|  |
| --- |
|  |
| 愛金卡電子支付系統SA共用文件 |
|  |

|  |
| --- |
| 綠界科技股份有限公司  2019/5/14 |

[1. 簡介 3](#_Toc8812821)

[**1.1.** **目的** 3](#_Toc8812822)

[**1.2.** **參考文件** 3](#_Toc8812823)

[**1.3.** **術語與定義** 5](#_Toc8812824)

[**1.3.1.** **相關專有名詞** 5](#_Toc8812825)

[**1.3.2.** **程式開發使用技術專有名詞** 8](#_Toc8812826)

[2. 功能模組 13](#_Toc8812827)

[3. 安全機制 14](#_Toc8812828)

[**3.1.** **App安全設計** 14](#_Toc8812831)

[**3.2.** **QR code規格及安全設計** 18](#_Toc8812832)

[**3.3.** **OTP安全設計** 20](#_Toc8812833)

[**3.4.** **交易電文安全設計** 21](#_Toc8812834)

[4. 系統記錄留存方式 23](#_Toc8812835)

[**4.1.** **系統記錄查詢方式** 23](#_Toc8812837)

[5. 機敏個資保護機制 24](#_Toc8812838)

[**5.1.** **資料保護方式** 24](#_Toc8812840)

[**5.2.** **資料調閱機制** 25](#_Toc8812841)

[6. 批次排程設計說明 26](#_Toc8812842)

[7. 系統效能規劃目標 27](#_Toc8812843)

[**7.1.** **會員註冊** 27](#_Toc8812846)

[**7.2.** **會員登入** 28](#_Toc8812847)

[**7.3.** **會員交易** 28](#_Toc8812848)

[**7.3.1.** **線下交易：指由POS發動扣款的交易類型。** 28](#_Toc8812849)

[**7.3.2.** **線上交易：指由APP主動發動扣款交易。** 29](#_Toc8812850)

1. **簡介**
   1. **目的**

本文件以APP及後台系統管理之開發，將針對功能模組、安全機制、系統記錄留存方式、機敏個資保護機制、批次排程設計說明、系統效能規劃目標等主要內容，依章節說明之。

* 1. **參考文件**

本文件所參考的文件資料清單如下表所示。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序號 | 文件名稱 | 版本 | 作者 | 備註 |
|  | -中信\_AccountLink-SECP規格書(愛金卡).pdf -中信電支批次檔案規格-20180731.pdf -中國信託\_虛擬帳號檢核邏輯\_金額檢核(53檢核).pdf -CTBC Payment API\_V2.4 (愛金卡).pdf |  |  | 中國信託 |
|  | -國泰世華銀行帳戶串接API規格書(v1 1 02).pdf |  |  | 國泰世華 |
|  | -第一銀行Acount Link平台API介面規格\_V1.1.pdf -即時銷帳客戶端開發說明.pdf -連線檢核介接規格(AP 2 AP) .pdf -虛擬帳號檢核公式.pdf -FXML系統-技術手冊.doc |  |  | 第一銀行 |
|  | -Mail2000\_API\_說明文件\_v7.2.pdf |  |  | 網擎(Mail2000) |
|  | -HTTP\_MitakeAPI\_v2.03.pdf |  |  | 三竹 |
|  | -電子發票應用API規格V1.7.pdf |  |  | 財政部電子發票 |
|  | -20190429\_B2BEIVCP\_RA013\_WebService介面資料.xls |  |  | PIC |
|  | -會員記名\_OPENAPP\_NEW\_PM\_20190513\_電支.xls -OPimidpush串接規格書\_icashpay\_20190430\_v2.1.doc |  |  | OPEN POINT |
|  |  |  |  |  |
|  |  |  |  |  |
|  | | | |

