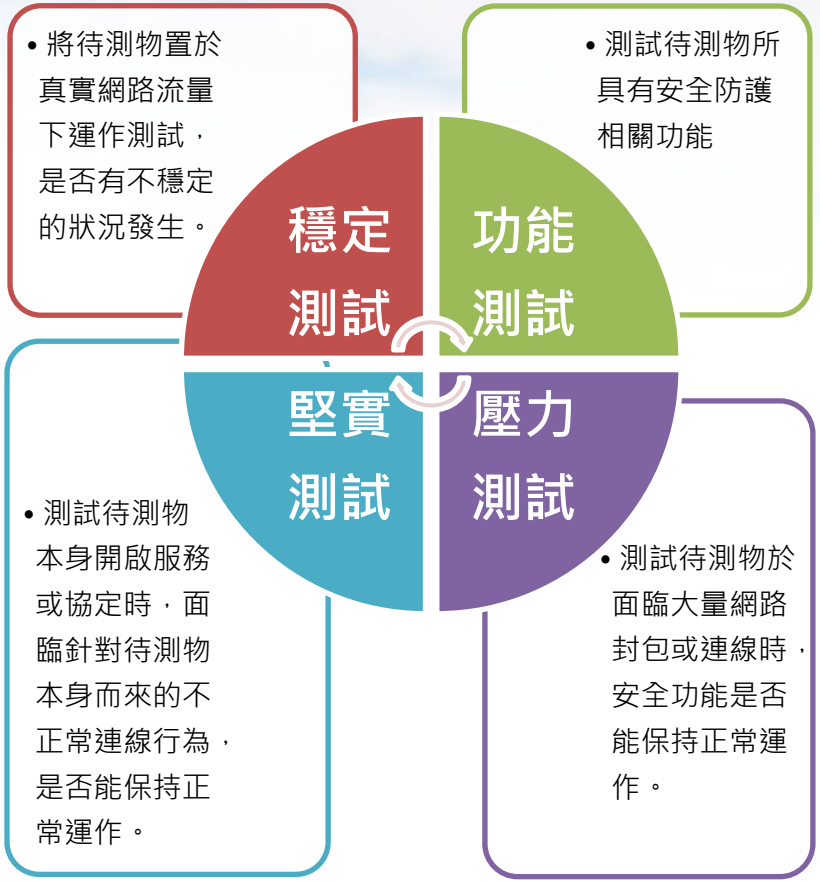
軟體測試實驗室認證

TAF Testing Laboratory 0263

中華電信 Chunghwa Telecom

❖ 軟體測試實驗室： NCC資通訊設備安全檢測

檢測標的	對應規範
網路型防火牆	NCC-IS0008-1
入侵偵測防禦系統	NCC-IS0009-1
防毒閘道設備	NCC-IS0010-0
網路型垃圾郵件過濾設備	NCC-IS0011-0
網頁應用防火牆	NCC-IS0012-0
應用軟體控管設備	NCC-IS0013-0
乙太網路交換器	NCC-IS0014-0
路由交換器	NCC-IS0015-0



檢測人力資源

CEH EC-Council 道德駭客

ECSA EC-Council 資安分析專家

CISSP ISC² 資安系統專家

CSSLP ISC² 資安軟體開發專家

CSTE CSQ 軟體測試工程師

GWAPT GIAC 資安滲透測試專家

行動應用App基本資安標章(1/2)

中華電信 Chunghwa Telecom

經濟部工業局邀集國內資安領域專家，參照國際相關資安規範，於105年2月完成「行動應用App基本資安規範」，引導行動應用App開發商研發產品導入資安概念。

- **MAS標章**：「行動應用App基本資安標章」(Mobile Application Basic Security)，將App檢測安全等級區分為三級，係表彰行動應用App檢測符合「行動應用App基本資安檢測基準」之證明。
- **認驗證合格登錄管理網站**：公開網站，登錄公告認證機構、合格檢測實驗室名單及通過檢測、授予檢測合格標章之行動應用程式。http://www.mas.org.tw/
- **檢測實驗室**：中華電信測試中心是TAF認證合格檢測實驗室，可提供行動應用APP開發者資安檢測服務之單位，並得經制度推動委員會之授權發放檢測合格證明、代為發放MAS標章。

行動應用App基本資安標章(2/2)

