科技部開放軟體研發專案計畫
『系統測試報告書』

System Testing Plan Document

數位貨幣交易之安全性提升的設計與實作
-以開放源碼之比特幣錢包為例

Design and Implementation of Security Improvement in Digital Currency Transaction - Open Source Bitcoin Wallet as an Example

MOST 105-2221-E-130-006 -

主持人: 王家輝副教授

銘傳大學資訊工程學系

Ministry of Science and Technology

2017/06/05

目　　錄

圖　　目　　錄

表　　目　　錄

Revision History

版次	變更項目	變更日期
1.0	第 1 版	2017/06/13

1. Introduction

本計畫將開發讓商家能夠結合商品與 RFID 標籤，以達到快速建構與管理商品資料庫之系統，並且讓商家及顧客可以運用手機 NFC 功能來實際運作比特幣的行動支付流程。店家只需要掃描商品上的 RFID 標籤，即可快速建立交易清單，再利用 NFC 功能與顧客之行動裝置進行訊息交換，輕鬆地將商家的收款地址以及交易資料傳送給顧客，收到資料後便能快速地以顧客之比特幣行動電子錢包付款，並將交易細項儲存下來，以便未來商家與顧客能夠快速查詢比特幣行動支付的交易紀錄。

本系統主要是以完成區塊鏈之數位加密貨幣的收款監督系統為主要目標，本計畫進而將積極利用自由軟體的利基：使用成本低、進入門檻低、開放原始碼、社群能力強、共通性及移植性強、資通安全性高等優勢來開發本計畫收款監督系統的應用服務平台。

本專案範圍包含建置下面主系統與各項子系統，主系統為：

基於區塊鏈技術的收款監督系統 (Blockchain-based Payment Collection Supervision system, BPCS)

各子系統分別為：

- 商家端建置與管理商品資訊子系統(Store and Merchandise Information Management Sub-System**, SMIMSS**):

  本系統可以讓商家在進貨時，快速地將 RFID 標籤之識別碼與進貨商品資訊整合在一起，並且透過本系統新增、修改或刪除資料庫內部的資訊，包括產品名稱、詳細資訊，存貨數量等資訊，商家與顧客便可依照該資料庫取得當前商品資訊與狀態。不僅讓商店的存貨資訊更加清楚明瞭，也可以提供顧客更多的即時服務。

- 商家端行動收銀與交易明細系統(Store Mobile payment Collection and Transaction Sub-System, **SMCTSS)**:

  本系統使商家在結帳時，能夠以手機 NFC 功能掃描商品上的 RFID 標籤，即可簡單地建立交易清單，並透過 NFC 與顧客手機碰觸，將交易清單以及商家之比特幣收款地址等等重要交易資訊一併傳遞給顧客，可以簡短結帳的速度，使結帳效率大幅提升。

- 顧客端行動支付與交易明細系統(Client Mobile Payment and Transaction Sub-System, **CMPTSS**):

  顧客在結帳時，不必再麻煩的拿出信用卡或是零錢包，只需要拿出手機讓店員以 NFC 將交易清單與比特幣地址轉送給自己，即可自動連結至比特幣電子錢包的應用程式當中，並且自動填妥相關資料，如:交易金額、收款地址等等與此同時也能將交易紀錄儲存於客戶端，以便日後顧客快速取得過往的交易紀錄，除此之外亦可讓廣大的民眾體驗數位加密貨幣與行動支付帶來的便利生活。

1.1 Scope of Testing

本文件主要是描述基於區塊鏈技術的收款監督系統的測試計畫。確認在系統整合前，必須先確認所有的設計元件均可正確的輸出，在此我們著重於整合系統測試 (Integration Test) 及接受度測試 (Acceptance Test)。本文件內容將依據系統需求規格書與系統設計文件，描述關於整合測試的相關計畫與內容。並希望透過此文件之描述與實踐，達到順利進行測試工作之目的。

