資安產業跨域聯防推動計畫-
資安募資輔導與資安認驗證機制推動

行動應用App基本資安檢測實驗室

檢測技術一致性會議

中華民國 115年 6月 17日


moda
數位發展部
Ministry of Digital Affairs
性別主流化與性別平權
重視性別意識　消除性別歧視
性別主流化
1.根據聯合國經濟暨社會理事會(ECOSOC)定義，「性別主流化」強調於各領域政治、經濟與社會層面政策與方案中，融入性別觀點降低不平等現象。
2.終極目標是達成性別的實質平等，即性別平權。
性別平權
1.消除社會中對婦女及性別一切形式的歧視
2.使社會大眾檢視生活週遭的性別不平等情況
3.促進女性參與決策，落實任一性別不少於三分之一，縮小性平差距。
4.建立尊重多元性別的態度及平等相處的互動
家庭暴力零容忍
1.被害人可撥打110或113保護專線
2.依需要就近向當地社政、警政、醫療衛生單位求助
3.可透過家暴庇護安置方案，接受緊急庇護或中長期安置服務。
性騷擾防治
1.防治性騷擾之政策宣示
2.舉辦性騷擾防治教育訓練
3.建立內部性騷擾申訴系統
性別平等相關政策與法規
國外
消除對婦女一切形式歧視公約(CEDAW)
國內
※消除對婦女一切形式歧視公約施行法
※性別平等政策綱領
※性別教育平等法
※性別工作平等法
※性騷擾防治法
關懷e起來
家暴案件線上通報
113線上諮詢
https://ecare.mohw.gov.tw
什麼是「性騷擾」
違反他人意願而向他實施與性或性別有關之行為，若造成對方的嫌惡，不當影響他的正常生活進行的，都算是「性騷擾」。
如有性別相關問題，可查詢行政院性別平等處網址http://www.gec.ey.gov.tw
moda
數位發展部
Ministry of Digital Affairs


性別主流化
與性別平權
重視性別意識 消除性別歧視
性別主流化
看見性別差異，正視弱勢性別的需要，拒絕「性別盲」。「性別主流化」強調於各領域皆融入性平觀點，彌平差異、滿足需要，以達成性別的實質平等為終極目標。
性別平權
消除社會中對婦女及性別一切形式的歧視。
促使大眾檢視生活週遭的性別不平等情況。
落實任一性別不少於三分之一之政策規定，不因性別影響升遷，僱用身心障礙及原住民等，促進多元及共榮之決策參與。
建立尊重多元性別的態度及平等相處的互動。
性別暴力零容忍暨性騷擾防治
親密關係受暴者可撥打110或113保護專線。
呼籲重視防治數位/網路性別暴力之情形。
關注弱勢性別、身心障礙者、兒童及少年、高齡者及不利處境者免受歧視及受暴之處遇。
防治性騷擾之政策宣示。
舉辦性騷擾防治教育訓練。
建立職場性騷擾及反霸凌申訴系統。
女性夜間工作安全措施 (交通或住宿安排)。
宣導對網路或數位性別暴力之認識與反霸凌措施。
性別平等相關政策與法規
國外
消除對婦女一切形式歧視公約 (CEDAW) 及兩公約
國內
※消除對婦女一切形式歧視公約施行法
※性別平等政策綱領
※性別平等工作法
※性騷擾防治法
※跟蹤騷擾防治法
※刑法
※兒童及少年性剝削防制條例
※性侵害犯罪防治法
※犯罪被害人權益保障法
關懷e起來
家暴案件線上通報
113線上諮詢
https://ecare.mohw.gov.tw
杜絕職場上的#MeToo
什麼是「性騷擾」?
違反他人意願而向他人實施與性或性別有關之行為，若造成對方的嫌惡，不當影響其正常生活進行的，都算是「性騷擾」。
moda
數位發展部
Ministry of Digital Affairs
產業發展署性別主流化專區
掃描QRcode了解更多資訊
網址 https://pse.is/5axvx4
如有性別相關問題
可查詢行政院性別平等處
網址 https://gec.ey.gov.tw/

數位發展部 數位產業署

蒐集個人資料告知事項暨個人資料提供同意書

- 數位發展部 數位產業署 委託計畫執行單位-台北市電腦商業同業公會辦理資安產業跨域聯防推動計畫(以下簡稱本計畫)，因應個人資料保護法及相關個人資料保護規定，在向您蒐集個人資料之前，依法向您告知下列事項，當您勾選「我同意」，表示您已閱讀、瞭解並同意接受本同意書之所有內容：
- 一、蒐集目的及類別
  為本計畫相關 報名作業管理、通知聯繫、活動訊息發布、問卷調查、相關統計分析之蒐集目的，而須獲取您下列個人資料類別：姓名、電話、E-mail、公司、職稱。
- 二、個人資料利用之期間、地區、對象及方式
  您的個人資料，除涉及國際業務或活動外，將提供本機關(構)於中華民國領域，於上述蒐集目的之必要合理範圍內加以利用至前述蒐集目的消失為止。
- 三、當事人權利行使
  依據個人資料保護法第3條，您可向計畫執行單位請求查詢或閱覽、製給複製本、補充或更正、停止蒐集/處理/利用或刪除您的個人資料。
- 四、不提供個人資料之權益影響
  如您不提供或未提供正確之個人資料，或要求停止蒐集/處理/利用/刪除個人資料、服務訊息的取消訂閱，本機關(構)將無法為您提供蒐集目的之相關服務。
- 五、各項通知服務、相關訊息之停止寄送
- 您可於上班時間聯繫計畫執行單位活動承辦人（電話(02)2570-2300，分機：9889）。

個人資料同意提供：

- 一、本人確已閱讀並瞭解上述告知事項，「同意」授權本機關(構)於所列目的之必要合理範圍內，蒐集、處理及利用本人之個人資料。
- 二、本人瞭解此同意書符合個人資料保護法及相關法規之要求，並同意提供予貴機關(構)留存及日後查證使用。

檢測技術一致性會議 議程

時間	內容	主講
13:00~13:10	開場致詞	行動應用資安聯盟 陳俊良 會長
13:10~13:20	行動應用資安聯盟推動現況說明	行動應用資安聯盟 秘書組
13:20~13:50	審案分享： 提升送審案件品質與技術一致性探討	行動應用資安聯盟 技術專家
13:50~16:00	技術議題討論與決議	行動應用資安聯盟 技術專家及實驗室代表
16:00~16:20	臨時動議	行動應用資安聯盟 秘書組
16:20~16:30	結論	行動應用資安聯盟 陳俊良 會長

行動應用App基本資安檢測實驗室

檢測技術一致性會議

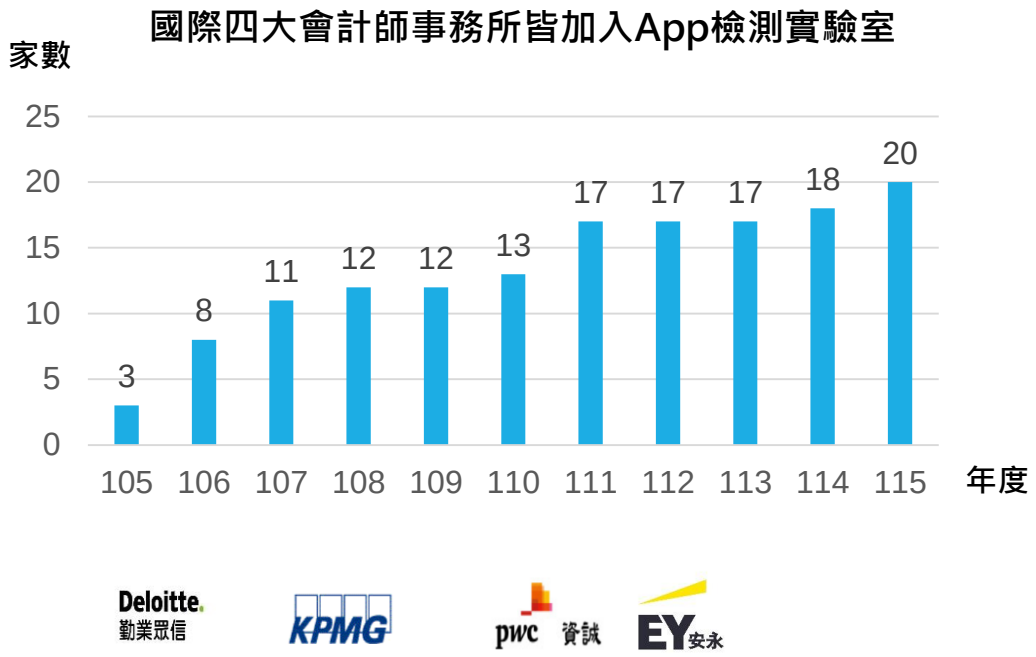
行動應用資安聯盟推動現況說明

行動應用App資安檢測實驗室

序號	資安檢測實驗室單位名稱
1	鑒真數位有限公司
2	**勤業眾信聯合會計師事務所**
3	中華電信(股)公司電信研究院
4	安華聯網科技(股)公司
5	行動檢測服務(股)公司
6	財團法人台灣商品檢測驗證中心
7	安碁資訊(股)公司
8	**安侯企業管理(股)公司**
9	#財團法人電信技術中心
10	數聯資安(股)公司
11	關貿網路(股)公司
12	**資誠企業管理顧問(股)公司**
13	光盾資訊科技(股)公司
14	#國家中山科學研究院
15	**安永諮詢服務(股)公司**
16	三甲科技(股)公司
17	耀睿科技(股)公司
18	#新北市政府資訊中心
19	全速科技有限公司 NEW
20	漢昕科技(股)有限公司 NEW