中華電信 Chunghwa Telecom

- **MAS 標章依「行動應用App 基本資安檢測基準」，將檢測安全等級區分為三級：**
  - 初級：檢測純功能之安全性。
  - 中級：檢測連網及認證之安全性(含初級)。
  - 高級：檢測付費資源之安全性(含中級)。

行動應用App基本資安規範

中華電信 Chunghwa Telecom

- App基本資安規範共有5大技術面向
  1. 行動應用程式發布安全

     發布 → 更新 → 回報

  2. 敏感性資料保護

     蒐集 → 利用 → 儲存 → 傳輸 → 分享 → 刪除

  3. 付費資源控管安全

     使用 → 控管

  4. 身分認證、授權與連線管理安全
  5. 行動應用程式碼安全

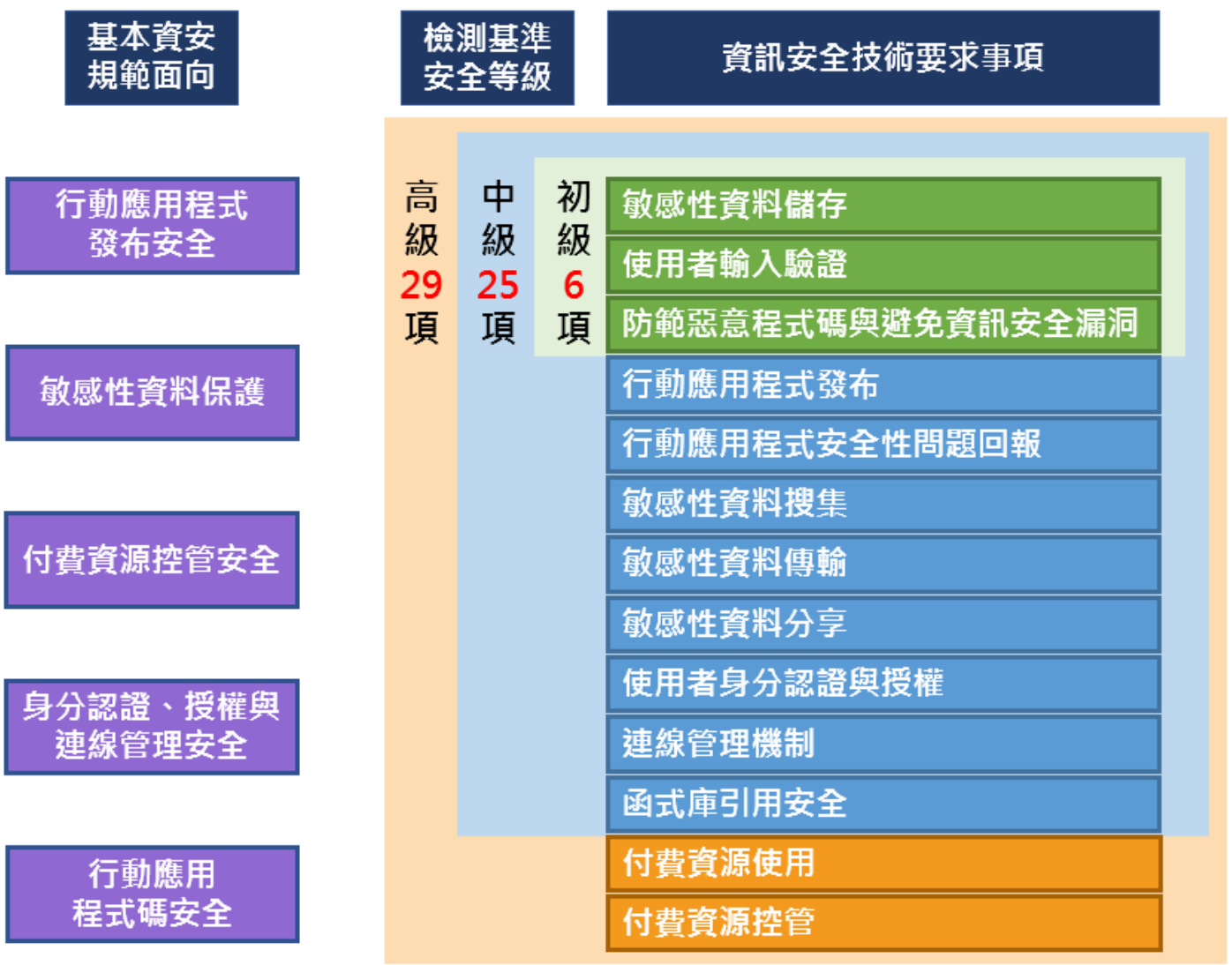
安全分類與技術要求

- **不同應用類別之行動應用程式對安全性有不同之要求，共有3種安全分類：**
  - 第一類：純功能性
  - 第二類：具認證功能與連網行為
  - 第三類：具交易功能(包含前2類)

