科技部資訊安全技術研發專案計畫

『系統測試計畫書』

System Testing Plan

IoT 可信賴架構之設計與實作

IoT Trusted Architecture

MOST 105-2221-E-011-070-MY3

研究團隊

主持人：吳宗成教授(臺灣科技大學資管系)

共同主持人：羅乃維教授(臺灣科技大學資管系)

查士朝副教授(臺灣科技大學資管系)

葉國暉副教授(東華大學資管系)

左瑞麟副教授(政治大學資學系)

專任研究助理：藍袖瑛(臺灣科技大學資管系)

Department of Information Management,

National Taiwan University of Science and Technology, Taiwan

2018/5/15

目錄

版次變更記錄

版次	變更項目	變更日期
1.0	第一版	2018.05.15

1. 緒論 (Introduction)

本平台 IoT 可信賴架構主要以一般家庭環境為考量，此環境內可分為三類角色：家庭成員(Home Owner)、訪問者(Roaming Visitors)、家庭內受照顧者(Caregivee)等角色，以物聯網可信賴架構為基礎，發展家庭雲環境身分即服務及隱私保護機制。本平台所需建置之家庭雲端伺服器包含者身分鑑別與權限控管、藍牙傳輸通道安全及資料外洩監控、裝置隱私政策及協商結果保存與查驗、裝置對裝置(M2M)連續性相互鑑別與安全通訊、遠端使用者身分鑑別與服務授權。

第二年(106 年至 107 年)已完成進度是在 IoT 可信賴架構之設計與實作上，呈現以下功能：(1)使用者向伺服器進行資訊存取前，需先透過身分鑑別模組確認使用者身分之合法性；通過身分鑑別後，權限控管模組依照其授權之角色，授予不同層級之資料存取權限。(2)檢測物聯網環境中藍牙傳輸的通道安全及監控資料外洩狀態。(3)使用者在取得物聯網裝置的服務前，可預先了解裝置蒐集個人敏感資訊之目的及裝置提供之個人隱私政策。(4)鑑別感測裝置時，感測裝置與室內閘道器雙方的身分合法性，需以連續性身分鑑別機制加速未來裝置間鑑別連線的速度。(5)驗證使用者權限遠端存取伺服器資料，並確保資料於閘道器與伺服器之間傳輸時的機密性及完整性。

本計畫所建構的 IoT 可信賴架構平台，使用者是以行動穿戴式裝置與智慧型手機存取服務，設定其使用者角色及授予相對應的資料存取權限，透過閘道器讀取個人生理或家庭環境感測之感測資料，並檢測使用者在藍牙傳輸環境是否洩漏敏感資訊，且所有個人生理或家庭環境感測資料皆由佈建於家庭環境的感測器及安裝於受照顧者身上之感測器所提供。本平台之貢獻是提供物聯網環境下的安全資料存取及各角色間身分鑑別功能。

依據本 IoT 可信賴架構平台下列各項子系統將進行各子系統測試以及模組整合測試和接受測試(Acceptance Testing)：

(1) 近端使用者身分鑑別與權限控管模組

(2) 藍牙傳輸通道安全及資料外洩監控模組

(3) 裝置隱私政策及協商結果保存與查驗模組

(4) 裝置對裝置(M2M)連續性相互鑑別與安全通訊模組

(5) 遠端使用者身分鑑別與服務授權模組

1.1 測試範圍 (Scope of Testing)

本 IoT 可信賴架構平台的測試計畫，確認在系統整合前，所有的子系統均可正確輸出並順利整合。因此，將著重於整合測試(Integration Test)與接受度測試(Acceptance Test)，進一步找出本系統中的缺失，測試各個子系統於整合時衝突的情況是否會發生，進行整合測試的相關計畫與內容，並希望透過此文件的規劃與實踐，達到順利測試並正確執行各子系統，以正確完成本模組之系統整合。

1.2 接受準則 (Acceptance Criteria)

本測試計畫需要滿足下列的測試接受準則：

(1) 行動裝置之 Wi-Fi 通訊功能需正常執行。

(2) 角色權限控管模組可控管所有使用者存取資料之權限。

(3) 使用者介面模組可提供使用者讀取資料。

(4) 藍牙傳輸協定安全檢測儀之 Wi-Fi 通訊功能需正常執行。

(5) 取得與接收智慧型行動裝置與智慧型穿戴式裝置間的傳輸封包。

(6) 取得與接收智慧型行動裝置與智慧型穿戴式裝置間的建立連線流程傳輸安全度檢測。

(7) 行動裝置之 BLE 通訊功能需正常執行。

(8) 感測裝置之 BLE 通訊功能需正常執行。

(9) 預先建置所須的區塊鏈系統環境。

(10) 隱私政策查詢模組需事先載入隱私政策。

(11) 閘道器須具備將使用者對於隱私政策選擇的結果成功寫入區塊鏈。

(12) 室內閘道器能正確鑑別感測裝置

(13) 感測裝置能正確鑑別室內閘道器

(14) 感測裝置與室內閘道器可以無誤接收與傳送資料

(15) 身分鑑別模組與連線配對模組以及資料傳輸模組三者可以彼此溝通

(16) 行動裝置之 3G/4G 通訊功能需正常執行。

(17) 使用者能透過身分鑑別模組正確鑑別身份。

(18) 身分鑑別模組能與資料傳輸模組以及加解密模組溝通。

(19) 使用者資料存取時，能夠透過資料傳輸模組安全傳輸。

(20) 各項參數及數據在資料流中能正確的傳遞。

(21) 系統模型可依實際環境變更進行調整。

(22) 測試程序需要依循本測試計畫所訂定的程序進行，且測試結果必須符合預期測試結果方能接受。

(23) 本系統需要對所有列為必要(Critical、Important、Desirable)之需求進行完整測試。

(24) 測試程序需要依照本測試計畫所訂定的程序進行，所有測試結果需要能符合系統需求規格書預期測試結果方能接受。

(25) 以測試案例為單位，當測試未通過時，需要進行該單元的測試，其接受的準則與前一項之規定相同。

2. 測試環境 (Testing Environment)

