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 Document

實現資訊安全傳輸機制於雲端物聯網架構之研究
Research on implementing information security transmission mechanism in cloud Internet of things architecture

MOST 106-2221-E-163-001

林華乙
陳叡融
中國科技大學 資訊管理學系
Department of Information Management,
China University of Technology

2018/05/15

目錄

版次變更記錄 (Revision History) 1

1. 簡介 (Introduction) 1
    1.1 測試目的 (Purpose of Testing) 2
    1.2 測試範圍 (Scope of Testing) 2
    1.2 接受準則 (Acceptance Criteria) 2
2. 測試環境 (Testing Environment) 3
    2.1 硬體規格 (Hardware Specification). 4
    2.2 軟體規格 (Software Specification) 4
    2.3 測試資料來源 (Test Data Sources) 5
3. 測試時程、程序與責任 (Testing Schedule, Procedure, and Responsibility) 5
    3.1 嵌入式橢圓密碼系統(EECCS) 5
        3.1.1 測試時程 (Testing Schedule) 5
        3.1.2 測試程序 (Testing Procedure) 6
        3.1.3 整合測試 (Integration Testing) 6
        3.1.4 接受測試 (Acceptance Testing) 6
        3.1.5 人員職責分配 (Personnel Responsibilities Assignment) 7
    3.2 橢圓曲線金鑰交換協議(ECDH) 7
        3.2.1 測試時程 (Testing Schedule) 7
        3.2.2 測試程序 (Testing Procedure) 7
        3.2.3 整合測試 (Integration Testing) 8
        3.2.4 接受測試 (Acceptance Testing) 8
        3.2.5 人員職責分配 (Personnel Responsibilities Assignment) 9
    3.3 雲端運算虛擬伺服器平台子系統(CCVMP) 9
        3.3.1 測試時程 (Testing Schedule) 9
        3.3.2 測試程序 (Testing Procedure) 10
        3.3.3 整合測試 (Integration Testing) 10
        3.3.4 接受測試 (Acceptance Testing) 10
        3.3.5 人員職責分配 (Personnel Responsibilities Assignment) 11
    3.4 映對聚合資料安全傳輸協定子系統(SMRDTP) 11
        3.4.1 測試時程 (Testing Schedule) 11
        3.4.2 測試程序 (Testing Procedure) 12
        3.4.3 整合測試 (Integration Testing) 12
        3.4.4 接受測試 (Acceptance Testing) 12
        3.4.5 人員職責分配 (Personnel Responsibilities Assignment) 14
    3.5 雲端物聯網資訊安全傳輸協定(ISTMCIT) 14
        3.5.1 測試時程 (Testing Schedule) 14
        3.5.2 測試程序 (Testing Procedure) 14
        3.5.3 整合測試 (Integration Testing) 15
        3.5.4 接受測試 (Acceptance Testing) 15
        3.5.5 人員職責分配 (Personnel Responsibilities Assignment) 16
4. 測試案例 (Test Cases) 16

4.1 整合測試案例 (Integration Testing Cases) 16
4.1.1 嵌入式橢圓密碼系統(EECCS) 16
4.1.1.1 IT1 Test Case 16
4.1.2 橢圓曲線金鑰交換協議(ECDH) 17
4.1.2.1 IT1 Test Case 17
4.1.3 雲端運算虛擬伺服器平台子系統(CCVMP) 17
4.1.3.1 IT1 Test Case 18
4.1.4 映對聚合資料安全傳輸協定子系統(SMRDTP) 18
4.1.4.1 IT1 Test Case 18
4.1.5 雲端物聯網資訊安全傳輸協定(ISTMCIT) 20
4.1.5.1 IT1 Test Case 20
4.2 接受測試案例 (Acceptance Testing Cases) 21
4.2.1 嵌入式橢圓密碼系統(EECCS) 21
4.2.1.1 AT1 Test Case 21
4.2.1.2 AT2 Test Case 22
4.2.1.3 AT3 Test Case 22
4.2.2 橢圓曲線金鑰交換協議(ECDH) 22
4.2.2.1 AT1 Test Case 22
4.2.2.2 AT2 Test Case 23
4.2.2.3 AT3 Test Case 23
4.2.3 雲端運算虛擬伺服器平台子系統(CCVMP) 24
4.2.3.1 AT1 Test Case 24
4.2.3.2 AT2 Test Case 24
4.2.3.3 AT3 Test Case 24
4.2.4 映對聚合資料安全傳輸協定子系統(SMRDTP) 25
4.2.4.1 AT1 Test Case 25
4.2.4.2 AT2 Test Case 25
4.2.4.3 AT3 Test Case 26
4.2.4.4 AT4 Test Case 27
4.2.5 雲端物聯網資訊安全傳輸協定(ISTMCIT) 28
4.2.5.1 AT1 Test Case 28
4.2.5.2 AT2 Test Case 28
4.2.5.3 AT3 Test Case 29
4.2.5.4 AT4 Test Case 29
4.2.5.5 AT5 Test Case 29
5. 測試結果與分析 (Test Results and Analysis) 30
5.1 整合測試案例 (Integration Testing Cases) 30
5.1.1 嵌入式橢圓密碼系統(EECCS) 30
5.1.2 橢圓曲線金鑰交換協議(ECDH) 31
5.1.3 雲端運算虛擬伺服器平台子系統(CCVMP) 31
5.1.4 映對聚合資料安全傳輸協定子系統(SMRDTP) 31
5.1.5 雲端物聯網資訊安全傳輸協定(ISTMCIT) 31
5.2 接受測試案例 (Acceptance Testing Cases) 31
5.2.1 嵌入式橢圓密碼系統(EECCS) 31
5.2.2 橢圓曲線金鑰交換協議(ECDH) 31
5.2.3 雲端運算虛擬伺服器平台子系統(CCVMP) 31

5.2.4 映對聚合資料安全傳輸協定子系統(SMRDTP).....32
5.2.5 雲端物聯網資訊安全傳輸協定(ISTMCIT) 32
Appendix A： 追朔表 Traceability.....33
A.1. 子系統 vs. 測試案例 (Subsystems vs. Test Cases) 33
A.2. 需求 vs. 測試案例 (Requirements vs. Test Cases) 34
Appendix B： Glossary.....36
Appendix C： References 37

版次變更記錄

測試日期	版次變更	測試描述	備註
2017/05/01	1.0	第一版	
2017/05/09	1.1	第二版	

1. 簡介 (Introduction)

本研究計畫雲端物聯網資訊安全傳輸協議主要的目是提出具備資訊安全傳輸之雲端物聯網架構。我們將物聯網端建構在橢圓曲線密碼學框架上，後端結合雲端運算映對聚合門檻分享金鑰資訊安全傳輸協議，使得感測器所接收的資料透過橢圓曲線密碼系統及金鑰交換協議執行資訊安全傳輸，再將資料後送雲端執行映對聚合(Map/Reduce)分散式平行運算。參與運算的感測器除了需通過身分認證外，雲端運算的 Master、Mapper 與 Reducer 彼此透過數位簽章機制確認對方身份以避免遭受仿冒身份者的參與。此外資料切割與合併時，本計畫運用門檻分享秘密金鑰機制與數位簽章方式進行身份驗證及資料完整性驗證，避免資料在運算或傳輸階段遭受到更改。目前各先進國家的企業，皆著手進行資訊系統雲端化，並落實物雲端物聯網資訊安全傳輸環境。

本計劃擬在雲端物聯網實現一個具備資訊安全的傳輸通訊協議的架構，並在測試工作進行期間預擬各項測試計畫，此測試計畫書的目的是為進行測試各項目任務及系統整合所需要準備之事項。本次測試將依據本系統項下各子系統進行個別測試與整合性測試：

- 嵌入式橢圓密碼子系統(Embedded Elliptic Curve Cryptography System, EECCS)
- 橢圓曲線金鑰交換協議子系統(Elliptic Curve Diffie Hellman key exchange protocol, ECDH)
- 雲端運算虛擬伺服器平台子系統 （Cloud Computing Virtual Machine Platform, CCVMP)
- 映對聚合(Map/Reduce)資料安全傳輸協議子系統(Secure Map/Reduce Data Transmission Protocol, SMRDTP)
- 雲端物聯網資訊安全傳輸協定(Information Security Transmission Mechanism in Cloud Internet of Things, ISTMCIT)

1.1 測試目的 (Purpose of Testing)

此計畫書的目的是為進行測試各項目任務及系統整合所需準備之事項。並測試系統各項開發功能與操作介面，確保測試結果皆能運作正常，俾利達到以下的目的：

(1) 定義執行方案為達成系統的『初步測試』(Beta Testing)與『接受測試』(Acceptance Testing)目標作預先的準備。

(2) 與執行人員進行溝通，決定系統的測試策略。

(3) 定義可接受的項目(deliverables)與相關的責任區分(responsible)。

1.2 系統範圍(System Scope)

本計畫研究重點主要在於提出能夠整合物聯網及雲端資訊安全的通訊協定，讓使用端的感應設備或使用者的智慧卡，透過所提出的架構實現雲端物聯網資通訊安全。此資訊安全傳輸機制於雲端物聯網架構（以下簡稱本系統）主要是以橢圓密碼系統為基礎進而實現雲端物聯網之資訊安全傳輸協定。本系統主要由五個部份所組成，分別為嵌入式橢圓密碼系統(EECCS)（子系統一）、橢圓曲線金鑰交換協議(ECDH)（子系統二）、雲端運算虛擬伺服器平台（子系統三）、映對聚合(Map/Reduce)資料安全傳輸協定 (SMRDTP)(子系統四)、雲端物聯網資訊安全傳輸協定(Information Security Transmission Mechanism in Cloud Internet of Things, ISTMCIT)（系統五）。本系統期望實現一個可在 TinyOS 平台上執行的應用程式，並且提供使用者實務作業的環境介面。

1.3 接受準則 (Acceptance Criteria)

本測試計劃需要滿足下面的測試接受準則：

(1) 本系統需要對所有列為必要 (Critical、Important、Desirable) 之需求作完整測試。

(2) 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預期測試結果方能接受。

(3) 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規定相同。

2. 測試環境 (Testing Environment)

本系統我們選用無線感應器、資料收集點、x86 虛擬伺服器及 Ethernet 網路作為雲端物聯網基礎架構。其中物聯網的基礎架構包括下列各元件:(1)嵌入式開發模組，微處理器。(2)感測器擴充基板，感測模組硬體基礎架構。雲端服務平台基礎架構包括下列元件：(1)伺服器，儲存設備及網路基礎架構。(2)虛擬伺服器平台服務，管理資源和整合備份，達到最佳化虛擬伺服器可運用的資源。(3)虛擬組態管理程式，用來虛擬化每個 x86 電腦，組態建構本測試環境採用 WMWare Workstion 來建置虛擬機器。 (4)提供特殊自動化組態功能解決方案及最佳化建置或災難復原等 IT 程序，進行系統測試階段的環境說明，各個場景之測試環境圖如下圖所示：