備註：依加入聯盟排序； “#” 不收民間單位案件

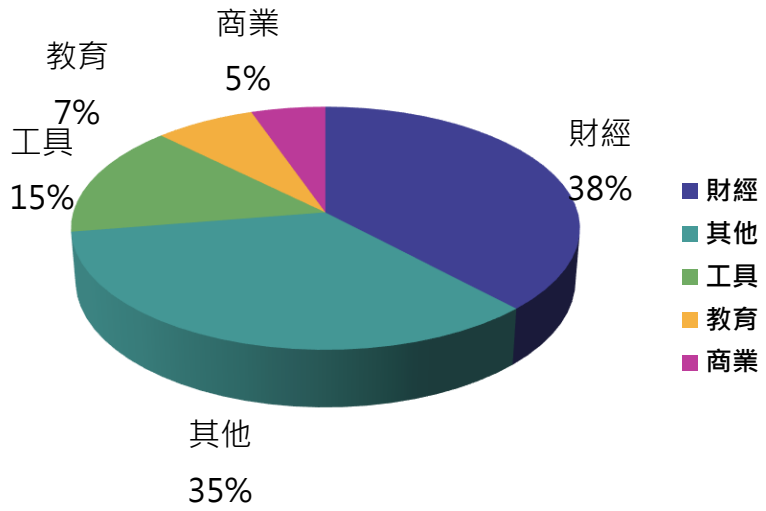
■ 截至115年5月31日，App資安檢測實驗室計20家



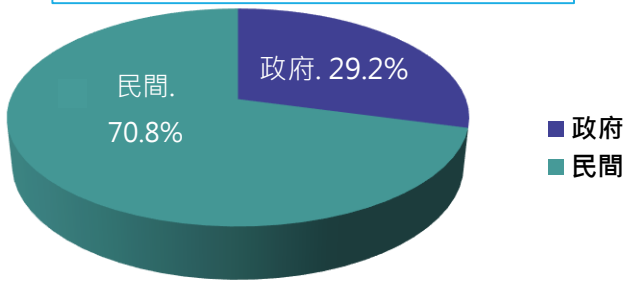
■ 國家資通安全研究院，以一般團體會員身份於115年5月25日申請加入聯盟

App資安標章整體概況_114年度

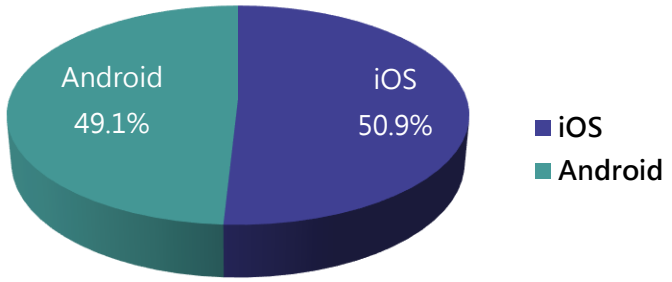
- 114年度行動應用App基本資安檢測基準App收件通過1,213件（政府354件、民間859件）。較113年同期（1,507件）負成長19.5%，政府成長率3.2%（113年同期政府343件）、民間負成長26.2%（113年同期民間1,164件）。
- 5大類分別為：財經461件、其他418件、工具181件、教育88件、商業65件



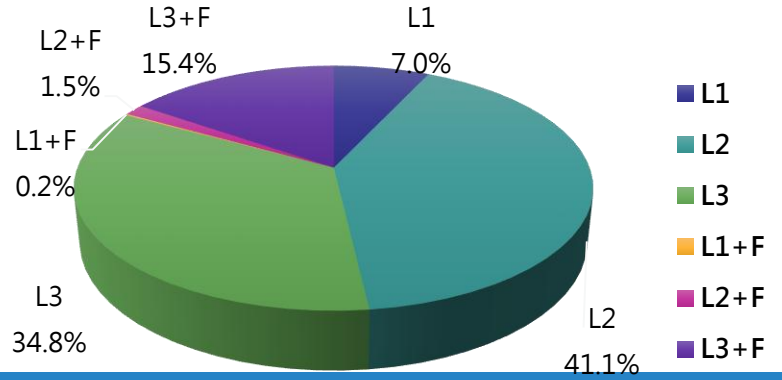
政府354件、民間859件



App作業系統：iOS 617件、Android：596件

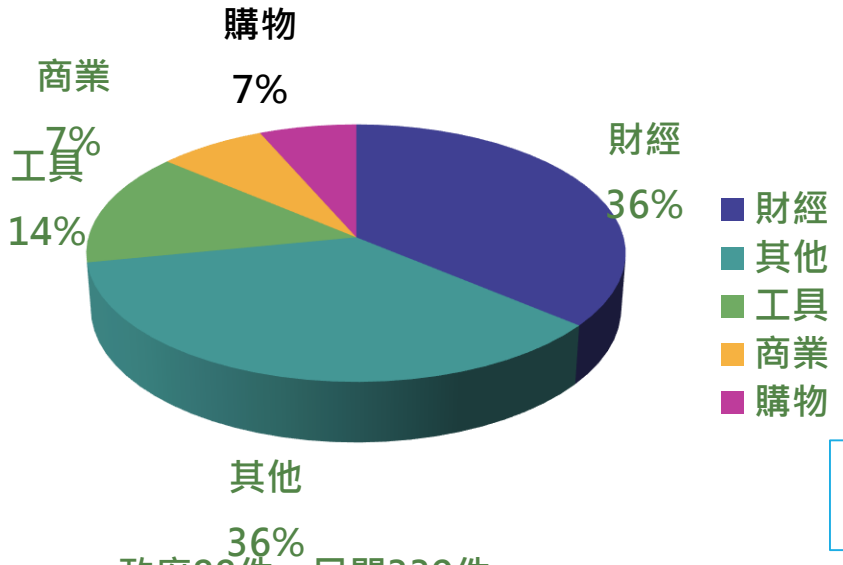


App安全類別： L1共85件、L2共499件、L3共422件
L1+F共2件、L2+F共18件、L3+F共187件

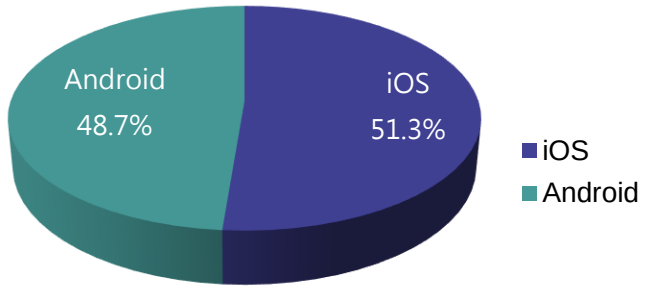


App資安標章整體概況_115年度

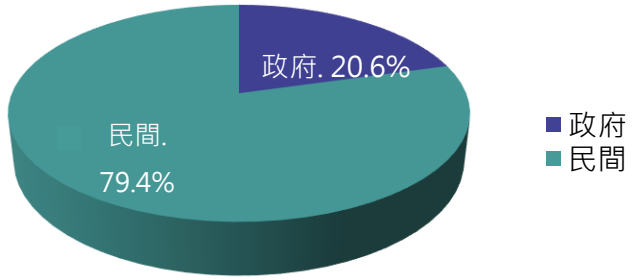
- 截至115/5/31，115年度行動應用App基本資安檢測基準App收件通過427件（政府88件、民間339件）。較114年同期（249件）成長71.5%，政府成長23.9%（114同期政府71件）、民間成長90.5%（114年同期民間178件）。
- 5大類分別為：財經154件、其他153件、工具61件、商業31件、購物28件