如圖 1 為 IoT 可信賴架構平台進行測試的環境描述：

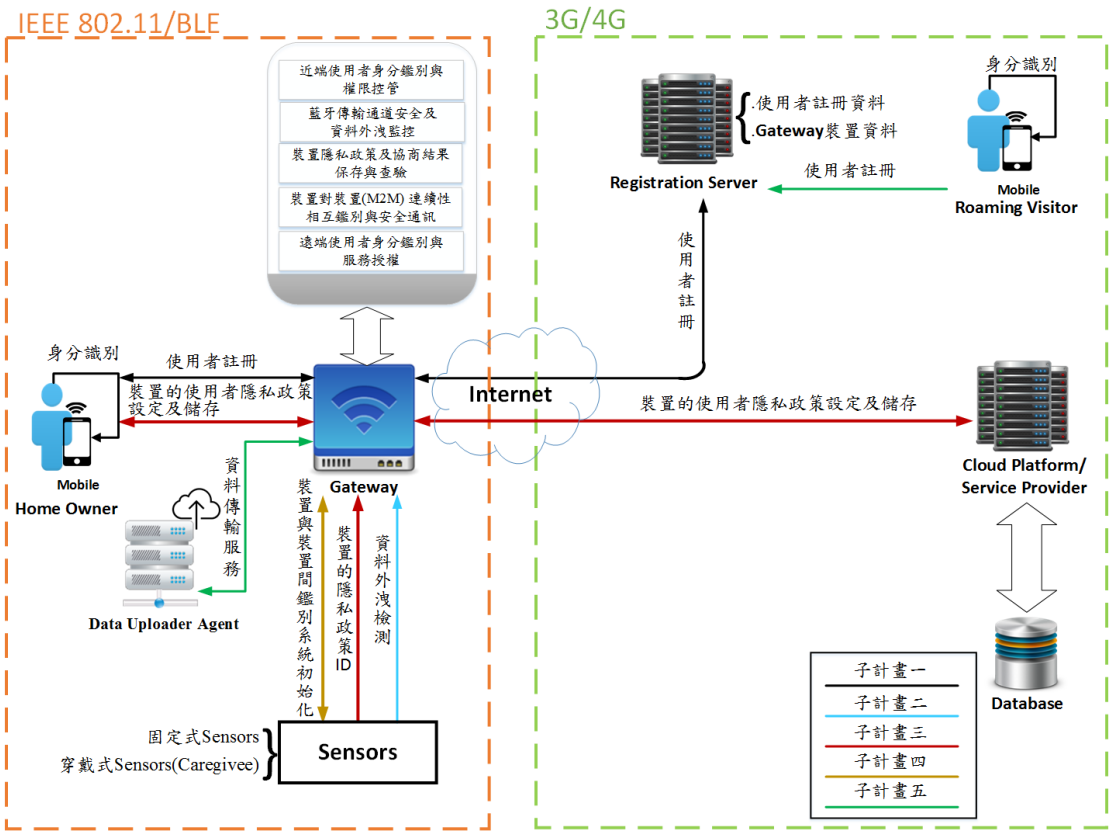


圖1. IoT 可信賴架構之設計與實作-系統設置初始化架構圖

2.1 硬體規格 (Hardware Specification)

依據圖 1 測試環境架構圖內容，進行測試之硬體規格說明，如下列所示：

(1) 使用者端(Home Owner/Roaming Visitor/Service User)：包含角色權限控管模組、角色鑑別模組、使用者裝置隱私協商模組與使用者介面模組

- 智慧型裝置：ZenFone 3
- 處理器：Snapdragon™ 625 @2.0Ghz
- 記憶體：3GB LPDDR3
- 儲存空間：32GB

(2) 閘道器端(Gateway)：包含資料傳輸模組、資料存取模組、身分鑑別模組、藍牙安全狀態檢視模組、裝置對裝置資料傳輸模組

- 設備名稱：NVIDIA Shield TV Pro
- 作業系統：Android 7.0 (Nougat)

- 處理器：NVIDIA® Tegra® X1 processor with a 256-core GPU
- 記憶體：3GB
- 儲存空間：500GB
- 支援無線連接：802.11ac 2x2 MIMO 2.4 GHz and 5 GHz Wi-Fi / Bluetooth 4.1(BLE) / Captive Portal support

(3) 感測器(Sensor)裝置：包含裝置隱私政策模組、感測裝置連線配對模組、傳輸安全狀態檢視模組

- Arduino Uno

  處理器：Atmel ATmega328p
  SRAM：2Kbytes
  Flash：32Kbytes
- 藍牙模組：HM-10CC2541 SensorTag：溫濕度感測
- Ubertooth-One

  處理器：LPC175x ARM Cortex-M3 microcontroller
  RF 晶片：德州儀器 CC2591、CC2400
  IO：RP-SMA RF connector、USB A plug、10-pin 50-mil JTAG 除錯腳位

(4) 雲端平台(Cloud Platform)伺服器：包含隱私政策協商模組、遠端身分鑑別模組

- CPU：Intel Core i7-3770 3.40 GHz
- RAM：8 GB
- 硬碟空間：500GB

2.2 軟體規格 (Software Specification)

依據圖 1 測試環境架構圖內容，測試環境之軟體規格說明，如下列所示：

(1) 閘道器端(Gateway)

- 開發板：Raspberry Pi 3 Model B
- 作業系統：Android 7.1.2
- 資料庫版本：MYSQL 5.6.19
- 應用程式開發語言：Java

(2) 雲端平台(Cloud Platform)伺服器

- 作業系統：Windows 10 64bits

- 網頁伺服器：Java Servlet/ JSP、Apache Tomcat 7.0.78
- 應用程式開發語言：Java 1.8.0_131
- 資料庫版本：MYSQL 5.7.18
- 應用程式開發語言：Java

(3) 感測器(Sensor)裝置

- 開發板：Arduino Uno
- 開發版系統版本：S132 3.1.0
- 應用程式開發語言：C
- 開發板：Ubertooth-One
- 開發版系統版本：
- 應用程式開發語言：C

(4) 智慧型裝置手機

- 手機作業系統：Android 7.0
- 應用程式開發語言：Java

2.3 測試資料來源 (Test Data Sources)

測試項目	數量	測試來源
註冊功能	一組	最高權限使用者創建一般使用者帳戶
登入功能	一組	可登入並鑑別已創建之帳戶
讀取資料功能	兩組	可向閘道器取得相關資訊
權限控管功能	一組	可控管使用者之讀取資訊權限
帳號密碼	四組	自行設定之帳號
感測器隱私政策	一組	感測器所預先寫入的範例隱私政策。

3. 測試時程、程序與責任(Testing Schedule, Procedure, Responsibility)

3.1 測試時程 (Testing Schedule)

(1) 時程

測試項目	時間
各子系統之內部元件整合測試 (Module Test)	2018/03/19~2018/05/31
ITA 系統整合測試 (Integration Test)	2018/06/01~2018/06/22
ITA 系統接受度測試 (Acceptance Test)	2018/06/23~2018/07/28

(2) 查核

測試項目	時間
各子系統之內部元件整合測試 (Module Test)	2018/06/01
ITA 系統整合測試 (Integration Test)	2018/06/23
ITA 系統接受度測試 (Acceptance Test)	2018/07/29

3.2 測試程序 (Testing Procedure)

各子系統的元件測試，由各子系統的開發負責人執行。待各子系統整合完成後，由全體人員協同執行整體計畫的整合測試。

3.2.1 整合測試(Integration Testing)

IoT 可信賴架構之設計與實作之使用案例(Use Case)，以測試近端使用者身分鑑別與權限控管、藍牙傳輸通道安全及資料外洩監控、裝置隱私政策及協商結果保存與查驗、裝置對裝置(M2M)連續性相互鑑別與安全通訊、遠端使用者身分鑑別與服務授權之整合為目的。

