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 測試中心

2016年08月11日

Refresh your life

大綱

TAF Testing Laboratory 0263

中華電信 Chunghwa Telecom

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

中華電信研究院測試中心(1/2)

- 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。
- 其中測試中心是專業測試實驗室，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，同時也是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/

NCC BSMI

中華電信研究院測試中心(2/2)

- 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

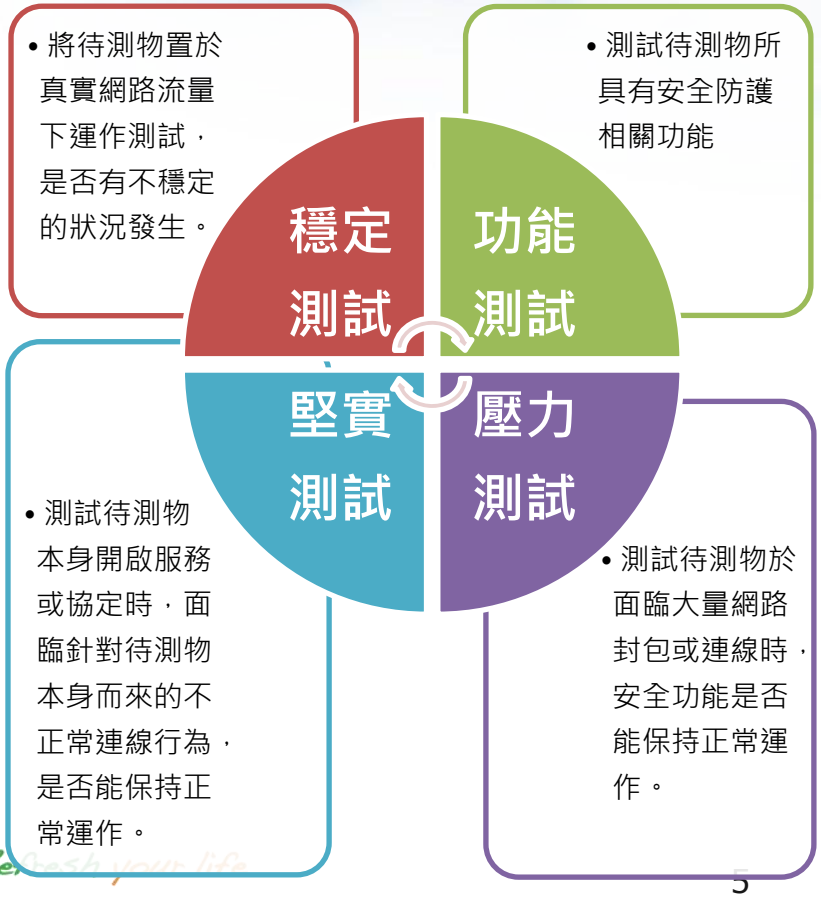
中華電信 Chunghwa Telecom

TAF Testing Laboratory 0263

❖ 軟體測試實驗室：

- 本實驗室通過TAF認證 ISO/IEC 17025，NCC、BSMI認證通過實驗室，同時也取得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

TAF Testing Laboratory 0263
中華電信 Chunghwa Telecom

CEH EC-Council
Certificated Ethical Hacker
道德駭客認證，具備資安攻防的技術能力

CISSP ISC²
Certified Information Systems Security Professional
資安系統專家認證，ISC2所認證之全方位資訊安全專家，精通包含風險管理、資產安全與網路安全等八大領域

CSSLP ISC²
Certified Secure Software Lifecycle Professional
資安軟體開發專家認證，特別針對安全軟體開發流程之認證，對高安全等級的軟體開發流程具高度了解