表格 1 – 參考文件總表

* 1. **術語與定義**

本節說明本文件中重要專有名詞定義以及所使用的術語、簡稱及定義。

* + 1. **相關專有名詞**

|  |  |
| --- | --- |
| 名詞或術語 | 定義或說明 |
| OTP | 一次性密碼 (One Time Password)，為本系統中用以驗證手機與電子郵件帳號真確性的機制。 |
| FXML | 金融XML (Financial eXtensible Markup Language)，係W3C公司於1997年底所通過的標準，主要運用在internet上傳送或處理文件資料，著重在文件資料結構描述。採用國際標準訂定，適用於國內之網路金融相關訊息共用標準，可達到資料交換格式一致化及互通式、可提供與企業電子商務整合之網際網路金流解決方案、可達成國內憑證共通性。 |
| 商戶 | 商務會員的法人機構 |
| 商店 | 商務會員於商務平台所開設的商店 |
| 虛擬帳號儲值 | ATM儲值 |
| 連結帳戶儲值 | 銀行帳號儲值 |
| 帳戶餘額 | icash帳戶 |
| 銀行帳戶驗證 | 銀行帳號驗證 |
| E-mail | 電子信箱 |
| 手機簡訊驗證 | 手機OTP驗證 |
| 登入帳號 | 註冊時會員自定的帳號 |
| 電支帳號 | 會員編號 |
| 安全密碼 | 支付密碼(同喚醒密碼) |
| 群組名稱 | 部門名稱 |
| 使用者帳號管理 | 愛金卡內部後台帳號管理 |
| 使用者帳號 | 愛金卡內部後台登入帳號 |
| 使用者名稱 | 愛金卡內部後台輸入員工的名稱(本名) |
| P11驗證 | 身分證換補發驗證 |
| P33驗證 | 身分證字號金融警示戶驗證 |
| 凍結款 | 當有交易糾紛或其他特殊原因時，可由客服人員從會員資料查詢功能進行設定，暫時將該會員帳戶內現有帳戶餘額中，設定金額做凍結，此筆金額無法進行提領或交易。 |
| 保留款 | 商戶建檔時，由風控人員評估商戶之風險，決定是否要限制商戶的帳戶內是否要保留有一定的金額(可設定)不可提領或交易，以作為風險控管之用。 |
| MCC code | Merchant Category Code 商戶類別代碼 |
| IP | Internet Protocol Address網際網路協定位址 |
| 裝置ID | 行動裝置的識別代碼 |
| PEPS | 高知名度政治性人物 |
| NN | 負面新聞 |
| RCA | 關係密切之人或家屬 |
| BL | 國際制裁黑名單 |
| AKA | 公司別名 |
| RC分數 | 從集保匯出的分數 |
| 代理收付實質交易款項 | 指電子支付機構獨立於實質交易之使用者以外，依交易雙方委任，接受付款方所移轉實質交易之金額，並經一定條件成就、一定期間屆至或付款方指示後，將該實質交易之金額移轉予收款方之業務。 |
| 收受儲值款項 | 指電子支付機構接受使用者將款項預先存放於電子支付帳戶，以供與電子支付機構以外之其他使用者進行資金移轉使用之業務。 |
| 電子支付帳戶間款項移轉 | 指電子支付機構依使用者非基於實質交易之支付指示，將其電子支付帳戶內之資金，移轉至該電子支付機構其他使用者之電子支付帳戶之業務。 |
| 電子支付機構業務 | 指本條例第三條第一項各款業務。 |
| 電子支付平臺 | 指辦理電子支付機構業務相關之應用軟體、系統軟體及硬體設備。 |
| 電子支付作業環境 | 指電子支付平臺、網路、作業人員及與該電子支付平臺網路直接連結之應用軟體、系統軟體及硬體設備。 |
| 電子支付帳戶 | 指電子支付機構接受使用者開立記錄資金移轉與儲值情形之網路帳戶。 |
| 使用者 | 指於電子支付機構註冊及開立電子支付帳戶，利用電子支付機構所提供服務進行資金移轉或儲值者。 |
| 收款使用者 | 指利用電子支付機構所提供代理收付實質交易款項服務，進行收款之使用者。 |
| 約定連結存款帳戶付款 | 指電子支付機構辦理電子支付機構業務，依使用者與開戶金融機構間之約定，向開戶金融機構提出扣款指示，連結該使用者存款帳戶進行轉帳，由電子支付機構收取支付款項，並於該使用者電子支付帳戶記錄支付款項金額及移轉情形之服務，作業機制如下：  （一）直接連結機制：指電子支付機構直接向開戶金融機構提出扣款指示，連結使用者存款帳戶進行轉帳之機制。  （二）間接連結機制：指電子支付機構經由專用存款帳戶銀行介接金融資訊服務事業或票據交換所，間接向開戶金融機構提出扣款指示，連結使用者存款帳戶進行轉帳之機制。 |
| 收款使用者收付訊息整合傳遞 | 指電子支付機構接受收款使用者及其他機構委任，提供端末設備或應用程式，整合傳遞收付訊息。 |
| 個人使用者 | 指自然人之使用者，包括外國自然人及大陸地區自然人。 |
| 非個人使用者 | 指我國政府機關、法人、行號、其他團體及外國法人與大陸地區法人之使用者。 |
| 系統維運人員 | 指電子支付平臺之作業人員，其管理或操作營運環境之應用軟體、系統軟體、硬體、網路、資料庫、使用者服務、業務推廣、帳務管理或會計管理等作業。 |
| 專屬網路 | 指利用電子設備或通訊設備直接以連線方式（撥接（Dial-Up）、專線（Leased-Line）或虛擬私有網路（VirtualPrivate Network，VPN）等）進行訊息傳輸。 |
| 網際網路（Internet） | 指利用電子設備或通訊設備，透過網際網路服務業者進行訊息傳輸。 |
| 行動網路 | 指利用電子設備或通訊設備，透過電信服務業者進行訊息傳輸。 |
| 訊息隱密性（Confidentiality） | 指訊息不會遭截取、窺竊而洩漏資料內容致損害其秘密性。 |
| 訊息完整性（Integrity） | 指訊息內容不會遭篡改而造成資料不正確，即訊息如遭篡改時，該筆訊息無效。 |
| 訊息來源辨識性（Authentication） | 指傳送方無法冒名傳送資料。 |
| 訊息不可重複性（Non-duplication） | 指訊息內容不得重複。 |
| 訊息不可否認性（Non-repudiation） | 指無法否認其傳送或接收訊息行為。 |
| 一次性密碼（One Time Password ；以下簡稱 OTP） | 指運用動態密碼產生器、晶片金融卡或以其他方式運用 OTP原理，產生限定一次使用之密碼。 |
| 行動裝置 | 指包含但不限於智慧型手機、平板電腦等具通信及連網功能之設備。 |
| 機敏資料 | 指包含但不限於密碼、個人資料、身分認證資料、信用卡卡號、信用卡驗證碼或個人化資料等。 |
| 近距離無線通訊（Near Field Communication；以下簡稱 NFC） | 指利用點對點功能，使行動裝置在近距離內與其他設備進行資料傳輸。 |
| 實體通路支付服務（Online To Offline，O2O） | 指電子支付機構就電子支付機構業務，利用行動裝置或其他可攜式設備於實體通路提供服務。 |
| 約定連結存款帳戶付款 | 指電子支付機構辦理電子支付機構業務，依使用者與開戶金融機構間之約定，向開戶金融機構提出扣款指示，連結該使用者存款帳戶進行轉帳，由電子支付機構收取支付款項，並於該使用者電子支付帳戶記錄支付款項金額及移轉情形之服務，作業機制如下：  （一）直接連結機制：指電子支付機構直接向開戶金融機構提出扣款指示，連結使用者存款帳戶進行轉帳之機制。  （二）間接連結機制：指電子支付機構經由專用存款帳戶銀行介接金融資訊服務事業或票據交換所，間接向開戶金融機構提出扣款指示，連結使用者存款帳戶進行轉帳之機制。 |

