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

114年第1次會議

中華民國 114年 5月 15日


moda
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


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
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)2577-4249，分機：889）。

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。

議 程

時間	內容	主講者
9:30~9:40	主席致詞	行動應用聯盟 陳俊良 會長
9:40~9:50	聯盟報告事項	行動應用聯盟 秘書組
9:50~11:00	檢測議題討論 聯盟宣導事項	行動應用聯盟 秘書組
11:00~11:20	臨時動議	行動應用聯盟 秘書組
11:20~11:30	結論	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

聯盟報告事項

行動應用App基本資安檢測實驗室一致性會議，於5/15(四) 501會議室召開，統計如下：

- 出席名單：17家檢測實驗室、委員及顧問
- 出席數：共65人包括實驗室55人(實體：18人；線上37人)；委員及顧問實體6人；秘書組4人
- 提案數：於5/2截止收件，共16案

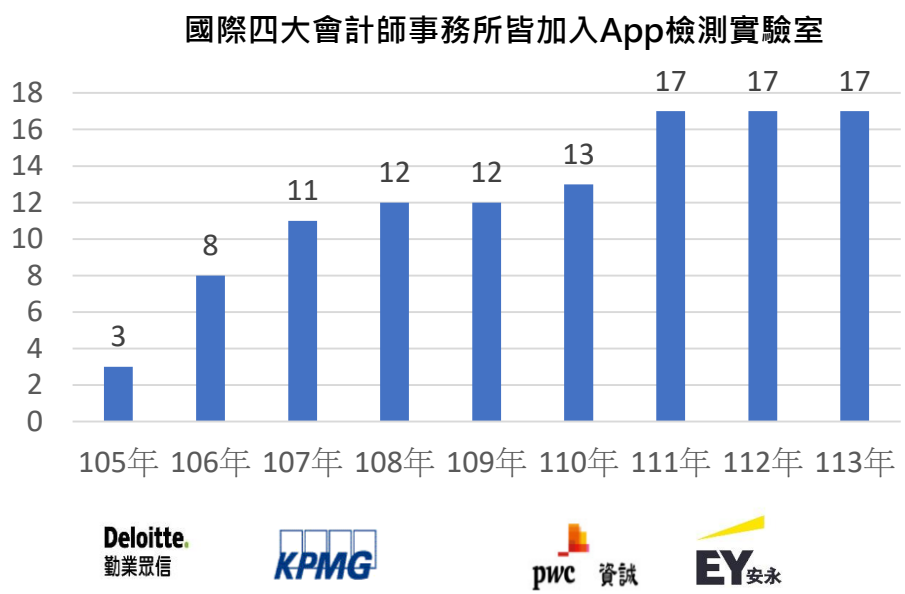
	實驗室	提案數	出席數
1	勤業眾信聯合會計師事務所	1題	實體：2人
2	財團法人台灣商品檢測驗證中心	1題	實體：1人；線上：2人
3	關貿網路(股)公司	1題	實體：2人；線上：2人
4	三甲科技(股)公司	1題	實體：2人
5	鑒真數位有限公司	2題	實體：2人
6	中華電信(股)公司電信研究院	2題	線上：9人
7	光盾資訊科技有限公司	2題	線上：3人
8	安碁資訊(股)公司	2題	實體：2人；線上：1人
9	安侯企業管理(股)公司	4題	實體：2人；線上：1人
10	安華聯網科技(股)公司	未提案	實體：2人
11	行動檢測服務(股)公司		實體：1人；線上：3人
12	財團法人電信技術中心		線上：3人
13	數聯資安(股)公司		實體：2人；線上：3人
14	資誠企業管理顧問(股)公司		線上：2人
15	國家中山科學研究院資訊安全中心		線上：2人
16	安永諮詢服務(股)公司		線上：4人
17	耀睿科技(股)公司		線上：2人

App資安標章整體概況

資安認驗證機制推動現況

行動應用App資安檢測實驗室17家

序	實驗室
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

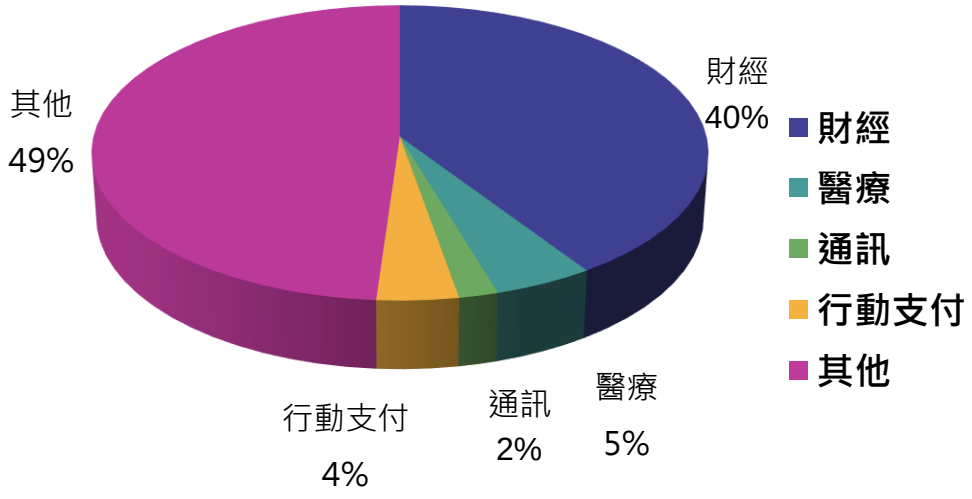


備註：

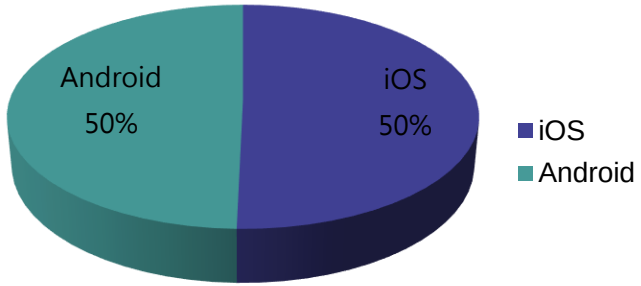
1. #不收民間單位案件
2. 新北市政府資訊中心未符合實驗室類團體會員身分，於4/22以【一般團體會員】身份加入聯盟

