全國農業金庫開放銀行第二階段集保 TSP 介接系統
規格及特別條款

全國農業金庫股份有限公司（以下稱本公司）標購開放銀行第二階段集保 TSP 介接系統建置（以下稱本案設備），其規格及特別條款規定如下：

甲、 規格

壹、 一般規定

一、 投標廠商須具有與本案設備需求相關之國內銀行建置經驗且運作正常，並於投標時提供截至投標日前 5 年內之採購契約、驗收文件、維護合約或使用單位上線運作證明等任一文件影本。

二、 投標廠商應按投標金額 5%之現金、金融機構簽發之本票或支票、銀行保付支票、郵政匯票繳納押標金，得標後押標金轉為履約保證金，履約保證金經履約完成無待解決事項後轉為保固保證金，保固期滿且無待解決事項後無息發還保固保證金，未得標者無息退還。

三、 本案設備須提供於正式作業環境、測試作業環境上運作。

四、 本案設備須於本公司現有硬體設備、作業系統及資料庫下執行運作且正常運轉。

五、 得標廠商須依作業系統需求提供相關修改維護。

六、 得標廠商得標後 1 個月提供服務建議書，規劃提供正式、開發測試等作業環境建置，並配置所需之開發工具、系統軟體（不含作業系統）、應用軟體等足夠合法使用版權數，本公司不另行付費。

七、 本案設備應符合本公司現行軟硬設備規劃（建置在 VMWare 系統上 Windows Server 及 MS SQL Server），並詳列本案設備所需軟硬體設備及數量，以供本公司審核及採購建置。

八、 得標廠商須配合完成本案相關主管機關之審核，驗收時應符合主管機關相關審核及其建議事項（包含法規修訂）。

九、 得標廠商須配合完成通過系統弱點掃描、本公司源碼檢測、且通過 WAF 網頁應用防火牆偵測弱點並配合修正高/中/低弱點完成，方能上線。

十、 投標廠商如有政府採購法第 101 條所列之情事，經刊登於政府採購公報者，依同法第 103 條規定之期限內，不得參加投標或作為決標對象或分包廠商。

十一、 本規格稱”以上”、”以下”、”以內”、”至少”、”高於”、”低於”具含本數。

貳、 系統需求

一、 資料庫伺服器 (DB Server)正式套及測試套虛擬機器 1 台：由本公司提供虛擬機器(VM)環境暨軟體授權。

二、 應用程式暨網頁伺服器（AP Server & Web Server）正式套及測試套虛擬機器各 1 台：由本公司提供虛擬機器(VM)環境暨軟體授權。

三、 使用者端：由本公司提供個人電腦，應可支援 Windows 10 以上作業系統；瀏覽器開啟之功能，應支援 Microsoft Edge、Google Chrome、Mozilla Firefox，以官方發佈現行支援版本的使用者端環境。

四、 開發工具：可使用套裝軟體、客製化軟體或其組合：

若使用套裝軟體應交付相關軟體授權文件，其授權有效期間於本案履約完成日起應不低於 3 年，並於服務建議書中敘明 3 年後每年需繳付之授權費預估金額。

若使用客製化軟體，得自行選擇使用之軟體開發方法及工具完成本案需求，惟應於服務建議書中敘明理由及規範的準則與方法論，原則上以對使用者安裝外掛程式之需求較少，能在不進行大幅修改的情況下於上列各瀏覽器中正常顯示並執行功能之程式語言為佳。

五、 編碼及語系：本案資訊系統應採用 Unicode 編碼，各項操作畫面執行時所產生之所有訊息以正體中文顯示。

六、 本案設備之系統開發主要採用.NET 技術，NET Framework 採用 4.8 以上版本；程式語言可使用 C# .NET Core，架構可為 Web 或 MVC。

