

陽信 eDDA 電子化授權開道
暨管理平台建置專案
邀標規格說明書

(V 1.0)

陽信商業銀行

中華民國 110 年 11 月

修訂歷史記錄欄

版本	修訂日期	修訂章節	修訂原因	修訂者
1.0	110.11.15		初版	
1.1				
1.2				
1.3				
1.4				

目 錄

壹、	前言	1
貳、	專案概述	2
一、	專案名稱.....	2
二、	專案目標.....	2
三、	專案範圍及要求.....	2
四、	專案時程.....	2
五、	其他.....	2
參、	專案需求	4
一、	業務功能需求.....	4
二、	系統環境需求.....	6
三、	資安需求及管理規範.....	7
四、	軟體開發原則管理規範.....	8
五、	系統監控管理機制.....	9
六、	交易接送機制.....	9
七、	系統備援及資料庫管理機制.....	9
八、	系統測試效能之需求.....	10
九、	服務水準協定.....	10
十、	保固及技術支援.....	11
十一、	保密責任.....	12
十二、	智慧財產權歸屬.....	12
肆、	上線需求	13
一、	教育訓練.....	13
二、	交付產品及文件.....	13
伍、	建議書製作規定	15
陸、	其他事項	15

壹、前言

87 年 4 月 16 日本行通過國際品保機構 ISO-9002 資訊系統及稽核體系品質認證，成為首家通過認證之本國銀行，並於同年 6 月 4 日股東常會前，舉行認證發表會，宣示本行將秉持「穩健、前瞻、專業、熱忱」之品質政策永續經營，全國分行家數達 99 家，服務網絡及金融版圖更加完整，經營據點能在地理環境上發揮業務併肩支援、業績相互提攜效果，並透過區域互補及通路整合，強化市場競爭力及規模，有利本行提升整體市場佔有率及發揮營運綜效。

為因應金融情勢快速變遷並提供客戶多元化金融服務，本行除持續不斷強化營運資本外，亦積極結合其他金融領域，發展多角化金融業務，在既有之人脈、地緣基礎上，擴大服務層面，以滿足客戶全方位的金融業務需求。

為強化本行代收代付服務，規劃建置資訊系統以加入台灣票據交換所推出之電子化授權(eDDA)業務。申請人經由網路，採電子化之方式進行授權申請或異動，辦理銀行帳戶授權，提供安全又即時的 24 小時全天候約定扣款服務，亦可進行定期重覆性的繳款。

本案之規格說明為整合之基本範圍依據，實際應用需求以承作廠商訪談確認後之內容為準。

貳、 專案概述

一、 專案名稱

陽信商業銀行(以下簡稱本行)eDDA 電子化授權開道暨管理平台建置專案(簡稱本專案)。

二、 專案目標

本專案主要目標如下：

- (一) 增加客戶選擇本行作為授扣及驗證之單位。
- (二) 24 小時全天候提供客戶服務。
- (三) 線上申請無紙化，加速業務流程，降低倉儲成本。
- (四) 客戶即時得知申請結果及生效時間。

三、 專案範圍及要求

承作廠商於本專案，須提供下列主要的服務項目包括：

- (一) 負責電子化授權開道平台建置及協助上線。
- (二) 負責電子化授權管理平台建置及協助上線。
- (三) 提供與本行現行系統整合的處理。
- (四) 提供完整的教育訓練，以確保使用者能自行操作及管理本系統。
- (五) 提供專業的專案管理服務:專案時程管理、專案品質管理。
- (六) 採用本行既有 AD 做系統使用者之帳號密碼認證。