App資安標章整體概況
113年度通過分析

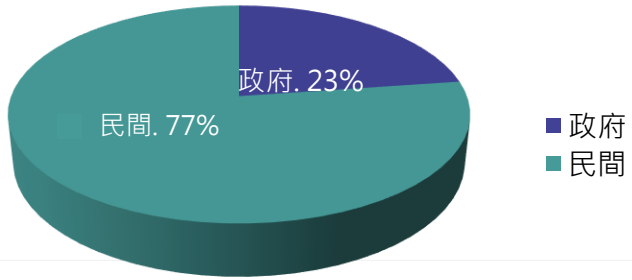
- 113年度行動應用App基本資安檢測基準App收件1,507件、通過1,507件（政府343件、民間1,164件）。較112年同期（1,270件）成長18.5%，政府成長率9.9%（112年同期政府312件）、民間成長21.3%（112年同期民間958件）
- App類別包括，通訊28件、財經613件、 行動支付58件、醫療71件、其他類別737件



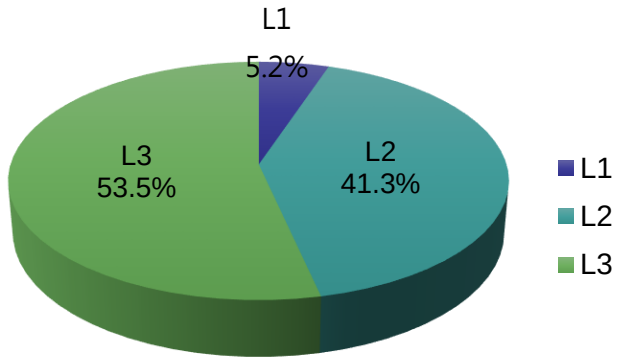
App作業系統：iOS 759件、Android：748件



政府343件、民間1,164件



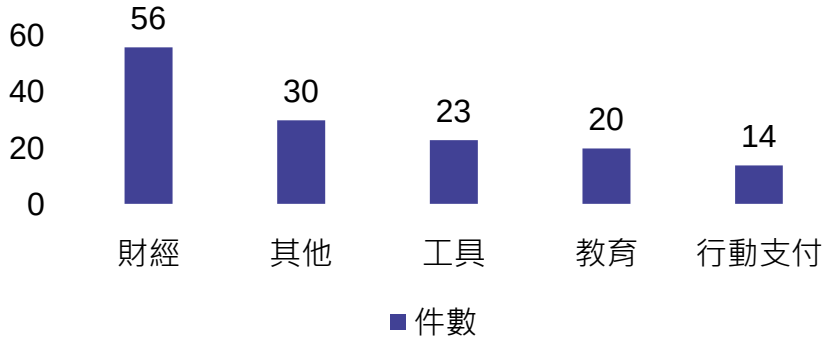
L1共78件、L2共623件、L3共806件



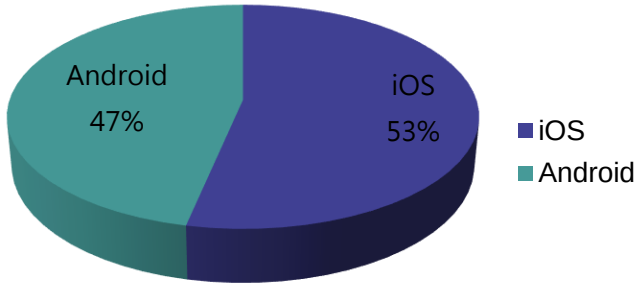
App資安標章整體概況
114年度通過分析

- 截至114/4/30，114年度行動應用App基本資安檢測基準App收件通過180件（政府51件、民間129件）。較113年同期（327件）負成長52.1%，政府負成長率37.5%（113年同期政府72件）、民間負成長56.1%（113年同期民間255件）。
- 前5大類分別為：財經56件、其他30件、工具23件、教育20件、行動支付14件