七、 使用者介面：採用套裝軟體預設介面，具有一致性，且操作介面設計應簡易明瞭。

八、 以模組化建構本案所需之應用系統功能，使系統具即時性、互動性與擴充性。

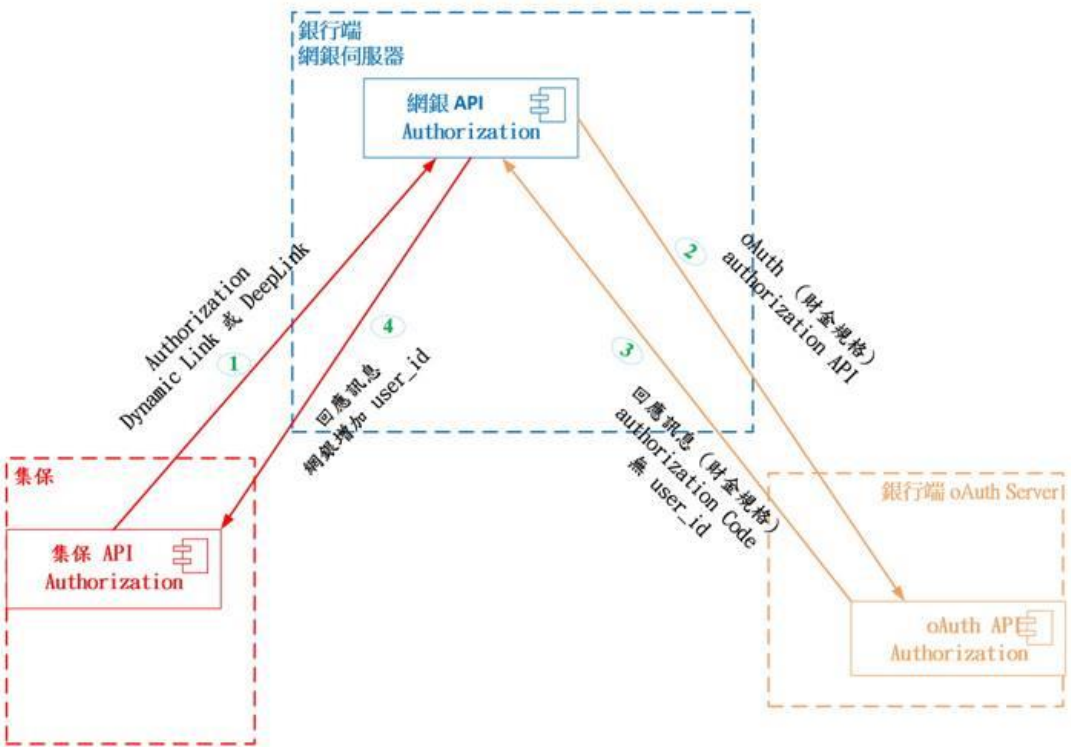
參、 應用軟體規格

一、 授權認證(authorization)

集保將採用與財金公司OAuth授權認證(authorization)API之相似規格，並新增user_id（身分證字號）參數並使用AES-256方式進行加密（加密方式詳見【加解密與憑證檔交換】一節），來呼叫銀行端之授權認證頁面或APP進行身分認證。

本公司需檢核集保傳入之身分證字號是否與核身流程為同一使用者，並於回傳結果時，也需新增user_id參數，並將user_id與authorization code進行AES加密回傳，詳細規格請見下方說明。