表1　各安全分類之資訊安全技術要求事項

編號	資訊安全技術要求事項	安全分類		
		一	二	三
1	4.1.1.1.行動應用程式發布	V	V	V
2	4.1.1.2.行動應用程式更新	V	V	V
3	4.1.1.3.行動應用程式安全性問題回報	V	V	V
4	4.1.2.1.敏感性資料蒐集	V	V	V
5	4.1.2.2.敏感性資料利用	V	V	V
6	4.1.2.3.敏感性資料儲存	V	V	V
7	4.1.2.4.敏感性資料傳輸		V	V
8	4.1.2.5.敏感性資料分享	V	V	V
9	4.1.2.6.敏感性資料刪除	V	V	V
10	4.1.3.1.付費資源使用			V
11	4.1.3.2.付費資源控管			V
12	4.1.4.1.使用者身分認證與授權		V	V
13	4.1.4.2.連線管理機制		V	V
14	4.1.5.1.防範惡意程式碼與避免資訊安全漏洞	V	V	V
15	4.1.5.2.行動應用程式完整性			V
16	4.1.5.3.函式庫引用安全	V	V	V
17	4.1.5.4.使用者輸入驗證	V	V	V

檢測項目


基本資安規範面向
檢測基準安全等級
資訊安全技術要求事項
行動應用程式發布安全
敏感性資料保護
付費資源控管安全
身分認證、授權與連線管理安全
行動應用程式碼安全
高級 29 項
中級 25 項
初級 6 項
敏感性資料儲存
使用者輸入驗證
防範惡意程式碼與避免資訊安全漏洞
行動應用程式發布
行動應用程式安全性問題回報
敏感性資料搜集
敏感性資料傳輸
敏感性資料分享
使用者身分認證與授權
連線管理機制
函式庫引用安全
付費資源使用
付費資源控管