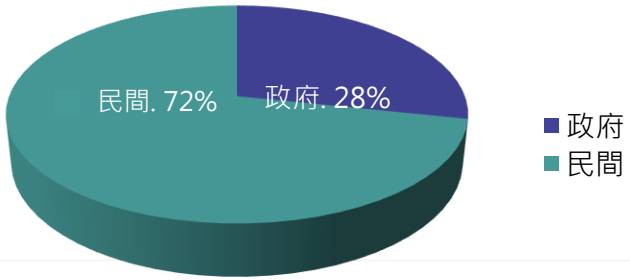
收件通過數



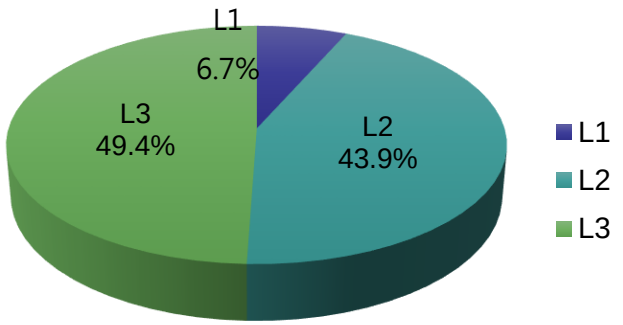
App作業系統：iOS 96件、Android：84件



政府51件、民間129件



L1共12件、L2共79件、L3共89件



行動應用App優良檢測實驗室表揚活動

行動應用資安聯盟年度優良檢測實驗室表揚活動，於2025年4月15日臺灣資安大會臺灣資安館舉辦，邀請數位產業署莊裕智副組長 (右4)及陳俊良會長與優良檢測實驗室之單位代表合影。

113年度優良檢測實驗室之單位代表由左至右包括：光盾、安華聯網、安碁、行動檢測、鑒真數位

行動應用App基本資安檢測實驗室

技術一致性會議

檢測實驗室提案

❑ 提案一：

- 測項：4.1.2.3.9
- 主旨：4.1.2.3.9.行動應用程式於非使用者主動進行的畫面擷取時應主動警示使用者，若iOS的App不符合檢測基準(2)的情況下，較難修復其問題
- 說明：

  1. 較難判定App處於多工模式

  2. 雖然可透過userDidTakeScreenshotNotification偵測截圖行為，但無法在多工模式下利用此通知來遮蔽App當前畫面。
- 建議：請問4.1.2.3.9.是否有建議的標準檢測作法？

決議：是指多工模式開始的那瞬間截圖，例如以下圖片。

❑ 提案二：

- 測項： 4.1.2.3.11
- 主旨：新增檢測基準4.1.2.3.11的檢測結果
- 說明：檢測基準要求：行動應用程式於使用者輸入敏感性資料時，是否未自動修正且未帶入可能字串。

  實驗室的檢測經驗及問題是受測行動應用程式未提供使用鍵盤進行「輸入」的字串輸入介面，但行動應用程式仍有蒐集敏感性資料的行為，例如相片、地理位置等。

  因基準要求是需要檢視鍵盤快取，若行動應用程式皆未使用鍵盤功能是否即可符合檢測基準。
- 建議：建議檢測項目4.1.2.3.11的符合要求判定方式可參考檢測項目4.1.5.4.1及4.1.5.4.2的符合要求：「符合所有檢測基準，或行動應用程式未提供字串輸入介面。」

決議：參考實驗室建議
符合要求改為：「符合所有檢測基準，或行動應用程式未提供字串輸入介面。」

❑ 提案三：

- 測項：4.1.2.4.1
- 主旨：4.1.2.4.1項目中，針對金融或保險業者視訊驗證、勘察等功能之 UDP協定、socket協定，證券期貨業者APP中使用socket協定傳輸資料之議題。
- 說明：如同前次會議討論，針對上述類型之視訊功能或股票報價等相關項目，可能因須確保即時性或後端固有設備或架構所導致APP無法調整傳輸機制之認定。因會議中委員們表示需在會後進行討論但目前並沒有收到結果通知。
- 建議：此類問題可以在會議記錄中加上註記針對某些情況之APP可在敏感性資料已加密，且封包中無法檢測出敏感性資料的狀態下排除一定要使用TLS1.2或更新的協定規則。

決議：針對檢測項目4.1.2.4.1行動應用程式資料傳輸安全，考量部分應用場景採用不可靠傳輸通訊協定（如 UDP），可接受行動應用程式使用 DTLS 1.2（含）以上版本 作為資料傳輸通道。其使用之加密演算法與金鑰長度應第 (2) 與第 (3) 項之規定。如符合則視為符合本項檢測基準。若有其他符合國際標準之協定，實驗室可遇案另行提起討論。

❑ 提案四：

- 測項：4.1.3.1.3
- 主旨：4.1.3.1.3收款功能是否有明確收款定義
- 說明：App如有提供QRCODE收款碼功能給民眾轉帳使用，於此項要如何判定呢？
  因目前於基準中未明確定義使用者端執行「交易收款」，是否單指店家端之收款行為，還是一般銀行轉帳也算是。
- 建議：建議可以再明確定義「收款」範圍為何。

決議：若為C2C交易，應納入範圍中，但無須包含交易商品資訊。

❑ 提案五：

- 測項：4.1.3.2.3
- 主旨：行動應用程式預授權之取消機制，其認定提供「取消功能」之主體範圍?
- 說明：

4.1.3.2.3. 行動應用程式應提供預授權交易之記錄其(2)檢查行動應用程式預授權交易之功能，是否提供使用者取消預授權之功能

其中定義行動應用程式須提供使用者取消預授權的功能，當假設行動應用程式只是一個橋接，換句話說行動應用程式公司只能透過API達成此功能，而非真正可以取消預授權交易時，舉例來說：

當某銀行行動應用程式提供eTag自動扣繳申請功能，當申請完成後須要取消此預授權功能，其行動應用程式只是提供取消，但實際需要遠通電收回覆後才能確認取消，故實際取消是遠通電收非銀行。當某銀行行動應用程式提供停車費自動扣繳，其取消也是必須要等待各縣市主管機關確認取消。