- **模組一(近端使用者身分鑑別與權限控管)如下圖所示：**

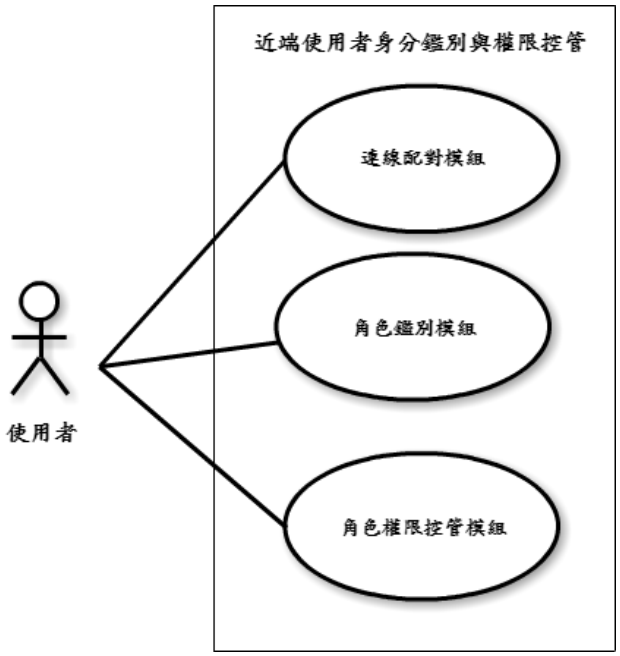


圖2.近端使用者身分鑑別與權限控管模組之使用案例

圖3.近端使用者身分鑑別與權限控管模組之接受度測試

✓ 模組二(藍牙傳輸通道安全及資料外洩監控)如下圖所示：

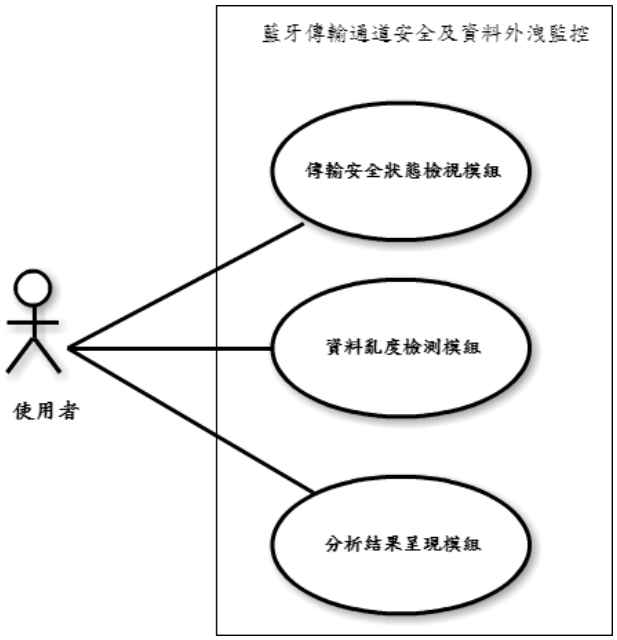


圖4. 藍牙傳輸通道安全及資料外洩監控模組之使用案例

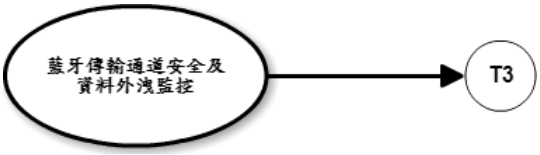


圖5. 藍牙傳輸通道安全及資料外洩監控模組之接受度測試

✓ 模組三(裝置隱私政策及協商結果保存與查驗)如下圖所示：

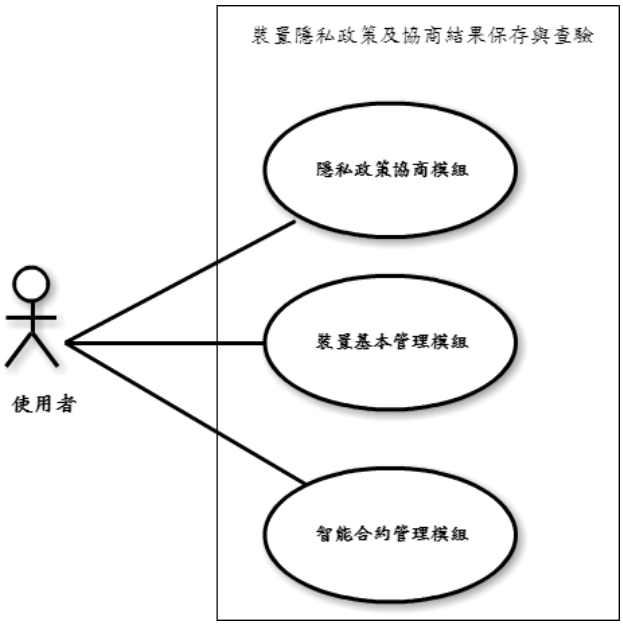


圖6.裝置隱私政策及協商結果保存與查驗模組之使用案例

圖7.裝置隱私政策及協商結果保存與查驗模組測試

✓ 模組四(裝置對裝置連續性相互鑑別與安全通訊)如下圖所示：

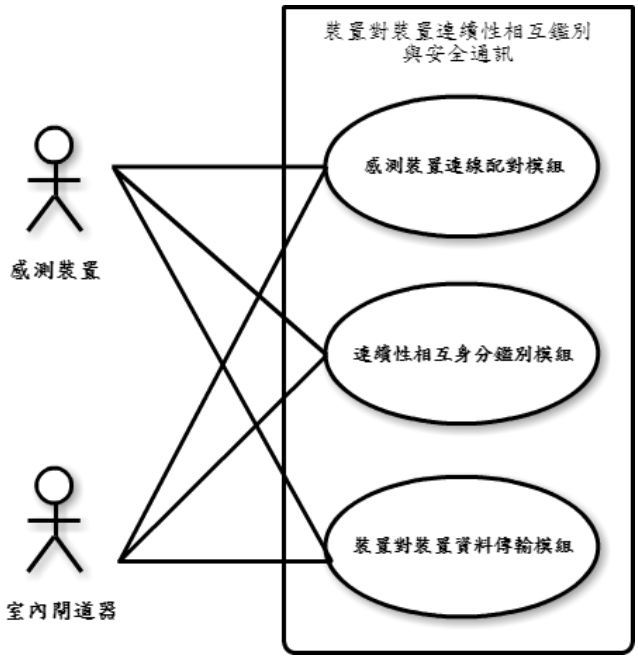


圖8. 裝置對裝置連續性相互鑑別與安全通訊模組之使用案例

圖9. 裝置對裝置連續性相互鑑別與安全通訊模組之接受度測試

✓ 模組五(遠端使用者身分鑑別與服務授權)如下圖所示：

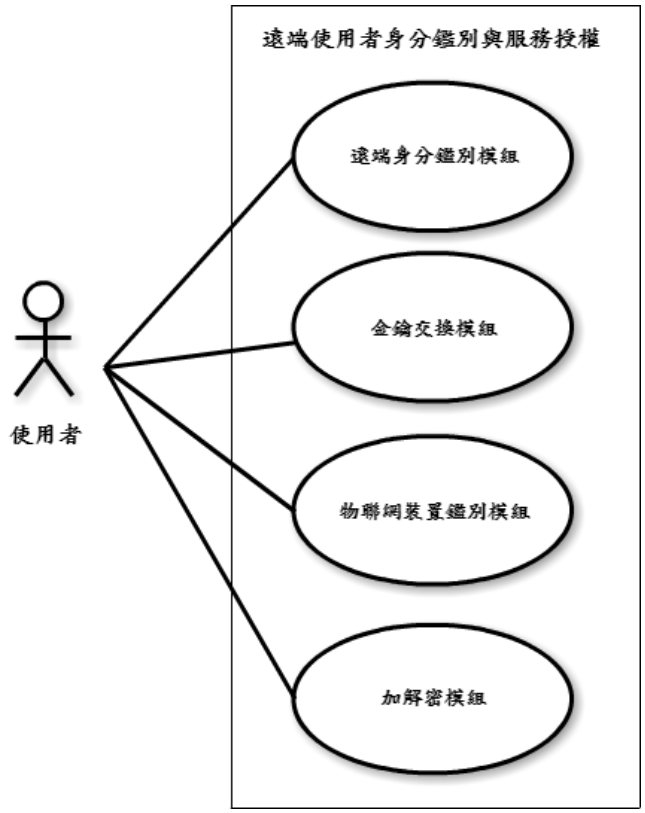


圖10. 遠端使用者身分鑑別與服務授權模組之使用案例

圖11. 遠端使用者身分鑑別與服務授權模組之接受度測試

3.3 人員職責分配 (Personnel Responsibility Assignment)

表1. 人員職責分配表

Testing Activities	Personnel
Acceptance Testing (AT1)	藍袖瑛 黃婷瑋
Acceptance Testing (AT2)	藍袖瑛 陳俊佑
Acceptance Testing (AT3)	藍袖瑛 黃婷瑋 陳俊佑 李奕欣
Integration Testing (IT1)	高慧媛 李雅雯 謝家蓉
Integration Testing (IT2)	郭峻鴻 李宇正
Integration Testing (IT3)	陳俊甫 徐梓洋 黃子嘉 彭偉慶
Integration Testing (IT4)	徐梓洋 黃子嘉
Integration Testing (IT5)	徐梓洋 黃子嘉 彭偉慶
Integration Testing (IT6)	莊祐軒 黎哲宇 洪麒鈞 賴孟泫 詹哲宇
Integration Testing (IT7)	許仁傑 蘇勤文 劉子源 莊禾暘 鄭禮呈 蔡亞哲

3.3.1 接受測試 (Acceptance Testing)