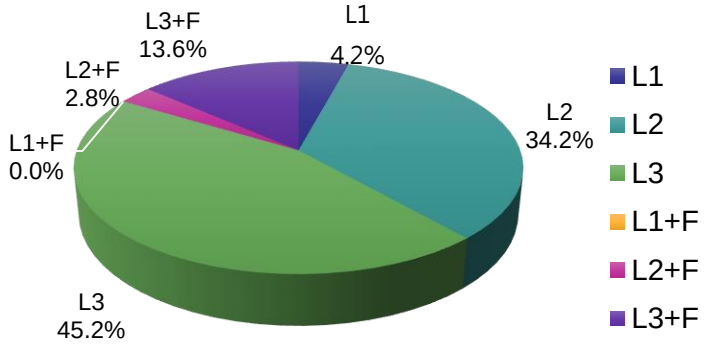
App作業系統：iOS 219件、Android：208件



政府88件、民間339件



App安全類別： L1共18件、L2共146件、L3共193件
L1+F共0件、L2+F共12件、L3+F共58件



檢測技術一致性會議

序號	檢測實驗室	提案數	調查表意見與格式
1	鑒真數位有限公司	1案	提交
2	安華聯網科技(股)公司	1案	提交
3	安碁資訊(股)公司	1案	提交
4	漢昕科技(股)公司	1案	
5	中華電信(股)公司電信研究院	3案	
6	(財)台灣商品檢測驗證中心	1案	提交
7	全速科技有限公司		提交
8	勤業眾信聯合會計師事務所		提交
9	關貿網路(股)公司		提交
10	光盾資訊科技有限公司		提交
11	新北市政府資訊中心		
12	安侯企業管理(股)公司		
13	三甲科技(股)公司		
14	數聯資安(股)公司		
15	中科院資訊安全中心		
16	資誠企業管理顧問(股)公司		
17	安永諮詢服務(股)公司		
18	耀睿科技(股)公司		
19	行動檢測服務(股)公司		
20	(財)電信技術中心		

檢測技術一致性會議，於6/17(三) B102會議室召開，重點說明如下：

■ **出席人數：**

- 實驗室：實體19位；線上45位（共 64位）
- 團體會員：實體-資安院（共2位）

■ **提案數：**共8案

■ **調查表意見與格式：** 共8案

114 年度行動應用 App 優良檢測實驗室名單

評核背景與機制

行動應用資安聯盟為鼓勵實驗室積極參與各項活動、持續精進檢測品質並確保標準一致性，依據「行動應用 App 基本資安檢測實驗室績效評核辦法」，每年定期辦理評核作業，已於MAS官網公告 114 年度評核結果，並函知相關機關團體。

30%
無條件捨去

擇優篩選機制

依評核計點機制，擇優選取前 30% 之優良檢測實驗室（共計 5 家），提供各界辦理檢測需求時優先參考。

20家
檢測實驗室

認證合格名錄

目前累計有 20 家實驗室經 TAF 認可，符合行動應用資安聯盟「行動應用 App 基本資安自主檢測推動制度v4.3」。

- 中華電信(股)公司電信研究院 - 測試中心 — 筆劃首位
- 光盾資訊科技有限公司 - 光盾資訊檢測實驗室 — 推薦優良
- 安華聯網科技(股)公司 - 資安檢測實驗室 — 推薦優良
- 安碁資訊(股)公司 - 數位鑑識中心實驗室 — 推薦優良
- 鑒真數位有限公司 - 鑒真數位鑑識實驗室 — 推薦優良

於115年2月9日公告，5月26日修訂

規劃中

辦理資安培力線上課程(App開發安全主題)
促進業者提升App開發資安意識

線上課程規劃內容

- 深化 《 行動應用 App 基本資安自主檢測V4.3 》 防護意識
- 全面對接《App 基本資安規範 V1.5》核心精神
- 嚴格依循《App 基本資安檢測基準 V4.0》技術指標
- 將「Security by Design」植入安全軟體開發生命週期SSDLC
- 規劃以實務案例引導開發廠商落實合規

推廣上架平台

中小企業網路大學校
經濟部中小及新創企業署

行動應用資安聯盟
mas.org.tw 官方平台

ACW 網站
資安產業跨域聯防推動計畫

預期效益：將資安防護思維深植於開發設計階段，有效擴散資安標章的重要性及專業性，塑造產業資安自主檢測形象，邁向「開發即合規」的新里程碑。

成果推廣：為延伸上述效益並持續強化產業資安防護，將建置線上課程之影音與圖文成果紀錄，透過數位媒體之傳播與推廣，全面深化企業資安意識。

規劃中

推動項目｜MAS 資安標章版本異動監管系統

問題背景：行動應用 App 版本更新頻繁，既有「單次靜態審驗」模式已難以即時因應動態多變之資安威脅與供應鏈風險

1 雙平台數據自動化勾稽

建立 iOS/Android MAS 標章名單清冊，每月執行自動化比對，產出版本差異資料庫

2 合規標章追蹤主動通知機制

版本不一致者列入監管，主動通知標章持有者及實驗室送測；廣告不實案件限期改善

3 優化標章通報機制

設立聯盟信箱通報窗口，建立被通報清冊，主動諮詢合規說明；跨部會通報政府機關

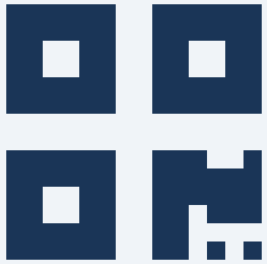
4 數位防偽與滾動式更新

新核發證書嵌入 QR Code，即時比對最新合規狀態，呈現「有效」、「警示」、「App 未公開」及「查詢中」等判定

規劃中

數位防偽機制｜QR Code 動態查核與合規狀態判定(1/2)

MAS 資安標章證書



掃描 QR Code

實體證書
全面導入防偽機制

+

系統即時比對

- ✓ App 最新驗證狀態
- ✓ iOS 商城版本
- ✓ Android 商城版本
- ✓ 證書效期
- ✓ 版本一致性

+

【證書有效】✓

證書效期內
且 App 未改版

雙平台版本 = 驗證版本
安全合規

【證書警示】✗

杜絕舊證冒用
或更版長期未測

預期效益：即時確認驗證 App 版本是否與雙平台上架版本一致，確保標章時效性與真實性。

規劃中

數位防偽機制｜QR Code 動態查核與合規狀態判定 (2/2)

MAS 資安標章證書

掃描 QR Code

實體證書
全面導入防偽機制

系統即時比對

- ✓ App 最新驗證狀態
- ✓ iOS 商城版本
- ✓ Android 商城版本
- ✓ 證書效期
- ✓ 版本一致性

【App未公開】✓

證書效期內
且 App 僅供內部使用，不公開發布

【查詢中】▲

本月新通過尚未勾稽

商城查詢不到指定 App

預期效益：即時確認驗證 App 版本是否與雙平台上架版本一致，確保標章時效性與真實性。

數位防偽機制｜證書QR Code狀態顯示總覽

勾稽說明	顯示狀態	觸發條件摘要
一致	證書有效	商城名稱及商城版本 一致 【商城名稱 = 證書名稱，且商城版本 = 證書版本(二者須相符】
不一致	證書警示	1.商城名稱或商城版本不一致 【商城名稱 ≠ 證書名稱或 商城版本 ≠ 證書版本（任一不符即觸發）】 2.效期內已改版或已逾效期
App 未公開	App 僅供內部使用，不公開發布	
查詢中		1.本月新通過尚未於商城比對 2.商城查詢不到指定 App

預期效益：即時確認驗證 App 版本是否與雙平台上架版本一致，確保標章時效性與真實性。

規劃中

數位防偽機制｜QR Code 動態查核與合規狀態判定

證書QR Code 範例

MAS-0263-11500011

行動應用App基本資安
檢測合格證明

茲證明下述行動應用程式（App）符合數位發展部數位產業署公告之「行動應用App基本資安檢測基準」要求，特頒此證明。

單位名稱　：臺中市政府環境保護局
App名稱　：臺中垃圾清運大車隊
App版本　：v2.96(Android)
基準版本　：v4.0
安全類別　：「L1」：無需使用者身分鑑別之應用程式。
證書效期　：民國116年5月27日
檢測實驗室署名：中華電信股份有限公司電信研究院測試中心