故依據上述描述，想請教以下問題：
1.請問當行動應用程式本身提供取消功能，但實際取消預授權為第三方，這樣是否符合聯盟定義的「提供使用者取消預授權」

- 建議：請聯盟回覆「提供使用者取消預授權」定義。

決議：具有[提出取消授權申請]之功能，即符合檢測基準。

❑ 提案六：

- 測項：4.1.3.2.3
- 主旨：預授權交易的宣告內容
- 說明：4.1.3.2.3. 行動應用程式應提供預授權交易之記錄，檢測基準(3)提到須於取得使用者提供之授權時進行宣告，實驗室理解此處宣告為 “告知使用者當下做的事情，並取得使用者的同意”
- 建議：請問是否有明確制式的預授權宣告（例：需要包含哪些要點），還是簡單告知使用者該筆交易的風險即可？

決議：主要宣告讓使用者瞭解授權目的、範圍與風險等。

❑ 提案七：

- 測項：4.1.5.5.7
- 主旨：測項「4.1.5.5.7 行動應用程式須偵測當前的執行環境是否為模擬器」於iOS是否改為不適用?
- 說明：測項「4.1.5.5.7 行動應用程式須偵測當前的執行環境是否為模擬器」檢測內容為查看行動應用程式是否能主動偵測環境是否為模擬器。但iOS系統目前仍未有完整的模擬器環境，較為接近的環境也需要原始碼才能模擬，實際執行時很難達成。
- 建議：該測項於iOS環境是否可改為不適用?

決議：可使用包含Xcode Simulator等工具。

❑ 提案八：

- 測項：其他
- 主旨：iOS Emulator測試上的可行性議題
- 說明：最新MASv4.0定義的模擬器為Emulator，如下圖所示：

> 3.27. 模擬器（Emulator）
>
> 指在電腦或是其他非行動裝置之設備上，模擬行動裝置之執行環境，用於在非行動裝置上執行行動應用程式。

但iOS當前沒有實際上的Emulator模擬器(行動裝置模擬)，幾乎全部現今的iOS模擬器只會聲明自己為simulator(非行動裝置模擬)，當前沒有可以於本地端實際模擬iOS行動裝置的軟體。

當前有聲稱Emulator且具有Root權限的只有Corellium，但其為雲端服務，實驗室在執行測試期間，不可能上傳將客戶APP檔案到第三方平台進行測試，可能會導致洩漏客戶程式的資料。

故依據上述描述，想請教以下問題：

iOS Emulator現今沒有可用的平台可以進行檢測，那此項目要如何進行測試

- 建議：請聯盟針對iOS平台對於Emulator檢測的當前可行性進行評估，並且確認是否iOS可執行此項目檢測。

決議：Simulator亦符合此處的名詞解釋，可使用包含Xcode Simulator等工具。

❑ 提案九：

- 測項：其他
- 主旨：Android 12以上之螢幕覆蓋測試判定標準之一致性釋疑
- 說明：自Android S (12、SDK 31) 及以上版本，Google已經內建螢幕覆蓋風險進行系統層級防護設計調整。
  根據Google開發者指南「防範Tapjacking螢幕覆蓋攻擊」章節：「對於其他 UID 中不受信任的疊加層，Android S (12、SDK 31) 及以上版本預設會封鎖其中的觸控事件，藉此預防完全遮蔽攻擊。」
  Ref: https://developer.android.com/privacy-and-security/risks/tapjacking?hl=zh-tw&hl=zh-tw
  現行針對Android版本12以上若使用藍光覆蓋App檢測方式，系統內建並不會跳出任何偵測警示訊息，仍可正常使用。

檢測方式	Android 11以下	Android 12以上
以抗藍光覆蓋App檢測		

- 建議：
  1.若待測App可安裝於Android版本11以下之裝置，則須檢測且必須有防護機制或跳出警示訊息；但Android版本12以上可正常使用，應視為符合(因OS層已封鎖)。
  2.或建請教授專家或所有實驗室專家們集體思考其他檢測方式，以求基準符合/不符合判斷之一致性。

決議：1.若待測App可安裝於Android版本11以下之裝置，則須檢測且必須有防護機制或跳出警示訊息；若僅有Android版本12以上可使用，視為符合(因OS層已封鎖)。

❑ 提案十：

- 測項：其他
- 主旨：針對 App中包含 WebView功能之情境。
- 說明：若 App 中包含 WebView，其載入頁面或所涵蓋之第三方頁面產生的封包是否應納入測試範圍，並列入封包流向分析？
- 建議：無

決議：應納入範圍內，例如有使用第三方的Javascript或CSS等。

❑ 提案十一：

- 測項：其他
- 主旨：待測物為L1 App且無蒐集任何敏感性資料時，仍需取得使用者同意拒絕之議題
- 說明：

  4.1.2.1.1、4.1.2.1.2、4.1.2.3.1、4.1.2.3.2...等測項於V4.0基準「改為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」(將『或』改為『且』)。

  1.若待測物App為L1等級(無須帳密登入)且並無蒐集、儲存、分享及傳輸任何敏感性資料(內容皆為公告資訊)，是否仍須一定要在行動應用程式內聲明及取得使用者同意？

  2.若待測物App為L1等級(無須帳密登入)但有蒐集、儲存、分享及傳輸敏感性資料(譬如蒐集使用者GPS座標)，是否仍須一定要在行動應用程式內聲明及取得使用者同意，還是可以在應用程式商店內聲明即可？(因有眾多送測單位反映做在App內會影響使用者體驗)

- 建議：

  1.若待測物App為L1等級且並無蒐集、儲存、分享及傳輸任何敏感性資料，請考量是否視為同意選項。
  2.若待測物App為L1等級但有無蒐集、儲存、分享及傳輸任何敏感性資料，請考量是否可僅於應用程式商店內聲明。