1.2 Acceptance Criteria

本測試計劃需要滿足下列的測試接受準則：

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

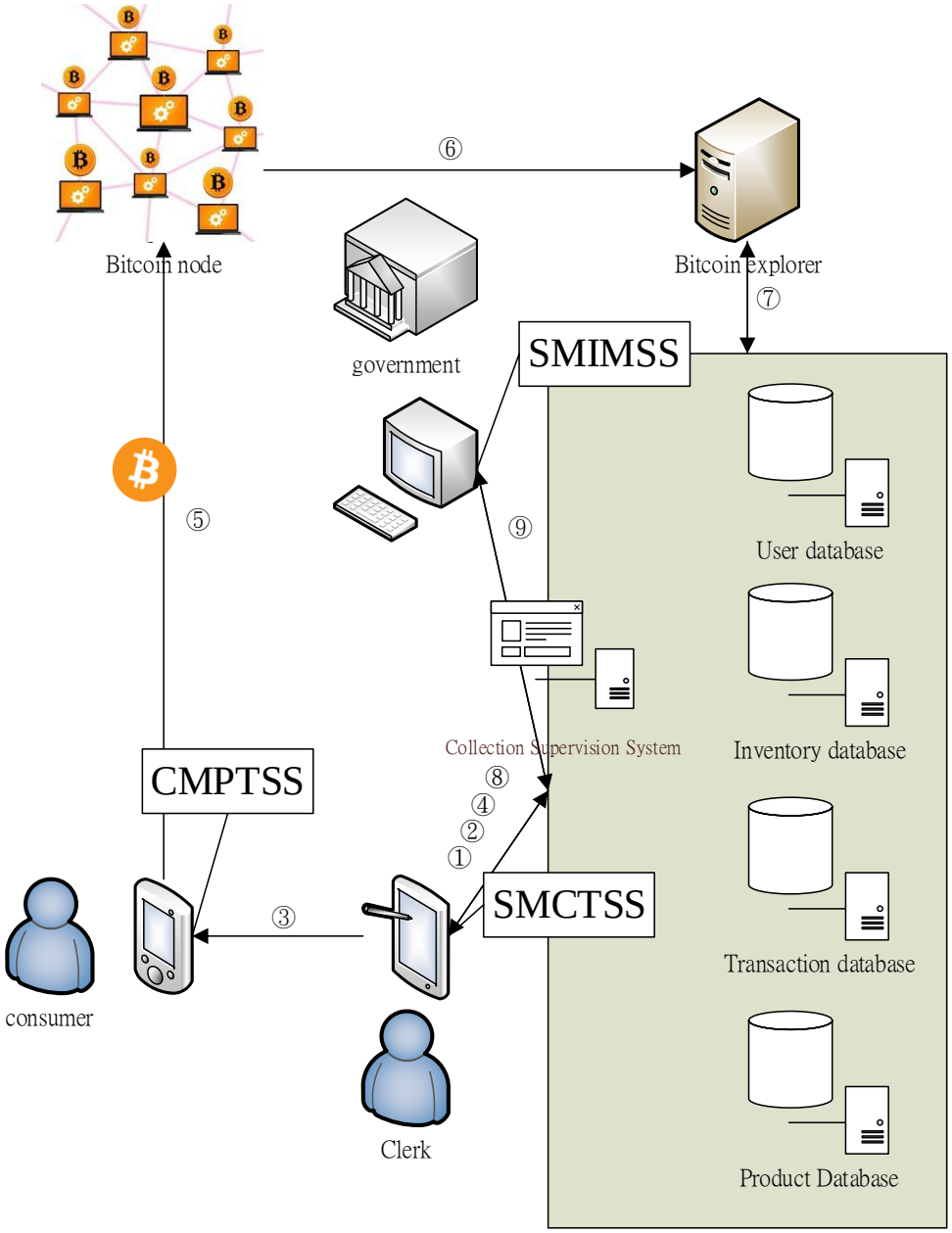

Figure 1 BPCS 主系統示意圖與測試環境

2. Testing Environment

2.1 Hardware Specification

關於測試環境所需的硬體規格說明，如下列所示：

- 系統主機：一台以上主機，每台主機 CPU 為 Intel P4 1.0GHz 或以上，256 MB RAM 或以上，60G 以上硬碟空間。
- 周邊設備：一台以上智慧型手機，與用來代表虛擬商品的數個 RFID 標籤；已可供測試 NFC 用的智慧型手機包含小米 3 WCDMA 版與 Google Nexus 5。