其他記載事項　：

掃描QRCode驗證證書即時狀態

本證書效力僅及於上述App與版本

行動應用資安聯盟
Mobile Application Security Alliance

臺中垃圾清運大車隊
MAS-0263-11500011

證書有效

App 版本與商城一致，本證書目前有效。

檢測合格證明資訊	
證書編號	MAS-0263-11500011
證書效期	民國116年5月27日
受測單位名稱	臺中市政府環境保護局

應用程式資訊	
App 名稱	臺中垃圾清運大車隊
作業系統	Android
App 版本	v2.96
App 安全類別	L1
檢測基準版本	v4.0
檢測實驗室	中華電信股份有限公司電信研究院 / 測試中心

版本驗證資訊	
商店版本	2.96
版本比對結果	一致

© 台北市電腦商業同業公會 Taipei Computer Association

規劃中

數位防偽機制｜QR Code 動態查核與合規狀態判定

證書QR Code 範例

MAS-3334-11400007

行動應用App基本資安
檢測合格證明

茲證明下述行動應用程式（App）符合數位發展部數位產業署公告之「行動應用App基本資安檢測基準」要求，特頒此證明。

單位名稱　：雲林縣政府教育處
App名稱　：雲林智慧校園親師生平台
App版本　：v1.01.210(iOS)
基準版本　：v4.0
安全類別　：「L2」：需使用者身分鑑別之應用。
證書效期　：民國115年6月9日

檢測實驗室署名：安碁資訊股份有限公司 數位鑑識中心實驗室

其他記載事項　：

掃描QRCode 驗證證書即時狀態

本證書效力僅及於上述App與版本

行動應用資安聯盟
Mobile Application Security Alliance

雲林智慧校園親師生平台
MAS-3334-11400007

證書警示

已逾效期

檢測合格證明資訊	
證書編號	MAS-3334-11400007
證書效期	民國115年6月9日
受測單位名稱	雲林縣政府教育處

應用程式資訊	
App 名稱	雲林智慧校園親師生平台
作業系統	iOS
App 版本	v1.01.210
App 安全類別	L2
檢測基準版本	v4.0
檢測實驗室	安碁資訊股份有限公司 / 數位鑑識中心實驗室

版本驗證資訊	
商店版本	1.01.241
版本比對結果	商店版本較高

© 台北市電腦商業同業公會 Taipei Computer Association

規劃中

數位防偽機制｜QR Code 動態查核與合規狀態判定

證書QR Code 範例

MAS-0263-11400020

行動應用App基本資安
檢測合格證明

茲證明下述行動應用程式（App）符合數位發展部數位產業署公告之「行動應用App基本資安檢測基準」要求，特頒此證明。

單位名稱	：	台塑石化股份有限公司(油品部汽柴油營業處)
App名稱	：	台塑石油商務卡
App版本	：	v1.6.8(iOS)
基準版本	：	v4.0
安全類別	：	「L2」：需使用者身分鑑別之應用。
證書效期	：	民國115年8月19日
檢測實驗室署名	：	**中華電信股份有限公司電信研究院測試中心**

其他記載事項 ：

掃描QRCode
驗證證書即時狀態

本證書效力僅及於上述App與版本

行動應用資安聯盟
Mobile Application Security Alliance

台塑石油商務卡
MAS-0263-11400020

證書警示

效期內已改版

檢測合格證明資訊	
證書編號	MAS-0263-11400020
證書效期	民國115年8月19日
受測單位名稱	台塑石化股份有限公司(油品部汽柴油營業處)

應用程式資訊	
App 名稱	台塑石油商務卡
作業系統	iOS
App 版本	v1.6.8
App 安全類別	L2
檢測基準版本	v4.0
檢測實驗室	中華電信股份有限公司電信研究院 / 測試中心

版本驗證資訊	
商店版本	1.7.6
版本比對結果	商店版本較高

© 台北市電腦商業同業公會 Taipei Computer Association

數位防偽機制｜QR Code 動態查核與合規狀態判定

證書QR Code 範例

MAS-3302-11500036

行動應用App基本資安
檢測合格證明

茲證明下述行動應用程式（App）符合數位發展部數位產業署公告之「行動應用App基本資安檢測基準」要求，特頒此證明。

單位名稱　：桃園市政府智慧城鄉發展委員會
App名稱　：桃園市政府公務雲
App版本　：v1.5.5(Android)
基準版本　：v4.0
安全類別　：「L2」：需使用者身分鑑別之應用。
證書效期　：民國116年5月22日

檢測實驗室署名：行動檢測服務股份有限公司
智能物聯網資安檢測實驗室

其他記載事項　：

掃描QRCode
驗證證書即時狀態

本證書效力僅及於上述App與版本

規劃中

數位防偽機制｜QR Code 動態查核與合規狀態判定

證書QR Code 範例

MAS-3334-11500032

行動應用App基本資安
檢測合格證明

茲證明下述行動應用程式（App）符合數位發展部數位產業署公告之「行動應用App基本資安檢測基準」要求，特頒此證明。

單位名稱　：兆豐期貨股份有限公司
App名稱　：兆期Go
App版本　：v3.26.10(Android)
基準版本　：v4.0
安全類別　：「L3」：含有交易行為之應用程式。
「F」：屬於安全需求較高之行動應用程式。
證書效期　：民國116年5月6日
檢測實驗室署名：安碁資訊股份有限公司
數位鑑識中心實驗室

其他記載事項　：

檢證QR Code
驗證證書即時狀態

本證書效力僅及於上述App與版本

行動應用資安聯盟
Mobile Application Security Alliance

兆期Go
MAS-3334-11500032

查詢中

版本比對中，請稍後查詢。

檢測合格證明資訊	
證書編號	MAS-3334-11500032
證書效期	民國116年5月6日
受測單位名稱	兆豐期貨股份有限公司

應用程式資訊	
App 名稱	兆期Go
作業系統	Android
App 版本	v3.26.10
App 安全類別	L3
檢測基準版本	v4.0
檢測實驗室	安碁資訊股份有限公司 / 數位鑑識中心實驗室

版本驗證資訊	
商店版本	查詢中
版本比對結果	商城查詢不到指定App

© 台北市電腦商業同業公會 Taipei Computer Association

規劃中

檢測實驗室

115年度精進重點

MAS 管理系統
功能調整說明

壹｜送審填寫新制

提升MAS資安標章之公信力、即時性與管理效能，避免商城查詢不到指定 App

- 【已發布】商城網址為必填，未填寫將予以退件
- 【尚未發布】網址暫為選填，通過後暫不正式公告，待確定網址通知秘書組後正式公告
- 【內部使用/不公開】免填商城網址

貳｜後市場管理合規宣導

- 標章屆期盤點：協助通知客戶 / 開發商效期屆滿前完成送測
  「標章效期屆滿名單」 已於三月發送提醒(3/13-7/13)
- 標章「認版本」原則：僅對證書載明之特定版本有效；重大更新須重新申請
- 標章使用核備：揭露標章或證書請依制度附錄七完成核備程序

參｜115 年度強化監管（納入評核）

- 建立「版本差異主動通報機制」，聯盟信箱（APP@mas.org.tw）為通報平台
- 績效評核：報告不實或抽驗不合格，公告並通知 TAF 撤銷證書，影響優良實驗室資格
- 常態化技術交流訪視：確保檢測基準一致性，協助精進作業標準

App 開發商｜資安合規宣導重點

01 標章「認版本」

- 標章僅對「證書載明特定版本」有效
- 版本號異動 → 原標章效力不自動延續
- 建議依 V4.0 最新基準重新申請檢測

02 商城網址填寫規範

- 已發布 App：行動應用商城網址為必填
- 尚未發布：網址選填，確定後再通知更新
- 內部使用/不公開：可免填商城網址

03 標章使用合規核備

- 官網、社群、DM 揭露標章須完成核備
- 下載填寫「附錄七-基本資安標章例外需求使用申請書」
- 嚴格遵循《推動制度》第 3.2.1 節規範

04 效期管理與主動送測

- 效期屆滿前主動完成送測，避免資安防護缺口
- 改版後請主動聯繫實驗室重新申請檢測驗證
- 可透過 QR Code 即時確認最新合規狀態

❑ 宣導事項一：

於115年2月9日MAS官網公告

■ 落實行動應用 App資安標章（MAS 標章）使用規範及版本異動取證要求

為維護「行動應用 App 基本資安自主檢測制度」(以下簡稱本制度)之公正性與嚴謹性，行動應用資安聯盟 特別發布此重要宣導。請各實驗室針對取得資安標章(以下簡稱取證)之客戶加強輔導與查核，確保標章使用符合本制度。