決議：
1.若待測物App為L1等級且並無蒐集、儲存、分享及傳輸任何敏感性資料，視為「符合」。
2.若待測物App為L1等級但並有蒐集、儲存、分享及傳輸任何敏感性資料，若行動應用程式內的宣告，包含作業系統觸發或行動應用程式本身的宣告均可符合此條文。

❑ 提案十二：

■測項：其他

■主旨：針對MASv4.0的檢測標準此次新版的「取得使用者同意」議題討論 Part1

■說明：新版本條文對於取得使用者同意更改為：
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。
依據描敘可以認為，新版本要求取得使用者同意須要在行動應用程式內取得依據台灣個人資料保護法，其第19條描述，對於取得使用者同意沒有明定取得方式。歐盟GDPR，其Art. 7與Art. 8描述，也沒有定義取得使用者同意取得方式。美國ADPPA定義為Affirmative express consent也沒有定義取得使用者同意取得方式。台灣、歐盟與美國皆是可證明取得使用者同意即可。故當MAS檢測標準定義，認定取得使用者同意須強制於行動應用程式內取得，其結果就是MAS規範比起全球法規更加嚴格。

目前有很多金融相關的行動應用程式都會在辦理開戶、申請帳號時，同步簽署實體文件，或是線上透過網頁進行申請時，來取得使用者同意。台灣企業只有國內客戶時，對於行動應用程式內取得使用者同意，此要求通常不會有意見。
但當行動應用程式已經於國外上架並使用多年，且行動應用程式於國外上線時，是透過其他管道取得使用者同意後(如開戶、實體或線上申請帳號等)，獲得行動應用程式可登入之帳號。當轉而要於台灣上線時，須符合MAS規範，但國外沒有強制要求在行動應用程式內取得同意的條文，故國外廠商法務認為沒有法源依據。

另外補充詢問MAS4.0版本PDF14頁，其中「取得使用者同意」，其中描述為行動商店內以「使用者下載安裝使用即視為同意」，其描述跟4.1.2.1.1.條文內的行動應用程式內聲明及取得使用者同意其判斷標準跟聯盟委員說法互相衝突，描述如下：

所有須「取得使用者同意」之檢測項目，可於信任之行動應用程式商店以「使用者下載安裝使用即視為同意」之聲明方式或行動應用程式至少於第一次執行時，以「主動提供說明及同意與不同意選項」方式，取得使用者同意，當送檢之行動應用程式同時提供上述兩種取得使用者同意之方式時，以行動應用程式內取得使用者同意之方式為檢測判定是否符合之依據。

故依據上述描述，想請教以下問題：
1.取得使用者同意是否一定強制要在行動應用程式內取得?
2.當透過實體文件或其他管道取得使用者同意(聲明有包含行動應用程式內的蒐集、儲存、分享等內容)，聯盟是否接受?
3.條文4.1.2.1.1聲明一定要在行動應用程式內取得同意，但另外PDF14頁又說可以在行動商店聲明下載即同意，請問要依據哪一項標準取得同意?

■建議：實驗室對於使用者同意的方式沒有特定意見，但針對取得使用者同意之方法，請聯盟委員決議，並且提供具有合理說明且有法源依據的聲明，讓實驗室可以依據此決議回覆客戶。

決議：
1,2. 使用者同意需要在行動應用程式內同意，實體管道不包含在內。
3. 第14頁條文已於基準V4.0進行修正調整，請依據條文4.1.2.1.1。

❑ 提案十三：

- 測項：其他
- 主旨：針對MASv4.0的檢測標準此次新版的「取得使用者同意」議題討論 Part2
- 說明：由於MASv4.0，對於不公開發布APP，取得使用者同意已經更改為「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。」
  假設當前APP為保險人員使用的「不公開發布」APP，即公司內部使用之APP，其功能包含輸入客戶的敏感性資料。
  當保險人員甲，須透過APP輸入客戶A的敏感性資料，依照合理邏輯來說，由於是輸入客戶A的敏感性資料，依照正常邏輯來說不可能是取得保險人員甲的同意，故應該是客戶A之「取得使用者同意」，故目前的情況是操作APP是保險人員甲，但輸入的卻是客戶A的敏感性資料。
  假設情況一：
  當保險人員甲跟客戶A，位於相同地理位置下，由於MASv4.0強制之使用者同意一定要在APP取得，故APP的取得使用者同意這行為，需要把APP讓給客戶A來按同意?，但是當前登入的帳號是保險人員甲?，要怎麼保證取得之使用者同意是客戶A?
  假設情況二：
  當保險人員甲跟客戶A，位於不同地理位置下，由於MASv4.0強制之使用者同意一定要在APP取得，要如何取得客戶A的使用者同意?
  MASv3.2沒有強制取得使用者同意一定要在APP上取得，故當透過實體，線上等方式取得也是符合。故當客戶A已經透過保險申請文件，授權使用者同意後，後續的所有敏感性資料都屬於個人資料保護法的「處理」，故保險人員甲不需要再透過APP去取得客戶A之使用者同意，因為都是屬於蒐集後之任何行為都是屬於「處理」範疇內
  故依據上述描述，想請教以下問題：
  1.當操作APP為保險人員甲，輸入客戶A人員的敏感性資料時，那APP是要取得「客戶A的同意」還是「保險人員甲的的同意」?
  2.當APP使用者輸入的敏感性資料，不是當事人的敏感性資料情況下，要如何取得當事人使用者同意?
  聯盟定義使用者同意應該是何人?在此情境下，APP要如何取得使用者同意?
  4/29聯盟回覆：
  測試項目中，要求需要有宣告、同意並有拒絕的權利都是針對「敏感性資料」「個人資料」是「敏感性資料」的子集合，但如果是公司員工存取客戶的「個人資料」
  這時對於公司員工來講，這些資料就是公司的「營業秘密」，也屬於「敏感性資料」的子集合
  同樣的概念A使用者，透過行動銀行轉帳給B使用者，有可能會輸入B使用者的銀行帳號，甚至手機號碼，
  這種狀況我們僅需要取得A使用者的授權，並不需要額外取得B使用者的同意才能完成這筆轉帳
  B使用者本身會透過行動應用程式以外的方式，授權給A使用者使用他的手機號碼進行轉帳。