CSTE CSQ
Certified Software Test Engineer
軟體測試工程師，精通軟體品質驗證之技術與程序

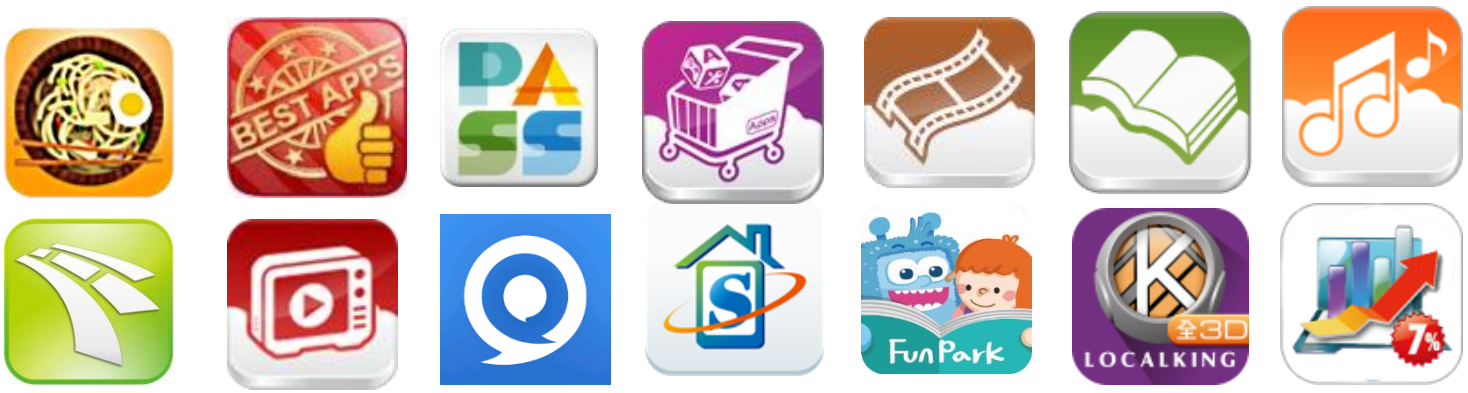
GWAPT GIAC
GIAC Web Application Penetration Tester
資安滲透測試專家，精通網頁應用系統之滲透測試技術與方法

檢測實績-案件說明

TAF Testing Laboratory 0263 中華電信 Chunghwa Telecom

- **每年執行超過30件行動應用APP資安測試案**
  - 包含公司及合作廠商重要行動應用APP
  - 以104年1至10月執行之案件為例，列舉如下：

HAMI 飲食男女	HAMIPASS	HAMI 軟體商店
生活秘書	路況快易通	HTV短片
QMI 企業即時通	基隆環保局清運車	中華影視
SmartHome 智慧家庭	導航王	QR扣款



行動應用App基本資安標章(1/2)

- **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)