以下為本次宣導的三大重點：

一、 導正標章性質描述

近期發現部分取得資安標章業者於宣傳中誤稱 MAS 標章為「國家級認證」或「政府法定證書」，此舉恐造成公眾誤解。

- 正確定義： MAS 標章屬「民間業界自主成立之組織推動」及「業者自願性參與」之自主檢測性質。
- 配合事項： 請於交付檢測報告或取證前，明確告知業者其自主檢測性質，避免誤導性宣傳。

二、 嚴守版本異動規範

依據本制度之標章管理規範第 4.2 條，App 名稱或版本變更時，應重新申請授權，標章效力並非自動延伸。

- 違規態樣： 部分 App 上架使用版本已大幅領先取證版本（如：取證 v4.1.0，上架使用為 v5.x.x），但於官網或宣傳DM掛載資安標章。
- 配合事項： 請於每年至少一次定期追蹤，主動提醒業者若涉及影響資安功能設計時(如架構或版本更新等)，原已取證版本即失效，建議重新取證。

三、 強化實驗室宣導職責

實驗室為制度推動的第一線，建請將上述守則納入客戶說明文件。

- 通報義務： 若發現客戶嚴重誤導大眾或濫用標章，請及時提醒並通報本聯盟。
- 年度查核： 本項執行情形將納入年度實驗室績效評核項目。

請各實驗室務必配合落實，共同維護資安標章之公信力。

❑ 宣導事項二：

於115年3月23日MAS官網公告

■ 嚴格規範行動應用App資安標章（MAS）之使用與核備程序

為維護行動應用App基本資安制度之嚴謹性與標章公信力，本聯盟再次重申：凡使用、揭露「行動應用App基本資安標章（MAS標章）」者，務必嚴格遵循《推動制度》第 3.2.1 節規範。

若有於「官方網站、社群媒體、行銷 DM 或任何相關宣傳媒介」展示或揭露 MAS 標章之需求，請務必配合辦理以下程序以維護使用合法性：

1. 下載文件： 請至本聯盟官網下載並填寫「制度之附錄七 – 行動應用App基本資安標章例外需求使用申請書」。

2. 完成核備： 申請書填妥後，請協助取證單位提交至本聯盟完成正式核備程序。

特別警示：

未經正式核備程序擅自於公司官網、社群、DM或相關行銷媒體揭露MAS標章者，即屬違反推動制度規範。本聯盟將定期進行市場稽核，若發現不符規範之情事，將依制度採取撤銷標章或相關法律追訴行動，請各單位切勿自誤。

❑ 宣導事項三：

於115年4月20日email通知

■ MAS 管理系統功能調整暨 2026 年度後市場管理精進

為落實後市場管理機制、提升 MAS 標章公信力，並優化雙平台（iOS/Android）勾稽作業，秘書組針對「系統送審規範」與「管理監控重點」進行以下說明，懇請貴實驗室配合辦理：

壹、 MAS 管理系統送審填寫新制

送審時「行動應用程式商城網址」依發布狀態規範：

1.已發布： 必填。未填一律退件，請提醒受測單位提供。

2.尚未發布： 選填。通過後暫不公告，待單位確認網址並來信通知後始正式公告。

3.內部使用/不公開： 免填。

貳、 後市場管理與合規宣導重點

針對市場上標章等級、版本不符問題，請各實驗室落實下列管理機制：

1.屆期盤點與主動通知

- •主動提醒機制：依秘書組 3/16 提供之「即將屆滿清單(3.13-7.13)」，主動聯繫客戶，提醒於到期前送測。
- •進度追蹤： 請落實執行進度回饋，共同維持公告名錄之有效性。

2.恪遵標章「認版本」之原則：請主動向客戶(或開發商)重申，標章效力具備「高度特定性」，嚴禁誤用：

- •特定版本有效： 標章僅對證書載明之特定版本有效。
- •重大更新重測：程式碼變更、資安功能調整或版本異動，效力不延續，建議依 V4.0 最新基準重新送檢。

3.規範標章使用與核備程序

- •樣式規範： 使用標章須嚴格遵循《推動制度》第 3.2.1 節規範。
- •核備程序：行銷媒體（官網、社群、DM等）揭露標章前，須填寫「制度附錄七 – 例外需求使用申請書」完成核備。

參、 2026 年度強化監管與精進作為

本年度將針對以下項目加強管理，並納入實驗室評核考量：

1.版本差異通報：發現市售 App 與證書版本不符，可向 APP@mas.org.tw 通報。

2.績效評核與計點：依《制度 V4.3》，報告不實或抽驗不合格者，公告並通知 TAF 撤銷證書；若涉重大資安事件，影響「優良檢測實驗室」資格。

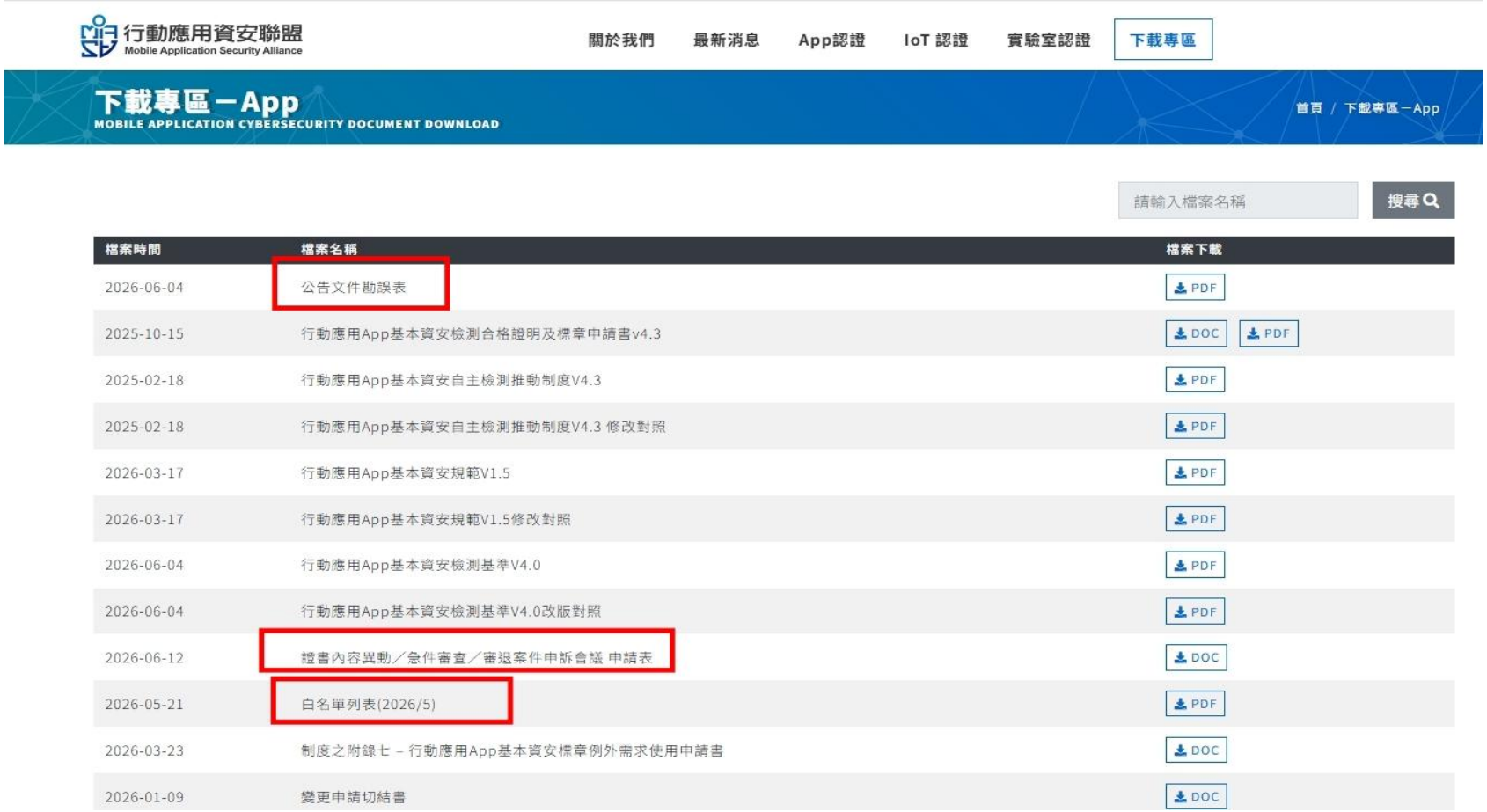
3.常態化技術交流與訪視：啟動專案實地訪視，統一檢測基準並落實公信力。

❑ 宣導事項四：

- 每季更新即將到期資安標章 App 清單，請各實驗室協助通知開發商辦理續約檢測。
- 說明：本聯盟每季 16 號前，將定期更新即將到期之資安標章 App 表單，並以 Email 個別通知相關實驗室。以 115 年度為例，首季已於 3 月 16 日下午 3:51 發送首波通知（針對 3/13-7/13 到期者）；第二季於 6 月 16 日發送第二波通知（針對 6/16-10/13 到期者），請各實驗室夥伴留意相關信件並協助配合。
  - 【主動聯繫提醒】 務必主動通知清單中即將到期之客戶，提醒其儘早規劃並完成送測。
  - 【確保防護不中斷】 引導客戶辦理續約，避免證書逾期導致標章失效，影響開發商權益。
  - 【進度追蹤回饋】 若獲知開發商有「放棄檢測」或「版本重大異動」之需求，請及時回報聯盟，以利即時更新名錄。