2.2 Software Specification

關於測試環境所需的軟體規格說明，如下列所示：

作業系統：Window 10、Android 6.0.1/7.1.1

2.3 Test Data Sources

在銘傳大學桃園校區資工系實驗室，由本計畫主持人及助理人員透過 Android 手機進行的交易模擬實驗，測試環境如 0 的示意。

3. Testing Schedule, Procedure, and Responsibility

3.1 Testing Schedule

時程

- 各子系統之內部元件整合測試 (Module Test)(106/2/25~106/6/8)
- 基於區塊鏈技術的收款監督系統整合測試 (Integration Test) (106/6/8~106/6/21)
- 基於區塊鏈技術的收款監督系統接受度測試 (Acceptance Test) (106/7/10~106/7/21)

查核點

- 各子系統之內部元件整合測試 (Module Test)(106/5/10)
- 基於區塊鏈技術的收款監督系統整合測試 (Integration Test) (106/7/1)
- 基於區塊鏈技術的收款監督系統接受度測試 (Acceptance Test) (106/7/1)

3.2 Testing Procedure

3.2.1 Integration Testing

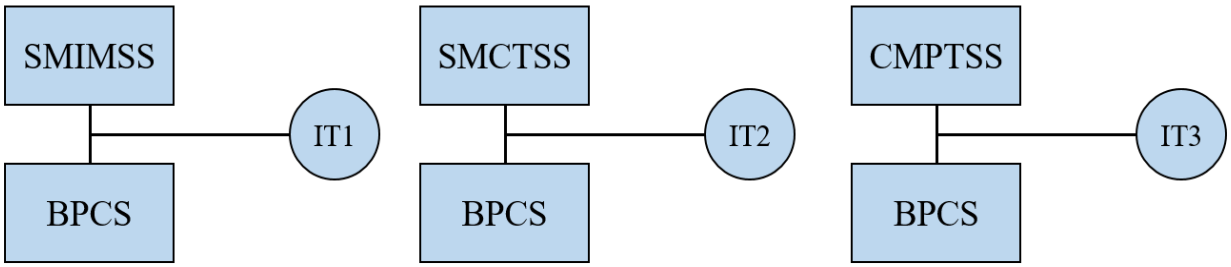

Figure 2 整合子系統測試

3.2.2 Acceptance Testing

本系統須達成使用案例(use case)所列功能：