❑ 提案十三：

- 測項：其他
- 主旨：針對MASv4.0的檢測標準此次新版的「取得使用者同意」議題討論 Part2
- 說明：

實驗室再提問：
先釐清以下狀態
1.APP是「不公開發佈」
2.使用人：保險人員
3.敏感性資料：保險人員A 與 客戶B

依據MAS聯盟回覆再詢問：
依據MASv4.0的定義，只要是APP內的蒐集、儲存、分享等敏感性資料，都要依據「行動應用程式內取得使用者同意」來進行檢測
但依據聯盟的回覆意思請問是定義為何?
1.此APP檢測中的取得使用者同意之敏感性資料，只要針對保險人員A即可? 客戶B的敏感性資料不在檢測範圍內?其他檢測項目也比照辦理不在檢測範圍內?如輸入欄位檢查、儲存、分享等等?
2.保險人員A使用者同意採用MASv4.0定義檢測，客戶B是透過上述黃底說明，透過APP以外方式取得使用者同意? 其他檢測項目還是檢測範圍內?

決議：
1.針對裝置使用者，即保險人員A。
2.客戶B的個人資料屬於此案例的敏感性資料，也就是對保險人員A來講即是公司的營業祕密，因此使用者(保險人員A)，針對行動應用程式的敏感性資料，應符合相關連之檢測基準。

❑ 提案十四：

- 測項：其他
- 主旨：「行動應用App安全開發指引」的更新
- 說明：
  於行動應用資安聯盟官網下載專區的「行動應用App安全開發指引」，目前的內容還停留在108年。
- 建議：
  建議可以更新內容與v4.0基準一致

決議：鑒於行動應用App開發技術日趨成熟，且「行動應用App基本資安檢測基準」將持續優化精進，原有的「行動應用App安全開發指引」將不再進行更新，並將自聯盟官網下架。

❑ 提案十五：

- 測項：其他
- 主旨：行動應用App基本資安檢測基準V4.0之英文版
- 說明：

  因為金融業相關部分銀行為國外銀行，故國外銀行會想要實驗室提供行動應用App基本資安檢測基準V4.0之英文。
- 建議：

  於下載專區 - App，提供行動應用App基本資安檢測基準V4.0之英文版。

決議：待「行動應用App基本資安檢測基準V4.0」穩定推行，且國際應用需求明確提升後，將再擬訂推動其英文版本之規劃。

❑ 提案十六：

- 測項：其他
- 主旨：聯盟系統建議
- 說明：

1.實驗室後台系統的APP檢測實驗室知識庫已許久未更新。

2.證書審查通知目前內容狀態一律都是 狀態邊更 難以識別。

- 建議：

1.建議持續將一致性會議討論結果更新至該檔案，或是將過去一致性會議的紀錄定期更新在該區域。以便新進實驗室或舊有實驗室可隨時查閱相關紀錄以確認過去是否針對該議題有過討論，避免相同問題重複討論的狀況。

2.建議系統通知信可加註變更後的狀態，例如審查中、退回、審查通過等。這樣可以減少每次都需再進到系統才能知道內容的麻煩。

決議：

1.實驗室後台系統中的APP檢測實驗室知識庫，預計將於今年度進行更新作業。

2.系統通知信可增列變更後狀態說明，系統商預計於6月起展開相關系統調整作業。

行動應用App基本資安檢測實驗室

檢測技術一致性會議

聯盟宣導事項

❑ 宣導一：

■ **App 軟體已做加殼服務之檢測做法，於106年一致性會議決議如下，提醒實驗室夥伴留意語配合。**

行動應用資安聯盟
Mobile Application Security Alliance

關於我們 | 最新消息 | App認證 | IoT 認證 | 實驗室認證 | 下載專區

首頁 / 主要公告 / 【行動應用資安聯盟】App 軟體已做加殼服務之檢測做法

App **【行動應用資安聯盟】App 軟體已做加殼服務之檢測做法**

2019/07/04 【四】

依據106年08月15日一致性會議決議：

針對App 軟體已做加殼服務，決議作法如下：

1. 檢測實驗室須依據 App 檢測基準所規範檢測項目逐項進行檢測，App 開發商應提供未加殼前 App 軟體進行測試，檢測通過後將出具未加殼前 App 軟體檢測合格證明， 建議 App 開發商可於 App 資安檢測通過後再進行加殼服務，並須取得經加殼服務後， App 軟體前後一致證明。
2. App 開發商如使用 App 加殼服務，向聯盟申請 MAS 標章時，須同時提供未加殼前檢測合格證明，及加殼服務後 App 軟體前後一致證明。
3. 檢測實驗室須依據 App 檢測基準所規範檢測項目逐項進行檢測，不可因是否有加殼或其他特定 App 因素，而減少任何應檢測項目。
4. 檢測實驗室若有其他技術因素導致無法檢出是否符合檢測基準要求，僅可出具檢測報告，不可出具檢測合格證明。