四、 專案時程

- (一) 本案所列之各功能須於簽約後 10 個月(含)內完成系統建置。
- (二) 系統建置完成且交付相關文件予本行進行驗收程序。

五、 其他

- (一) 本專案須配合本行作業內容執行。
- (二) 本專案功能規格均須符合主管機關法律規範。

- (三) 本專案系統維護費為原專案採購合約總價 4%以下。
- (四) 本邀標規格說明書開放投標廠商進行建議修改，惟有修改範圍內容須告知本行修改原因及內容。

參、專案需求

eDDA 電子化授權業務，包含開道平台及管理平台功能，串接票交所及本行內部相關系統，並依本行所提之應用功能需求完整建置及測試，且通過本行驗收後上線。

一、業務功能需求

(一) 電子化授權開道平台

1. 票交所 eDDA 電文收發處理

依照票交所 eDDA 傳送規格，解析或封裝交易電文。

2. 扣款行電文處理

- (1) 通知扣款行進行授權交易
- (2) 通知扣款行進行網銀雙因機制
- (3) 向扣款行提出網銀雙因機制申請資料單筆交易狀態查詢
- (4) 通知扣款行同意 MID/扣款行發送 OTP 機制驗證
- (5) 扣款行提出用戶資料查詢
- (6) 扣款行提出授權成功交易
- (7) 扣款行提出網銀雙因機制交易

3. 發動行電文處理

- (1) 通知發動行授權交易結果
- (2) 向發動行進行用戶資料查詢
- (3) 發動行提出授權申請電文
- (4) 發動行提出網銀雙因機制申請
- (5) 發動者(行)提出 MID/扣款行發送 OTP 機制申請 API
- (6) 發動者(行)以轉址方式(HTTP)提出產生卡片簽章/TAC 相關資料申請

4. 共用性電文

- (1) 銀行提出單筆交易狀態查詢
- (2) 交易訊息異常通知
- (3) 系統啟動/關閉/一般公告通知

- (4) 系統啟動/關閉/一般公告通知
- (5) 票交發送系統線路保持活動通知
- (6) 參加單位發送系統線路保持活動通知
- 5. eDDA 資料檔案下載
- 6. 依據需求確認階段本行所提出之內部身份認證規格，串接身份認證服務。
- 7. 串接本行內部申請服務系統
將 eDDA 電文規格形式轉換為本行內部電文規格形式。
- 8. eACH 電文處理
 - (1) 作業程序子系統電文交易
 - (2) 圈存扣款子系統電文交易
 - (3) 結帳清算子系統電文交易
 - (4) eACH 資料檔案下載
 - (5) eACH 之通訊基碼及押碼基碼應以主基碼加以保護，主基碼應儲存於本行所提供之亂碼化設備中，主基碼僅可透過亂碼化設備之應用程式介面操作使用。

(二) 電子化授權管理平台

- 1. 角色功能權限管理
管理平台需具備角色對應功能之權限管理機制，管理平台使用者登入需結合本行 AD 服務。
- 2. 開道平台系統設定及參數管理
開道平台之系統設定需可透過管理平台進行。系統應用層之設定應優先參數化，並可於管理平台調整。
- 3. 電文記錄查詢
自票交所接收之電文，及發送至票交所之電文，均應完整記錄，並可供查詢。
- 4. 稽核記錄查詢

管理平台使用者之各項操作記錄均應留存稽核軌跡，並可供查詢。

5. 報表功能

以上查詢應提供可下載為報表之功能。

二. 系統環境需求

(一) 應用系統架構

本系統運作所需之軟、硬體架構及數量請依 貴公司方案之實際需要進行評估，必須包括正式營運、同地備援及開發測試環境所需設備。且系統架構依銀行公會之資訊安全定義及 ISO-27001 規範，至少應符合以下之要求：

1. 應用系統伺服器應建置於本行內部網路。
2. 資料庫伺服器應獨立建置於本行內部網路，避免與應用系統伺服器共用相同設備。
3. 系統應提供正式營運環境及測試環境，並可獨立運作。