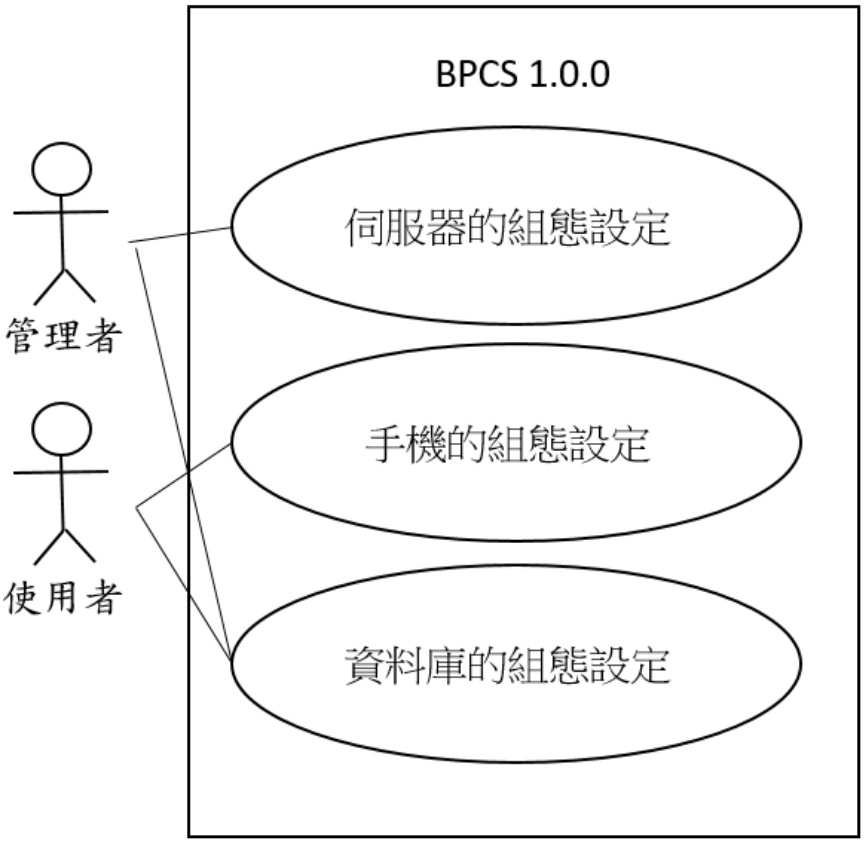

Figure 3 BPCS 使用案例圖 (use case diagram)

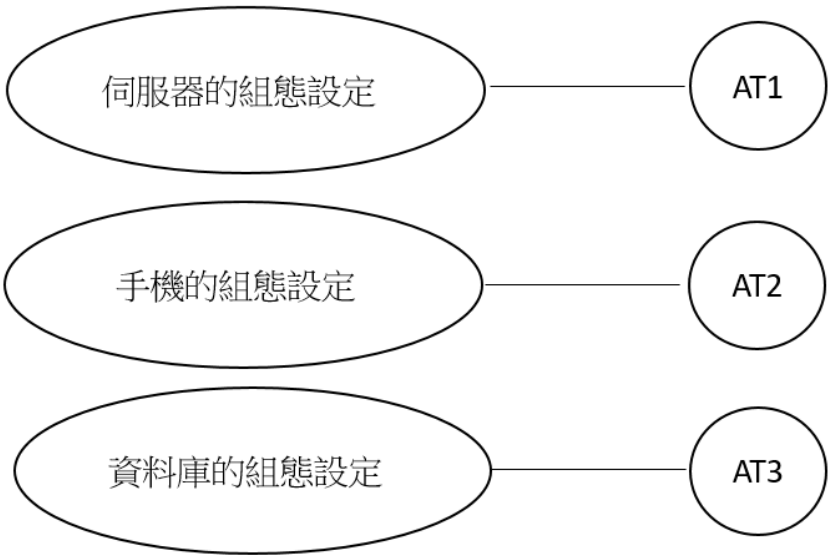

Figure 4 Acceptance Testing

3.3 Personnel Responsibilities Assignment

Table 1.　人員與職責分配表

Testing Activities	Personnel
IT1	王長勁
IT2	陳伯韋
IT3	江柏憲
AT1	王長勁
AT2	陳伯韋
AT3	江柏憲

4. Test Cases

4.1 Integration Testing Cases

4.1.1 IT1 Test Case

目的：

- 驗證〔SMIMSS 1.1.0〕能正確管理商品資訊

Table 2. IT1 Test Case

Identification	IT1
Name	整合 SMIMSS 至 BPCS
Tested target	[SMIMSS 1.1.0]、[BPCS 1.0.0]
Reference	**SMIMSS-F-001~ SMIMSS-F-005**
Severity	1(Critical)
Instructions	1. 能夠新增店家帳戶 2. 能夠新增/修改/刪除店員帳戶 3. 能夠新增/刪除/修改商品資訊 4. 能夠取得產品資訊 5. 能夠接收交易資訊
Expected result	1. 成功新增店家帳戶 2. 成功新增/修改/刪除店員帳戶 3. 成功新增/修改/刪除商品資訊 4. 成功取得產品資訊 5. 成功接收交易資訊
Cleanup	無