本計畫將進行使用者相關資訊進行系統測試，系統測試流程如下：

使用者(Home Owner/Roaming Visitor/Service User)：當使用者註冊時，需向行動裝置輸入身分之機敏資料，Home Owner 將會透過權限控管模組依照其授權之角色，授予不同層級之資料存取權限。在使用者裝置隱私政策協商模組會先取得裝置 ID 並連線到區塊鏈取得完整的隱私政策。接著，透過使用者介面模組將隱私政策呈現給訪客決定是否接受該裝置的隱私政策，訪客可以透過閘道器對於裝置的隱私政策表達同意或拒絕，同時也能夠掌控系統會蒐取訪客的哪些資訊，選取完畢後，隱私政策協商模組會將使用者的隱私選擇產生 HMAC 並存入區塊鏈中，之後訪客可依此隱私政策進行選擇並取得相對應物聯網裝置服務。

感測裝置(Sensor)：感測裝置在進行連線配對時向閘道器進行註冊，感測裝置傳送其裝置識別碼至室內閘道器，再由室內閘道器產生秘密金鑰且安全地將秘密金鑰回傳至感測裝置。當室內閘道器對感測裝置進行身分鑑別，將其確認訊息是否由合法的感測裝置傳送至室內閘道器，並驗證訊息是否有被竄改。完成室內閘道器對感測裝置進行身分鑑別之後，感測裝置亦會對室內閘道器進行身分鑑別，故達成雙向性的身分鑑別。當雙向的靜態身分鑑別成功後，在一定的時間週期內每次傳送感測資料會進行一次連續性身分鑑別以確保資料是經由合法的感測裝置傳輸並且訊息沒有竄改，當過了設定時間週期後會再次啟動靜態身分鑑別階段，以確保感測裝置及訊息的完整性

閘道器(Gateway)：使用者註冊後，為確保裝置雙方的身分合法性，欲驗證通訊之感測裝置與室內閘道器雙方的身分合法性，以確保訊息之真實性，行動裝置向閘道器進行相互鑑別後，進行資料存取，確保感測裝置與閘道器間能正常地傳送與接收資料，並透過 Raspberry Pi3 運行傳輸安全狀態模組以及封包檢測模組擷取穿戴式裝置傳輸的封包，經安全檢測模組分析確認穿戴式裝置與行動裝置建立安全連線，提醒使用者所持有的行動裝置及穿戴裝置所處的連線模式是否安全。

註冊伺服器(Registration Server)：當使用者註冊時，伺服器會收到使用者申請註冊的資料，伺服器會向區塊鏈(BlockChain)申請一組公私鑰對(基於 secp256k1 之橢圓曲線)。在申請成功後，伺服器會將其公鑰(PK_U)和使用者申請註冊資料一併存下，並回傳這組公私鑰對給使用者；此後伺服器在傳遞資料給使用者時，資料

都會先經過使用者的公鑰加密再傳給使用者，收到資料的使用者可透過自己的私鑰(SK_U)解開伺服器傳來的密文。

雲端平台(Cloud Platform)：當遠端使用者欲取得資料時，須先進行身分驗證，驗證通過後，閘道器傳送票據給遠端使用者及雲端資料庫，以便遠端使用者及伺服器溝通取得資料，其中遠端使用者、閘道器以及雲端資料庫三者之間的傳輸資料皆透過加解密傳輸模組進行加密以防止敏感資料遭到竊取。