金融業者應用程式注意事項

銀行公會頒佈「金融機構辦理電子銀行業務安全控管作業基準」，規範金融機構對行動應用裝置應用程式注意項目：

1.應針對應用程式檢視系統所需最小權限，並進行存取控制。

2.於行動裝置上如有必要儲存敏感資料，應採取加密或亂碼化等相關機制保護以有效防範資料外洩。

3.應針對應用程式進行原始碼掃描、黑箱測試或滲透測試，並針對中、高風險弱點及可影響敏感資料被竊取或竄改之弱點進行改善。

4.啟動應用程式時，如偵測行動裝置疑似遭破解，應提示使用者注意風險。

5.於安裝或首次啟動應用程式時，應提示使用者於行動裝置上安裝防毒軟體。

6.採用憑證技術進行傳輸加密時，應用程式應建立可信任憑證清單並驗證完整憑證鏈及其憑證有效性。

7.採用空中傳輸（OTA）方式下載敏感資料前，應確認使用者身分（如密碼）並採用嚴密的技術防護措施，且能有效防範相關資料被竊取。

8.採用空中傳輸（OTA）方式下載敏感資料時，應確認行動裝置及應用程式之正確性，並進行端點（銀行端）對端點（應用程式）全程加密防護。

9.採用安全儲存媒介（SE）作為儲存裝置時，應確認使用者指定之安全儲存媒介編號（如SE ID）、並於 SE內增設存取控管，限制由可信任應用程式存取。

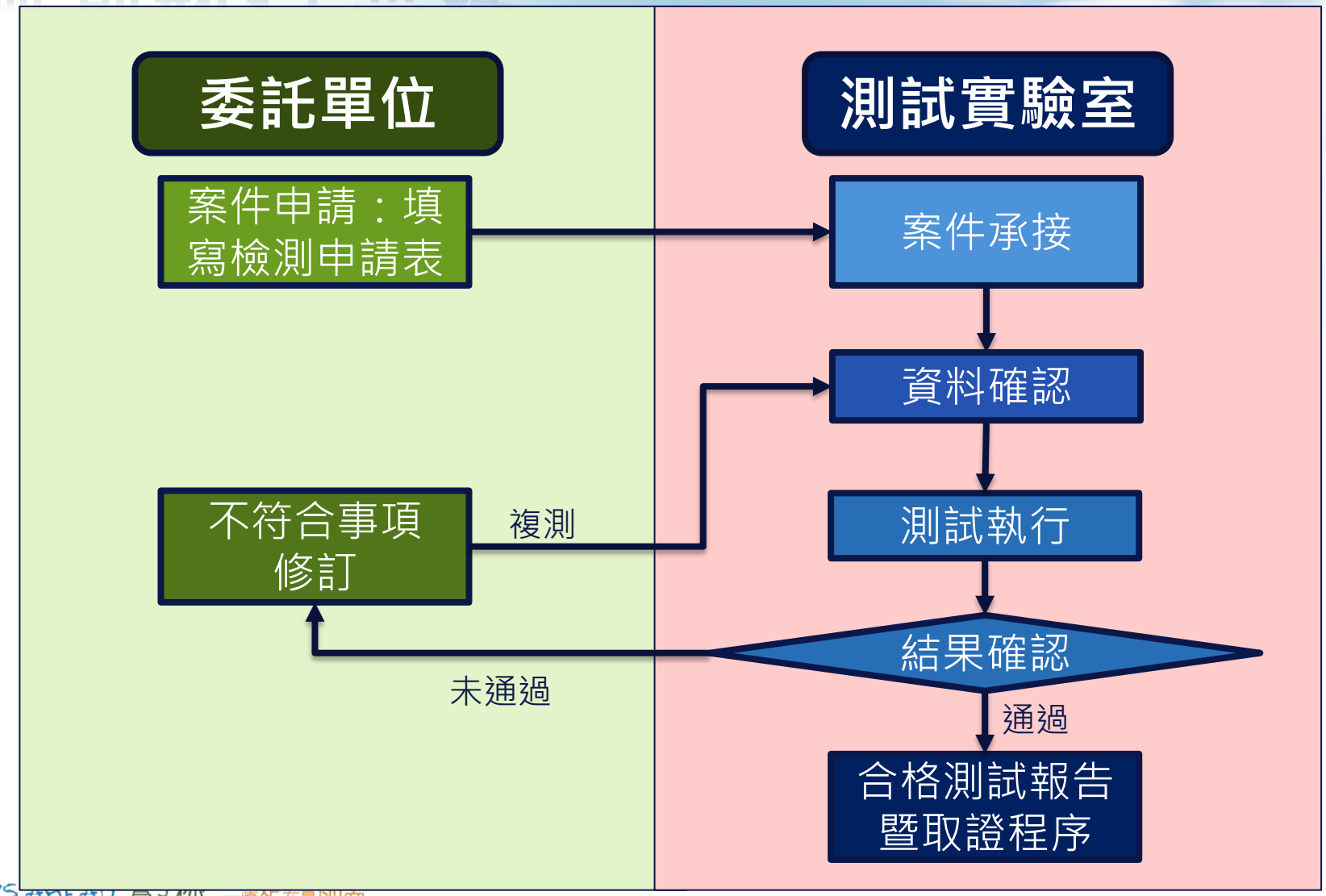
10. 採用近距離無線通訊（NFC）技術進行付款交易資料傳輸前，應經由使用者人工確認。