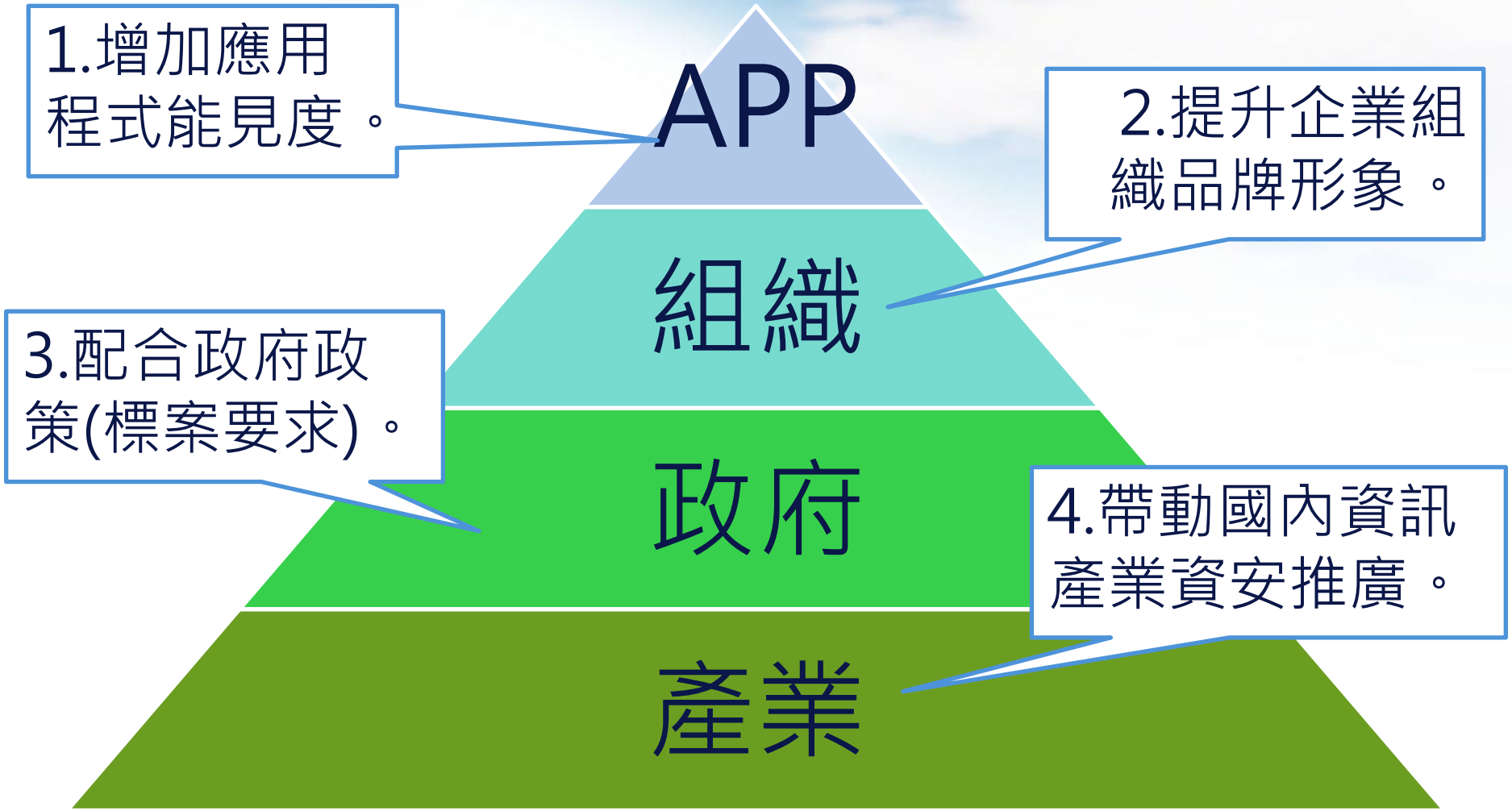
中華電信 Chunghwa Telecom

- **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)。

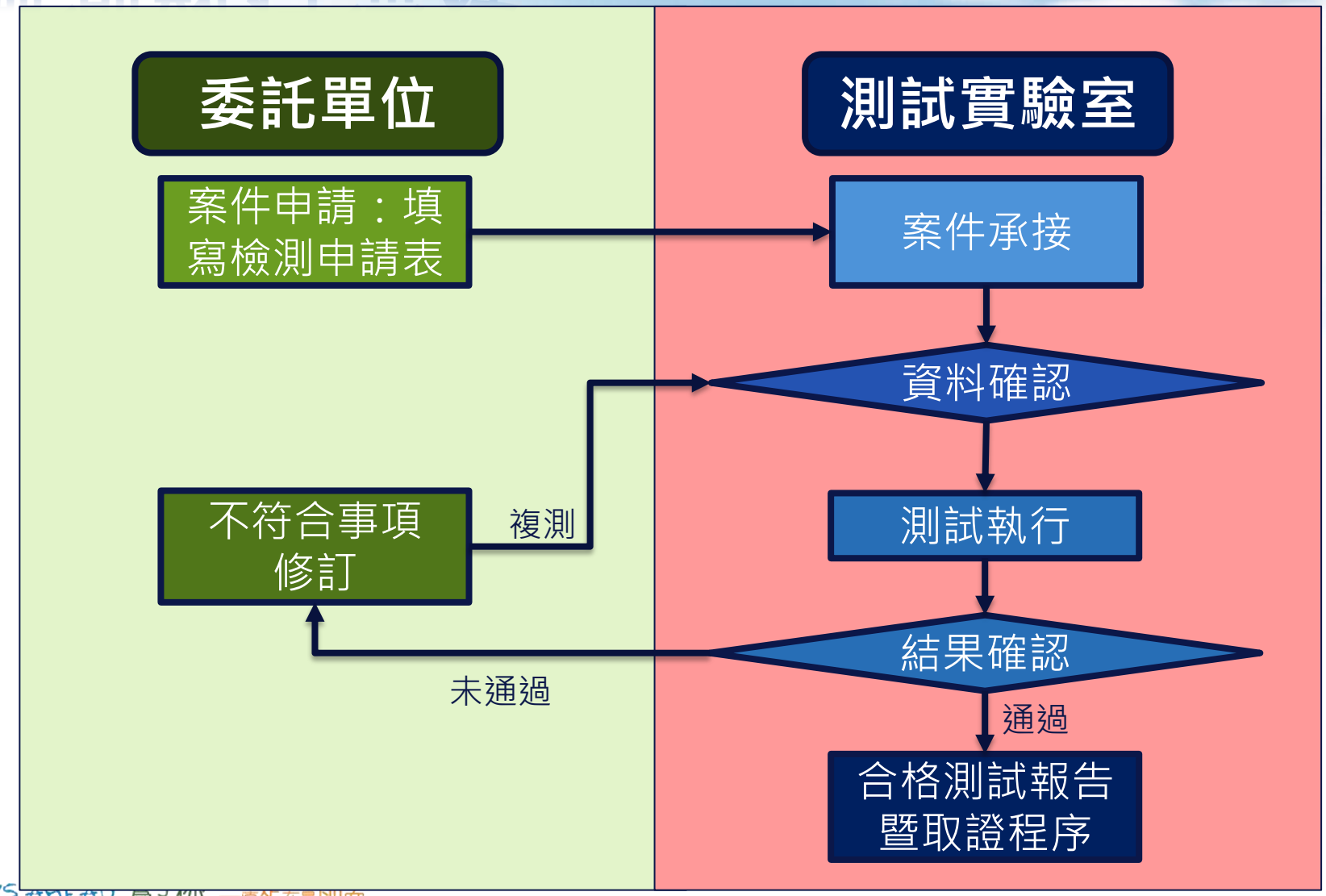
檢測項目

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	高級29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
敏感性資料保護	中級25項	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
付費資源控管安全		使用者身分認證與授權
		連線管理機制
身分認證、授權與連線管理安全	初級6項	函式庫引用安全
		付費資源使用
行動應用程式碼安全		付費資源控管