表格 2 – 專有名詞定義表

* + 1. **程式開發使用技術專有名詞**

|  |  |
| --- | --- |
| 名詞或術語 | 定義或說明 |
| RWD | 響應式網頁設計（Responsive Web Design）是一種網頁設計的技術做法，該設計可使網站在多種瀏覽裝置（從桌面電腦顯示器到行動電話或其他行動產品裝置）上閱讀和導航，同時減少縮放、平移和捲動。 |
| jQuery | jQuery是開放原始碼軟體，使用MIT許可證授權。jQuery是一套跨瀏覽器的JavaScript函式庫，簡化HTML與JavaScript之間的操作，例如:DOM的操作選擇、建立動畫效果、處理事件以及開發AJAX程式。 |
| Bootstrap | Bootstrap是一組用於網站和網頁應用程序開發的開放原始碼前端框架，包括HTML、CSS及JavaScript的框架，提供字體排印、表單、按鈕、導航及其他各種元件及Javascript擴充套件，旨在使動態網頁和Web應用的開發更加容易。 |
| ASP.NET MVC Framework | ASP.NET MVC Framework是微軟在ASP.NET中所添加的一組類別庫，這組類別庫可以使用Model-View-Controller的設計模式來開發ASP.NET的應用程式。  MVC是遵循軟體模式的Model-View-Controller來發展，其中Model指的是資料或是業務邏輯元件，View是呈現給使用者看的資訊，而Controller則是接取來自使用者的指令與資料，並將Model與View做整合的控制器，當伺服器接到對ASP.NET MVC應用程式的要求時，伺服器（IIS）會先使用UrlRoutingModule(ASP.NET Routing的 HTTP 模組)，由它來解析是否有包含ASP.NET MVC應用程式的URL，若有，則會產生一個MvcRouteHandler物件，這個物件會裝載執行的必要資訊，並且會呼叫包含在URL中的Controller的Execute方法來執行工作 |
| SQL Server | Microsoft SQL Server(微軟結構化查詢語言服務器)是由美國微軟公司所推出的關聯式資料庫解決方案，最新的版本是SQL Server 2017，已在美國時間2017年10月2日發佈。  資料庫的內置語言原本是採用美國標準局和國際標準組織所定義的SQL語言，但是微軟公司對它進行了部分擴充而成為作業用SQL。 |
| Stored Procedure | 預存程序是一段T-SQL語法之集合。 類似其他程式語言中的函數或方法。 可以封裝隱藏資料/商業邏輯。 Stored Procedure 是已經編譯過的, 所以執行效率快。 可以提升安全性，可以只賦予EXEC權限。無需存取資料表。適當的時候可以開放其他Select或Insert等權限 |
| 對稱性加解密演算法 | 指資料加密標準（Data Encryption Standard；以下簡稱 DES）、三重資料加密標準（Triple DES；以下簡稱 3DES） 、進階資料加密標準（Advanced Encryption Standard；以下簡稱 AES）。 |
| 非對稱性加解密演算法 | 指 RSA 加密演算法（Rivest, Shamir and Adleman Encryption Algorithm；以下簡稱 RSA）、橢圓曲線密碼學（Elliptic Curve Cryptography ；以下簡稱 ECC） |
| 雜湊函數 | 指安全雜湊演算法（Secure Hash Algorithm； 以下簡稱 SHA）。 |
| Android | 是一個基於Linux核心的開放原始碼行動作業系統。 |
| Android Studio | android 開發工具。 |
| Eclipse | android 早期開發工具，目前已使用Android Studio為主。 |
| Java | Android 開發使用的程式語言。 |
| Kotlin | 程式語言，目前Android官方指定程式語言。 |
| gradle | Gradle是一個基於Apache Ant和Apache Maven概念的專案自動化建構工具。它使用一種基於Groovy的特定領域語言來聲明專案設定，而不是傳統的XML。 |
| groovy | Apache的Groovy是Java平台上設計的物件導向程式設計語言。這門動態語言擁有類似Python、Ruby和Smalltalk中的一些特性，可以作為Java平台的手稿語言使用，Groovy代碼動態地編譯成執行於Java虛擬機器上的Java位元組碼，並與其他Java代碼和庫進行互操作。 |
| maven | Apache Maven，是一個軟體專案管理及自動構建工具，由Apache軟體基金會所提供。基於專案物件模型概念，Maven利用一個中央資訊片斷能管理一個專案的構建、報告和文件等步驟。 |
| Data Binding | android 官方推出用XML資源檔綁定元件而不是使用程式碼方式。 |
| aar | Android library檔案名稱的附檔名。 |
| apk | Android app應用的檔案名稱的附檔名。 |
| Activity | Android與使用者互動的元件。 |
| Fragment | Android Activity裡面的一個顯示介面。 |
| androidx | 基於Jetpack開發的用來取代 android.support 的官方套件。 |
| Jetpack | 幫助開發人員更輕鬆地編寫高質量的應用程序的官方套件。 |
| Google Play | android app應用官方市集。 |
| Firebase | Google官方推薦雲端開發平台。 |
| GCM | Google Cloud Messaging ，Google官方推播平台，目前已轉移到FCM。 |
| FCM | Firebase Cloud Messaging，Google架構再Firebase上的官方推播平台 |
| iOS | iOS是蘋果公司為其行動裝置所開發的專有行動作業系統，為其公司的許多行動裝置提供操作介面，支援裝置包括iPhone、iPad和iPod touch。 |
| iPhone | iPhone是蘋果公司研發及銷售的智慧型手機系列，它搭載蘋果公司研發的iOS行動作業系統。 |
| iOS Certificates | iOS 開發需要請求Apple 公鑰交換，並使用此憑證認證 |
| Apple App IDs | 也是 Bundle ID(Bundle Identifier)是一款iOS應用的唯一標識，應用與Bundle ID之間是唯一對應關係。 |
| Provisioning Profiles | 描述編譯出來的IPA 使用了哪個Apple IDs 此App 用途，綁定的憑證，測試用還有可以測試的裝置 |
| Apple Store | Apple app應用官方市集。 |
| APNS （Apple Push Notification Service） | Apple 推播通知服務是蘋果公司2009年6月17日隨iOS 3.0推出的一項服務。它通過長IP連線推播技術從第三方應用向蘋果裝置提供推播通知服務，通知中可能包括標記、聲音、提醒/橫幅。在iOS 5中，通知中心加強了推播和本地通知的用戶體驗。 |
| XCode | Xcode是蘋果公司向開發人員提供的整合開發環境，用於開發macOS、iOS、WatchOS和tvOS的應用程式。 |
| CocoaPods | CocoaPods 是一應用級別的依賴管理器，針對Objective-C、Swift和其他任一在Objective-C運行時上運行的語言，如RubyMotion，它為額外的庫的管理提供了標準的格式。 |
| Objective-C | Objective-C是一種通用、進階、物件導向的程式語言。它擴充了標準的ANSI C程式語言，將Smalltalk式的訊息傳遞機制加入到ANSI C中。目前主要支援的編譯器有GCC和Clang。 |
| Swift | Swift程式語言，支援多編程範式和編譯式，用來撰寫基於macOS/OS X、iOS、watchOS和tvOS的軟體。 蘋果公司於2014年在蘋果開發者年會發布了Swift程式語言。 |