❑ 宣導事項五：

1. 本聯盟之制度、規範及基準等各項文件，均不定期公告於官方網站。若有內容修正，將以「公告文件勘誤表」之形式發布；白名單之更新異動亦同，請各會員單位隨時留意官網資訊。
2. 針對證書內容異動或急件審查需求請參閱「證書內容異動 / 急件審查 / 審退案件申訴會議 申請表」之完整說明



❑ 宣導事項六：

- 請實驗室於每月 10 日前填報「未申領標章案件清冊」，並妥善保存相關檢測報告以供抽查。。
- 說明：

一、 依據本聯盟最新發布之《行動應用App基本資安自主檢測推動制度 V4.3》第一部分第 4.5 條（其他標章管理事項）規定，凡經檢測合格卻未申領合格證明與 MAS 標章之案件，受託實驗室須完整記錄並建立清冊，每月定期提報，並配合相關抽查。

二、 為落實上述規章，請貴實驗室務必配合於每月 10 日前，將「上月檢測合格卻未申領標章」之案件完整填寫清冊並正式提報本聯盟；同時，應妥善保存相關檢測報告，以配合後續認證機構及本聯盟之定期或不定期抽查複核。

三、 檢附法規原文供參：

《行動應用App基本資安自主檢測推動制度規章》第 4.5 條：
「經檢測實驗室依據『行動應用App基本資安檢測基準』檢測合格之行動應用App，如未依前述4.1條規定，不申領合格證明與MAS標章，受委託執行檢測之實驗室須完整紀錄受測行動應用程式資訊包括單位名稱、App名稱、App版本、基準版本、安全類別等建立清冊，每月提報行動應用資安聯盟，並配合認證機構及行動應用資安聯盟定期或不定期抽查複核檢測實驗室出具之檢測報告。」

❑ 宣導事項七：

- **行動應用 App 基本資安檢測資料調查表（公版草案）落實說明**
- **說明：為確保送測流程之嚴謹性，請各實驗室務必落實把關責任。後續送審時，務必將「客戶簽名或用印之調查表」列為檢測報告後之必要檢附文件，以利業者自我檢視敏感資料權限，並協助檢測人員加速掌握商業邏輯。**

【調查表公版使用規範】

- **允許客製調整： 實驗室可依需求彈性新增欄位、公司 LOGO 或宣導事項。**
- **嚴守合規底線： 調整後之內容，務必完整涵蓋公版所列之 25 項基本要件。**
- **資訊對齊： 其餘與證書相關之欄位，均以實驗室於 MAS 系統內實際申請之資訊為準。**

行動應用App基本資安檢測實驗室

檢測技術一致性會議

審案分享：
提升送審案件品質與技術一致性探討

行動應用App基本資安檢測實驗室

檢測技術一致性會議

技術議題討論與決議

❑ 提案一：

- 測項： 4.1.2.1.1、4.1.2.3.1、4.1.2.5.1
- 主旨： 4.1.2.1.1、4.1.2.3.1 、4.1.2.5.1條文中關於應用程式商城中需宣告的要求內容與4.1.1.1.2內容重複，且對於符合、不符合以及不適用的定義不一致。
- 說明： 4.1.2.1.1、4.1.2.3.1 、4.1.2.5.1均在條文中要求須檢查行動應用程式商城中對於敏感性資料要求的宣告，但實際上這段內容再4.1.1.1.2已經有確認過了，重複的要求在這邊出像兩次顯得有點多此一舉。且在4.1.1.1.2中針對商城說明部分有不公開發布的不適用選項， 4.1.2.1.1、4.1.2.3.1 、4.1.2.5.1中卻沒有這段是會有爭議的。
- 建議：針對疑問分為過去實驗室提出的相關想法、以及短期、長期建議來說明。

過去實驗室提出的相關想法：這部分條文在4.0中有這樣的變動我想跟過去一致性會議討論的一個想法有關。該次討論到說有個APP廠商會將蒐集、儲存和分享敏感性資料的取得使用者同意文字加註在APP商城的說明或隱私權政策頁面中，故在APP中就不會有相關的說明以及取得使用者同意這個動作。

短期建議： 4.1.2.1.1、4.1.2.3.1 、4.1.2.5.1中應主要在確定使用者是否有同意蒐集、儲存和分享敏感性資料的部分。而不是重複去商城確認是否有說明(這件事在4.1.1.1.2已經完成了)相關內容。故以下

1. APP內已說明了敏感性資料使用的相關事項且有明確取得使用者同意的動作，報告中就無需一再對商城的說明提出佐證。

2. APP內沒有相關說明或動作才需要去探討商城裡是否有適當的宣告或做法來達到使用者同意蒐集或儲存敏感性資料的內容。

長期建議： 未來基準更新時因針對商城說明部分做調整，並明確定義各種情況下的判斷基準以避免不同條文間過多的冗餘內容。且4.1.1.1.2中是有不公開發布的不適用選項，但因4.1.2.1.1、4.1.2.3.1 、4.1.2.5.1並沒有不適用的選項，這部分是前後矛盾的。這部分建議未來基準調整時考慮是否回到3.2時的設定，或邀請各實驗室討論相關可能的情境再進行評估。

決議：同意提案，4.1.2.1.1、4.1.2.3.1 、4.1.2.5.1這三題重點是在應用程式內宣告無誤。

❑ 提案一：

檢測編號	4.1.1.1.2
檢測項目	行動應用程式發布說明
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.1.1. 行動應用程式發布、MASVS-PLATFORM-1、MASVS-PRIVACY-1
技術要求	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
檢測基準	若行動應用程式已發布，檢查行動應用程式是否於應用程式商店，依實際需要說明欲存取之敏感性資料、行動裝置資源及宣告權限用途。 若行動應用程式尚未發布，檢查調查表內是否有說明預計提供欲存取之敏感性資料、行動裝置資源及宣告權限用途之說明。 如為「是」則符合檢測基準；「否」則不符合檢測基準。
檢測結果	符合要求：符合檢測基準。 不符合要求：不符合檢測基準。 不適用：行動應用程式不公開發布，則此項不須檢測。
備註	須於「行動應用程式基本資料調查表」(附錄三、 行動應用 App 基本資安檢測資料調查表）自我宣告發布來源。 應用程式商店之宣告以行動裝置之商店介面為主。