4.1.2 IT2 Test Case

目的：

- 驗證〔SMCTSS 1.2.0〕完成一筆行動支付之交易

Table 3. IT2 Test Case

Identification	IT2
Name	整合 SMCTSS 至 BPCS
Tested target	[SMCTSS1.2.0]、[BPCS 1.0.0]
Reference	**SMCTSS-F-001~ SMCTSS-F-007**
Severity	1(Critical)
Instructions	1. 能夠登入店員帳戶 2. 能夠掃描 NFC 標籤 3. 能夠讀取商品資訊 4. 能夠建立交易清單 5. 能夠傳送交易資訊 6. 能夠認證交易資訊 7. 能夠儲存交易明細
Expected result	1. 成功登入店員帳戶 2. 成功掃描 NFC 標籤 3. 成功讀取商品資訊 4. 成功建立交易清單 5. 成功傳送交易資訊 6. 成功認證交易資訊 7. 成功儲存交易明細
Cleanup	無

4.1.3 IT3 Test Case

目的：

- 驗證〔CMPTSS1.3.0〕能正確接收 SMCTSS 所傳送的交易資料，並以其交易資訊執行以比特幣付款之動作。可以查詢商品資訊，且能夠儲存並且查看使用者過往之交易紀錄。

Table 4. IT3 Test Case

Identification	IT3
Name	整合 CMPTSS 至 BPCS
Tested target	[CMPTSS.1.3.0]、[BPCS 1.0.0]
Reference	**CMPTSS-F-001~ CMPTSS-F-007**
Severity	1(Critical)
Instructions	1. 能夠登入客戶帳號 2. 能夠讀取商品資訊 3. 能夠接收交易清單 4. 能夠認證交易資訊 5. 能夠執行行動支付 6. 能夠儲存交易明細 7. 能夠查看交易紀錄
Expected result	1. 成功登入客戶帳號 2. 成功讀取商品資訊 3. 成功接收交易清單 4. 成功認證交易資訊 5. 成功執行行動支付 6. 成功儲存交易紀錄 7. 成功查看交易紀錄
Cleanup	無

4.2 Acceptance Testing Cases

4.2.1 AT1 Test Case

目的：

驗證使用案例（Use case ）1

透過組態檔案的修改對伺服器進行組態設定。

Table 5. AT1 Test Case

Identification	AT1	
Name	伺服器的組態設定	
Tested target	[SMIMSS 1.1.0]、	
Reference	**BPCS-F-001**	
Severity	1	
Instructions	*Actor actions*	*System responses*
	1.管理人員依照環境設定伺服器組態。	2.伺服器依照管理人員所做的組態設定啟動服務。
Expected result	成功啟動伺服器的相關服務	
Cleanup	無	

4.2.2 AT2 Test Case

目的：

驗證使用案例（Use case ）2

透過組態檔案的修改對手機進行組態設定。

Table 6. AT2 Test Case

Identification	AT2	
Name	手機的組態設定	
Tested target	[SMCTSS 1.2.0]、[CMPTSS 1.3.0]	
Reference	**BPCS-F-002~ BPCS-F-003**	
Severity	1	
Instructions	*Actor actions*	*System responses*
	1. 使用者修改手機組態設定參數。	2. 手機依照使用者在設定檔中所填入的數值運作。
Expected result	成功完成手機的組態設定	
Cleanup	無	

4.2.3 AT3 Test Case

目的：

驗證使用案例（Use case ）3

透過組態檔案的修改對資料庫進行組態設定。

Table 7. AT3 Test Case

Identification	AT2	
Name	資料庫的組態設定	
Tested target	[SMIMSS 1.1.0]、[SMCTSS 1.2.0]、[CMPTSS 1.3.0]	
Reference	**BPCS-F-001~ BPCS-F-003**	
Severity	1	
Instructions	*Actor actions*	*System responses*
	1. 管理者設定資料庫組態。 3.使用者修改資料庫之資料及檔案	2.資料庫依照管理人員所做的組態設定啟動服務。 4.資料庫依照使用者所做的組態設定啟動服務。
Expected result	成功設定完成資料庫的相關設定。	
Cleanup	無	