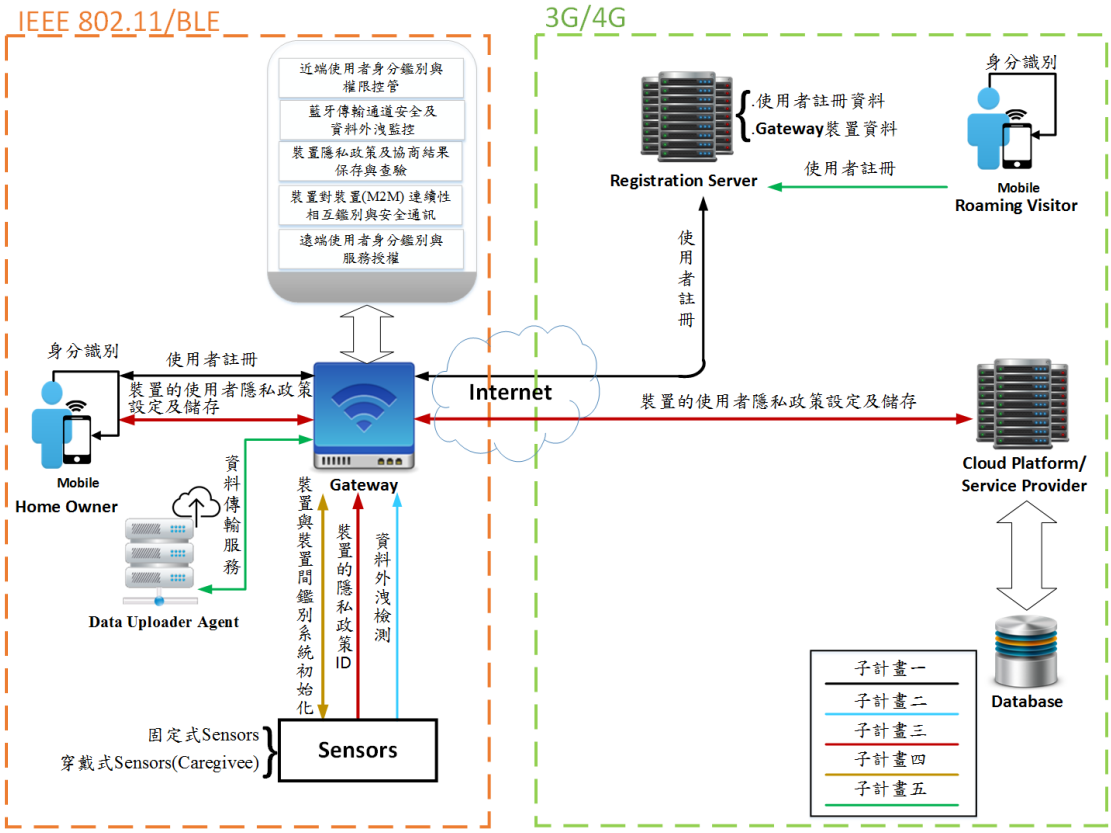


圖12.　IoT 可信賴架構之設計與實作系統流程

再者，將進行系統接受測試，其次序為：AT1→AT2→AT3，AT1 驗證系統使用者身分鑑別與權限控管與遠端使用者資料存取可正確輸出並順利整合運作，AT2 分析各系統的藍牙傳輸安全狀態檢視與裝置隱私政策及裝置對裝置連性續相互鑑別明確列出相關安全與分析，AT3 各子系統需正確執行並符合系統需求規格書[1]之預期測試結果。

ITA：IoT 可信賴架構之設計與實作

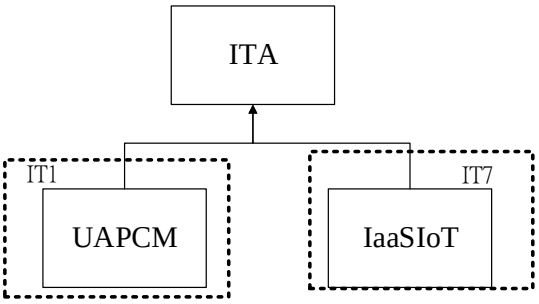
UAPCM：近端使用者身分鑑別與權限控管

SBAN：藍牙傳輸通道安全及資料外洩監控

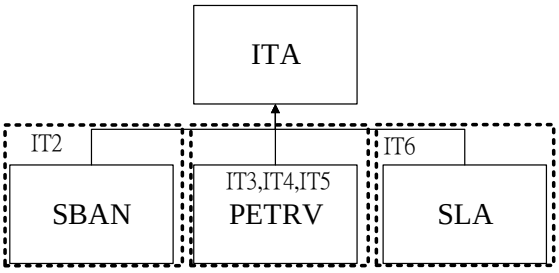
PETRV：裝置隱私政策及協商結果保存與查驗

SLA：裝置對裝置(M2M)連續性相互鑑別與安全通訊

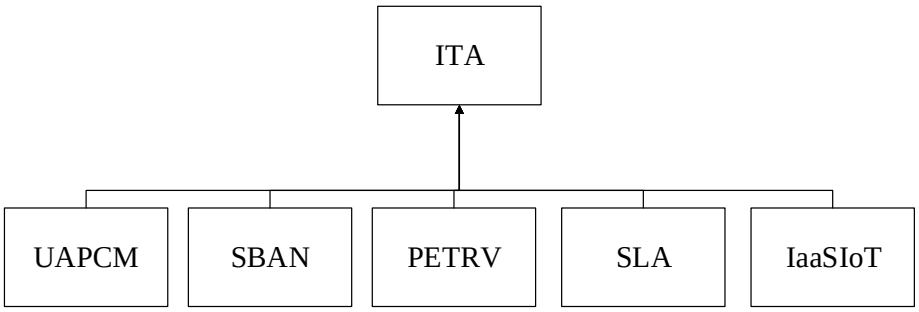
IaaSTIoT：遠端使用者身分鑑別與服務授權



(a)接受度測試 AT1



(b)接受度測試 AT2



(c)接受度測試 AT3

圖13.　IoT 可信賴架構之設計與實作系統整合與可接受度測試架構圖

4. 測試案例 (Test Cases)

4.1 整合測試案例 (Integration Testing Cases)

4.1.1 IT1 測試案例

目的：

(1) 驗證使用案例 1。

(2) Home Owner 設定成員之角色權限。

(3) 使用者透過 Wi-Fi 連接閘道進行使用者之身分鑑別。

(4) 使用者依其權限存取資料並瀏覽即時資料與歷史資料。

表2. IT1 測試案例

Identification	IT1	
Name	近端使用者身分鑑別與權限控管模組	
Tested target	UAPCM	
Reference	UAPCM-UIR-001、UAPCM-UIR-002、UAPCM-UIR-002、UAPCM-UIR-004、UAPCM-EIR-001	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1.開啟 App	
		2.帳號及密碼輸入頁面
	3.輸入帳號及密碼	
		4.透過 Wi-Fi 與閘道器連線，並透過身分鑑別模組驗證使用者資料
	5.登入成功後，顯示功能選單	
	6.選擇功能選單中的成員管理	
		7.顯示成員管理
	8.可查詢成員角色與修改其權限	
Expected result	1.能正確鑑別使用者身分 2.能對使用者進行身分權限控管 3.能正確存取即時資料	
Cleanup	無	