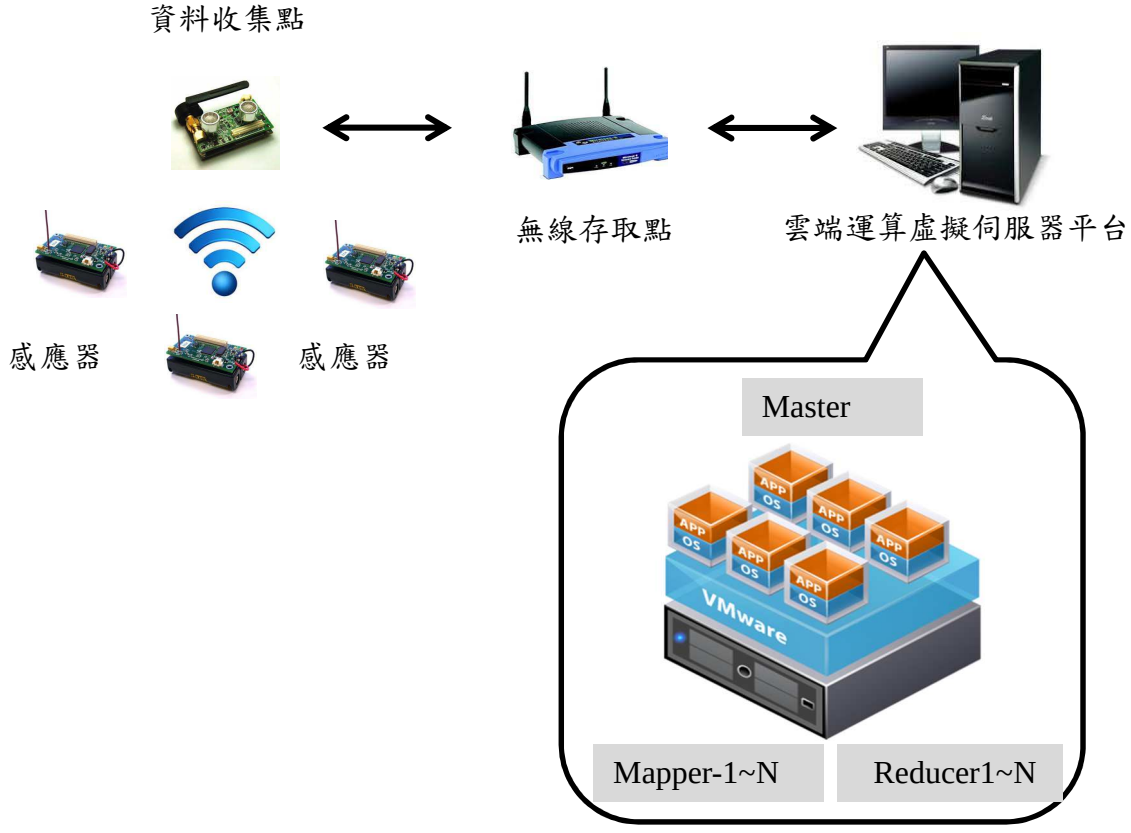

圖 2.1、雲端物聯網資訊安全傳輸(ISTMCIT)架構圖

2.1硬體規格 (Hardware Specification)

項次	設備名稱	數量	規　　格	備註
1	伺服器	1	1. Intel Core I7-3770 四核心處理器 3.4 ~ 3.9GHz，8 線多工， 8MB Level 3 快取，64Bits 指令集。 2. RAM 24GB/2TGB SATA HD/ Windows 7 專業版。 3. VMware Workstation 14。	
2	個人電腦	1	1. Intel Core i5-4210U 雙核心處理器 1.7~2.7GHz，4 線多工，3MB Level 3 快取，64Bits 指令集。 2.RAM 8GB/256GB SSD/1TB USB3.0 HD。 3.Windows 8 個人版。	
3	Embeded Development Board	6	MCU ATmega328 16MHz Flash 32KB RAM 2KB EEP ROM 1KB RF module	
4	Sensor Modules	6	溫度、濕度、GPS、加速度、照度、聲音感測模組	
5	Smart Card/Card Reader	1	智慧卡及讀卡機	
6	有線網路	1	Ethernet Network 10/100Mbps	
7	無線基地台	1	IEEE 802.11/a/b/gn 4Port Switch HUB	

2.2軟體規格 (Software Specification)

項次	設備名稱	數量	規 格	備註
1	Tiny OS	5	2.0	
2	Windows	1	Windows 8 專業版/8 個人版	
3	Virtual Machine	1	VMware Workstation 14	
4	CenOS Linux	1	5.7 64bits	
5	MySQL DB Server	1	5.0	
6	Oracle	1	5.0	
7	Apache Hadoop NextGen MapReduce	1	YARN	

8	Oracle Java Development Kit JDK	1	1.7.0	
9	Cloudera Public GPG Key	1	GPG	
10	Hadoop Distributed File System	1	HDFS	

2.3 測試資料來源 (Test Data Sources)

感測器溫模組(sensor node)所收集的資料傳輸到資料收集端(sink node)之間透過橢圓密碼曲線加解密運算為測試資料。關於測試期間所需的測試資料來源及數量，說明如下：

項次	名稱	測試來源	數量
1	感測模組	溫溼度、光照度等感測資料	感測模組 5 組
2	測試帳號	伺服器管理員	管理員帳號和密碼 3 組
3	測試帳號	資料庫管理員	管理員帳號和密碼 3 組
4	測試伺服器	伺服器 VMWare Workstations	VMWare Workstations 3 台
5	使用者UIA	筆腦	筆電 1 台
6	測試連線	無線基地台802.11 a/b/gn	無線基地台1 台

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

3.1. 嵌入式橢圓密碼系統(EECCS)

3.1.1.測試時程 (Testing Schedule)

時程表

測試項目	時間
各子系統之內部元件整合測試(Module Test)	107/04/01~107/07/01
EECCS 整合測試(Integration Test)	107/04/01~107/07/01
EECCS 接受度測試(AcceptanceTest)	107/04/01~107/07/01

檢核點

測試項目	時間
各子系統之內部元件整合測試(Module Test)	107/05/01
EECCS 整合測試(Integration Test)	107/06/01
EECCS 接受度測試(AcceptanceTest)	107/07/01

3.1.2 測試程序(Testing Procedure)

各子系統之內部元件的整合測試，交由各子系統開發負責人完成，在此我們著重於本系統在嵌入式橢圓密碼系統之架構建置，及系統整合測試與接受度測試。

3.1.3 整合測試(Integration Testing)

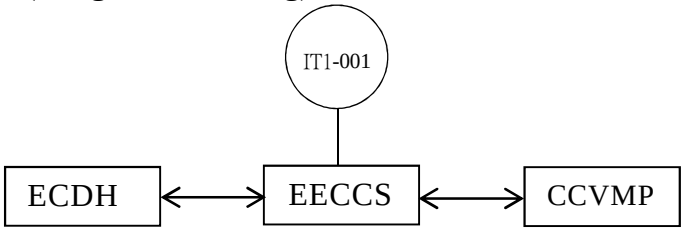

圖 3.1.1、ECCS 整合測試圖

3.1.4 接受測試(Acceptance Testing)

本子系統必須達到下列所述功能：

需求編號	優先順序	需求說明描述
EECCS-001	1	感測點嵌入橢圓密碼系統。
EECCS-002	1	資料收集器嵌入橢圓密碼系統。
EECCS-003	1	CCVMP 嵌入橢圓密碼系統及加解密運算。

本系統須達成使用案例(usecase)所列功能：

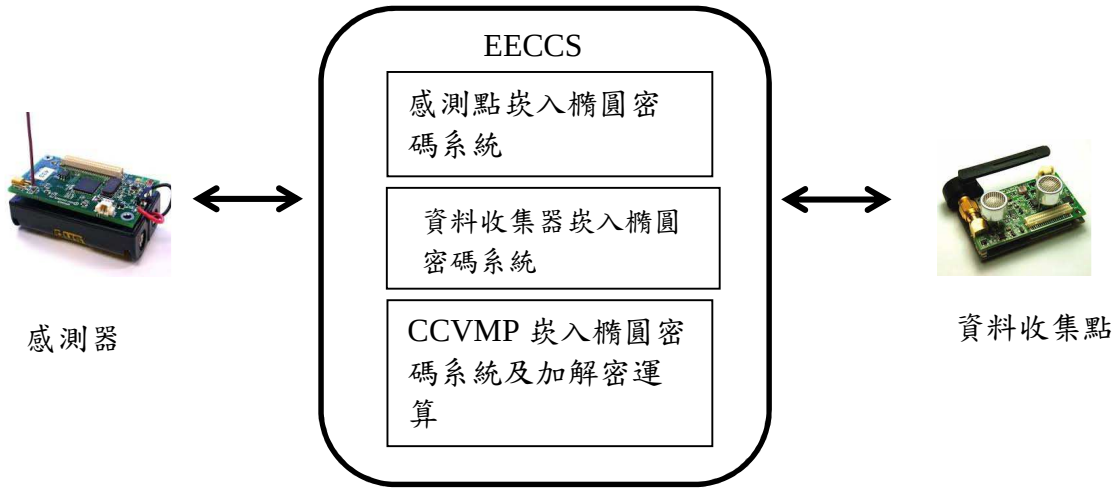

圖 3.1.2、EECCS 使用案例圖

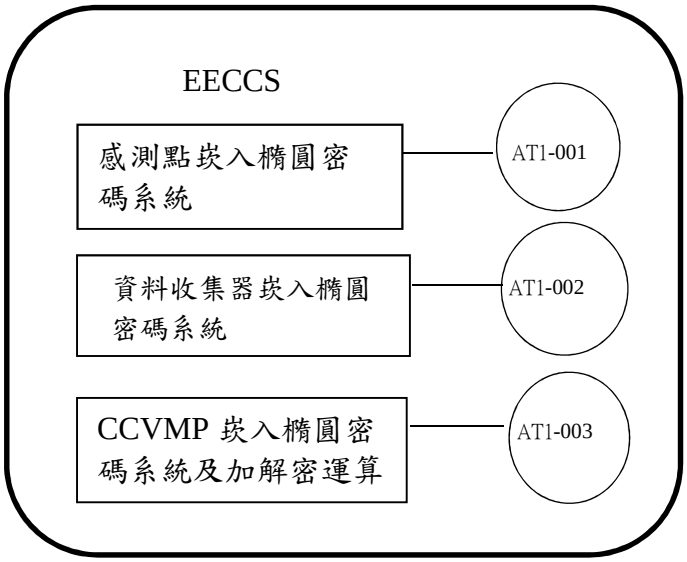

圖 3.1.3、EECCS 接受度測試圖

3.1.5 人員職責分配 (Personnel Responsibilities Assignment)

本系統之測試項目、測試人員姓名及職責如下列所示：

Testing Activities	Personnel
IT1-001	全體人員
AT1-001	全體人員
AT1-002	全體人員
AT1-003	全體人員

3.2 橢圓曲線金鑰交換協議(ECDH)

3.2.1.測試時程 (Testing Schedule).