5. Test Results and Analysis

5.1 Integration Testing Cases

Table 8. 整合子系統測試結果

Test Case #	Results (PASS/FAIL)	Comment
IT1	PASS	1. 成功新增店家帳戶 2. 成功新增/修改/刪除店員帳戶 3. 成功新增/修改/刪除商品資訊 4. 成功取得產品資訊 5. 成功接收交易資訊
IT2	PASS	1. 成功登入店員帳戶 2. 成功掃描 NFC 標籤 3. 成功讀取商品資訊 4. 成功建立交易清單 5. 成功傳送交易資訊 6. 成功認證交易資訊 7. 成功儲存交易明細
IT3	PASS	1. 成功登入客戶帳號 2. 成功讀取商品資訊 3. 成功接收交易清單 4. 成功認證交易資訊 5. 成功執行行動支付 6. 成功儲存交易紀錄 7. 成功查看交易紀錄
RATE	90%	BPCS 開發透過手機讓商家及顧客以手機傳送交易資訊，如：商品名稱、商品金額，商家收款地址等……。並且及時將商品資訊更新至伺服器之資料庫，以便商家控管商品資訊狀態，同時讓顧客可以享受數位加密貨幣的方便性。

5.2 Acceptance Testing Cases

Table 9. 接受度測試結果

Test Case #	Results(PASS/FAIL)	Comment
AT1	PASS	成功啟動伺服器的相關服務
AT2	PASS	成功完成手機的組態設定
AT3	PASS	成功設定完成資料庫的相關設定。
Rate	100%	BPCS 可透過組態設定的方式來設定各個子系統的環境參數。

Appendix A: Traceability

A.1. Subsystems vs. Test Cases

Table 10. Subsystems vs. Test Cases Traceability Table

Subsystems / Test Cases	SMIMSS 1.1.0	SMCTSS 1.2.0	CMPISS 1.3.0
IT1	X		
IT2		X	
IT3			X
AT1	X		
AT2		X	X
AT3	X	X	X

A.2 Requirements vs. Test Cases

Table 11. Requirements vs. Test Cases Traceability Table

Test Cases / Requirements	IT1	IT2	IT3
BPCS-F-001	X		
BPCS-F-002		X	
BPCS-F-003			X
SMIMSS-F-001	X		
SMIMSS-F-002	X		
SMIMSS-F-003	X		
SMIMSS-F-004	X		
SMIMSS-F-005	X		
SMCTSS-F-001		X	
SMCTSS-F-002		X	
SMCTSS-F-003		X	
SMCTSS-F-004		X	
SMCTSS-F-005		X	
SMCTSS-F-006		X	
SMCTSS-F-007		X	
CMPTSS-F-001			X
CMPTSS-F-002			X
CMPTSS-F-003			X
CMPTSS-F-004			X
CMPTSS-F-005			X
CMPTSS-F-006			X
CMPTSS-F-007			X

Test Cases / Requirements	AT1	AT2	AT3
BPCS-F-001	X		X
BPCS-F-002		X	X
BPCS-F-003		X	X

Reference

[1] 王家輝, 陳伯韋, 江柏憲, 王長勁 "數位貨幣交易之安全性提升的設計與實作-以開放源碼之比特幣錢包為例," 科技部開放軟體專案計畫系統需求規格書, MOST 105-2221-E-130-006 –

[2] Po-Wei Chen、Chia-Hui Wang、 Jan-Ming Ho, " Discussion on the Security of Electronic Wallet of Digital Currency - Bitcoin Wallet as an Example ", the 9th Cross-Strait Conference on Information Science and Technology, National Quemoy University, Kinmen, 06~08 November, 2015

[3] 潘育群, 張瑞益, 王家輝 "開放原始碼手機上感測網路代理人之自由軟體系統開發-以個人遠端健康管理應用為例," 國科會自由軟體專案計畫系統測試報告書, NSC 99-2220-E-002-029

[4] 蘇維宗 (2016)" 軟體系統測試簡介暨系統測試報告書撰寫說明", https://cpr.twisc.flyelephant.com.tw/?p=514

[5] Bitcoin wallet on Github " https://github.com/bitcoin-wallet/bitcoin-wallet"