表格 3 – 程式開發使用技術專有名詞

1. **功能模組**

|  |  |
| --- | --- |
| **會員系統** -會員資訊  -安全設定  -支付綁定  -帳戶管理 | **交易系統** -代收代付  -儲值  -轉帳  -自動儲值 |
| **驗證系統** -銀行帳戶驗證  -手機OTP驗證  -身分證驗 | **付款系統** -電支帳戶  -銀行帳戶 |
| **管理系統** -系統管理  -會員管理  -商家管理  -交易查詢 | **風控系統** -會員風控  -商家風控  -黑名單  -洗錢防制  -告警機制 |
| **帳務系統** -電支帳戶管理  -代理收付帳務管理  -專用存款帳戶管理 | **電子發票系統**  -手機載具發票明細  -會員載具歸戶手機條碼載具  -中獎發票通知 |
| **財務報表系統**  -營收統計報表  -會員轉帳報表  -手續費統計  -ERP資料檔提供 | **廣告行銷獎勵活動系統** -廣告管理  -獎勵活動管理 |
| **郵件系統** | **簡訊系統** |

1. **安全機制**
3. 1. **App安全設計**

App安全設計，符合經濟部工業局-行動應用App基本資安檢測基準。

|  |  |  |  |
| --- | --- | --- | --- |
| **資訊安全技術要求面向** | **資訊安全技術要求事項** | **技術要求** | **實施方式** |
| 4.1.2.安全敏感性 資料保護 | 4.1.2.1.安全敏感性資料蒐集 | 4.1.2.1.1.行動應用程式應於蒐集安全敏感性資料前，取得 使用者同意。 | 行動應用程式所有蒐集之安全敏感性資料，皆已於 App Store 或行動應用程式內使用條款說明並取得使用者同意。 |
| 4.1.2.1.2.行動應用程式應提供使用者拒絕蒐集安全敏感 性資料之權利。 | 行動應用程式有提供使者拒絕蒐集安全敏感性資料之選項，且拒絕同意時不使搜集安全敏感資料。 |
| 4.1.2.2.安全敏感性資料利用 | 4.1.2.2.1.行動應用程式應於使用安全敏感性資料前，取得 使用者同意。 | 行動應用程式所有蒐集之安全敏感性資料，皆已於 App Store 或行動應用程式內使用條款說明並取得使用者同意。 |
| 4.1.2.3.安全敏感性資料儲存 | 4.1.2.3.1.行動應用程式應於儲存安全敏感性資料前，取得使用者同意。 | 行動應用程式內不儲存敏感性資料。 |
| 4.1.2.3.2.行動應用程式應提供使用者拒絕儲存安全敏感性資料之權利。 | 行動應用程式內不儲存敏感性資料。 |
| 4.1.2.3.5.行動應用程式應避免將安全敏感性資料儲存於冗餘檔案或日誌檔案中。 | 行動應用程式內不儲存敏感性資料。 |
| 4.1.2.3.6.安全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。 | 敏感性資料儲存資料會使用AES128以上的加密演算法儲存。 |
| 4.1.2.3.7.安全敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取。 | 資料儲存於該行動應用程式作用範圍，令其他應用程式無法存取。 |
| 4.1.2.3.8.安全敏感性資料應避免出現於行動應用程式之程式碼。 | 行動應用程式之程式碼和安裝檔不放置敏感性資料如密碼金鑰演算法金鑰。 |
| 4.1.2.4.安全敏感性資料傳輸 | 4.1.2.4.1.行動應用程式透過網路傳輸安全敏感性資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密。 | 行動應用程式採用TLS1.1（含）以上版本加密協定進行傳輸。 |
| 行動應用程式採用金鑰有效長度128位元（含）之進階加密標準(AES) 。 |
| 4.1.2.5.安全敏感性資料分享 | 4.1.2.5.1.行動裝置內之不同行動應用程式間，應於分享安全敏感性資料前，取得使用者同意。 | 未分享敏感性資料。 |