時程表

測試項目	時間
各子系統之內部元件整合測試(Module Test)	107/04/01~107/07/01
ECDH 整合測試(Integration Test)	107/04/01~107/07/01
ECDH 接受度測試(AcceptanceTest)	107/04/01~107/07/01

檢核點

測試項目	時間
各子系統之內部元件整合測試(Module Test)	107/05/01
ECDH 整合測試(Integration Test)	107/06/01
ECDH 接受度測試(AcceptanceTest)	107/07/01

3.2.2 測試程序(Testing Procedure)

各子系統之內部元件的整合測試，交由各子系統開發負責人完成，在此我們著重於本系統在感測器與資料接收器之間執行 ECDH 協議產出共同會議金鑰，及著

重於系統整合測試與系統接受度測試。

3.2.3 整合測試(Integration Testing)

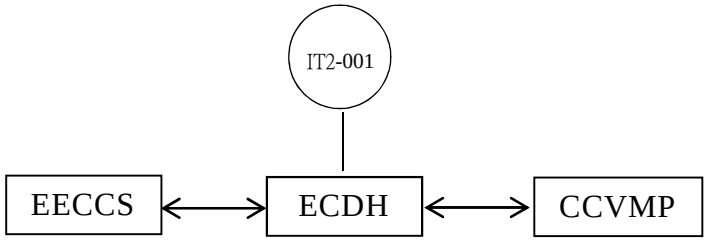

圖 3.2.1、ECDH 整合測試圖

3.2.4 接受測試(Acceptance Testing)

本子系統必須達到下列所述功能：

需求編號	優先順序	需求說明描述
ECDH-001	1	選擇私密金鑰及橢圓曲線。
ECDH-002	1	交換共享金鑰。
ECDH-003	1	計算共同會議金鑰

本系統須達成使用案例(usecase)所列功能：

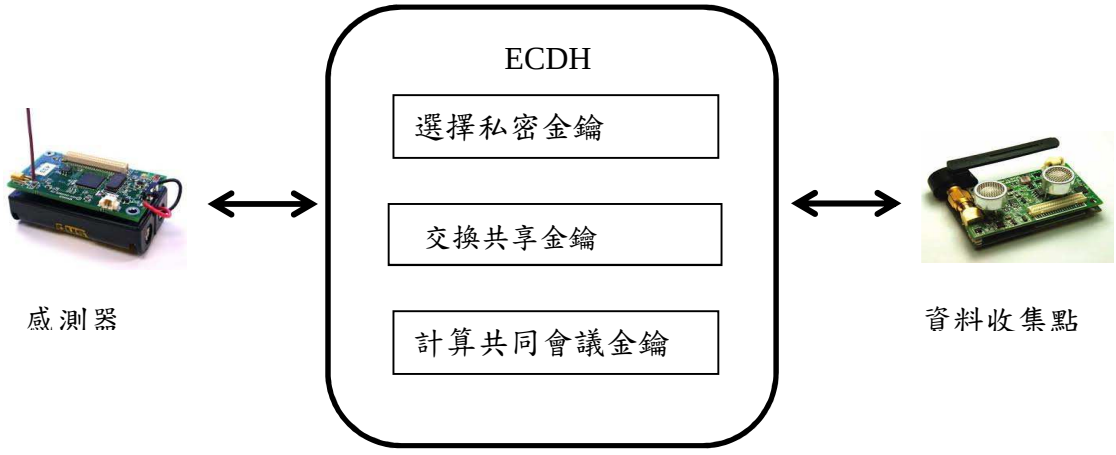

圖 3.2.2、ECDH 使用者案例圖

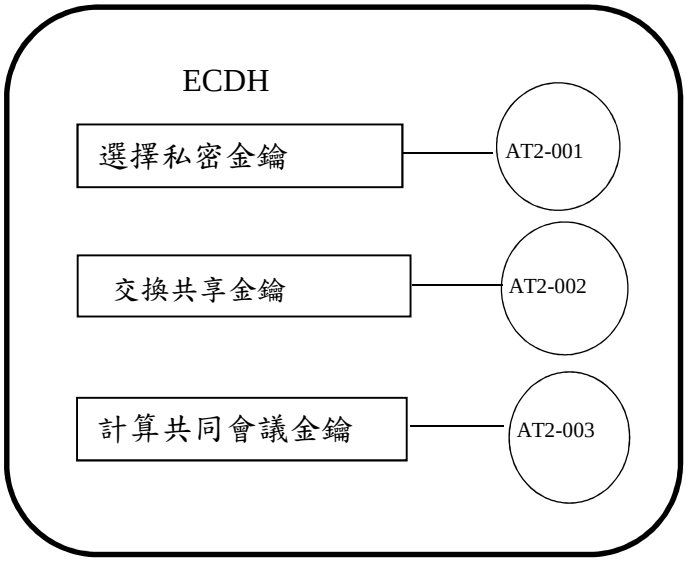

圖 3.2.3、ECDH 接受度測試圖

3.2.5 人員職責分配 (Personnel Responsibilities Assignment)

本系統之測試項目、測試人員姓名及職責如下列所示：

Testing Activities	Personnel
IT2-001	全體人員
AT2-001	全體人員
AT2-002	全體人員
AT2-003	全體人員

3.3 雲端運算虛擬伺服器平台子系統(CCVMP)

3.3.1.測試時程 (Testing Schedule).

時程表

測試項目	時間
各子系統之內部元件整合測試(Module Test)	107/04/01~107/07/01
CCVMP 整合測試(Integration Test)	107/04/01~107/07/01
CCVMP 接受度測試(AcceptanceTest)	107/04/01~107/07/01

檢核點

測試項目	時間
各子系統之內部元件整合測試(Module Test)	107/05/01
CCVMP 整合測試(Integration Test)	107/06/01
CCVMP 接受度測試(AcceptanceTest)	107/07/01

3.3.2 測試程序(Testing Procedure)

各子系統之內部元件的整合測試，交由各子系統開發負責人完成，在此我們著重於本系統在虛擬伺服器平台之架構建置,及著重於系統整合測試與系統接受度測試。

3.3.3 整合測試(Integration Testing)

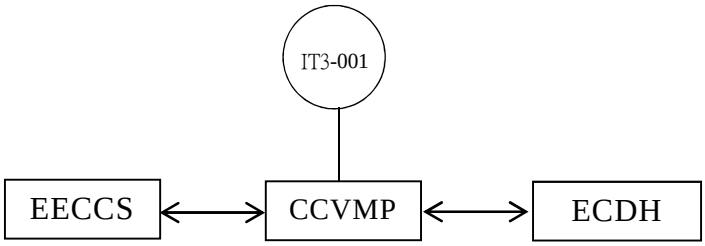

圖 3.3.1、CCVMP 整合測試圖

3.3.4 接受測試(Acceptance Testing)

本子系統必須達到需求規格書所列之所有功能，如下表所示：

需求編號	優先順序	需求說明描述
CCVMP-001	1	接受使用者對資料收集器的資料進行運算請求。
CCVMP-002	1	任務接受回應功能。
CCVMP-003	1	指派參與運算電腦。

本系統須達成使用案例(usecase)所列功能：

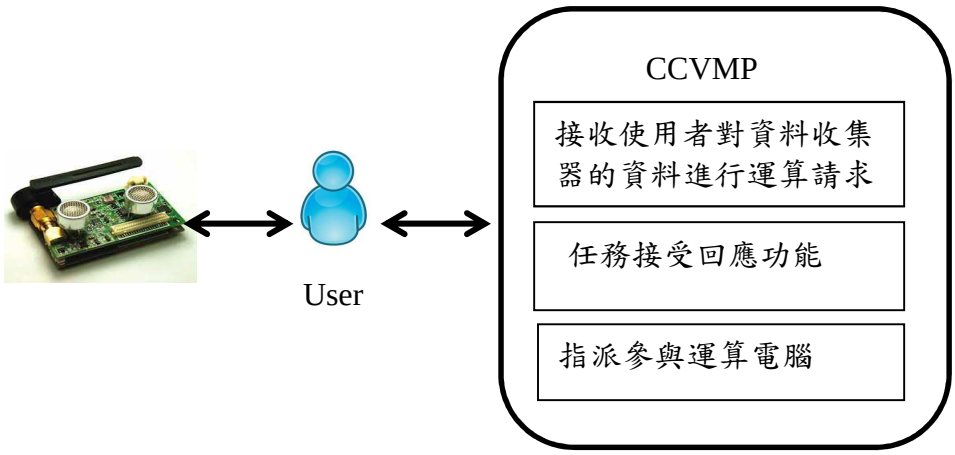

圖 3.3.2、CCVMP 使用者案例圖

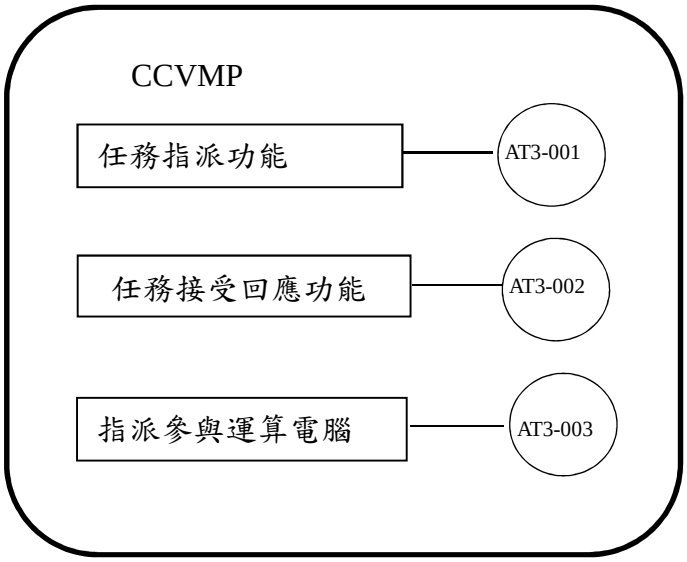

圖 3.3.3、CCVMP 接受度測試圖

3.3.5 人員職責分配 (Personnel Responsibilities Assignment)

本系統之測試項目、測試人員姓名及職責如下列所示：

Testing Activities	Personnel
IT3-001	全體人員
AT3-001	全體人員
AT3-002	全體人員
AT3-003	全體人員

3.4 映對聚合資料安全傳輸協定子系統(SMRDTP)

3.4.1.測試時程 (Testing Schedule)