流程如下

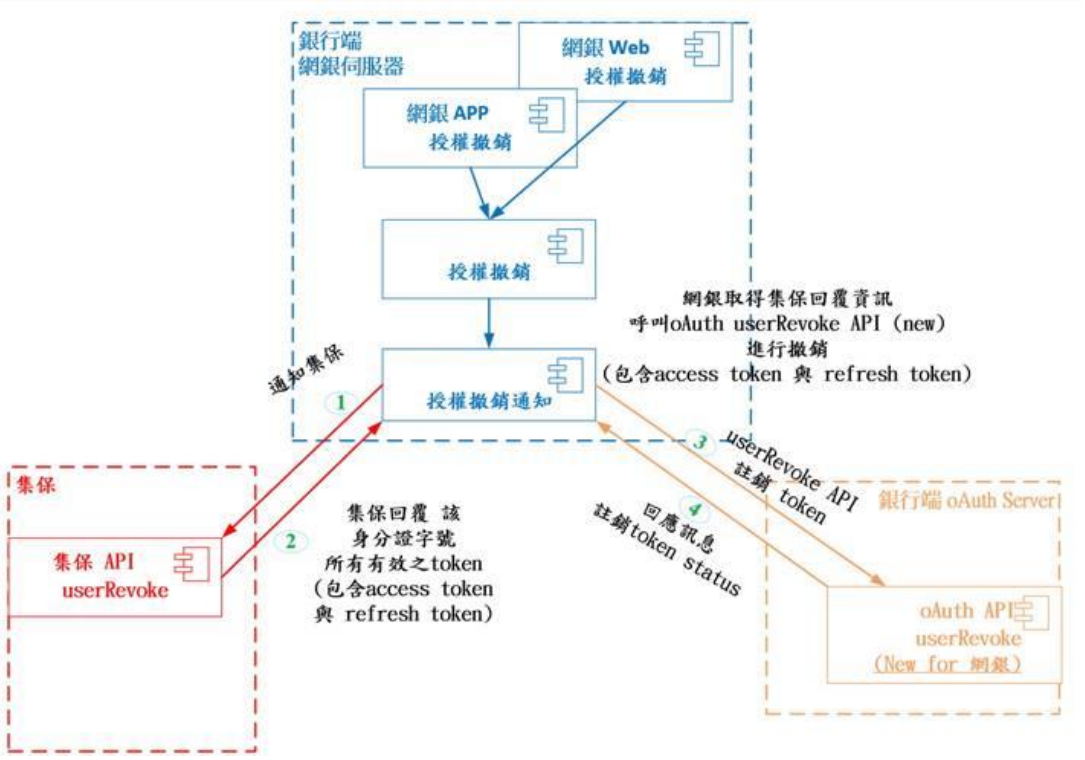


API Path	GET 本公司之 APP Dynamic Link、DeepLink 或授權認證頁		
API 功能說明	呼叫銀行端之 APP 或授權認證頁進行身分認證，授權成功後回傳 authorization code		
	欄位名稱	欄位型態	欄位說明
Request Header	Content-Type	string	application/x-www-form-urlencoded
Request Parameter	user_id	string	使用者身分證字號，使用 AES 對稱式金鑰進行加密。
	response_type	string	本案採用 authorization code grant，故本欄位需填 code
	client_id	string	註冊在各銀行 authorization server 的 client id
	redirect_uri	string	要返回的 client uri，為當初 client 註冊在各銀行 authorization server 的 uri
	scope	string	代表 access token 可存取的資源範圍
	state	string	用以防止 cross-site request forgery
Response	user_id	string	使用者身分證字號，使用 AES 對稱式金鑰進行加密。
	code	string	授權成功產生的 authorization code，使用 AES 對稱式金鑰進行加密。
	state	string	是使用者的登入狀態記錄，類似 session，供後

			續 client 使用
呼叫範例	Deep Link（參數使用 GET 傳遞） https://bank.deep.link/TSPAuthorize?redirect_uri=https://epassbooksys-t.tdcc.com.tw/MPSBKV2/rest/tsp/TSP012/001&scope=deposit:account:inquiry%20credit:inquiry&response_type=code&client_id=12345678-aaa-bbb-ccc-123456789012&state=123456&user_id=1764AF1A366F32AC869453C86FB2BBA6 上述 URL 集保 APP 透過外開瀏覽器方式唯一喚醒銀行 APP 並將參數帶入。		
回應範例	本公司 APP 透過外開瀏覽器，開啟下方 URL 即可喚醒集保 APP 完成認證 https://epassbooksys-t.tdcc.com.tw/MPSBKV2/rest/tsp/TSP012/001?user_id=1764AF1A366F32AC869453C86FB2BBA6&code=A855DE014FFA771BFFDA331D4F6BA712&state=123456		