(二) 系統硬體規格

請依據功能面及業務面需求，提出本專案系統架構規劃，規劃內容至少應包括：

1. 新系統之架構及網路圖。
2. 作業平台(Unix、Windows...)。
3. 伺服器及客戶端硬體、通信設備規格。

(三) 系統環境需求

作業系統：Windows Server 2012 R2 standard 以上版本/ Linux

資料庫：Microsoft SQL Server 2012 standard 64bit 以上版本

程式語言：JAVA 或 NET（需包含版權授權或保證無授權問題）

終端環境：作業系統 WINDOWS 7、10 之個人電腦，瀏覽器版本支援 Chrome、Edge

AP 伺服器：IIS 或包含版權授權或保證無授權問題之 AP 伺服器

三. 資安需求及管理規範

- (一) 須符合本行「資訊安全政策」規範。
- (二) 所提供之模組功能與後端系統或服務應相互整合，例如：應用系統軟體執行使用之帳號、密碼須與本行 AD 系統整合。（本系統要求於系統登入時必須以 AD 系統驗證登入）
- (三) 必須配合本行定期進行弱點掃描、入侵滲透測試、程式碼安全檢測工具（具公信力之 Code Review 工具）產出第三方檢測報告，並依報告結果進行修正，符合本行檢核通過方可上線。保固及維護期間內皆要修正風險等級為嚴重、高、中及低的內容，低風險等級則可以提出說明經資安顧問同意不修正。
- (四) 檔案傳送時，須檢核合法之 IP 及加密程序，提供加解密程式。
- (五) 系統需支援多層式（n-Tier）系統架構。
- (六) 配合本行虛擬機器（VM）達到同地備援功能。
- (七) 配合本行虛擬機器（VM）支援雙主動式叢集故障自動接管（Active Standby）機制。
- (八) 配合本行虛擬機器（VM）達到網站伺服器與應用程式伺服器分離。
- (九) 配合本行虛擬機器（VM）應用系統伺服器與資料庫伺服器需分離。
- (十) （應用程式禁止寫入特定帳號密碼及 IP。
- (十一) 禁止使用網路芳鄰、SAMBA 等資料傳輸方式，並依本行「防火牆開放規則」辦理。若有特殊考量需使用時，須事前經本行同意。
- (十二) 如業務或系統之需求須使用時，應增列安全控管措施並依「防火牆開放規則」辦理。
- (十三) 應限制特定 IP 透過特定網路服務埠存取資料庫主機。

- (十四) 資料傳輸加密：對外提供交易服務之網站需具備加密機制，對外傳輸檔案應有保護機制。
- (十五) 程式版控：需配合本行軟體變更程序。
- (十六) 開發人員必須使用獨立 ID，不可共用。
- (十七) 密碼儲存於特定檔案/表格中，並已加密。
- (十八) 系統讀取帳號密碼時僅限單向存取。
- (十九) 密碼原則設定非寫在程式中（透過程式介面或檔案設定）。
- (二十) 授權管控機制（使用權設定及分類），授權流程及範圍管理（區分不同人員使用不同畫面），授權、登錄、使用記錄及檢核介面。
- (二十一) 管理者管理專用帳號登入及資料維護服務。
- (二十二) 廠商所開發之相關系統應符合主管機關法令法規。
- (二十三) 應用系統平台須可運行於加密通道(https)。(資訊處提供陽信銀行全網域憑證供廠商於陽信銀行內部使用)

四. 軟體開發原則管理規範

(一) 軟體開發一致性

1. 建置廠商應提交過程中的分析、設計文件與本行本專案執行團隊，以檢討規劃與開發建置的一致性與協調性。
2. 建置廠商應依循規劃結果與需求，逐序開發系統。
3. 建置廠商應與本行充分溝通討論應用與開發的優先順序。
4. 建置廠商如需轉包其他合作廠商，請詳細說明轉包之原因以及與轉包廠商合作之方式。

(二) 開發物件模組化

1. 建置廠商應將所需功能以模組化方式彈性設計，使能在應用系統建置時因應需求組裝導入，降低客製差異影響。
2. 建置廠商應將系統物件予以封裝，提供各模組應用。
3. 建置廠商應將模組溝通方式物件化，使系統間溝通方式共同使用相同模組，且須降低系統耦合性，提供重複使用的機制。

(三) 模組設定管理機制。

1. 需能提供模組設定管理機制。
2. 需能提供模組設定，經由參數設定而不需修改程式碼。
3. 需能提供彈性的設定架構，提高參數設定性，降低系統程式客製化。

(四) 軟體版本控管及佈署原則

1. 軟體版本控管應符合本行資安管理等規範。
2. 軟體佈署應符合本行資安管理等規範。
3. 需提出系統維運相關系統軟體版本控管及佈署的具體計畫和 SOP 程序，並在測試期間進行演練，正式上線期間進行相關技術移轉和訓練。