時程表

測試項目	時間
各子系統之內部元件整合測試(Module Test)	107/04/01~107/07/01
SMRDTP 整合測試(Integration Test)	107/04/01~107/07/01
SMRDTP 接受度測試(AcceptanceTest)	107/04/01~107/07/01

檢核點

測試項目	時間

各子系統之內部元件整合測試(Module Test)	107/05/01
SMRDTP 整合測試(Integration Test)	107/06/01
SMRDTP 接受度測試(AcceptanceTest)	107/07/01

3.4.2 測試程序 (Testing Procedure)

各子系統內部元件的整合測試，交由各子系統開發負責人完成，在此我們著重於映對聚合資料安全傳輸協定之系統整合測試與系統接受度測試。

3.4.3 整合測試(Integration Testing)

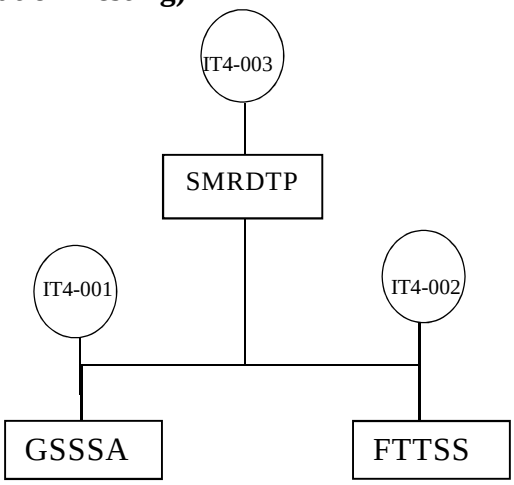

圖 3.4.1、SMRDTP 整合測試圖

3.4.4 接受測試 (Acceptance Testing)

本子系統必須達到需求規格書所列之所有功能，如下表所示：

需求編號	優先順序	需求說明描述
SMRDTP-001	1	門檻分享金鑰容錯運算功能 FTTSS
SMRDTP-002	1	群組數位簽章與分享金鑰傳輸協議 GSSSA。
SMRDTP-003	1	映對聚合資料安全傳輸功能
SMRDTP-004	1	回傳完整訊息給使用者

本系統須達成使用案例(usecase)所列功能：

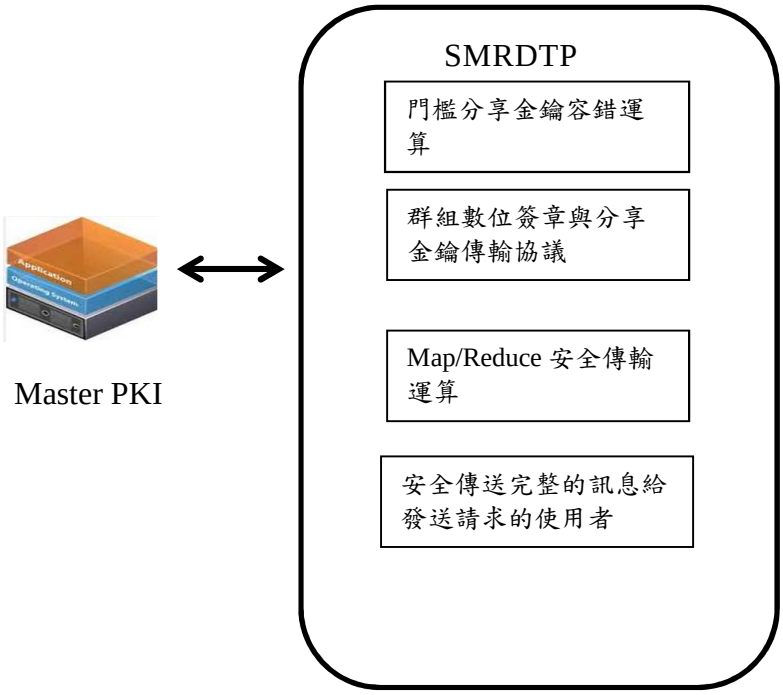

圖 3.4.2、SMRDTP 使用案例圖

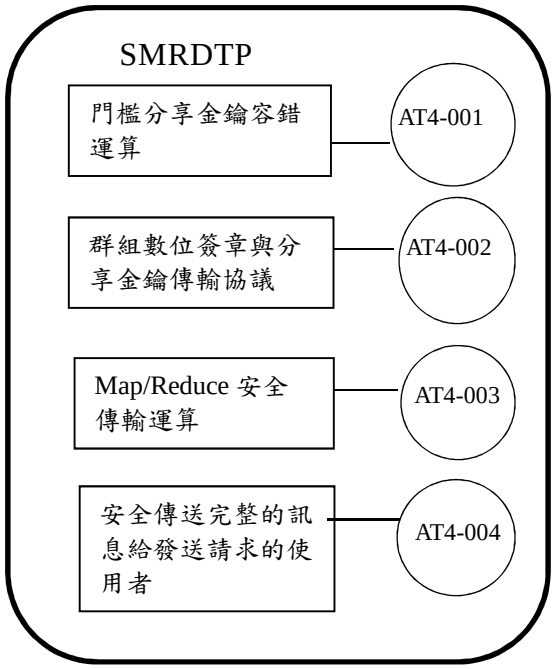

圖 3.4.3、SMRDTP 接受度測試圖

3.4.5 人員職責分配(Personnel Responsibilities Assignment)

本系統之測試項目、測試人員姓名及職責如下列所示：

Testing Activities	Personnel
IT4-001	全體人員
IT4-002	全體人員
IT4-003	全體人員
AT4-001	全體人員
AT4-002	全體人員
AT4-003	全體人員
AT4-004	全體人員
AT4-005	全體人員

3.5 雲端物聯網資訊安全傳輸協定(ISTMCIT)

3.5.1.測試時程 (Testing Schedule).

時程表

測試項目	時間
各子系統之內部元件整合測試(Module Test)	107/04/01~107/07/01
ISTMCIT 整合測試(IntegrationTest)	107/04/01~107/07/01
ISTMCIT 接受度測試(AcceptanceTest)	107/04/01~107/07/01

檢核點

測試項目	時間
各子系統之內部元件整合測試(Module Test)	107/05/01
ISTMCIT 整合測試(IntegrationTest)	107/06/01
ISTMCIT 接受度測試(AcceptanceTest)	107/07/01

3.5.2 測試程序 (Testing Procedure)

各子系統內部元件的整合測試，交由各子系統開發負責人完成，在此我們著重於系統整合測試與系統接受度測試。

3.5.3 整合測試 (Integration Testing)

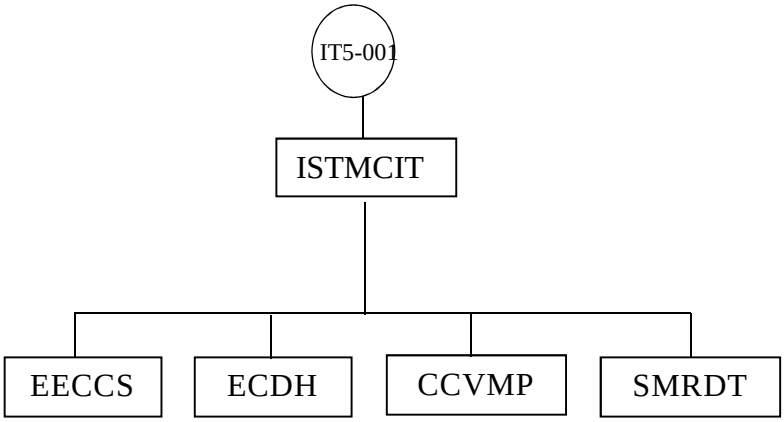

圖 3.5.1、ISTMCIT 整合測試圖

3.5.4 接受測試 (Acceptance Testing)

本子系統必須達到需求規格書所列之所有功能，如下表所示：

需求編號	優先順	需求說明描述
ISTMCIT-001	1	嵌入式橢圓密碼系統
ISTMCIT-002	1	橢圓曲線金鑰交換協議
ISTMCIT-003	1	雲端運算虛擬伺服器平台子系統
ISTMCIT-004	1	映對聚合資料安全傳輸協定子系統
ISTMCIT-005	1	雲端物聯網資訊安全傳輸協定