4.1.2 IT2 測試案例

目的：

(1) 驗證使用案例 2。

(2) 驗證封包檢測模組是否能測錄智穿戴裝置與智慧型行動裝置傳輸。

(3) 驗證安全檢測模組是否能分析測錄封包。

(4) 驗證亂度檢測模組是否能分析傳輸封包。

表3. IT2 測試案例

Identification	IT2	
Name	行動閘道器上之安全人體區域網路之整合測試	
Tested target	SBAN	
Reference	SBAN-UIR-001、SBAN-EIR-001、SBAN-EIR-002、SBAN-EIR-003	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1.行動閘道器傳輸 App 應用程式	
	2.穿戴式裝置與行動閘道器進行配對	
		3.系統擷取傳輸封包資料
		4.傳送至後端檢測伺服器檢測過程是否採用具洩漏風險之配對方式，並回傳分析結果
	5.穿戴式裝置與行動閘道器進行資料傳輸	
		6.系統擷取傳輸封包資料
		7.傳送至後端檢測伺服器檢測傳輸資料是否可通過 NIST-SP-800-22 亂度檢測，並回傳分析結果
	8.使用者檢視分析成果	
Expected result	1.進行配對後可以驗證智慧型穿戴裝置與智慧型行動裝置彼此連線封包是否可被側錄 2.在安全的狀況下進行資料傳輸 3.為經加密之傳輸資料是否通過亂度檢測	
Cleanup	無	

4.1.3 IT3 測試案例

目的：

(1) 驗證使用案例 3。

(2) Home Owner 新增 IoT 裝置到閘道器上，並建立 IoT 裝置的智能合約管理相關資訊與其使用者隱私政策。

表4. IT3 測試案例

Identification	IT3	
Name	隱私政策協商模組、智慧合約管理模組	
Tested target	PETRV	
Reference	PETRV-EIR-001、PETRV-EIR-002、PETRV-EIR-003、PETRV-EIR-004	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1. Home Owner 向 Blockchain Network 發出 Transaction，上傳裝置資訊與其使用者隱私政策	
		2.回傳該 Transaction ID
	3.利用 Transaction ID 建立 IoT 裝置的智能合約	
		4.取得 IoT 裝置的智能合約的位址
	5. Home Owner 透過閘道器的智能合約與 IoT 裝置智能合約的位址發出綁定要求	
		6. Home Owner 同意綁定要求，回傳綁定成功訊息
Expected result	Home Owner 可以上傳裝置相關資訊與隱私政策到區塊鏈	
Cleanup	無	

4.1.4 IT4 測試案例

目的：

(1) 驗證使用案例 4。

(2) 訪客取得周邊裝置相關資訊。

表5. IT4 測試案例

Identification	IT4	
Name	裝置基本管理模組	
Tested target	PETRV	
Reference	PETRV-EIR-001、PETRV-EIR-002、PETRV-EIR-003、PETRV-EIR-004	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1.訪客向 Gateway 發出裝置發現請求	
		2.AM 模組確認訪客權限
		3.DC 模組連結到 Blockchain Network 將儲存在區塊鏈中已連接到 Gateway 的裝置資訊回傳給使用者
Expected result	使用者(Home Owner 及 Roaming Visitor)可以取得裝置資訊及相關隱私政策	
Cleanup	無	

4.1.5 IT5 測試案例

目的：

(1) 驗證使用案例 5。

(2) 訪客使用智慧型手機連結到 Gateway，Gateway 會顯示目前可以連接的 IoT 裝置並取得儲存在區塊鏈中的裝置相關資訊與使用者隱私政策提供給訪客，然後訪客針對取得的隱私政策表達隱私選擇並取得共識，最後透過 Gateway 加密後儲存進區塊鏈中。

表6. IT5 測試案例

Identification	IT5	
Name	隱私政策協商模組、智慧合約管理模組	
Tested target	PETRV	
Reference	PETRV-EIR-001、PETRV-EIR-002、PETRV-EIR-003、PETRV-EIR-004	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1.訪客使用智慧型手機連結到 Gateway	
		2.Gateway 顯示目前已連結且可使用的裝置
	3.訪客選擇欲使用的裝置，連結到該裝置的智能合約並透過裝置 ID 取得儲存在區塊鏈中的裝置相關資訊與使用者隱私政策	
		4.訪客連結到 Gateway 對裝置的隱私政策表達同意或拒絕
	5.Gateway 將使用者的隱私選擇加密後儲存至區塊鏈中	
		6.訪客確認協商結果，接著根據取得的權限與訪客表達的隱私選擇使用相對應的 IoT 裝置服務
Expected result	使用者(訪客)能和 Gateway 進行隱私協商，並且將協商結果儲存至區塊鏈	
Cleanup	無	

4.1.6 IT6 測試案例

目的：

(1) 驗證使用案例 6。

(2) 驗證感測裝置是否能正確鑑別室內閘道器。

(3) 驗證室內閘道器是否能正確鑑別感測裝置。

(4) 驗證感測裝置與室內閘道器之間的資料傳輸是否能正常傳送與接收。

表7. IT6 測試案例

Identification	IT6	
Name	物聯網裝置與室內閘道器之感測層鑑別與安全通訊技術模組(SLA)之整合測試	
Tested target	SLA	
Reference	SLA-FNR-001、SLA-FNR-002、SLA-FNR-003	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1. 在初始化階段時，必須為感測裝置與閘道器設定參數。首先，感測裝置必須透過安全通道傳送其識別碼至閘道器	
		2. 閘道器接收到感測裝置的請求後，將產生秘密值。並將該秘密值透過安全通道送回感測節點
	3. 感測裝置收到秘密值後，該秘密值將被儲存於安全空間	
		4. 閘道器將感測裝置之識別碼、秘密值、鑑別週期紀錄至對應的資料庫或對應表(Mapping Table)
	5. 於靜態鑑別階段時，感測節點將使用 Real-time clock 產生遮蔽值，再利用該遮蔽值與中介變數產生 HMAC，最後再將識別碼與先前所產生之中介變數傳送至閘道器	
		6. 閘道器收到來自感測裝置的資料時，將利用資料庫來檢索相應的秘密值，再使用識別碼來計算

		出中介變數之對應值，並對照該對應值與中介變數是否相等，倘若相等，閘道器將會利用該裝置之識別碼檢索相應的鑑別週期，並利用隨機數經過數次計算後產生中介變數與初始符記，並將初始符記儲存於資料庫中，再將各中介變數傳送至感測裝置
	7. 當感測裝置收到閘道器傳送之資料，將使用秘密值產生中介變數，用以與閘道器所傳送之資訊對照是否相等，倘若相等，則代表鑑別成功，並將初始符記儲存至安全空間。感測裝置將可在鑑別週期內對每筆所傳輸的資料進行連續性鑑別	
	8.完成靜態鑑別後，當感測裝置欲傳送資料至閘道器時，需進行連續性鑑別，該鑑別將利用隨機數與初始符記產生 Real-time clock 的遮蔽值，再計算靜態鑑別階段的中介變數來遮蔽所感測之資料，最後再產生 HMAC，並傳送中介變數、遮蔽的感測資料與識別碼至閘道器	
		9. 閘道器接收到感測裝置的資料後，必須先確認所接收訊息是否為當前鑑別週期中所產生，倘若超出當前的鑑別週期，將必須再次進行靜態鑑別。反之，閘道器將根據所接收之識別碼與初始符記來計算出對應值來驗證資料之完整性，倘若對應值與接收值相等，則