二、 授權撤銷通知(userRevoke)

流程如下



API Method	POST		
API 功能說明	本公司通知 TSP 業者使用者提出終止授權存取代碼(token)		
	欄位名稱	欄位型態	欄位說明
Request Header	Content-Type	string	application/x-www-form-urlencoded
Request Body	token	string	本次被廢止的 token 或使用者身分證字號， ● 若為 access token 被廢止，其相關的 refresh

			token 亦會一併廢止。 ● 若為使用者身分證字號，內容請以 AES 對稱式金鑰進行加密。
	token_type_hint	string	定義 token 欄位的資料類型，定義以下三種： access_token，用 access token 為條件撤銷； refresh_token，用 refresh_token 為條件撤銷； user_id，用身分證字號為條件撤銷
	aud	string	通知 token revoked 的對象，放 TSP 的 call back url，ex: https://tsp.com/cb
	iss	string	原 token 的發行者，採用銀行 Auth server 的 host url，ex: https://my.AuthServer.com
	exp	string	token 被廢止的時間點。整數型態，是自 1970-01-01T00:00:00Z UTC 開始的秒數，可參考 RFC 3339 的格式，或定義在 RFC 7519 的內容
Success Response	code	string	成功通知回應：**received**； 若 TSP Server 未收到通知，並回傳收到通知訊息時，則銀行端於 6 小時內，每小時重新傳遞 1 次，直到收到回應。都未收到則不再發送通知訊息。
	message	string	TSP在收到廢止通知後，處理方式的進一步描述，由TSP自訂。
成功回應範例	{ "code": " received", "message": "In progress, notify user when complete. 1 token found, 1 token revoked." }		
失敗回應範例	{ "code": "received", "message": "no token revoked. 1 token found, 0 token revoked. " }		

三、 授權逾期處理

當授權(token)逾期時，請回應 HTTP 401 Unauthorized。

四、 查詢台外幣活存存款帳戶餘額

API Method & Path	POST /deposit/demandDeposit/accounts		
API 功能說明	查詢所有活期存款帳戶清單的相關基本資料及餘額		
訊息安全設計		重要指示或回覆訊息	具身份識別力之機敏資料組合
	TSP to 參加單位	N	N
	參加單位 to TSP	N	Y：JWE
	欄位名稱	欄位型態	(欄位路徑) 欄位說明
Request Body	accountNo	string	(非必填) 活期存款帳號，如為空值則回傳所有帳戶資訊。
Success Response Field	appRepBody	object array	(appRepBody[i]) 成功回應資料的最外層屬性欄位，對應回應的資料模型
	accountNo	string	(appRepBody[i].accountNo) 活期存款帳號，長度 16 碼
	accountType	string	(appRepBody[i].accountType) 活期存款帳戶類別，Ex:活期存款、活期儲蓄存款、薪資轉帳活期儲蓄存款、證券戶活期儲蓄存款、數位存款、綜合存款、外匯活期存款、外匯綜合活期存款

	currency	string	(appRepBody[i].currency) 此帳戶使用的幣別，長度 3 碼，請參考央行外幣幣別代碼表，Ex:TWD、USD
	balance	string	(appRepBody[i].balance) 帳戶餘額，依帳戶幣別顯示數字。第 1 位數為＋、－符號，接續為整數位數長度最多 15 碼，小數位數最多 4 碼，ex:1234.5678
	availableBalance	string	(appRepBody[i].availableBalance) 帳戶可用餘額，依帳戶幣別顯示數字。第 1 位數為＋、－符號，接續為整數位數長度最多 15 碼，小數位數最多 4 碼，ex:1234.5678
	appRepExtension	object	(appRepExtension) 成功回應資料的最外層屬性欄位，對應回應的自訂物件，可含任意數量的 additionalProp*
	additionalProp* (自訂鍵值名稱)	object	(appRepExtension.additionalProp*) 自訂物件的屬性欄位，為補充用的擴充欄位，可自訂此鍵值欄位的名稱及對應值