本系統須達成使用案例(usecase)所列功能：

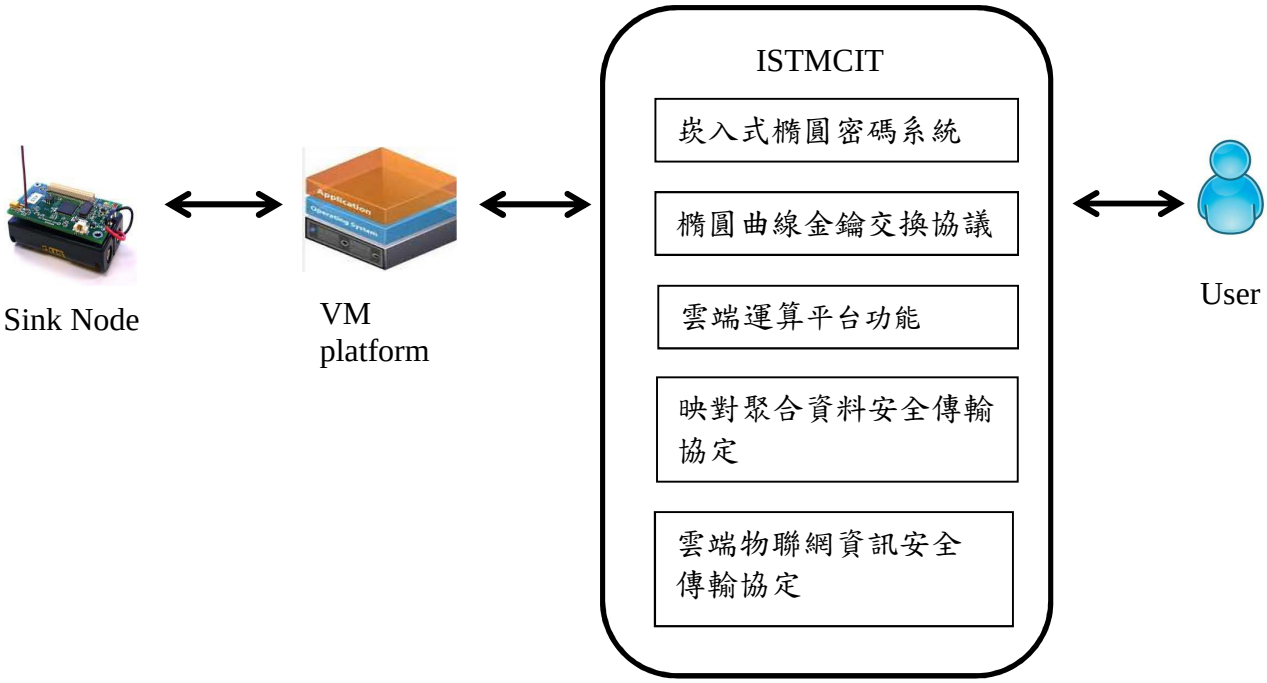

圖 3.5.2、ISTMCIT 使用案例圖

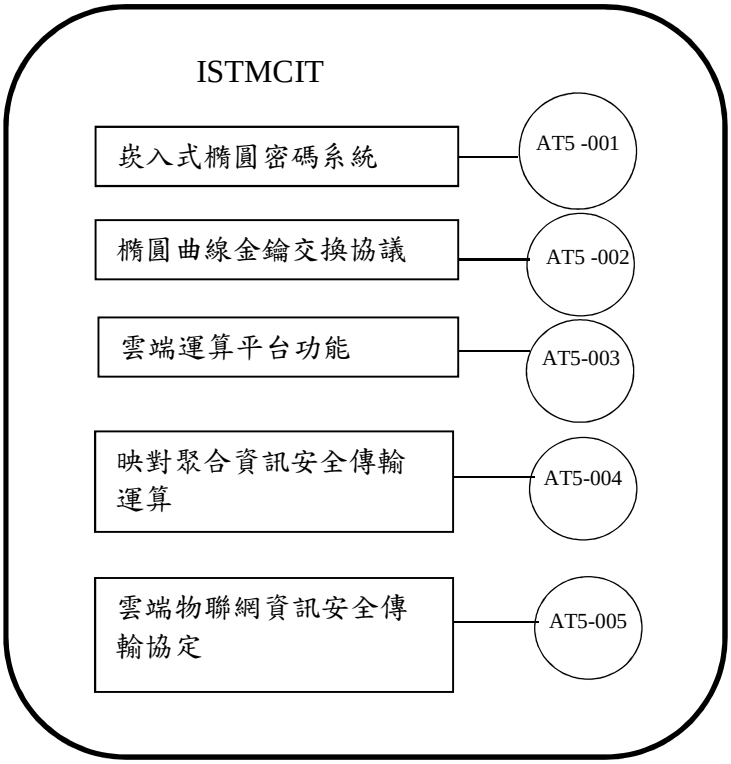

圖 3.5.3、ISTMCIT 接受度測試圖

3.5.5 人員職責分配 (Personnel Responsibilities Assignment)

本系統之測試項目、測試人員姓名及職責如下列所示：

TestingActivities	Personnel
IT5-001	全體人員
AT5-001	全體人員
AT5-002	全體人員
AT5-003	全體人員
AT5-004	全體人員

4. 測試案例 (Test Cases)

4.1 整合測試案例 (Integration Testing Cases)

4.1.1 嵌入式橢圓密碼系統(EECCS)測試案例

目的：

■驗證橢圓密碼系統是否可正確嵌入感測器。

■驗證橢圓密碼系統產出的金鑰對。

輸入與輸出：

■輸入為橢圓密碼曲線、生成點，輸出為金鑰對。

4.1.1.1 IT1-001 Test Case

Identification	IT1-001
Name	嵌入式橢圓密碼系統測試
Tested target	EECCS
Reference	EECCS-001~EECCS003
Severity	Important
Instructions	1. 產出橢圓密碼曲線及金鑰對 2. 植入橢圓密碼系統及金鑰於感測器及資料收集器 3. 註冊感測器 4. 身份認證階段
Expected result	1. 完成生成數橢圓曲線及產生 60 組金鑰對 2. 完成寫入橢圓密碼系統及金鑰 3. 感測器向伺服器完成註冊 4. 完成身份認證階段

4.1.2 橢圓曲線金鑰交換協議(ECDH)測試案例

目的：

■驗證共同會議金鑰。

輸入與輸出：

■輸入為私密金鑰、個別私密金鑰及公開金鑰，輸出為共同會議金鑰。

4.1.2.1 IT2-001 Test Case

Identification	IT2-001
Name	橢圓曲線金鑰交換協議
Tested target	ECDH
Reference	ECDH001-ECDH003
Severity	Critical
Instructions	1.個別選出私密金鑰 2.個別將私密金鑰乘公開金鑰之後取得共享金鑰傳給對方 3.雙方收到共享金鑰乘上私密金鑰後獲得共同會議金鑰
Expected result	1.完成私密金鑰選取 2.計算出私密金鑰乘公開金鑰得共享金鑰 3.計算出共同會議金鑰

4.1.3 雲端運算虛擬伺服器平台子系統(CCVMP)測試案例

目的：

■嵌入 EECCS 橢圓密碼系統及執行 ECDH 金要交換協議，接受使用者對資

料收集器的資料進行運算請求。

輸入與輸出：

■輸入為加密運算任務、輸出為金鑰產生、派送、管理、錯誤回復。

4.1.3.1 IT3-001 Test Case

Identification	IT3-001
Name	雲端運算虛擬伺服器平台整合測試。
Tested target	接受使用者對資料收集器的資料進行運算請求。
Reference	CCVMP-001~CCVMP-003
Severity	Important
Instructions	1. Master 伺服器用 ECDH 解密資料收集器的資料。 2.指派參與運算之 Mapper 及 Reducer。 3. Master 伺服器擔任 PKI 伺服器。 4.產生參與者 Mapper/Reducer 的公開及私密金鑰。 5.透過數位簽章驗證彼此的身份。 6.金鑰產生、派送、管理、錯誤回復。
Expected result	1.確定 Master 伺服器用 ECDH 解密資料收集器請求。 2.正確指派參與運算之 Mapper 及 Reducer。 3.指派 Master 伺服器擔任 PKI 伺服器。 4.正確產生參與者 Mapper/Reducer 的公開及私密金鑰。 5.正確透過數位簽章驗證彼此的身份。 6.正確執行金鑰的產生、派送、管理、錯誤回復。

4.1.4 映對聚合資料安全傳輸協定子系統(SMRDTP)測試案例

目的：

■驗證是否可正確產生金鑰。

■驗證是否可正確分享金鑰。

■驗證是否可正確重組金鑰。

輸入與輸出：

■輸入為 PKI 伺服器執行參與 Mapper/Reducer 運算電腦之分享金鑰，輸出為系統秘密金鑰、*n* 個分享金鑰。

4.1.4.1 IT4-001 Test Case

Identification	IT4-001
Name	映對聚合資料安全傳輸協定
Tested Target	整合 FTTSS 至 SMRDTP
Reference	SMRDTP-001~ SMRDTP-005
Severity	Critical

Instructions	1. PKI 伺服器執行派送分享金鑰及復原秘密金鑰之任務。 2. PKI 伺服器產生系統秘密金鑰，依據金鑰分享演算法將秘密金鑰切個成 *n* 個分享金鑰，派送給參與 Mapper/Reducer 運算之電腦。
Expected Result	1. 可正確產生系統秘密金鑰。 2. 可正確分享金鑰。 3. 可正確重組金鑰。 4. 可正確管理金鑰。

目的：

■驗證部分簽章的正確性。

輸入與輸出：

■輸入為一個公開金鑰當作團體公開金鑰，輸出為每位成員的公開金鑰及個人秘鑰作為參與成員 VM_i 的金鑰配對。

4.1.4.2 IT4-002 Test Case

Identification	IT4-002
Name	映對聚合資料安全傳輸協定
Tested Target	整合 GSSSA 至 SMRDTP
Reference	SMRDTP-001~ SMRDTP-005
Severity	Critical
Instructions	1. 透過 PKI 伺服器選擇一個公開金鑰當作團體公開金鑰，並對每位成員指派公開金鑰及個人秘鑰作為參與成員 VM_i 的金鑰配對。 2. 各個參與者 VM_i 簽暑所接受運算的部分資料片段並計算出承諾值，將此{承諾值，及部分資料簽章}作為個別簽章，傳輸給 PKI 伺服器。 3. 接受到{承諾值，及部分資料簽章}訊息，驗證群組簽章的正確性。 4. PKI 伺服器宣布一個公開金鑰給參與的群組組員以驗證對{承諾值，及部分資料簽章}訊息。
Expected Result	1. 選取一部 VM_i 當作 PKI VM_{master} 伺服器扮演可信任的金鑰管理中心(KDC)，負責決定各項共通參數以及運算各雲端成員 VM_i 的私密金鑰。 2. 接受{承諾值，及部分資料簽章}訊息，驗證群組簽章的正確性。

目的：

■產生完整聚合資料。

輸入與輸出：

■輸入為一個中間值 intermediate 資料，輸出為一個完整的訊息。

4.1.4.3 IT4-003 Test Case

Identification	IT4-003
Name	映對聚合資料安全傳輸協定
Tested Target	整合 FTTSS 及 GSSSA 至 SMRDTP
Reference	SMRDTP-001~ SMRDTP-005
Severity	Critical
Instructions	1. 對 Map 運算所產出的中間值 intermediate 資料進行保護。 2. Reduce 運算從 intermediate 資料讀取時亦必須進行身份確認及資料完整性判斷。 3.PKI VM_{master} 用接收端的秘密分享金鑰 Sh_i 簽署整個資料，並將簽章結果傳送給 Mapper VM_i。 4. Mapper VM_i 接收到傳輸的資料隨即用秘密分享金鑰 Sh_i 解開，並驗證分享金鑰 Sh_i 的正確性與 HMAC 資料的完整性。
Expected Result	1. Map/Reduce 運算期間的資料傳輸是安全無虞。 2. .Reducer VM_x 使用公開金鑰 y 驗證群組簽章$\{w, Data_{Sign}\}$ 並合併各個資料段成一個完整的訊息。

4.1.5 雲端物聯網資訊安全傳輸協定(ISTMCIT)測試案例

目的：

■接收請求產生完整聚合資料。

輸入與輸出：

■輸入為一個 EECCS 及 ECDH 加密資料，輸出為一個完整的聚合訊息。

4.1.5.1 IT5-001 Test Case

Identification	IT5-001
Name	各模組系統整合
Tested Target	ISTMCIT
Reference	EECCS-001~EECCS-003, ECDH-001~ECDH-003, CCVMP-001~CCVMP-003, SMRDTP-001~005, ISTMCIT-001~ISTMCIT-005
Severity	Critical

Instructions	1. 使用者發出執行映射聚合運算要求，將資料收集點加密資料透過 EECCS 及 ECDH 協定傳給 CCVMP。 2. CCVMP 接受任務指派、回應、即時判斷參予運算虛擬伺服器。 3. SMRDTP 執行金鑰產生、分享、重組及管理金鑰機制功能。 4. SMRDTP 執行群組數位簽章與分享金鑰。 5. SMRDTP 執行安全傳輸 Map/Reduce 資料。
Expected Result	1. CCVMP 接收資料收集點資料正確解密後將所接受的任務指派、回應、即時判斷參予的運算虛擬伺服器。 2. FTTSS 確實執行金鑰產生、分享、重組及管理金鑰機制功能。 3. GSSSA 確實執行執行群組數位簽章與分享金鑰。 4. SMPTSSGP 確實執行安全傳輸 Map/Reduce 資料。 5. Reducer 確實回傳聚合運算結果給使用者。