**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。

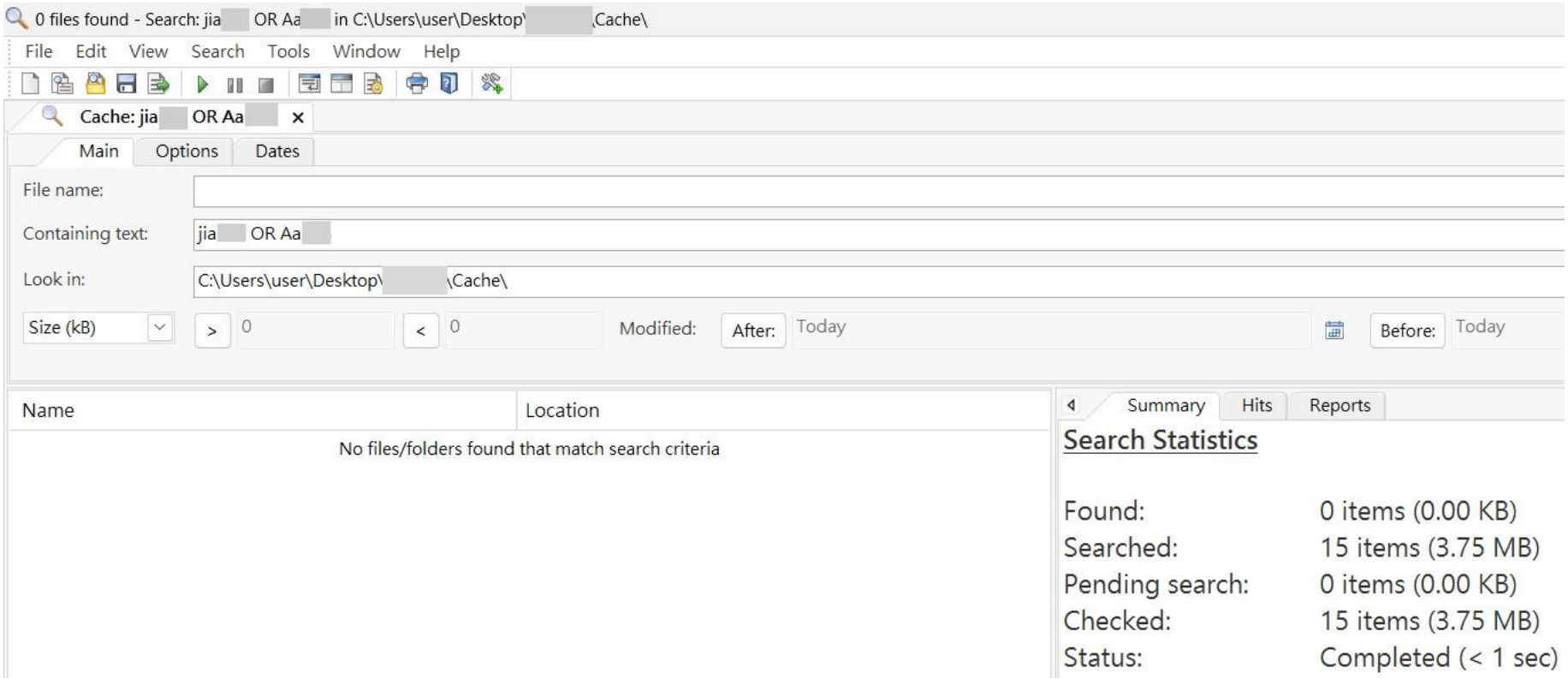
https://www.mas.org.tw/news/detail/59

❑ 宣導二：

- **建議請實驗室，於檢測報告中務必敘明所測試使用的敏感性資料為何?**
- **說明：**

  檢測報告應符合完整性及一致性，以下圖為例，若敏感性資料帳號是jia....密碼是Aa...

  請於報告中標示，且請留意檢測報告相關截圖，前後須一致。



❑ 宣導三：

■ **提醒應於每月10日前填覆未送件列表，感謝配合。**

行動應用 App基本資安自主檢測推動制度 V4.2

4.5其他標章管理事項：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，不申領合格證書與資安標章，受委託執行檢測之實驗室須要請App開發者提出切結聲明書，並以此聲明書向行動應用資安聯盟提報，相關作業規定由行動應用資安聯盟另訂定公告之。

改版

行動應用 App基本資安自主檢測推動制度 V4.3

4.5其他標章管理事項：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。

行動應用App基本資安檢測實驗室

技術一致性會議

臨時動議

❑ 臨時動議一：

- 測項：4.1.3.2.3
- 主旨：預授權交易有哪些樣態可以情境式說明?
- 說明：

  以下情境為例：

  1. 以停車場的App為例：由於實務上難以在車輛駛離停車場時進行交易前認證。因此，會需要預先綁定付款方式，於結束停車後進行處理。
  2. 以證券交易為例：由於爭取時效之故，難以在下單時要求進行交易前認證。因此，會需要預先綁定付款方式，於委託成功時進行處理。
  3. 訂閱制：第一次綁定信用卡後，往後的每個月/年，App就會在固定的時間進行扣款。
  4. 以基金/股票的定期定額為例：一旦確認定期定額的資訊，往後的每週/月就會按照合約上的金額進行帳戶的扣款。
- 建議：無