取得標章之效益


1.增加應用程式能見度。
APP
2.提升企業組織品牌形象。
組織
3.配合政府政策(標案要求)。
政府
4.帶動國內資訊產業資安推廣。
產業

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
通過
合格測試報告暨取證程序
不符合事項修訂
複測
未通過

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

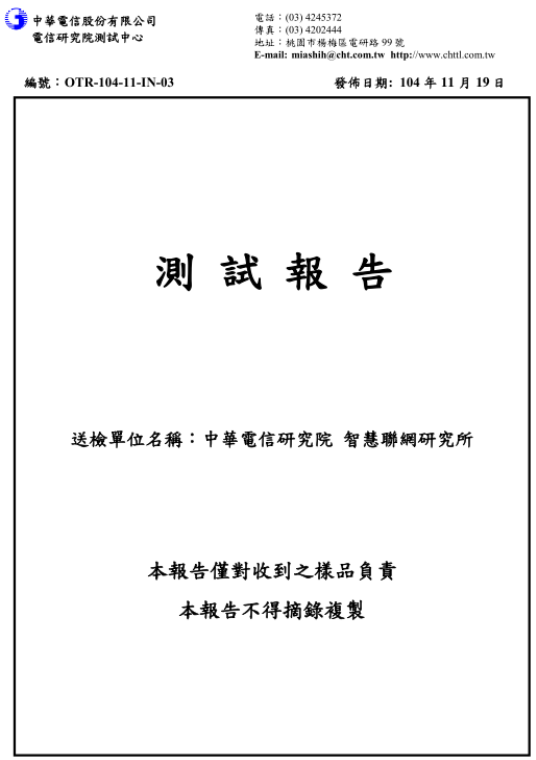
TAF Testing Laboratory 0263

中華電信 Chunghwa Telecom

測試報告封面

測試報告摘要

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) 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

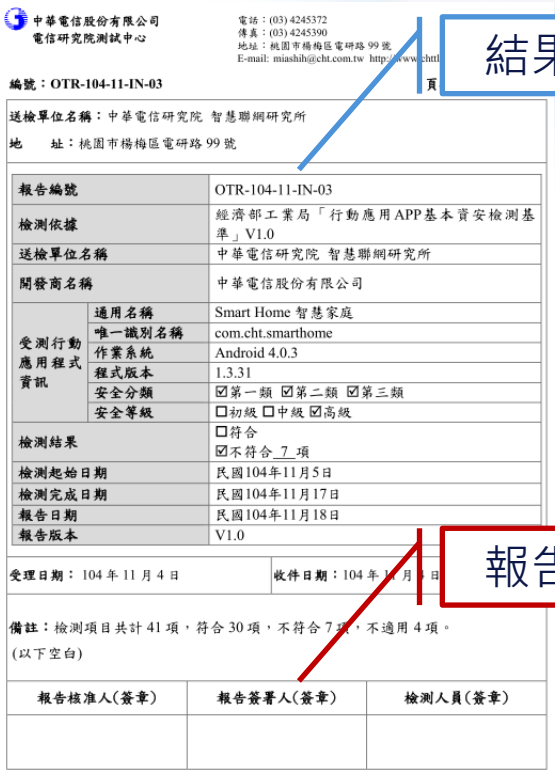
編號：OTR-104-11-IN-03　　發佈日期：104 年 11 月 19 日

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



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

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

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

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：林玉嬌
- Email：tlz70105@cht.com.tw
- 電話：03-424-5771

參考資料

- 行動應用APP基本資安檢測基準及自主檢測推動制度修訂版公告
  - http://www.mas.org.tw/news_detail.php?id=11
- 「行動應用App基本資安檢測基準」V2.0
  - http://www.mas.org.tw/spaw2/uploads/files/1050219-1.pdf
- 「行動應用App基本資安自主檢測推動制度」V2.0
  - http://www.mas.org.tw/spaw2/uploads/files/1050219-2.pdf

TAF
Testing Laboratory
0263

中華電信
Chunghwa Telecom

Q&A

Thanks for your attention.

Refresh your life