| 4.1.2.5.2.行動應用程式應提供使用者拒絕分享安全敏感性資料之權利。 | 未分享敏感性資料。 |
| 4.1.2.5.3.行動應用程式分享安全敏感性資料時，應避免未授權之行動應用程式存取。 | 未分享敏感性資料。 |
| 4.1.3.交易資源控管安全 | 4.1.3.1.交易資源使用 | 4.1.3.1.1.行動應用程式應於使用交易資源前主動通知使用者。 | 行動應用程式於交易前，會主動告知使用者交易資源名稱金額及方式。 |
| 4.1.3.1.2.行動應用程式應提供使用者拒絕使用交易資源之權利。 | 有提供使用者拒絕交易的按鈕，使用者拒絕交易的情況下，將不會進行交易。 |
| 4.1.3.2.交易資源控管 | 4.1.3.2.1.行動應用程式應於使用交易資源前進行使用者身分鑑別。 | 使用交易前，會提供身份鑑別機制，需要使用登入密碼或安全密碼。 |
| 4.1.3.2.2.行動應用程式應記錄使用之交易資源與時間。 | 交易後，有提供查詢交易資源交易紀錄之管道，且有標注交易金額交易時間之紀錄。 |
| 4.1.4.行動應用程式使用者身分鑑別、授權與連線管理安全 | 4.1.4.1.使用者身分鑑別與授權 | 4.1.4.1.1.行動應用程式應有適當之身分鑑別機制，確認使用者身分。 | 有提供登入機制和安全密碼驗證，確認使用者。 |
| 4.1.4.1.2.行動應用程式應依使用者身分授權。 | 有提供使用者授權機制。 |
| 4.1.4.2.連線管理機制 | 4.1.4.2.1.行動應用程式應避免使用具有規則性之交談識別碼。 | 1.採用128為元以上的交談式別碼。 |
| 2.使用交談式別碼與時間使用者提交資料，具歸數字或字串有直接關連難以偽造。 |
| 3.使用者交談識別碼具登出失效機制。 |
| 4.1.4.2.2.行動應用程式應確認伺服器憑證之有效性。 | 1.行動應用程式使之伺服器憑證仍於有效期間內、未被註銷，且憑證之主體名稱與別包含連線伺服器網域名稱。 |
| 2.行動應用程式有 使用憑證綁定 (Certificate Pinning) 方式驗證， 以確保連線之伺服器為行動應用程式開發者所指定。 |
| 4.1.4.2.3.行動應用程式應確認伺服器憑證為可信任之憑證機構所簽發。 | 行動應用程式有驗證並確保伺服器憑為作業系統內建可信任之憑證機構所簽發。 |
| 4.1.4.2.4.行動應用程式應避免與未具有效憑證之伺服器，進行連線與傳輸資料。 | 行動應用程式會符合檢測編號 4.1.4.2.2 之憑證與伺服器進行連線與傳輸安全敏感性資料。 |
| 4.1.5.行動應用程式碼安全 | 4.1.5.1.防範惡意程式碼與避免資訊安全漏洞 | 4.1.5.1.1.行動應用程式應避免含有惡意程式碼。 | 行動應用程式未對其他或作業系統之檔案，在未授權情況下，嘗試進行查詢、新增修改刪除存取遠端服務、提權等行為，且未包括可導致動作業系統發生預期錯誤、資源明顯耗損、重新啟動或關閉等行為。 |
| 4.1.5.1.2.行動應用程式應避免資訊安全漏洞。 | 程式碼進行資安檢測，確保不會有漏洞。 |
| 4.1.5.3.函式庫引用安全 | 4.1.5.3.1.行動應用程式於引用之函式庫有更新時，應備妥對應之更新版本，更新方式請參酌4.1.1.行動應用程式發布安全。 | 會檢查使用函式庫，是否符合使用。 |
| 4.1.5.4.使用者輸入驗證 | 4.1.5.4.1.行動應用程式應針對使用者於輸入階段之字串，進行安全檢查。 | 會對使用者輸入資料進行檢查型別及長度。 |
| 4.1.5.4.2.行動應用程式應提供相關注入攻擊防護機制。 | 會使用注入文字進行檢測確保無法注入成功。 |
| 4.2.2. 伺服器端  安全檢測 | 4.2.2.1. Web view安全檢測 | 4.2.2.1.2.行動應用程式於Web view呈現功能時，所連線之網域應為安全網域。 | 只會連線至信任的網站。 |
| 確保目標網站都採用金密協定。 |