		代表資料未遭惡意竄改。而後閘道器將產生隨機數，以計算出中介變數與確認訊息，並將該資料傳送至感測裝置
	10. 感測裝置收到來自閘道器的資料後，將利用其接收之資料以驗證感測資料之完整性，倘若感測資料完整，且連續性鑑別在有效之鑑別週期內，即連續性鑑別成功	
		11. 室內閘道器持續將接收的感測資料存入資料庫中。每過一段特定的時間，室內閘道器會把感測資料傳送至雲端伺服器
Expected result	1.完成靜態鑑別後，當感測裝置與閘道器欲傳送資料時，必須進行連續性鑑別 2.在鑑別期間內，連續性鑑別可以保證資料完整性與裝置之合法性 3.閘道器可接收來自感測裝置所蒐集之感測資料	
Cleanup	無	

4.1.7 IT7 測試案例

目的：

(1) 驗證使用案例 7。

(2) 使用者透過身分驗證模組將帳號密碼傳至伺服器，檢測伺服器需正確收到資料，並驗證使用者身分是否正確。

(3) 伺服器若驗證使用者身分正確，則回傳 Token。

(4) 使用者傳送取得資料的需求(包含 ID 及加密後的 Token)至伺服器，伺服 器需正確收到資料，並驗證所傳來資料中的 Token 是否正確。

(5) 伺服器驗證正確則回傳資料。

表8. IT7 測試案例

Identification	IT7	
Name	遠端使用者身分鑑別與服務授權模組登入並取得資料功能	
Tested target	IaaSTIoT	
Reference	IaaSIoT-FNR-001、IaaSIoT-FNR-002、IaaSIoT-FNR-003	
Severity	Level 1 (Critical)	
Instructions	*Actor actions*	*System responses*
	1.使用者輸入帳號密碼進行登入	
		2.系統收到資料後，進行身分比對，回傳 Token
	3.使用者按下取得即時資料按鈕，傳送取得資料的需求至伺服器	
		4.伺服器驗證 Token 是否正確，並回傳結果
	5.使用者按下取得歷史資料按鈕，傳送取得資料的需求至伺服器	
		6.伺服器驗證 Token 是否正確，並回傳結果
Expected result	使用者可進入取得資料頁面	
Cleanup	無	

4.2 接受測試案例 (Acceptance Testing Cases)

4.2.1 AT1 測試案例

目的：

(1) 驗證 UAPCM、IaaSIoT 能依流程正確整合運作。

(2) Home Owner 設定成員之角色權限。

(3) 使用者透過 Wi-Fi 連接閘道進行使用者之身分鑑別。

(4) 使用者依其權限存取資料並瀏覽即時資料與歷史資料。

(5) 使用者透過身分驗證模組將帳號密碼傳至伺服器，檢測伺服器需正確收到資料，並驗證使用者身分是否正確。

(6) 伺服器若驗證使用者身分正確，則回傳 Token。

(7) 使用者傳送取得資料的需求(包含 ID 及加密後的 Token)至伺服器，伺服 器需正確收到資料，並驗證所傳來資料中的 Token 是否正確。

(8) 伺服器驗證正確則回傳資料。

表9. AT1 測試案例

Identification	AT1
Name	UAPCM、IaSIoT 整合至 ITA
Tested target	UAPCM、IaaSIoT
Reference	UAPCM-UIR-001 、 UAPCM-UIR-002 、 UAPCM-UIR-002 、 UAPCM-UIR-004 、 UAPCM-EIR-001 、 IaaSIoT-FNR-001 、 IaaSIoT-FNR-002、IaaIoT-FNR-003
Severity	Level 2 (Critical)
Instructions & Expected result	1. 使用者開啟 App 及輸入帳號、密碼進行登入 2. 系統收到資料後，進行身分比對，回傳 Token 3. 登入成功後，使用者取得資料頁面，選擇讀取即時資料或歷史資料，傳送取得資料的需求至伺服器 4. 伺服器驗證 Token 是否正確，並回傳結果
Cleanup	無

4.2.3 AT2 測試案例

目的：

(1) 驗證 SBAN、PETRV、SLA 能正確執行風險評估功能。

(2) 驗證封包檢測模組是否能測錄智穿戴裝置與智慧型行動裝置傳輸。

(3) Home Owner 新增 IoT 裝置到閘道器上，並建立 IoT 裝置的智能合約管理相關資訊與其使用者隱私政策。

(4) 訪客使用智慧型手機連結到 Gateway，Gateway 會顯示目前可以連接的 IoT 裝置並取得儲存在區塊鏈中的裝置相關資訊與使用者隱私政策提供給訪客，然後訪客針對取得的隱私政策表達隱私選擇並取得共識，最後透過 Gateway 加密後儲存進區塊鏈中。

(5) 驗證感測裝置是否能正確鑑別室內閘道器。

(6) 驗證室內閘道器是否能正確鑑別感測裝置。

(7) 驗證感測裝置與室內閘道器之間的資料傳輸是否能正常傳送與接收。

表10. AT2 測試案例

Identification	AT2
Name	SBAN、PETRV、SLA 整合至 ITA
Tested target	SBAN、PETRV、SLA
Reference	SBAN-UIR-001 、 SBAN-EIR-001 、 SBAN-EIR-002 、 SBAN-EIR-003 、 PETRV-EIR-001 、 PETRV-EIR-002 、 PETRV-EIR-003 、 PETRV-EIR-004 、 SLA-FNR-001 、 SLA-FNR-002、SLA-FNR-003
Severity	Level 2 (Important)
Instructions & Expected result	1. 當穿戴式裝置與行動閘道器進行資料傳輸 2. 系統將擷取傳輸封包資料，傳送至後端檢測伺服器檢測傳輸資料是否可通過NIST-SP-800-22亂度檢測，並回傳分析結果，使用者檢視傳輸狀態分析後結果 3. Home Owner向Blockchain Network發出Transaction，上傳裝置資訊與其使用者隱私政策，系統將回傳該Transaction ID，使用者利用Transaction ID建立IoT裝置的智能合約，系統取得IoT裝置的智能合約的位址 4. Home Owner透過閘道器的智能合約與IoT裝置智能合約的位址發出綁定要求，Home Owner同意綁定要求，回傳綁定成功訊息 5. 當訪客使用智慧型手機連結到Gateway 6. Gateway顯示目前已連結且可使用的裝置