4.2 接受測試案例 (Acceptance Testing Cases)

4.2.1 嵌入式橢圓密碼系統(EECCS)接受測試案例

4.2.1.1 AT1-001 Test Case

Identification	AT1-001	
Name	嵌入式橢圓密碼系統	
Tested Target	感測點嵌入橢圓密碼系統。	
Reference	EECCS-001~EECCS003	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1.選出生成器橢圓曲線及產生金鑰配對。	2. 決定哪些那些金鑰對將來要植入感測點。
	3. 將橢圓密碼系統及金鑰配對寫入嵌入感測器。	
Expected Result	1. 正確產出金鑰配對。 2. 嵌入感測器。	

4.2.1.2 AT1-002 Test Case

Identification	AT1-002
Name	嵌入式橢圓密碼系統
Tested Target	資料收集器嵌入橢圓密碼系統
Reference	EECCS-001~EECCS003
Severity	Critical

Instructions	Actor Actions	System Responses
	1.選出生成器橢圓曲線及產生金鑰配對。	2. 決定哪些那些金鑰對將來要植入資料收集點。
	3. 將橢圓密碼系統及金鑰配對寫入嵌入資料收集點。	
Expected Result	1. 正確產出金鑰配對。 2. 嵌入資料收集點。	

4.2.1.3 AT1-003 Test Case

Identification	AT1-003	
Name	嵌入式橢圓密碼系統	
Tested Target	CCVMP 嵌入橢圓密碼系統及加解密運算	
Reference	EECCS-001~EECCS003	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1.嵌入橢圓密碼系統選出私密金鑰。	2. 計算共同會議金鑰。
	3. 雙方運用會議金鑰執行加解密運算。	
Expected Result	1. 雙方正確執行點對點加解密運算。	

4.2.2 橢圓曲線金鑰交換協議(ECDH)接受測試案例

4.2.2.1 AT2-001 Test Case

Identification	AT2-001	
Name	橢圓曲線金鑰交換協議	
Tested Target	選擇私密金鑰及橢圓曲線	
Reference	ECDH-001~ECDH-003	
Severity	Critical	
	Actor Actions	System Responses

Instructions	1.雙方選擇一組相同參數的橢圓曲線。 2.橢圓曲線上選出公共點 P(x,y) 作為公開金鑰。 3.A 方任選擇一小於 p 的亂數 r_A 接著計算 r_A 乘以公共點 P(x,y), 得到一點 $Q_A(x,y)= r_A*P(x,y)$。 A 方私密金鑰={r_A}；A 方的公開金鑰={$Q_A(x,y)$}。	
	4.雙方選擇一組相同參數的橢圓曲線。 5.橢圓曲線上選出公共點 P(x,y) 作為公開金鑰。 6. B 方任選擇一小於 p 的亂數 r_B 接著計算 r_B 乘以公共點 P(x,y), 得到一點 $Q_B(x,y)= r_B*P(x,y)$ B 方私密金鑰={r_B}；B 方公開金鑰= {$Q_B(x,y)$}。	
Expected Result	1. 雙方正確產出橢圓密碼曲線、私密金鑰及公開金鑰。	

4.2.2.2 AT2-002 Test Case

Identification	AT2-002	
Name	橢圓曲線金鑰交換協議	
Tested Target	交換公開金鑰	
Reference	ECDH-001~ECDH-003	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1.A 方計算共享金鑰 $S_{AB} = r_A*Q_B$。 2.B 方計算共享金鑰 $S_{AB} = r_B*Q_A$。	3. A 方將公鑰 Q_A 傳送給 B 方。 4. B 方將公鑰 Q_B 傳送給 A 方。
		5. A 與 B 擁有對方的公鑰與共享一把相同的共享會議金鑰 $S_{AB} = r_A*Q_B= r_B*Q_A$ 雙方共享機密。
Expected Result	1. 雙方互相傳送共享金鑰 Q_A 及 Q_B 給對方。	

4.2.2.3 AT2-003 Test Case

Identification	AT2-003	
Name	橢圓曲線金鑰交換協議	
Tested Target	計算共同會議金鑰	
Reference	ECDH-001~ECDH-003	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1. A 計算出共用會議金鑰 $S_{AB} = r_A*Q_B = r_B*Q_A$ 雙方擁有共同會議金鑰。	2. B 計算出與 A 共享的會議金鑰 $S_{AB} = r_B*Q_A = r_A*Q_B$ 雙方擁有共同會議金鑰。
Expected Result	1. 正確計算出共享會議金鑰。	

4.2.3 雲端運算虛擬伺服器平台子系統(CCVMP)接受測試案例

4.2.3.1 AT3-001 Test Case

Identification	AT3-001	
Name	雲端運算虛擬伺服器平台	
Tested Target	運算任務指派	
Reference	CCVMP-001~CCVMP-003	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1.CCVMP 接收使用者提出運算請求。	2. CCVMP Master 指派參與運算的 Mappers/Reducers。
Expected Result	1.可正確接收使用者所提出的執行任務。 2.可正確將工作指派給 Mappers 與 Reducers。	

4.2.3.2 AT3-002 Test Case

Identification	AT3-002	
Name	雲端運算虛擬伺服器平台	
Tested Target	任務接受回應	
Reference	CCVMP-001~CCVMP-003	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1. CCVMP Master 指派參與運算的 Mappers/Reducers。	2. Mapper/Reducer 回應接受執行任務確認。

Expected Result	1.可正確接收使用者所提出的執行任務。 2.可正確回應給 Master 接受執行任務。

4.2.3.3 AT3-003 Test Case

Identification	AT3-003	
Name	雲端運算虛擬伺服器平台	
Tested Target	判斷參與執行運算的電腦	
Reference	CCVMP-001~CCVMP-003	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1. CCVMP 接收使用者提出運算請求。	2. Master 即時判斷參與運算的電腦。
Expected Result	1.可正確接收使用者所提出的執行任務。 2. Master 可即時判斷參與運算的電腦。	

4.2.4 映對聚合資料安全傳輸協定子系統(SMRDTP)接受測試案例

4.2.4.1 AT4-001 Test Case

Identification	AT4-001	
Name	映對聚合資料安全傳輸協定	
Tested Target	門檻分享金鑰容錯運算	
Reference	SMRDTP-001~ SMRDTP-004	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1. FTTSS PKI 伺服器挑選一質數。	2. FTTSS PKI 伺服器算出秘密金鑰。 3. FTTSS PKI 伺服器算出參與運算成員的金鑰對。
	4.FTTSS 對秘密金鑰執行分享金鑰的運算。	5.FTTSS 計算 *n* 個分享金鑰。
	6.FTTSS 接收各 Mapper/Reducer 端的分享金鑰。	7. PKI 伺服器透過 Shrmir 演算法算出系統秘密金鑰。
	8.FTTSS 接收任務開始計算系統金鑰。	9.FTTSS 計算分享金鑰給各 Mapper/Reducer，若系統金鑰損毀可重組系統金鑰。

Expected Result	1.可正確產生秘密金鑰及計算參與運算成員金鑰對。 2.可正確產出 n 個分享金鑰。 3.可正確算出系統秘密金鑰。 4.可正確執行金鑰管理各項功能。

4.2.4.2 AT4-002 Test Case

Identification	AT4-002	
Name	映對聚合資料安全傳輸協定	
Tested Target	群組數位簽章與分享金鑰傳輸協議	
Reference	SMRDTP-001~ SMRDTP-004	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1. 選取團體公開金鑰。 2. 為每位成員任選 x_i 為公開值。	3. 計算 $f(x_i) \bmod q$ 為其秘鑰。 4. 計算 $y_i=g^{f(xi)}$為其公開祕鑰，成員 VM_i 的金鑰配對為 $(f(x_i) \bmod q, y_i=g^{f(xi)})$。
	5. GSSSA 計算部分資料片段的承諾值。	6.各個 Mapper m_i 計算出本身的承諾值 w_i，並廣播 w_i 給其它 Mapper。
	7.GSSSA 判斷參與運算的組員 VM_i 部分簽章的正確性。	8. GSSSA 將各個 VM_i 的簽章、w_i 及 $Data_{signi}$ $(i=1,2,3,\ldots,n)$ 組合而成團體簽名 $\{w, Data_{Sign}\}$。
Expected Result	1. 可正確算出團體公開金鑰。 2. 可正確運算每個成員的金鑰配對。 3. 可正確算出部分資料片段的承諾值。 4. 可正確驗證群組簽章的正確性。	

4.2.4.3 AT4-003 Test Case

Identification	AT4-003	
Name	映對聚合資料安全傳輸協定	
Tested Target	映對聚合資料安全傳輸功能	
Reference	SMRDTP-001~ SMRDTP-004	
Severity	Critical	
	Actor Actions	System Responses
	1.PKI VM_{master} 接收到使用者所提出的請求。 3.確認發出請求者身份。	2.決定哪些 Mapper VM_i 將來可參與此次的運算。 4.金鑰驗證請求者身份。

Instructions	5.Mapped VM_i 收到資料後，隨即運用 PKI VM_{master} 的公開金鑰驗證請求者 PKI VM_{master} 的身份是否無誤後，接著簽署回覆可參與Map運算的回應訊息 *Reply*、Mapper VM_i 本身的 $ID_{mapper\text{-}VMi}$，以及負責傳輸資料的{w_i, $Data_{Signi}$}。	6.PKI VM_{master} 將資料段 $Data_{Segi}$ 當作輸入並計算其HMAC($Data_{segi}$)值，並伴隨Mapper VM_i 的 $ID_{mapper\text{-}VMi}$，原始資料 $Data_{segi}$、時截 *Time stamp* 以及部分群組簽章的結果{w_i, $Data_{Signi}$}。最後 PKI VM_{master} 用接收端的秘密分享金鑰 Sh_i 簽署整個資料，並將簽章結果傳送給 Mapper VM_i。
	7. Mapper VM_i 接收到傳輸的資料隨即用秘密分享金鑰 Sh_i 解開，並驗證分享金鑰 Sh_i 的正確性與 HMAC 資料的完整性。	
	8.Reducer VM_x 從 PKI VM_{master} 接收到指派任務。	9.Reducer VM_{master} 隨後能夠驗證 PKI VM_{master} 的身份。
	10.Reducer VM_x 從 Mappers VM_i (i=1~n)接收到由 Mapper VM_i 的秘密分享金鑰 Sh_i 所簽章後的資料段{w_i, $Data_{Signi}$ }~{w_n, $Data_{Signn}$ }、*Time stamp* 以及 *SeqNo*。	11. Reducer VM_x 從 Mapper $VM_{(1\sim n)}$ 接收到傳輸的資料後，Reducer VM_x 隨即向 PKI VM_{master} 要求 Mapper VM_i 所對應的公開金鑰 Sh_i。
	12. Reducer VM_x 從 PKI VM_{master} 取得參與運算 Mapper $VM_{(1\sim n)}$ 的 Sh_i 所對應的公開金鑰。	13. Reducer VM_x 獲取 Sh_i 所對應的公開金鑰後，隨即解開加密資料，合併 VM 的簽章{w_i, $Data_{Signi}$} (i=1, 2, 3,…, n) 成為群組簽章{w, $Data_{Sign}$}，其中 $Data_{Sign}= Data_{Sign1}+ Data_{Sign2}+ Data_{Sign3}+ \ldots + Data_{Signn} \bmod q$。隨即 Reducer VM_x 使用公開金鑰 y 驗證群組簽章{w, $Data_{Sign}$}並合併各個資料段成一個完整的訊息。
Expected Result	1. FTTSS 提供 SMRDTP 映對聚合資料安全傳輸協定所需用到的簽章、身份驗證、資料加解密等金鑰管理功能。 2. 可正確執行 Map 資料安全傳輸協定。 3. 可正確算出部分資料片段的承諾值。 4. 可正確驗證群組簽章的正確性。	