* 1. **QR code規格及安全設計**

符合中華民國銀行商業同業公會全國聯合會為確保金融機構，提供QR Code（Quick Response Code）掃描支付應用具有一致性之安全控管作業，所訂定的『金融機構提供QR Code掃描支付應用安全控管規範』。

|  |  |
| --- | --- |
| 條 文 | 執行方式 |
| 第一條 中華民國銀行商業同業公會全國聯合會（以下簡稱本會）為確保金融機構提供QR Code（Quick Response Code）掃描支付應用具有一致性之安全控管作業，俾於國內建立方便及安全之QR Code支付環境，特訂定本規範。  第二條 本規範用詞定義如下：  一、QR Code：係二維條碼的一種，為矩陣式黑白相間的點狀或條狀圖形，除能表示文字、圖形及聲音等資訊，尚有容量大、可靠性高及資料完整性等特性。  二、QR Code受理終端：指參與QR Code條碼解析與生成之終端裝置，包含但不限於行動、POS 及自動化服務設備等裝置，並依照QR Code資訊以進行相關交易作業。  三、消費商店：指提供商品販售或服務等場所，採QR Code支付技術向客戶收取商品或服務費用，簡稱商店。  四、QR Code處理平臺：QR Code之管理平臺，提供 QR Code條碼解析與生成、重要資料之加解密、加解密系統金鑰管理及交易訊息處理等功能。  五、主掃模式：金融機構、商店、收款機構或收款客戶生成交易之QR Code，付款客戶持行動裝置應用程式掃描以確認交易， 傳輸至QR Code處理平臺或其他支付系統，完成支付交易。  六、被掃模式：付款客戶持行動裝置應用程式生成QR Code，提供商店或收款客戶掃描後，傳輸至QR Code處理平臺或其他支付系統，完成支付交易。  七、交易資訊類：係指該QR Code用於取代人工輸入之行為，該QR Code被掃描後，掃描之處理端應用程式顯示相關資訊，經使用者檢視 QR Code內容後，由客戶另啟動交易指示者。  八、交易指示類：係指該QR Code被QR Code受理終端掃描解析後，應用程式依所含指示內容進行交易，涉及資金轉移或直接影響客戶及商店權益者。 | 不適用。 |
| 第三條 QR Code掃描支付過程中，所存取之資訊應遵循該業務所需最小化原則。 | 付款QR Code：IC 開頭 18 碼為亂數，無法直接識別資料  如：IC115A0SOD506UKHLUXX |
| 第四條 採用交易資訊類QR Code者，應用程式應以彈出式視窗或其他方式提供接收方檢視QR Code之資料內容，再由接收方處理後續事宜。 | 符合現行電子支付法規，網際網路實質交易，會經過支付指示確認後，方能繼續交易。 |
| 第五條 被掃模式採用交易指示類 QR Code 者，因係屬使用者產生授權資訊同意扣款性質，應設定QR Code合理使用時效，且在時效內以使用一次為限。 | 是，當被掃模式產生之QR Code ，將於產生後60秒後失效，且無法重覆使用，且交易條碼只能被使用一次。 |
| 第六條 QR Code受理終端所提交之QR Code 訊息請求應確保傳輸過程中的資訊完整性及隱密性，並確保在傳輸過程中不被篡改及洩露。 | 訊息傳輸採用SSL加密通道，確保完整性及隱密性，並不會被竄改。 |
| 第七條 QR Code受理終端相關應用程式，應能針對所解析之QR Code進行格式檢查，確保資料格式合理性，預防程式碼注入。 | 受理終端，須依提供檢核公式，檢核碼是否正確。 |
| 第八條 QR Code受理終端相關應用程式，應能針對所解析之交易指示類 QR Code進行來源辨識性及完整性檢查，對於未驗證通過之 QR Code應予明確提示並拒絕執行交易。 | QR Code處理平臺，會檢核是否QR Cod受理終端確認產生，且於有效時限內，否會對提示並拒絕交易(伺服器端)。 |
| 第九條 QR Code 受理終端相關應用程式，對所解析之 QR Code 產生網站連結，應採包括但不限於白名單或伺服器認證等機制進行網站合法性檢查，以預防連結惡意網站或執行惡意程式風險。 | 不適用 (SDK內無此功能)。 |
| 第十條 主掃模式及被掃模式等各類應用情境，所生成之交易指示類QR Code收付不得共用，以確保專碼專用。 | 交易，及收款儲值QR Code採用不同規則；且在不同功能頁面產生。 |
| 第十一條 本規範經本會理事會通過並函報金融監督管理委員會核備後實施，修正時亦同。 | 不適用。 |

* 1. **OTP安全設計**

本專案OTP設計上，為提供驗證服務，除限定只發送至會員手機號碼中，並包含以下幾項安全設計：

**一次有效性：**當OTP被使用之後，會立即失效。

**時效性：**所有OTP皆有時效限制，超過時效後就無法再被使用。

**不可預測性：**採用亂數隨機生成，無特定規則。

* 1. **交易電文安全設計**

符合電子支付機構資訊系統標準及安全控管作業基準辦法-第8條第二項：

網際網路或行動網路：應符合訊息隱密性、訊息完整性、訊息來源辨識性及訊息不可重複性之訊息防護措施

符合電子支付機構資訊系統標準及安全控管作業基準辦法第9條：

一、**訊息隱密性**：應採用 3DES 112bits、AES 128bits、RSA 2048bits、ECC 256bits 以上或其他安全強度相同（含）以上之演算法進行加密運算。