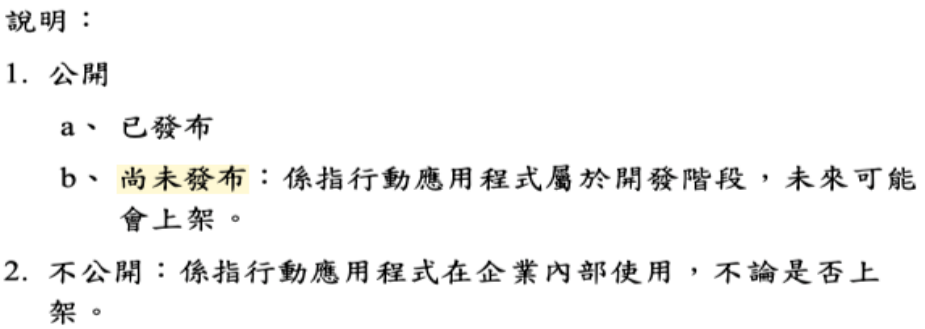
決議：

1. 檢測基準中名詞解釋如下：指使用者事先給予應用程式特定目的的交易許可權，在未來進行多次連續交易時無須再額外取得使用者同意，可直接交易。重點目的在於「無須再額外取得使用者同意」因此情境1,3,4屬於預授權交易，每次交易使用者均不需要再額外確認，但情境2使用者仍須要再額外確認數量金額等資訊。
2. 檢送基準編修團隊，完成修正名詞定義(詳公告文件勘誤表)

❑ 臨時動議二：

- 測項：其他
- 主旨：行動應用程式檢測「尚未發布」定義詢問
- 說明：

MAS其對於行動應用程式的發布定義，如圖：



說明：

1. 公開
   a、已發布
   b、尚未發布：係指行動應用程式屬於開發階段，未來可能會上架。
2. 不公開：係指行動應用程式在企業內部使用，不論是否上架。

假設當行動應用程式已經上架且已持續營運多年，其版本目前為v1.0。當實驗室收到的版本為v2.0版本且尚未上架，處於內部開發中的版本，因開發商想要通過檢測後才上架。

因其已發布與尚未發布，其定義沒有明確指定為行動應用程式本身，還是行動應用程式版本。

1.行動應用程式本體為依據，雖然測試版本未上架，但可以認定為已發布。

2.行動應用程式本體+版本為依據，因為此版本未上架，故可以認定尚未發布。

故依據上述描述，想請教以下問題：

1.故當收到v2.0版本進行檢測，檢測環境是「已發布」還是「尚未發布」？

- 建議：

請聯盟回覆「已發布」與「尚未發布」定義

決議：此檢測目的在於驗證行動應用商城之宣告是否正確，應用程式已於行動應用商城上架，因此可以進行對應的測試項目，列為已發布，若個案尚未更新商城資訊，亦可額外將預計更新的宣告內容，於測試報告中說明清楚。

❑ 臨時動議三：

- 測項：其他
- 主旨：行動應用App基本資安檢測基準 V4.0 用語及定義中的3.59.多工模式（Multitasking Mode），描述的行為可能不夠完備，因此在認知與檢測上可能出現歧異。
- 說明：

多工模式通常指的是以下幾種行為：

- 背景執行： App 在使用者切換畫面後仍持續執行某些任務（例如下載、音樂播放）。
- 分割畫面（Split Screen）： 兩個 App 並排顯示並同時使用（Android 、iPad常見）。
- 畫中畫（Picture in Picture，PiP）： 例如觀看影片時可以縮小成浮動視窗繼續使用其他 App。
- App 快速切換（Task Switcher）： 使用者可在最近使用的 App 間快速切換。

而MAS V4.0中的多工模式（Multitasking Mode）定義為:

指一個行動設備（如智慧手機或平板電腦）的執行模式，其中使用者可以同時預覽多個應用程式。

由以上可知MAS v4.0的定義屬於「背景執行」或「App 快速切換」。

於檢測項目4.1.2.3.9的檢測基準(2)中的描述，可精準對應到MASTG-TEST-0010: Finding Sensitive Information in Auto-Generated Screenshots和MASTG-TEST-0059: Testing Auto-Generated Screenshots for Sensitive Information。

以上兩項MASTG-TEST檢測要點:

App進入背景時，為了讓使用者預覽當前畫面，系統會自動生成圖片，若未對此狀態的畫面做遮蔽或模糊處理，就會被攻擊者利用(尤其當前畫面含有敏感性資料時)。

攻擊者可以透過以下路徑的取得上述的圖片

Android：/data/system_ce/<USER_ID>/<IMAGE_FOLDER_NAME>

iOS ： /var/mobile/Containers/Data/Application/$APP_ID/Library/SplashBoard/Snapshots/sceneID:$APP_NAME-default/

❑ 臨時動議三：

- 測項：其他
- 主旨：行動應用App基本資安檢測基準 V4.0 用語及定義中的3.59.多工模式（Multitasking Mode），描述的行為可能不夠完備，因此在認知與檢測上可能出現歧異。
- 說明：如上頁
- 建議：

  可將用語及定義中的「多工模式」修改定義的名稱，來更符合聯盟所需要的檢測要點，檢測執行上也較為直觀。

  例如:

  定義名稱:

  將「多工模式」更改成「背景應用程式切換模式」或「螢幕背景模式」

  定義的內容則可保留:

  指一個行動設備（如智慧手機或平板電腦）的執行模式，其中使用者可以同時預覽多個應用程式。

決議：檢送基準編修團隊，完成修正名詞定義(詳公告文件勘誤表)