11. 應於官網上提供應用程式之名稱、版本與下載位置。

工業局MAS

金融機構辦理電子銀行業務安全控管作業基準

檢測執行流程


委託單位
測試實驗室
案件申請：填寫檢測申請表
案件承接
資料確認
測試執行
結果確認
不符合事項修訂
複測
未通過
通過
合格測試報告暨取證程序

檢測申請表

TAF Testing Laboratory 0263 中華電信 Chunghwa Telecom

- 填寫「行動應用程式基本資安檢測申請書」之系統資訊，可幫助申請單位了解測試項目的資訊，並縮短資訊往返，加速檢測流程。

八、本機構之基本資料如下：

機構名稱				
負責人			統一編號	
通訊地址				
聯絡人資訊	姓名		部門	
	電話		email	

九、本服務送測之行動應用 App 資料如下，「送測行動應用 App 宣告表」如附件。

App 名稱			
App 版本		作業系統	
安全分類	□第一類 □第二類 □第三類	送測級別	□初級 □中級 □高級

註 1：無連網行為且無身分認證機制為第一類；具連網行為或身分認證機制為第二類；第三類為具網路交易功能。

註 2：安全分類之第一類須送測初級(含)以上、第二類須送測中級(含)以上，第三類須送測高級之安全檢測。

機構名稱：　　負責人：

送測行動應用 App 宣告表

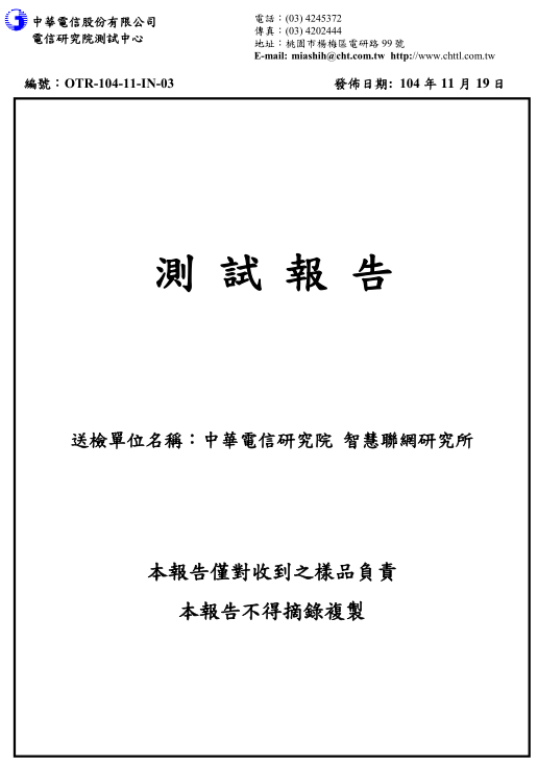
編號	項目	內容
1	程式識別名稱	(例如Android為於Google Play之Package Name)
2	App簽章憑證指紋 (MD5、SHA1、SHA256值)	MD5： SHA1： SHA256：
3	適用作業系統版本	
4	發布狀態	□已發布 □內部使用，不公開發布 □未發布，預計發布日期：民國___年___月___日
		□ 行動作業系統業者提供之行動應用程式商店： □ Apple App Store (URL)：_____

測試報告

Testing Laboratory 0263

中華電信 Chunghwa Telecom

測試報告封面



中華電信股份有限公司
電信研究院測試中心

電話：(03) 4245372
傳真：(03) 4202444
地址：桃園市楊梅區電研路 99 號
E-mail: miashih@cht.com.tw http://www.chttl.com.tw

編號：OTR-104-11-IN-03　　發佈日期：104 年 11 月 19 日

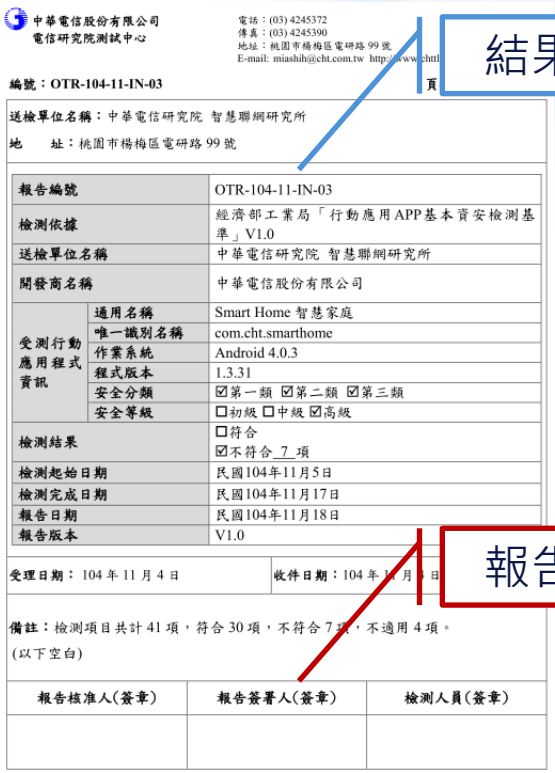
測 試 報 告

送檢單位名稱：中華電信研究院 智慧聯網研究所

本報告僅對收到之樣品負責

本報告不得摘錄複製

測試報告摘要



中華電信股份有限公司
電信研究院測試中心

電話：(03) 4245372
傳真：(03) 4245390
地址：桃園市楊梅區電研路 99 號
E-mail: miashih@cht.com.tw http://www.chttl.com.tw