二、**訊息完整性**：應採用 SHA 160bits、3DES 112bits、AES 128bits、RSA 2048bits、ECC 256bits 以上或其他安全強度相同（含）以上之演算法進行壓碼或加密運算。

三、**訊息來源辨識性**：應採用 SHA 160bits、3DES 112bits、AES128bits、RSA 2048bits、ECC 256bits 以上或其他安全強度相同（含）以上之演算法進行壓碼、加密運算或數位簽章。

四、**訊息不可重複性**：應採用序號、一次性亂數、時間戳記等機制產生。

五、**訊息不可否認性**：應採用 SHA256 以上或其他安全強度相同（含）以上之演算法進行壓碼，及採用 RSA 2048bits、ECC 256bits 以上或其他安全強度相同（含）以上之演算法進行數位簽章。

交易電文安全設計如下：

1. 訊息隱密性採用**AES 256bits**之演算法進行加密運算。
2. 訊息完整性採用**AES 256bits**之演算法加密運算。
3. 訊息來源辨識性採用**RSA 2048bits**之演算法進行數位簽章。
4. 訊息不可重複性採用序號(**交易編號**)、一次性亂數(**交易識別碼(條碼)**)、時間戳記(**用戶端簽章**)等機制產生。
5. 訊息不可否認性採用 **SHA256withRSA**之演算法進行數位簽章壓碼。

金鑰交換方式流程圖如下：



1. **系統記錄留存方式**

系統log記錄會儲存到資料庫及檔案中，預設存到資料庫，若存到資料庫失敗時會暫存文字檔案系統，資料庫回覆正常時，再由排程回存文字檔案log內容回資料庫中。

1. 1. **系統記錄查詢方式**

查詢方式依系統記錄分類分別為：

1. 系統異常記錄查詢。
2. 後台使用者操作記錄查詢。
3. APP API作業記錄查詢。
4. 廠商交易作業記錄查詢。
5. 管理銀行作業記錄查詢。
6. 銀行帳戶連結作業記錄查詢。
7. ATM儲值作業記錄查詢。
8. 交易紅利抵扣記錄查詢(財務報表) 。
9. 會員簡訊及推播及Email記錄查詢。
10. 聯合徵信中心作業記錄查詢。
11. 財政部電子發票相關作業記錄查詢。
12. PIC發票開立相關作業記錄查詢。
13. 系統排程作業記錄查詢。
14. **機敏個資保護機制**

依電子支付機構資訊系統標準及安全控管作業基準辦法第3條第10項定義，機敏資料：指包含但不限於密碼、個人資料、身分認證資料、信用卡卡號、信用卡驗證碼或個人化資料等。

1. 1. **資料保護方式**

符合電子支付機構資訊系統標準及安全控管作業基準辦法第10條第一項第一點，機敏資料於網際網路傳輸時全程使用加密保護。

符合電子支付機構資訊系統標準及安全控管作業基準辦法第10條第一項第八點，系統設計個人資料顯示之隱碼機制如下：

使用者姓名：顯示首字與末字，其餘以隱碼；若僅兩個字則顯示首字，第二字以隱碼顯示。

E-mail：顯示 @前保留頭尾各一個字其餘以＊隱碼，＠後第一字，頭尾字需＊隱碼其餘皆顯示。

帳號：顯示頭尾各兩碼，其餘以＊隱碼顯示

密碼：全部以＊隱碼顯示。

身分證字號欄位：此欄位需顯示使用者身分證字號，顯示格式：英文字母＋三碼數字＋三碼隱碼＋三碼數字。

符合電子支付機構資訊系統標準及安全控管作業基準辦法第10條第三項第三點，App端程式設計儲存機敏資料，採取加密機制進行保護。

符合電子支付機構資訊系統標準及安全控管作業基準辦法第10條第九項，設計個人資料檔案及資料庫之存取控制與保護監控措施，使用DB的遮罩MASK處理機制。

符合電子支付機構資訊系統標準及安全控管作業基準辦法第14條第一項第一點及第二點，機敏資料儲存於使用者端操作環境時建立訊息隱密性機制，機敏資料於網際網路上傳輸建立訊息隱密性機制，系統採取加密機制進行儲存及傳輸保護機制。

符合電子支付機構資訊系統標準及安全控管作業基準辦法第18條第一項，機敏資料僅能存放於安全的網路區域，不得存放於網際網路及DMZ等區域。對外網際網路服務僅能透過DMZ進行，再由DMZ 連線至其他網路區域。

* 1. **資料調閱機制**

符合電子支付機構資訊系統標準及安全控管作業基準辦法第13條第一項第五點，建置留存個人資料使用稽核軌跡（如登入帳號、系統功能、時間、系統名稱、查詢指令或結果）或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況，包括檔案、螢幕畫面、列表等。

在系統規劃上有含機敏個資相關的調閱功能，如「電支使用者資料查詢」、「未成年註冊審核」、「客服驗證」、「洗錢防制」、「商戶建檔」、「電支使用者刪除資料查詢」...等功能，皆以權限控管的方式，需具有該功能權限的操作者帳號，始得進入該功能調閱相關資訊；權限控管的相關功能，可參考「後台系統管理\_權限設定功能」之SA文件內容說明。