五. 系統監控管理機制

- (一) 須提供依使用角色設定權限控管的功能。
- (二) 須提供管理性報表。
- (三) 須提供系統記錄及稽核軌跡，包含批次執行程式。
- (四) 須提供交易原始記錄 LOG。
- (五) 須提供批次自動排程作業。
- (六) 資料交換發生異常需具備主動通知機制(以電子郵件、簡訊或廣播通知系統人員)。

六. 交易接送機制

配合本行交易接送機制透過中介系統(如有需要)與後台交易主機接送。

七. 系統備援及資料庫管理機制

- (一) 營運系統設備異常時，必須有相互支援機制。得以完整接替營運系統執行應用程式之基本需求。並應提供系統管理維護手冊說明相關維運系統異常回復機制的具體緊急備援計畫和 SOP，並在測試期間進行演練，正式上線期間進行相關技術和訓練移轉。
- (二) 資料備份機制：

1. 需提供系統備份、資料庫備份、資料備份及程式備份功能並能配合本行資料備份機制。
2. 需提出系統維運相關系統備份機制的具體計畫和 SOP 程序，並在測試期間進行演練，正式上線期間進行相關技術和訓練移轉。

(三) 資料清理(House Keeping)及資料搬移

1. 資料清理：依照本行業務需求估算資料儲存年份是否到期，並保留彈性的系統資料清理機制模式。
2. 資料搬移：依照本行業務需求，將線上資料搬移到歷史資料區，並保留彈性的系統資料搬移機制模式。
3. 系統相關交易資料及機敏性資料(如個資)永久保存，其他資料至少保存 5 年以上機制。

八. 系統測試效能之需求

- (一) 廠商須提供相關測試計畫，包括測試個案及方法、驗收之水準，測試項目應包含功能性測試與非功能性測試。
 1. 功能性測試：測試系統是否符合本行需求與設計規格。
 2. 非功能性測試：效能測試(Performance Testing)、程式碼安全檢測、壓力測試(Pressure Testing)。
- (二) 須提供應用系統效能測試計畫及報告(包含說明於何種測試條件與環境下可達到的效能數據)。
- (三) 須提供應用系統安全性測試計畫及安全性測試報告書。
- (四) 須提供應用系統壓力測試計畫及壓力測試報告書。
- (五) 須提供復原演練測試計畫。

九. 服務水準協定

- (一) 廠商應自本系統經本行驗收完成之次日起免費提供一年之保固維護服務(下稱保固期間)，得標廠商維護範圍如下：
 1. 本系統之錯誤修正：本系統若無法正常執行須負責修正，如造成檔