五、 查詢台外幣定存存款帳戶餘額

API Method & Path	POST /deposit/timeDeposit/accounts		
API 功能說明	查詢所有定期存款帳戶清單的相關基本資料及餘額		
訊息安全設計		重要指示或回覆訊息	具身份識別力之機敏資料組合
	TSP to 參加單位	N	N
	參加單位 to TSP	N	Y：JWE
	欄位名稱	欄位型態	(欄位路徑) 欄位說明
Request Body	accountNo	string	(非必填) 定期存款帳號
	receiptNo	string	(非必填) 存單字號
Success Response Field	appRepBody	object array	(appRepBody) 成功回應資料的最外層屬性欄位，對應回應的資料模型
	accountNo	string	(appRepBody[i].accountNo) 定期存款帳號，長度 16 碼
	receiptNo	string	(appRepBody[i].receiptNo) 存單字號
	accountType	string	(appRepBody[i].accountType) 定期存款帳戶類別，Ex:1:存本取息 2:

			整存整付 3:一般定存(整筆存入)4:零存整付 9:其他(以數字表示)
	currency	string	(appRepBody[i].currency) 此帳戶使用的幣別，長度3碼，請參考央行外幣幣別代碼表，Ex:TWD、USD
	amount	number double	(appRepBody[i].amount) 本金金額，依帳戶幣別顯示數字。整數位數長度最多15碼，小數位數最多4碼，ex:1234.5678
	rate	number double	(appRepBody[i].rate) 此帳戶所用的利率，利率值請以小數點表示，不帶百分比符號，Ex：0.005即代表0.5%。
	period	object	(appRepBody[i].period) 存款期間物件
	timeLength	string	(appRepBody[i].period.timeLength) 表示時間長度用，Ex:1/2/3/4...等
	timeType	string	(appRepBody[i].period.timeType) 表示時間類型， Ex:day/week/month/year
	valueDate	string	(appRepBody[i].valueDate) 帳戶起存日，格式yyyyMMdd
	maturityDate	string	(appRepBody[i].maturityDate) 帳戶到期日，格式yyyyMMdd
	transferType	string	(appRepBody[i].transferType) 利息轉存方式/轉存方式：1.本息轉存 2.本金轉存 3.不轉期 4.到期解約入活存 9.其他(以數字表示)
	interestRateType	string	(appRepBody[i].interestRateType) 利率別：1.機動 2.固定(以數字表示)
	designateAccountNo	string	(appRepBody[i].designateAccountNo) 利息轉存帳號

	interestPayInfo	object array	(appRepBody[i].interestPayInfo) 領息明細物件
	payAtMaturity	string	(appRepBody[i].interesPayInfo[j].payAtMaturity) 領息日期
	proceeds	number double	(appRepBody[i].interesPayInfo[j].proceeds) 領息金額
	maturityInstruction	string	(appRepBody[i].maturityInstruction) 本金到期處理方式（自動展期續存/本利轉入指定的帳戶）
	appRepExtension	object	(appRepExtension) 成功回應資料的最外層屬性欄位，對應回應的自訂物件，可含任意數量的additionalProp*
	additionalProp* (自訂鍵值名稱)	object	(appRepExtension.additionalProp*) 自訂物件的屬性欄位，為補充用的擴充欄位，可自訂此鍵值欄位的名稱及對應值