❑ 提案一：

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

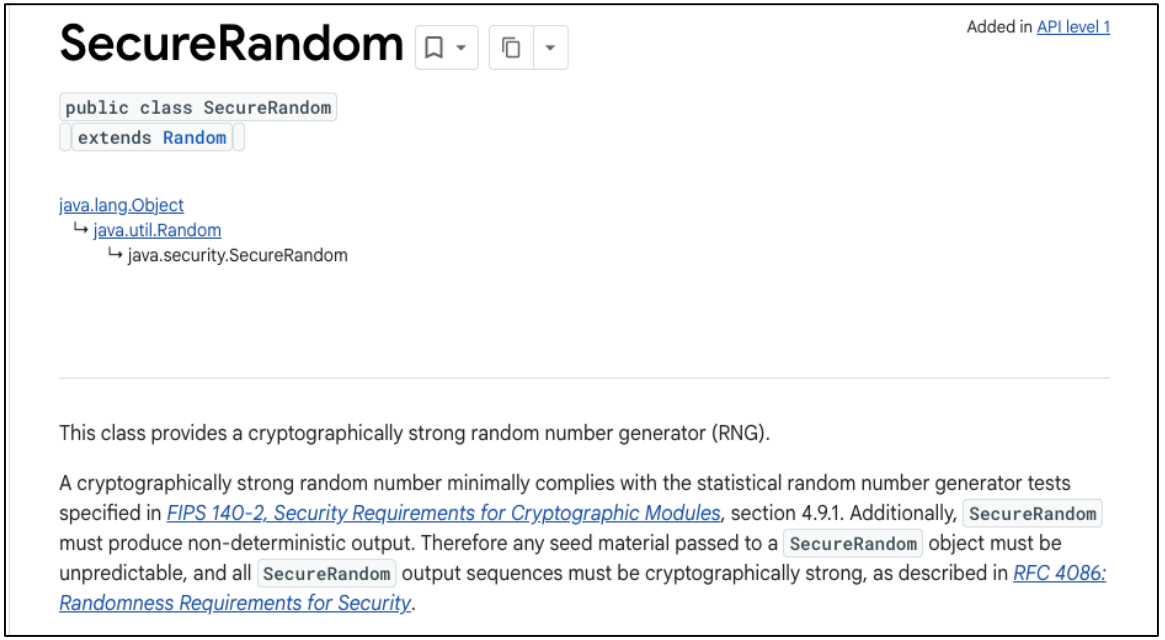
檢測編號	4.1.2.1.1
檢測項目	行動應用程式敏感性資料蒐集聲明
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.1. 敏感性資料蒐集、MASVS-STORAGE-1、MASVS-PRIVACY-3
技術要求	行動應用程式應於蒐集敏感性資料前，取得使用者同意
檢測基準	若行動應用程式已發布，檢查行動應用程式所有蒐集之敏感性資料，是否於應用程式商店內聲明，且於行動應用程式內聲明及取得使用者同意。 若行動應用程式尚未發布，檢查調查表內是否有填寫「需要之行動裝置敏感性資料類型（資源、權限）、用途說明、是否儲存於裝置內以及是否與其他應用分享」並說明將如何取得使用者同意，且在行動應用程式內聲明及取得使用者同意。 如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。 若行動應用程式不公開發布，檢查是否於行動應用程式內聲明及取得使用者同意。
檢測結果	符合要求：符合檢測基準，或行動應用程式未蒐集敏感性資料。 不符合要求：不符合檢測基準。
備註	應用程式商店之宣告以行動裝置之商店介面為主。

4.1.2.3.1. 行動應用程式應於儲存敏感性資料前，取得使用者同意

檢測編號	4.1.2.3.1
檢測項目	行動應用程式敏感性資料儲存聲明
檢測分類	L1、L2、L3
檢測依據	「行動應用 App 基本資安規範」4.1.2.3. 敏感性資料儲存、MASVS-PLATFORM-1、MASVS-STORAGE-1、MASVS-PRIVACY-4
技術要求	行動應用程式應於儲存敏感性資料前，取得使用者同意
檢測基準	若行動應用程式已發布，檢查行動應用程式所有儲存之敏感性資料，是否於應用程式商店內聲明，且於行動應用程式內聲明及取得使用者同意。 若行動應用程式尚未發布，檢查調查表內是否有填寫「需要之行動裝置敏感性資料類型（資源、權限）、用途說明、是否儲存於裝置內以及是否與其他應用分享」，並說明將如何取得使用者同意，且在行動應用程式內聲明及取得使用者同意。如為「是」則符合本項檢測基準；「否」則不符合本項檢測基準。 若行動應用程式不公開發布，檢查是否於行動應用程式內聲明及取得使用者同意。
檢測結果	符合要求：符合檢測基準，或行動應用程式未儲存敏感性資料。 不符合要求：不符合檢測基準。
備註	應用程式商店之宣告以行動裝置之商店介面為主。

❑ 提案二：

- 測項：4.1.2.3.6 行動應用程式敏感性資料儲存保護
- 主旨：檢測基準 (2) 提到所使用之加密函式之金鑰是否僅採用符合ANSI X9.17、FIPS 140-3、NIST SP 800-22及SP 800-90A (CAVP Testing: Random Number Generators)至少其中一項之安全的亂數產生函式之議題
- 說明：若加密函式之金鑰採用Android / iOS Developers 或文件所提到的安全亂數函式 (如：SecureRandom等等...)是否有需要再附上ANSI X9.17、FIPS 140-3、NIST SP 800-22及SP 800-90A 等相關文件來佐證亂數函式的安全性
- 建議：是否僅附上開發者文件即可符合審核委員的要求？



SecureRandom

Added in API level 1

```
public class SecureRandom
    extends Random
```

java.lang.Object
↳ java.util.Random
↳ java.security.SecureRandom

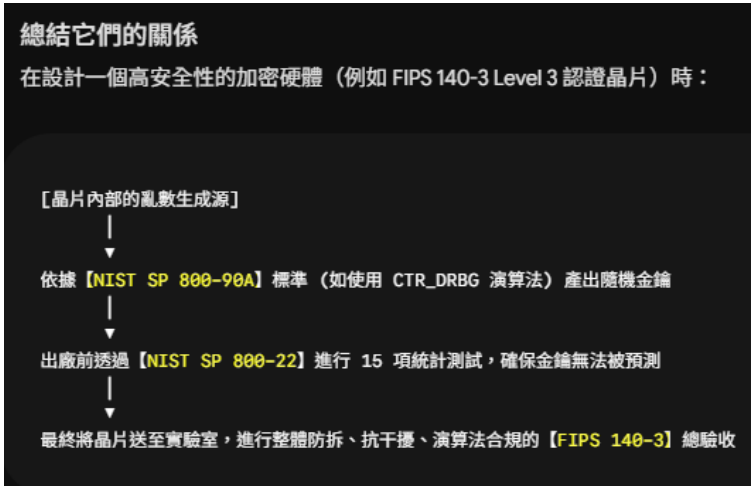
This class provides a cryptographically strong random number generator (RNG).

A cryptographically strong random number minimally complies with the statistical random number generator tests specified in *FIPS 140-2, Security Requirements for Cryptographic Modules*, section 4.9.1. Additionally, `SecureRandom` must produce non-deterministic output. Therefore any seed material passed to a `SecureRandom` object must be unpredictable, and all `SecureRandom` output sequences must be cryptographically strong, as described in *RFC 4086: Randomness Requirements for Security*.

決議：本案予以同意，亦接受附帶之開發者文件，落實應盡的確認與把關責任。

❑ 提案三：

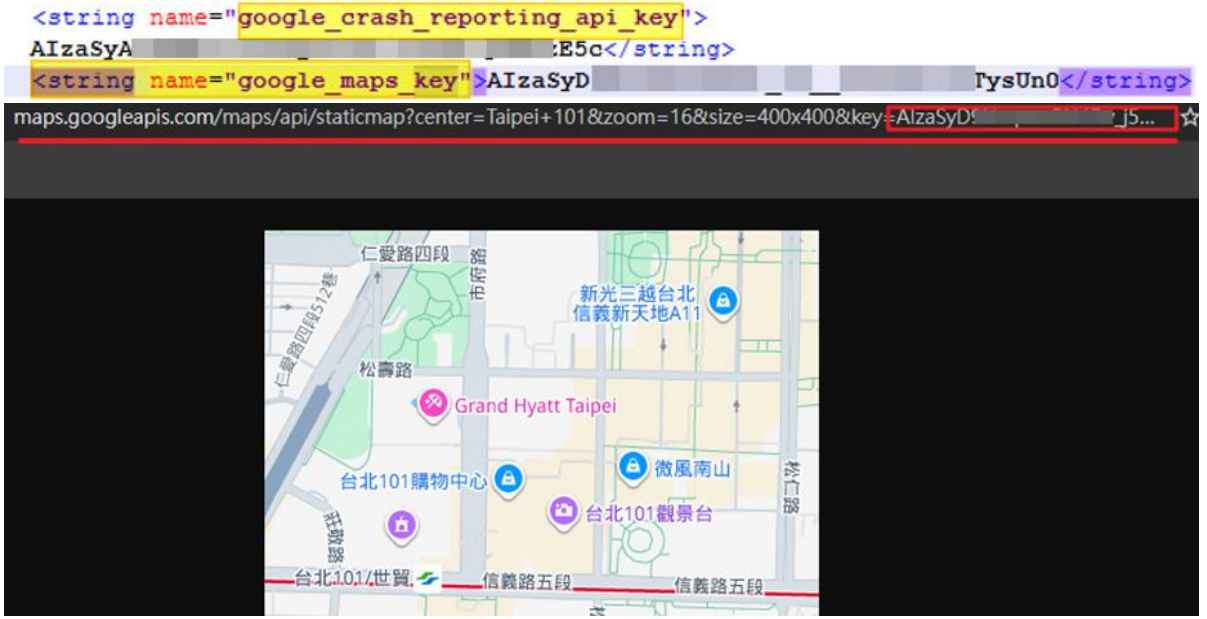
- 測項：4.1.2.3.6 敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存
- 主旨：修訂與釐清現行檢測基準所列之亂數相關標準，是否仍適合用於判定「安全亂數產生函式」
- 說明：4.1.2.3.6 (基準2) 加密函式之金鑰是否採安全的亂數產生函式產生之機制檢測，基準以 ANSI X9.17、FIPS 140-3、NIST SP 800-22、SP 800-90A 作為判定依據，然上述標準性質皆屬不同(如下所敘)，可能導致檢測判定標準不明確。應釐清各標準之適用範圍，避免混用不同性質之標準。
  - 舊版標準(ANSI X9.17)：為舊版金融亂數產生器，基於DES，已過時 (MAS 4.0基準已明確剔除3DES)
  - 模組驗證(FIPS 140-3)：屬於整體加密模組(包含金鑰管理、演算法、亂數產生)的規範，並不是專門定義RNG，而是僅間接要求「模組裡內 RNG 實作必須符合 SP 800-90A」
  - 統計測試(NIST SP 800-22)：為統計測試工具，不是 RNG 設計標準，無法判斷亂數是否具備安全性
  - 設計標準(NIST SP 800-90A)：定義密碼學安全亂數產生器(CSPRNG/DRBG)，適用於判斷亂數產生函式是否安全
- 建議：
  - 應立即移除 ANSI X9.17 (允用3DES已過時)
  - 考慮移除 FIPS 140-3 或列為建議，因其定位應為「模組驗證」，非直接 RNG 標準
  - 考慮移除 NIST SP 800-22，因其僅針對亂數輸出進行統計特性檢測，無法驗證其產生機制之不可預測性與密碼學安全性
  - 應以 NIST SP 800-90A 為主要判定標準