	7. 訪客選擇欲使用的裝置，連結到該裝置的智能合約並透過裝置ID取得儲存在區塊鏈中的裝置相關資訊與使用者隱私政策，訪客連結到Gateway對裝置的隱私政策表達同意或拒絕，Gateway將使用者的隱私選擇加密後儲存至區塊鏈中 8. 訪客確認協商結果，接著根據取得的權限與訪客表達的隱私選擇使用相對應的IoT裝置服務 9. 在初始化階段時，必須為感測裝置與閘道器設定參數。首先，感測裝置必須透過安全通道傳送其識別碼至閘道器 10. 閘道器將感測裝置之識別碼、秘密值、鑑別週期紀錄至對應的資料庫或對應表(Mapping Table) 11. 當感測裝置收到閘道器傳送之資料，將使用秘密值產生中介變數，用以與閘道器所傳送之資訊對照是否相等，倘若相等，則代表鑑別成功，並將初始符記儲存至安全空間。感測裝置將可在鑑別週期內對每筆所傳輸的資料進行連續性鑑別 12. 完成靜態鑑別後，當感測裝置與閘道器欲傳送資料時，必須進行連續性鑑別 13. 在鑑別期間內，連續性鑑別可以保證資料完整性與裝置之合法性
Cleanup	無

4.2.4 AT3 測試案例

目的：

(1) 在 AT1 與 AT2 測試成功的基礎上，再次重覆驗證 UAPCM、IaaSIoT、SBAN、PETRV、SLA 能正確地整合於 ITA 架構。

(2) 驗證 ITA 所有功能與流程能正確整合運作。

表11. AT3 測試案例

Identification	AT3
Name	UAPCM、IaaSIoT、SBAN、PETRV、SLA 整合至 ITA
Tested target	UAPCM、IaaSIoT、SBAN、PETRV、SLA
Reference	UAPCM-UIR-001、UAPCM-UIR-002、UAPCM-UIR-002、UAPCM-UIR-004、UAPCM-EIR-001、SBAN-UIR-001、SBAN-EIR-001、SBAN-EIR-002、SBAN-EIR-003、PETRV-EIR-001、PETRV-EIR-002、PETRV-EIR-003、PETRV-EIR-004、SLA-FNR-001、SLA-FNR-002、SLA-FNR-003、IaaSIoT-FNR-001、IaaSIoT-FNR-002、IaaSIoT-FNR-003、
Severity	Level 2 (Important)
Instructions & Expected result	1. 使用者開啟 App 及輸入帳號、密碼進行登入 2. 系統收到資料後，進行身分比對，回傳 Token 3. 登入成功後，使用者取得資料頁面，選擇讀取即時資料或歷史資料，傳送取得資料的需求至伺服器 4. 伺服器驗證 Token 是否正確，並回傳結果 5. 當使用者進行穿戴式裝置與行動閘道器之資料傳輸 6. 系統將擷取傳輸封包資料，傳送至後端檢測伺服器檢測傳輸資料是否可通過 NIST-SP-800-22 亂度檢測，並回傳分析結果，使用者檢視傳輸狀態分析後結果 7. Home Owner 向 Blockchain Network 發出 Transaction，上傳裝置資訊與其使用者隱私政策，系統將回傳該 Transaction ID，使用者利用 Transaction ID 建立 IoT 裝置的智能合約，系統取得 IoT 裝置的智能合約的位址 8. Home Owner 透過閘道器的智能合約與 IoT 裝置智能合約的位址發出綁定要求，Home Owner 同意綁定要求，回傳綁定成功訊息 9. 當訪客使用智慧型手機連結到 Gateway 10. Gateway 顯示目前已連結且可使用的裝置 11. 訪客選擇欲使用的裝置，連結到該裝置的智能合約並透過裝置 ID 取得儲存在區塊鏈中的裝置相關資訊與使用者隱私政策，訪客連結到 Gateway 對裝置的隱私政策表達同意或拒絕，Gateway 將使用者的隱私選擇加密後儲存至區塊鏈中 12. 訪客確認協商結果，接著根據取得的權限與訪客表達的

	隱私選擇使用相對應的 IoT 裝置服務 13. 在初始化階段時，必須為感測裝置與閘道器設定參數。首先，感測裝置必須透過安全通道傳送其識別碼至閘道器 14. 閘道器將感測裝置之識別碼、秘密值、鑑別週期紀錄至對應的資料庫或對應表(Mapping Table) 15. 當感測裝置收到閘道器傳送之資料，將使用秘密值產生中介變數，用以與閘道器所傳送之資訊對照是否相等，倘若相等，則代表鑑別成功，並將初始符記儲存至安全空間。感測裝置將可在鑑別週期內對每筆所傳輸的資料進行連續性鑑別 16. 完成靜態鑑別後，當感測裝置與閘道器欲傳送資料時，必須進行連續性鑑別 17. 在鑑別期間內，連續性鑑別可以保證資料完整性與裝置之合法性
Cleanup	無

5. 測試結果與分析 (Test Results and Analysis)

5.1 整合測試案例 (Integration Testing Cases)

表12. 整合測試案例結果

Test Case #	Results (Pass/Fail)	Comment
IT1	Pass	測試通過
IT2	Pass	測試通過
IT3	Pass	測試通過
IT4	Pass	測試通過
IT5	Pass	測試通過
IT6	Pass	測試通過
IT7	Pass	測試通過

5.2 接受測試案例 (Acceptance Testing Cases)

表13. 接受度測試案例結果

Test Case #	Results (Pass/Fail)	Comment
AT1	Pass	測試通過
AT2	Pass	測試通過
AT3	Pass	測試通過

Appendix A： 追朔表 Traceability

A.1. 子系統 vs. 測試案例 (Subsystems vs. Test Cases)

表14. Subsystems vs. Test Cases Traceability Table

Test Cases / Subsystems	IT1	IT2	IT3	IT4	IT5	IT6	IT7
UAPCM-UIR-001	✓						
UAPCM-UIR-002	✓						
UAPCM-UIR-004	✓						
UAPCM-EIR-001	✓						
SBAN-UIR-001		✓					
SBAN-EIR-001		✓					
SBAN-EIR-002		✓					
SBAN-EIR-003		✓					
PETRV-EIR-001			✓	✓	✓		
PETRV-EIR-002			✓	✓	✓		
PETRV-EIR-003			✓	✓	✓		
PETRV-EIR-004			✓	✓	✓		
SLA-FNR-001						✓	
SLA-FNR-002						✓	
SLA-FNR-003						✓	
IaaSIoT-FNR-001							✓
IaaSIoT-FNR-002							✓
IaaSIoT-FNR-003							✓

.

A.2. 需求 vs. 測試案例 (Requirements vs. Test Cases)

表15. Requirements vs. Test Cases Traceability Table

Test Cases / Requirements	UAPCM	SBAN	PETRV	SLA	IaaSIoT
AT1	✓				✓
AT2		✓	✓	✓	
AT3	✓	✓	✓	✓	✓

Appendix B： 參考資料 (References)

[1] 國立台灣科技大學吳宗成教授研究團隊，IoT 可信賴架構之設計與實作需求規格書，民國一零六年十二月三十日。