六、 查詢台外幣活存存款帳戶交易明細資訊

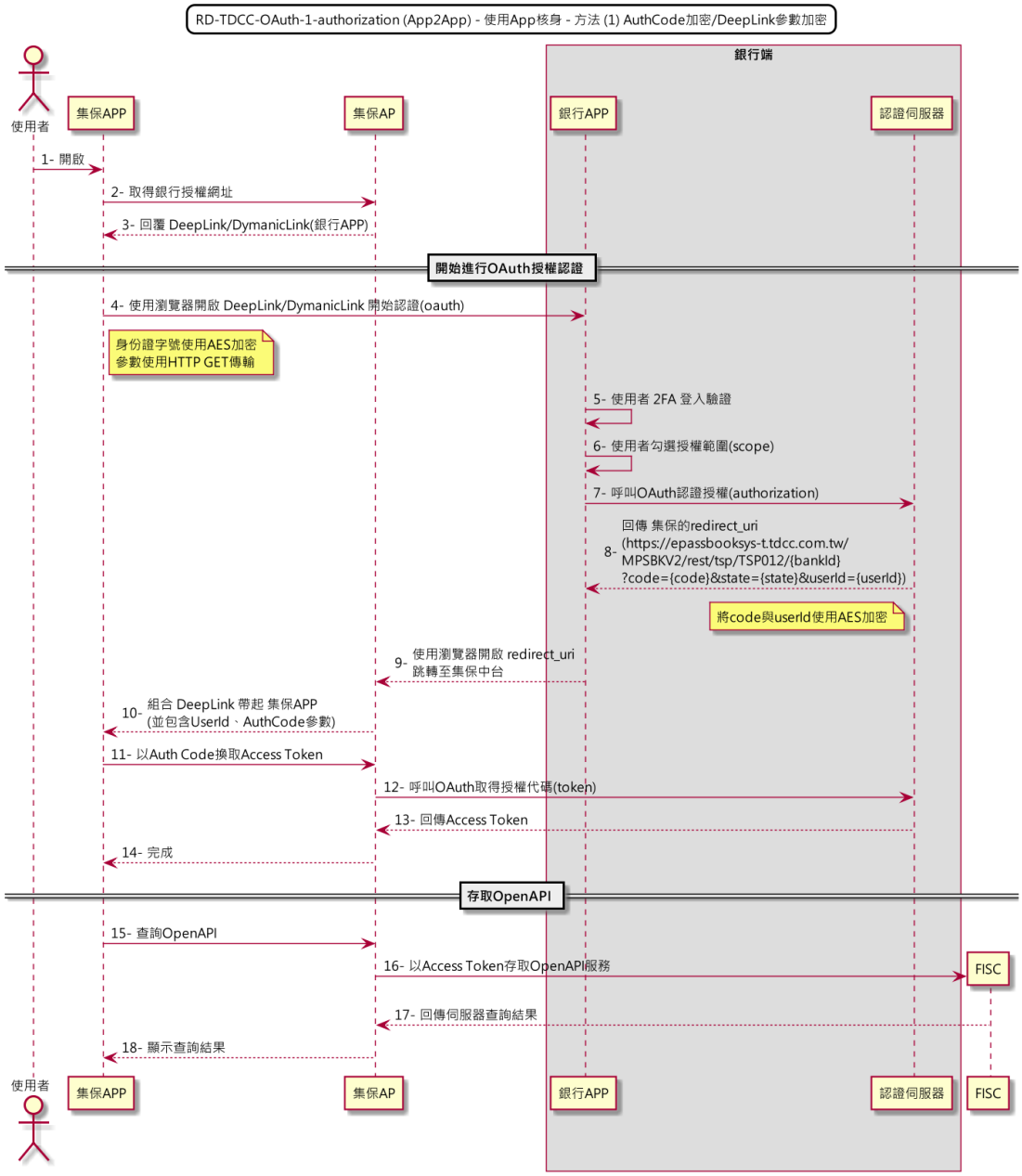
API Method & Path	POST /deposit/demandDeposit/transactionDetails		
API 功能說明	查詢台外幣活存存款帳戶交易明細資訊		
訊息安全設計		重要指示或回覆訊息	具身份識別力之機敏資料組合
	TSP to 參加單位	N	N
	參加單位 to TSP	N	Y：JWE
	欄位名稱	欄位型態	(欄位路徑) 欄位說明
Request Body	accountNo	string	(必填) 活期存款帳號
	startDate	string	(必填) 查詢起始日(暫訂一個月)，格式yyyyMMdd(西元年)。
	endDate	string	(必填) 查詢結束日(暫訂一個月)，格式