4.2.4.4 AT4-004 Test Case

Identification	AT4-004
Name	映對聚合資料安全傳輸協定

Tested Target	回傳運算結果完整訊息給使用者	
Reference	SMRDTP-001~ SMRDTP-004	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1. Reducer VM_x 獲取 Sh_i 所對應的公開金鑰後，隨即解開加密資料。	2. 合併 VM 的簽章 $\{w_i, Data_{Signi}\}$ $(i=1, 2, 3,\ldots, n)$ 成為群組簽章 $\{w, Data_{Sign}\}$，其中 $Data_{Sign}= Data_{Sign1}+ Data_{Sign2}+ Data_{Sign3}+ \ldots+ Data_{Signn} \bmod q$。
	3. Reducer VM_x 使用公開金鑰 y 驗證群組簽章 $\{w, Data_{Sign}\}$ 並合併各個資料段成一個完整的訊息。	4.Reducer VM_x 傳送此完整的訊息給發送請求的使用者。
Expected Result	1. 可正確執行映對聚合資料安全傳輸協定回傳資料。	

4.2.5 雲端物聯網資訊安全傳輸協定(ISTMCIT)接受測試案例

4.2.5.1 AT5-001 Test Case

Identification	AT5-001	
Name	雲端物聯網資訊安全傳輸協定	
Tested Target	崁入式橢圓密碼系統	
Reference	ISTMCIT-001~ISTMCIT-005	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1.選出生成器橢圓曲線及產生金鑰配對。	2. 決定哪些那些金鑰對將來要植入感測點。
	3. 將橢圓密碼系統及金鑰配對寫入嵌入感測器、資料收集器及雲端運算虛擬伺服器平台子系統。	
Expected Result	1.可正確崁入橢圓密碼系統。	

4.2.5.2 AT5-002 Test Case

Identification	AT5-002
Name	雲端物聯網資訊安全傳輸協定
Tested Target	橢圓曲線金鑰交換協議

Reference	ISTMCIT-001~ISTMCIT-005	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1.選擇私密金鑰及橢圓曲線	2. 交換公開金鑰
	3. 計算共同會議金鑰	
Expected Result	1.可正確嵌入橢圓密碼系統。	

4.2.5.3 AT5-003 Test Case

Identification	AT5-003	
Name	雲端物聯網資訊安全傳輸協定	
Tested Target	雲端運算虛擬伺服器平台子系統	
Reference	ISTMCIT-001~ISTMCIT-005	
Severity	Critical	
Instructions	Actor Actions	System Responses
	1.CCVMP 子系統之 Master 伺服器收到使用者請求後，指派參與運算之 Mapper 及 Reducer，並執行參與者身份驗證工作。	2. 選擇哪些 Mapper VM_i 將來可參與此次的運算。
	2. Mapper/Reducer 回應接受執行任務確認。	4. Master 決定參與運算的電腦。
Expected Result	1.可正確接收使用者所提出的執行任務。 2.可正確回應給 Master 接受執行任務。 2. Master 決定參與運算的電腦。	

4.2.5.4 AT5-004 Test Case

Identification	AT5-004	
Name	雲端物聯網資訊安全傳輸協定	
Tested Target	映對聚合資料安全傳輸協定子系統	
Reference	ISTMCIT-001~ISTMCIT-005	
Severity	Critical	
	Actor Actions	System Responses

Instructions	1. FTTSS 可計算分享金鑰給各 Mapper/Reducer，若系統金鑰損毀可重組系統金鑰。	2. GSSSA 各個 Mapper VM_i (m_1, m_2, m_3,…,m_n)必須代表群體簽署所接受運算的 *Data*。 3. PKI VM_{master} 接收到每個 $Data_{Signi}$ 並驗證 n 個 VM_i 的簽章後，將各個 VM_i 的簽章、w_i 及 $Data_{signi}$ (i=1,2,3,…,n)組合而成團體簽名{w, $Data_{Sign}$}。其中須滿足 $Data_{Sign}=Data_{Sign1}+Data_{Sign2}+Data_{Sign3}+…+Data_{Signn}$ mod q。
	4. PKI 將資料段 $Data_{Segi}$ 當作輸入並計算其 HMAC，並伴隨 *ID*、原始資料、時截及部分群組簽章的結果{w_i, $Data_{Signi}$}用接收端的秘密分享金鑰簽署後將簽章結果傳送給 Mapper。	5. Reducer 從 Mapper 接收到傳輸的資料後。
		6.用 Mapper 所對應的公開金鑰解開加密資料合併 VM 的簽章{w_i, $Data_{Signi}$}並重組資料段。
	7.使用者收到執行結果。	
Expected Result	1.正確指派參與運算之 Mapper 及 Reducer 。 2.對參與者 Mapper/Reducer 透過數位簽章驗證彼此的身份。 3.可正確執行門檻分享金鑰容錯子系統。 4.可正確整合及執行群組數位簽章。 5.可正確執行資料加解密保護運算。 6.可正確收到執行結果。	

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

5.1 整合測試案例 (Integration Testing Cases)

5.1.1 嵌入式橢圓密碼系統(EECCS)

Test Case#	Result(PASS/FAIL)	Comment
IT1-001	PASS	
RATE	100%	

5.1.2 橢圓曲線金鑰交換協議(ECDH)

Test Case#	Result(PASS/FAIL)	Comment
IT2-001	PASS	
RATE	90%	

5.1.3 雲端運算虛擬伺服器平台子系統(CCVMP)

Test Case#	Result(PASS/FAIL)	Comment
IT3-001	PASS	
RATE	90%	

5.1.4 映對聚合資料安全傳輸協定子系統(SMRDTP)

Test Case#	Result(PASS/FAIL)	Comment
IT4-001	PASS	
IT4-002	PASS	
RATE	70%	

5.1.5 雲端物聯網資訊安全傳輸協定(ISTMCIT)

Test Case#	Result(PASS/FAIL)	Comment
IT5-001	PASS	
RATE	60%	

5.2 接受測試案例 (Acceptance Testing Cases)

5.2.1 嵌入式橢圓密碼系統(EECCS)

Test Case#	Result(PASS/FAIL)	Comment
AT1-001	Incomplete	預計 107/07/14 完成 100%接受度測試
AT1-002	Incomplete	預計 107/07/14 完成 100%接受度測試
AT1-003	Incomplete	預計 107/07/14 完成 100%接受度測試
RATE	70%	

5.2.2 橢圓曲線金鑰交換協議(ECDH)

Test Case#	Result(PASS/FAIL)	Comment
AT2-001	Incomplete	預計 107/07/14 完成 100%接受度測試
AT2-002	Incomplete	預計 107/07/14 完成 100%接受度測試
AT2-003	Incomplete	預計 107/07/14 完成 100%接受度測試
RATE	70%	

5.2.3 雲端運算虛擬伺服器平台子系統(CCVMP)

Test Case#	Result(PASS/FAIL)	Comment
AT3-001	Incomplete	預計 107/07/14 完成 100%接受度測試

AT3-002	Incomplete	預計 107/07/14 完成 100%接受度測試
AT3-003	Incomplete	預計 107/07/14 完成 100%接受度測試
RATE	70%	

5.2.4 映對聚合資料安全傳輸協定子系統(SMRDTP)

Test Case#	Result(PASS/FAIL)	Comment
AT4-001	Incomplete	預計 107/07/14 完成 100%接受度測試
AT4-002	Incomplete	預計 107/07/14 完成 100%接受度測試
AT4-003	Incomplete	預計 107/07/14 完成 100%接受度測試
AT4-004	Incomplete	預計 107/07/14 完成 100%接受度測試
AT4-005	Incomplete	預計 107/07/14 完成 100%接受度測試
RATE	70%	

5.2.5 雲端物聯網資訊安全傳輸協定(ISTMCIT)

Test Case#	Result(PASS/FAIL)	Comment
AT5-001	Incomplete	預計 107/07/14 完成 100%接受度測試
AT5-002	Incomplete	預計 107/07/14 完成 100%接受度測試
AT5-003	Incomplete	預計 107/07/14 完成 100%接受度測試
AT5-004	Incomplete	預計 107/07/14 完成 100%接受度測試
RATE	70%	

Appendix A： 追朔表 Traceability

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

System or Subsystem Test Case	EECCS	ECDH	CCVMP	SMRDTP	ISTMCIT
IT1-001	✓				
IT2-001		✓			
IT3-001			✓		
IT4-001				✓	
IT4-002				✓	
IT4-003				✓	
IT5-001					✓
AT1-001	✓				
AT1-002	✓				
AT1-003	✓				
AT2-001		✓			
AT2-002		✓			
AT2-003		✓			
AT3-001			✓		
AT3-002			✓		
AT3-003			✓		
AT4-001				✓	
AT4-002				✓	
AT4-003				✓	
AT4-004				✓	
AT4-005	✓			✓	
AT5-001	✓				✓
AT5-002	✓				✓
AT5-003	✓				✓
AT5-004	✓				✓

表 A.1 System or Subsystem vs. Test Cases Trace ability Table

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

Test Case Requirement	IT1-001	IT2-001	IT3-001	IT4-001	IT4-002	IT4-003	IT5-001
EECCS-001	✓						
EECCS-002	✓						
EECCS-003	✓						
ECDH-001	✓	✓					
ECDH-002	✓	✓					
ECDH-003	✓	✓	✓				
CCVMP-001	✓	✓	✓				
CCVMP-002	✓	✓	✓				
CCVMP-003	✓	✓	✓				
SMRDTP-001				✓	✓	✓	
SMRDTP-002				✓	✓	✓	
SMRDTP-003				✓	✓	✓	
SMRDTP-004				✓	✓	✓	
ISTMCIT-001	✓	✓					
ISTMCIT-002	✓	✓					
ISTMCIT-003	✓	✓	✓				
ISTMCIT-004				✓	✓		
ISTMCIT-005	✓	✓	✓	✓	✓	✓	✓