編號：OTR-104-11-IN-03　　頁

送檢單位名稱：中華電信研究院 智慧聯網研究所
地　　址：桃園市楊梅區電研路 99 號

報告編號		OTR-104-11-IN-03
檢測依據		經濟部工業局「行動應用APP基本資安檢測基準」V1.0
送檢單位名稱		中華電信研究院 智慧聯網研究所
開發商名稱		中華電信股份有限公司
受測行動應用程式資訊	通用名稱	Smart Home 智慧家庭
	唯一識別名稱	com.cht.smarthome
	作業系統	Android 4.0.3
	程式版本	1.3.31
	安全分類	☑第一類 ☑第二類 ☑第三類
	安全等級	☐初級 ☐中級 ☑高級
檢測結果		☐符合 ☑不符合 7 項
檢測起始日期		民國104年11月5日
檢測完成日期		民國104年11月17日
報告日期		民國104年11月18日
報告版本		V1.0

受理日期：104 年 11 月 4 日　　收件日期：104 年 11 月 [illegible] 日

備註：檢測項目共計 41 項，符合 30 項，不符合 7 項，不適用 4 項。
(以下空白)

報告核准人(簽章)	報告簽署人(簽章)	檢測人員(簽章)

結果總表

報告簽署

測試報告結果(部分)

中華電信股份有限公司
電信研究院測試中心

電話：(03) 4245372
傳真：(03) 4245390
地址：桃園市楊梅區電研路 99 號
E-mail: miashih@cht.com.tw http://www.chttl.com.tw

編號：OTR-104-11-IN-03　　頁次：12 之 2 頁

壹、測試項目及結果

表 1 檢測結果摘要表

資訊安全技術要求面向	檢測項目	結果(符合/不符合/不適用)	備註
4.1.1.行動應用程式發布安全	4.1.1.1.1.行動應用程式應於可信任來源之行動應用程式商店發布	符合	無
	4.1.1.1.2.行動應用程式應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途	符合	無
	4.1.1.2.1.行動應用程式應於可信任來源之行動應用程式商店發布更新	符合	無
	4.1.1.2.2.行動應用程式應提供更新機制	符合	無
	4.1.1.2.3.行動應用程式應於安全性更新時主動公告	符合	無
	4.1.1.3.1.行動應用程式開發者應提供回報安全性問題之管道	符合	無
	4.1.1.3.2.行動應用程式開發者應於適當之期間內回覆問題並改善	符合	無
4.1.2.敏感性資料保護	4.1.2.1.1.行動應用程式應於蒐集敏感性資料前，取得使用者同意	符合	無
	4.1.2.1.2.行動應用程式應提供使用者拒絕蒐集敏感性資料之權利	符合	無
	4.1.2.2.1.行動應用程式應於使用敏感性資料前，取得使用者同意	符合	無
	4.1.2.2.2.行動應用程式應提供使用者拒絕使用敏感性資料之權利	符合	無

檢測結果摘要表

檢測時程與費用

安全等級	時程	費用
初級	檢測約須進行2~4工作天，視系統複雜度而定	依據送測系統複雜度與安全等級收費
中級	檢測約須進行4~7工作天，視系統複雜度而定	
高級	檢測約須進行6~10工作天，視系統複雜度而定	

聯絡窗口

- 姓名：施任峯
- Email：jfshih@cht.com.tw
- 電話：03-424-4335

- 姓名：林皇甫
- Email：hflin@cht.com.tw
- 電話：03-424-5458

參考資料

- 「行動應用App基本資安規範」V1.1
  - https://www.mas.org.tw/spaw2/uploads/images/01_1.pdf
- 「行動應用App基本資安檢測基準」V2.1
  - https://www.mas.org.tw/spaw2/uploads/images/02_1.pdf
- 「行動應用App基本資安自主檢測推動制度」V2.0
  - https://www.mas.org.tw/spaw2/uploads/images/03_1.pdf

TAF
Testing Laboratory
0263

中華電信
Chunghwa Telecom

Q&A

Thanks for your attention.

Refresh your life