決議：同意提案，僅保留NIST SP 800-90A，納入改版參考。

❑ 提案四：

- 測項：4.1.2.3.8 敏感性資料應避免出現於行動應用程式之程式碼
- 主旨：對 App 內檢出明文 API Key 是否為敏感性資料之判定與查驗標準
- 說明：於程式碼(或儲存空間)中檢出明文 API Key 是否屬 Hard-coded (或儲存)敏感性資料而判定不符合？
  實務上開發端常有第三方服務設計要求，而將 Public API Key 明文寫入程式碼(或設定檔) 。如本案例下圖所示，於行動應用程式內發現明文 Google_maps_key，雖非帳密或加密金鑰，該 API Key 未進行任何保護(如加密或混淆)、後端 Server 亦未設定來源限制(如限制 HTTP referrers 或綁定 Backend IP)，取得後可透過瀏覽器直接呼叫該 API 功能並取得 Google 地圖服務，非僅限本 App 使用，可能造成企業財產損失。
- 建議：
  - 方案一：API Key 一律不視為敏感性資料 (風險為開發單位自行負責)
  - 方案二：API 一律視為敏感性資料，不得明文檢出
  - 方案三：API Key 若可利用則判定不符合，若已有限制防護不可利用，則判定為符合 (實驗室要多花心力進一步驗證)
  - 方案四：若為 Public API Key經開發單位同意可排除，惟應敘明原因(同4.1.2.3.13敏感性資料不進行遮蔽之豁免條件)



決議：同意採用方案四。

❑ 提案五：

- 測項：4.1.3.2.1
- 主旨：交易前驗證
- 說明：關於規範中提及「交易前的身分認證」要求，想確認執行細節。請教在以下三種認證機制中，是否僅需擇一符合即可達到合規標準？
  - Something You Know（例如：交易密碼）
  - Something You Have（例如：簡訊 OTP）
  - Something You Are（例如：生物辨識）
- 建議：無

決議：只要使用一種即可符合身份鑑別的要求。

❑ 提案六：

- 測項：4.1.4.2.2 行動應用程式應確認伺服器憑證之有效性
- 主旨：基準(2) 憑證綁定 (Certificate Pinning) 之驗證標準是否需與時俱進
- 說明：檢測實務上遇到開發端以「採用90天短效期憑證，頻繁輪替易導致 App 沒更新就會立刻癱瘓；官方平台連線機制(ATS)已有強化；已啟用憑證透明度(CT)」等理由擬申請豁免，並引用光盾資訊文章『手機平台為何不再建議將「憑證綁定 Certificate Pinning」列為必要測試項目』佐證。基於MAS規範現狀明定，實驗室固無單因營運考量而豁免，然連線安全是否仍僅採憑證綁定唯一實作認可方式，確有討論空間。
  - 官方明確表態與不建議：Apple、Google 技術文章已敘明原因，詳如下面出處
  - 維護成本與營運風險高：憑證公鑰寫死在 App 程式碼或設定檔中，憑證輪替將導致未更新 App 失效
  - 系統已內建更強大機制：iOS 與 Android 皆已支援系統層級的憑證透明度(Certificate Transparency, CT)驗證。系統會自動驗證伺服器憑證是否登錄在公開的 CT Log 中，能有效防範偽造憑證
  - 面對現代攻擊防禦效益邊際化：Pinning 在 JB/Root 環境有諸多工具可輕易繞過，防禦駭客效益低
- 建議：
  - 方案一：維持現狀，一律強制要求實作 Certificate Pinning (既使官方都不推薦)
  - 方案二：基準(2) 建議修改文案為「檢查行動應用程式是否已於系統層級（如 Android Network Security Configuration 或 iOS App Transport Security）強制規範安全連線，或使用憑證綁定（Certificate Pinning）方式驗證……嚴格禁止傳輸未經加密之明文資料（Cleartext traffic）。」
  - 方案三：或將憑證綁定此較高標準要求單獨列為「特殊/高風險領域的選用/進階項目(F項)」測項。

● 光盾資訊文章：https://www.rayaegis.com.tw/ca-pinning/ ● iOS 明確指出多數情況應避免使用 pinning： (In most cases, pinning is not necessary and should be avoided) https://developer.apple.com/news/?id=g9ejcf8y	● Android 明確標註 pinning 為 not recommended： (Certificate pinning is not recommended for Android app) https://developer.android.com/privacy-and-security/security-ssl#Pinning

決議：參考提案二，新增信任系統層級傳輸安全驗證，並會公告修正方向。

❑ 提案七：

- 測項：4.1.5.5.5
- 主旨：客戶提供未加殼App軟體檢測之必要性提問
- 說明：

依據106年08月15日一致性會議決議 - https://www.mas.org.tw/news/detail/59

『App 若加殼不予檢測， 如需檢測，須以加殼前之 App 進行檢測，並出具加殼服務後App軟體前後一致證明』。

1. 由於加殼前後APP的Hash值會不同。廠商要如何提供加殼服務後，App軟體前後一致證明? 具體的做法是?
2. 客戶提供未加殼App軟體檢測之必要性? 是否為降低實驗室檢測難度?

- 建議：

1. 建議提供送檢廠商幾種做法能參照執行，並於MAS官網再次宣導「App若加殼不予檢測」或釘選過往之公告，以提升廠商另外提供未加殼的版本之意願。
2. 若需請客戶提供未加殼之 App，係為降低實驗室檢測難度，建議調整描述為：『App 開發商應提供未經安全保護之 App 軟體（如：加殼、混淆、 appGuard安全保護...等機制）』

決議：聯盟可再重新宣導「App若加殼不予檢測」，但同時請實驗室針對加殼檢測發表執行現況。

❑ 提案八

- 測項：MAS 檢測基準相關之敏感性資料宣告、靜態與動態加密等動態測試項
- 主旨：廠商的app，最低相容版本為18，鑑於現行高階 iOS 系統越獄（Jailbreak）技術發展限制，建請放寬或增列「免越獄」作為 iOS 17/18+ 以上高版本系統之合規動態檢測替代手段，以確保檢測涵蓋率與實務可行性
- 說明：目前 iOS 越獄生態遭遇晶片與核心漏洞修補之瓶頸
- 建議：聯盟可針對無法越獄事宜，建立標準 SOP指引，以維持各家實驗室檢測結果之一致性

決議：當實驗室有無法使用 JailBreak 檢測的項目時，可以參考 OWASP Mobile Application Security Testing Guide (MASTG) 中所列之工具，搭配逆向工程反組譯程式碼及 App 隱私權報告協助輔助測試。

行動應用App基本資安檢測實驗室

檢測技術一致性會議

臨時動議

行動應用App基本資安檢測實驗室

檢測技術一致性會議

結論