案資料錯誤須協助回復。

2. 緊急故障之協助排除。

3. 電話技術諮詢服務。

(二) 廠商應依本行指示至本系統所在位置進行維護服務。

(三) 遠端遙控程式使用限制：

1. 除本行書面同意外，得標廠商不得安裝任何遠端遙控程式及使用遠端遙控進行維護。

2. 如本行同意安裝以上程式、且此程式因任何理由損及本行資訊安全所產生之任何損害、廠商將負損害賠償責任。

(四) 異常維護方式：廠商同意於接獲本行電話或書面維護通知之時起，於約定時限內派遣工程師以電話或至本行指定地點進行修復。

十. 保固及技術支援

(一) 保固期間：

本系統經本行驗收完成之次日起免費提供一年保固維護服務。

(二) 保固範圍：

1. 本行於完成驗收本系統各項功能及交付後，若系統發生規格範圍內之異常現象，為本系統保固範圍。

2. 電話技術諮詢服務。

(三) 非保固範圍：

系統問題發生原因，非因本專案所提供之各應用系統時，不在本保固服務範圍。

(四) 保固方式：

1. 提供本行一週（5 天 x 8 小時）技術服務窗口，於本系統問題發生時，協助本行人員釐清並排除本系統問題。

2. 異常維護方式，於接獲本行電話或書面維護通知之時起八小時內，派遣人員以電話或本行指定地點進修復。

3. 本系統應用及程式作業之輔導。

4. 本系統應用及程式無法正常運作問題之排除、修錯。

5. 本系統應用及程式運作環境（含作業系統、資料庫、使用者端瀏覽器）升版或進行系統弱點漏洞修補致產生應用不相容情形之調整修正。

（五） 技術支援：

1. 系統作業服務發生異常後，應蒐集相關異常訊息及數據，供本行據以研判問題並協同其他維護廠商（如資料庫、設備作業系統、網路等）共同解決可能發生原因。
2. 提供本系統各項軟、硬體及應用之技術移轉教育訓練。
3. 提供本系統於專案期間及程式維護之技術指導。
4. 於保固維護狀況修復後，須交付本行書面及電子檔各一份做為保固記錄附件，內容至少需包含狀況說明、解決方案及後續待辦事項等項目。

十一. 保密責任

得標廠商就履行本專案所知悉之本行各項資訊系統作業事項（含文件、資料及報表等）應善盡保密責任，非經本行許可不得以任何方式將其內容洩漏，否則廠商應負法律責任，如直接造成本行損失（有形及無形）應負賠償責任。本行得於廠商在行內作業期間派員監督，廠商不得拒絕。

十二. 智慧財產權歸屬

廠商交付項目中，專為本專案開發者，其智慧財產權須授權與本行共有；非專為本專案開發者，廠商應授權本行基於內部需要及維護本專案之目的，使用、修改或重製原始程式碼（Source Code）或目的碼（Object Code）。

肆、 上線需求

一. 教育訓練

依下列原則提供教育訓練，必須使本行使用者、系統管理者、程式開發人員都能使用及操作本系統。並使本行系統開發人員能自行維護本系統。

人員	課程	時數
業務單位人員	後台管理系統教程	至少 4 小時
系統管理人員	平台系統管理者訓練	至少 4 小時
系統維護開發人員	平台系統技術移轉	至少 8 小時

二. 交付產品及文件

(一) 本專案相關軟、硬體。

(二) 系統文件及手冊，項目如下：

文件項目	文件內容說明
專案工作說明書	專案工作及時程規劃說明
需求規格確認書	需求規格及設計說明
系統分析設計規劃書	系統及作業流程架構文件
	輸出入資料與畫面設計
程式設計規格書	檔案清單及規格
	所有程式清單及功能模組說明
	資料庫及資料處理相關檔案清單及內容
	資料庫及資料處理相關檔案欄位說明

文件項目	文件內容說明
	資料處理流程說明文件
	異常訊息代碼表及說明
系統測試計畫及個案	系統整合測試計畫及個案
	使用者測試計畫及個案
	系統壓力測試計畫
	系統源碼檢測計畫
	系統滲透測試計畫
系統測試報告書	系統整合測試報告
	使用者測試報告
	系統壓力測試報告
	系統源碼檢測報告
	系統滲透測試報告
系統安裝說明手冊	安裝說明程序
	程式編譯環境及作業說明文件
系統管理維護手冊	開發環境設定程序
	執行環境設定程序
	系統異常問題檢測及障礙排除
	開關機程序
	系統回復程序
	系統過版程序
系統使用者操作手冊	使用者操作手冊
教育訓練計畫	教育訓練課程規劃安排說明
系統原始碼 (source coe)	全系統之原始碼程式(可用光碟交付)

伍、 建議書製作規定

請於收到本規格說明書後十個工作天內，提供建議書電子檔一份，紙本三份寄達陽信銀行業務管理處田凱元副理（台北市北投區石牌路一段 90 號三樓，(02)2820-8166 分機#722）。

建議書內容至少應包含以下項目：

- (一) 專案概述
- (二) 廠商資格及經驗能力
- (三) 專案團隊人員經歷及年資
- (四) 專案管理方法說明
- (五) 系統架構說明
- (六) 應用系統說明
- (七) 交易安全控管說明
- (八) 軟硬體規格需求
- (九) 專案建置費用報價
 1. 建置服務費用並說明計價基礎。
 2. 保固方式與維護費用及其計價基礎。

陸、 其他事項

對於需求說明書所提之內容，本行保留討論修改之權利。