1. **批次排程設計說明**

本專案系統批次排程分為下列三類

* + Windows Application

預先計劃在特定時間或指定時間頻率後啟動執行例行工作，如產製報表或與外部系統串接或交換資料，如取得電支會員電子發票清單等。

* + Windows Service

長時間於背景執行特定功能的服務應用程式，不需要使用者介面。亦不需使用者登入系統也可以自動開始結束的特性。是一種持續提供服務不需要使用者介入的程式，如簡訊發送功能或推播。

* + SQL Job

特定時間或指定時間頻率處理DB資料的新增/更新/統計…等，使用SQL Server Agent設定排程來執行stored procedure，如每日刪除註冊未完成會員資料等。

批次排程監控：

為了有效監控批次排程處理的狀況，執行階段會記錄該次執行的結果存入 DB中，以利有效的監控排程是否有正常運行。執行失敗時也會同步記錄log並發信通知管理者，重大錯誤訊息則會記錄至事件檢視器中。

1. **系統效能規劃目標**

本專案系統效能規劃目標分為下列三個項目

2. 1. **會員註冊**

依會員註冊流程系統測試規劃分為下列二類：

* 一般會員註冊。
* 未成年會員註冊。

未成年註冊需發送簡訊或推播後，須法定代理人同意才能完成註冊，不列入本次系統效能規劃測試。

會員註冊流程依APP\_使用者註冊之已需求確認SA文件為主，大致分為下列6個步驟：

1. 同意條款頁。
2. 註冊資訊頁：需使用已於OPEN WALLET所設定的手機號碼，且不可修改，才能取得OPEN WALLET會員資訊相關資訊。
   * 專案內部效能測試，不包含OPEN WALLET會員資訊相關測試。
   * 專案整合效能測試時，包含OPEN WALLET會員資訊相關測試。
3. 手機驗證頁：效能測試時，簡訊固定設定為6個0的數字，方便使用者測試。
4. 身分證掃描頁：效能測試時自動填入相關身分資料，不測試掃描功能部份。
5. 身分驗證頁：效能測試時不進行驗證P11驗證。
6. 安全密碼設定頁：效能測試時，自動固定設定為6個0的數字。

會員註冊系統效能測試方式，使用負載測試軟體進行測試

* 每秒鐘模擬10個使用者註冊流程。
* 每秒鐘依序增加10個模擬使用者註冊。
* 總模擬使用者同時註冊上限人數為200個。
* 持續測試時間為300秒鐘。
* 會員註冊測試只到第一類會員註冊完成為主。
  1. **會員登入**

會員登入測試為會員已註冊且已綁定OPEN WALLET會員的使用者登入情境，依會員登入流程系統測試。

* 登入頁。
* 預設帳密設定頁：不列入會員登入效能測試。

會員登入系統效能測試方式，使用負載測試軟體進行測試：

* 每秒鐘模擬10個使用者登入。
* 每秒鐘依序增加10個模擬使用者登入。
* 總模擬使用者同時登入人數上限為200個。
* 持續測試時間為300秒鐘。
  1. **會員交易**

會員交易測試分為線下交易及線上交易。

* + 1. **線下交易：指由POS發動扣款的交易類型。**

POS相關API：

* 1. POS交易(CheckOut) 。
  2. 取消交易（Cancel）。
  3. 退貨交易（Refund）。
  4. 條碼查詢（QueryMemberInfo）。
  5. 儲值交易（TopUp）。
  6. 取消儲值（TopUpCancel）。
  7. 退貨儲值（TopUpRefund）。

線下交易測試分為一般交易及儲值交易二種。

一般交易測試方式為使用負載測試軟體進行測試：

1. 每秒鐘模擬10個條碼查詢（QueryMemberInfo）。
2. 每秒鐘模擬10個POS交易(CheckOut) 。
3. 每秒鐘依序增加10個模擬使用者條碼查詢。
4. 每秒鐘依序增加10個模擬使用者POS交易。
5. 總模擬使用者同時交易上限為200筆。
6. 持續測試時間為300秒鐘。
7. 一般交易測試不包含取消交易及退貨交易二支API測試。

儲值交易測試方式為使用負載測試軟體進行測試：

1. 每秒鐘產生模擬10個付款條碼。
2. 每秒鐘模擬10個條碼查詢（QueryMemberInfo）。
3. 每秒鐘模擬10個儲值交易（TopUp）。
4. 每秒鐘依序增加10個模擬使用者條碼查詢。
5. 每秒鐘依序增加10個模擬使用者儲值交易（TopUp）。
6. 總模擬使用者同時交易上限為200筆。
7. 持續測試時間為300秒鐘。
8. 儲值交易測試不包含取消儲值及儲值退貨二支API測試。
   * 1. **線上交易：指由APP主動發動扣款交易。**

線上交易相關API：

1. WC020 線上交易授權付款。
2. WC021 線上退貨交易。
3. WC022 交易授權結果查詢。
4. WC023 線上交易訂單查詢。

線上交易測試方式為使用負載測試軟體進行測試：

1. 每秒鐘模擬10個線上交易訂單查詢。
2. 每秒鐘模擬10個使用者APP交易簽章值。
3. 每秒鐘模擬10個線上交易授權付款。
4. 每秒鐘依序增加10個模擬線上交易訂單查詢。
5. 每秒鐘依序增加10個模擬使用者APP交易簽章值。
6. 每秒鐘依序增加10個線上交易授權付款。
7. 總模擬線上同時交易上限為200筆。
8. 持續測試時間為300秒鐘。
9. 線上交易測試不包含退貨交易API測試。