表 A.2 Integration Test Cases vs. Requirements Traceability Table

Test Case Requirement	AT1-001	AT1-002	AT1-003	AT2-001	AT2-002	AT2-003	AT3-001	AT3-002	AT3-003	AT4-001	AT4-002	AT4-003	AT4-004	AT5-001	AT5-002	AT5-003	AT5-004	AT5-005
EECCS-001	✓																	
EECCS-002		✓																
EECCS-003	✓	✓	✓															
ECDH-001	✓			✓														
ECDH-002	✓				✓													
ECDH-003	✓					✓												
CCVMP-001	✓	✓					✓											
CCVMP-002								✓										
CCVMP-003									✓									
SMRDTP-001										✓								
SMRDTP-002											✓							
SMRDTP-003										✓	✓	✓						
SMRDTP-004										✓	✓	✓	✓					
ISTMCIT-001	✓																	
ISTMCIT-002	✓	✓																
ISTMCIT-003	✓	✓					✓	✓	✓									
ISTMCIT-004										✓	✓	✓	✓					
ISTMCIT-005	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

表 A.3 Acceptance Test Cases vs. Requirements Traceability Table

Appendix B： Glossary

EC
橢圓曲線密碼系統屬於非對稱是密碼系統，架構在橢圓曲線數學在某些情況下比其他的非對稱式密碼系統具備更小的金鑰長度[34]。

ECDH
橢圓曲線狄菲-霍夫曼金鑰交換協議，在這個協定下，雙方基於橢圓曲線密碼系統透過狄菲-霍夫曼金鑰交換演算法建立公鑰與私鑰對。使得雙方在不安全的通道中，建立起安全加密資料的通道[34]。

Cloud Computing
雲端運算是建置在網際網路的基礎架構上，根據使用者的需求提供網網互連設備的共享軟體及硬體等運算資源供使用者運算[34]。

Virtual Machine
虛擬伺服器是一種特殊軟體，架構在電腦硬體、作業系統和使用者之間，建立一種作業環境讓使用者在這個虛擬軟體的環境來安裝各種軟體，就如同擁有一部實體電腦般[34]。

Internet of Things
物聯網是基於網際網路、無線網路、電信網路等各種資訊的載體，將所有能連接網路的物件彼此互聯所形成的物物相連的網路[34]。

Sensor
感應器應用在偵測環境中的產生的事件或變化，並將這些偵測的數值訊息傳送給其他電子設備的裝置，感測器通常是由感應元件和轉換元件所組合而成，常見的有溫溼度、速度、光度等感測器[34]。

TinyOS
是一種針對無線感應網路所開發的自由軟體，運用在嵌入式作業系統 [34]。

Sink Node
資料收集點主要是擔任接收及匯集感測器所傳送過來的感應資料，再透過網路後送到伺服端進行運算產生出更有價值的資訊[34]。

PKI
公開金鑰基礎架構是以公開金鑰密碼學為基礎而衍生的架構，由硬體、軟體、參與者、管理政策與流程等所組成的基礎架構，提供在 Intranet、Extranet 及 Internet網路環境間交換資訊的信任基礎。PKI 架構中包含了憑證機構（Certificate Authority，CA）、註冊中心（Register Authority， RA）、目錄服務（Directory Service， DS）伺服器、身份認證 (Authentication) 伺服器或認證模組等等[34]。

KDC
金鑰管理中心是密碼系統的一部分，主要在降低交換金鑰的風險。KDC通常在一些資訊系統中運行，而在這些系統中，使用者被允許在某些特定的時間內有權使用服

務，而無法在其他非授權時間內使用[34]。

Private Key
私密金鑰為一組密碼由使用者保管不可透漏他人，可與公開金鑰互相驗證。

Public Key
公開金鑰是一組密碼經過認證機構發給憑證後，可作為驗證私密金鑰的憑據。

Session Key
會議金鑰使用在雙方資料傳輸交換時加密用的對稱式金鑰，雙方使用同一把金鑰來加密明文、解密密文，在此次連線結束該金鑰即無效，若需重新通訊則必須再次執行會議金鑰的計算、產生及交換等步驟[34]。

Threshold Value
門檻值運用在設計事件開始發生或改變的邊界值。

Group Signature
群組簽章是一種允許群組成員匿名簽署代表群組的消息的方法。

Map Reduce
是一種由Google所提出的軟體架構，運行在眾多不可靠電腦所組成的叢集架構，執行大規模資訊的平行運算。Map（映射）是從主節點(master node)輸入一組input，此input是一組key/value，將這組輸入切分成好幾個小的子部分，分散到各個工作節點去做運算。Reduce（聚合）是主節點(master node)收回處理完的子部分，將子部分重新組合產生輸出。

Appendix C： References

[1] TinyOS: Operating System Design for Wireless Sensor Networks, https://www.sensorsmag.com/iot-wireless/tinyos-operating-system-design-for-wireless-sensor-networks

[2] TinyOS Installation Guide, https://www.advanticsys.com/wiki/index.php?title=TinyOS_Installation_Guide

[3] S. Hu, Y. Yu and L, Xie"Comparing Power Management Strategies of Android and TinyOS",Circuits, Communications and System (PACCS), 2011 Third Pacific-Asia Conference on, 2011.

[4] TinyOS programming, https://books.google.com.tw/books?id=y3KcnZ0jB_MC&pg=PA252&lpg=PA252&dq=tinyos&source=bl&ots=UHybg6RqsJ&sig=p0sZYyp7PNeAfB8tUAOF_Im1Izs&hl=zh-TW&sa=X&ved=0ahUKEwiY6d-N5v_aAhWHjZQKHVgCCu44ChDoAQhCMAc#v=onepage&q=tinyos&f=false

[5] P Levis,"Experiences from a Decade of TinyOS Development". 10th USENIX Symposium on Operating Systems Design and Implementation, 2012.

[6] Z. Rehena, K. Kumar, S. Roy, and N. Mukherjee,"SPIN implementation in TinyOS environment using nesC, International Conference on Computing Communication and Networking Technologies, July, 2010.

[7] C. Zhang, A. Syed, Y. H. Cho, and J. Heidemann,”Steam-Powered Sensing”, In Proceedings of the Ninth International Conference on Embedded Networked Sensor Systems, 2011.

[8] D.J. Malan, M. Welsh, and M.D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography", Sensor and Ad Hoc Communications and Networks ,Oct., 2004.HDFS http://hadoop.apache.org/docs/r2.9.0/hadoop-project-dist/hadoop-hdfs/HDFSRouterFederation.html

[9] Using ECDH on Android, https://nelenkov.blogspot.tw/2011/12/using-ecdh-on-android.html

[10] M. A. Dar and J. Parvez, “A Novel Strategy to Enhance the Android Security Framework”, International

[11] Journal of Computer Applications (IJCA), Foundation of Computer Science (FCS), New York, USA, Vol. 91, No. 8, pp. 37-41, 2014.

[12] M. A. Dar and J. Parvez, “Enhancing Security of Android & iOS by implementing Need-Based Security”, IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies, 10th and 11th, 2014.

[13] M. A. Darand J. Parvez,"Security Enhancement in Android using Ellipic Curve Cryptography", International Journal of Security and Its Applications, Vol.11, No, 6, pp. 27-34, 2017.

[14] Apache HBase http://hbase.apache.org/

[15] CDH5 Overview https://www.cloudera.com/documentation/enterprise/5-9-x/topics/cdh_intro.html

[16] CDH5 http://www.cloudera.com/documentation/cdh/5-1-x/CDH-Version-and-Packaging-Information/cdhvd_cdh_download_previous.html

[17] CDH 5 and MapReduce https://www.cloudera.com/documentation/enterprise/5-8-x/topics/cdh_ig_cdh5_mapreduce.html

[18] Cloudera 實現 Hadoop, http://wiki.ubuntu.org.cn/%E5%88%A9%E7%94%A8Cloudera%E5%AE%9E%E7

%8E%B0Hadoop
[19] Hadoop 新 MapReduce 框架 Yarn 詳解, https://www.ibm.com/developerworks/cn/opensource/os-cn-hadoop-yarn/
[20] VMware Workstation 14, https://www.vmware.com/tw/products/workstation-pro/workstation-pro-evaluation.html
[21] Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing," *5th Int'l Conference on Computer Sciences and Convergence Information Technology*, pp. 18-21, Seoul, Nov. 30- Dec. 2, 2010.
[22] J. Ekanayake, S. Pallickara and G. Fox, "Mapreduce for Data Intensive Scientific Analysis", *in IEEE Fourth International Conference on eScience*'08, pp. 277–284, 2008.
[23] S. Creese, P. Hopkins, S. Pearson and Y. Shen, "Data Protection-Aware Design for Cloud Services", *Lecture Notes in Computer Science*, Vol. 5931, pp. 119-130, 2009.
[24] G. Mackey, S. Sehrish, J. Lopez, J. Bent, S. Habib and J. Wang, "Introducing Map Reduce to High End Computing", *in Petascale Data Storage Workshop Held in conjunction with SC*08, 2008.
[25] J. Ekanayake, S. Pallickara and G. Fox, "Mapreduce for Data Intensive Scientific Analysis", *in IEEE Fourth International Conference on eScience*'08, pp. 277–284, 2008.
[26] W. Itani, A. Kayssi and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures", *the Proceeding of the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing*, pp.711-716, 2009.
[27] K. Begnum, "Simplified Cloud-Oriented Virtual Machine Management with MLN", *The Journal of Supercomputing*, Springer, DOI 10.1007/s11227-010-0424-0, 2010.
[28] D. Zhou, L. Zhong, T. Wo and J. Kang, "Cloud View: Describe and Maintain Resource View in Cloud", *IEEE Second International Conference on Cloud Computing Technology and Science*, pp. 151–158.
[29] T. Miyamoto, M. Hayashi and K. Nishimura, "Sustainable Network Resource Management System for Virtual Private Clouds", *IEEE Second International Conference on Cloud Computing Technology and Science*, pp.512-520, 2010.
[30] Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing," *5th Int'l Conference on Computer Sciences and Convergence Information Technology*, pp. 18-21, Seoul, Nov. 30- Dec. 2, 2010.
[31] Y. Desmedt and Y. Frankel, "Threshold Crypto-Systems", *Advances in Cryptology* (*Crypto*'89), pp. 307-315, August, 1990.
[32] D. R. Stinson and R. Wei, "Unconditionally Secure Proactive Secret Sharing Scheme with Combinatorial", *in Proceeding of the 6th Annual International Workshop Selected Areas in Cryptography*, August, 1999.
[33] G. L. Wang, "Security Analysis of Several Group Signature Schemes", Lecture Notes in Computer Science, Vol. 2904, pp. 252-265, 2003.
[34] 維基百科 https://zh.wikipedia.org