			yyyyMMdd(西元年)。
	limitsInPage	number int	(必填) 分頁的筆數上限;不能為負數,如為空字串預設為 10 筆,上限為 100 筆
	pageToken	string	(必填) 放置 response 所帶的 nextPageToken,需採 Base64URLEncoding;欄位空字串("")時,代表為第一頁
Success Response Field	appRepBody	object	(appRepBody) 成功回應資料的最外層屬性欄位,對應回應的資料模型
	accountNo	string	(appRepBody.accountNo) 活期存款帳號,長度 16 碼
	transactionDetail	object array	(appRepBody.transactionDetail) 交易明細物件
	stan	string	(appRepBody.transactionDetail[i].stan) 交易序號
	txnDateTime	string	(appRepBody.transactionDetail[i].txnDateTime) 交易日期時間,格式 yyyyMMddhhmmss(西元年)
	currency	string	(appRepBody.transactionDetail[i].currency) 此帳戶使用的幣別,長度 3 碼,請參考央行外幣幣別代碼表,Ex:TWD、USD
	transferInAmount	number double	(appRepBody.transactionDetail[i].transferInAmount) 轉入金額,依帳戶幣別顯示數字。整數位數長度最多 15 碼,小數位數最多 4 碼,ex:1234.5678

	transferOutAmount	number double	(appRepBody.transactionDetail[i].transferOutAmount) 轉出金額，依帳戶幣別顯示數字。整數位數長度最多 15 碼，小數位數最多 4 碼，ex:1234.5678
	balance	string	(appRepBody.transactionDetail[i].balance) 帳戶餘額，依帳戶幣別顯示數字。第 1 位數為＋、－符號，接續為整數位數長度最多 15 碼，小數位數最多 4 碼，ex:1234.5678
	summary	string	(appRepBody.transactionDetail[i].summary) 交易摘要,長度最多 10 碼(5 個中文字)
	transferOutBankId	string	(appRepBody.transactionDetail[i].transferOutBankId) 轉出銀行代號，長度最多 3 碼
	transferOutAccountNo	string	(appRepBody.transactionDetail[i].transferOutAccountNo) 轉出帳號，長度最多 16 碼
	transferInBankId	string	(appRepBody.transactionDetail[i].transferInBankId) 轉入銀行代號，長度最多 3 碼
	transferInAccountNo	string	(appRepBody.transactionDetail[i].transferOutAccountNo) 轉入帳號，長度最多 16 碼
	memo	string	(appRepBody.transactionDetail[i].memo) 其他備註資訊，長度最多 40 碼(20 個中文字)
	hcode	string	(appRepBody.transactionDetail[i].hcode) 更正記號

	detailPaging	object	(appRepBody.detailPaging) 查詢結果分頁物件
	nextPageToken	string	(appRepBody.detailPaging.nextPageToken) 往下一頁用的查詢 token，需 Base64URLEncoding；欄位空字串("")時，代表無下一頁。
	total	number long	(appRepBody.detailPaging.total) 在相同查詢條件下，查詢的總筆數
	appRepExtension	object	(appRepExtension) 成功回應資料的最外層屬性欄位，對應回應的自訂物件，可含任意數量的 additionalProp*
	additionalProp* (自訂鍵值名稱)	object	(appRepExtension.additionalProp*) 自訂物件的屬性欄位，為補充用的擴充欄位，可自訂此鍵值欄位的名稱及對應值

肆、 OAuth 授權認證流程



伍、 加解密與憑證檔交換

一、 對稱式金鑰（AES-256）

集保使用此對稱式金鑰，將使用者身分證字號進行加密；本公司也使用此金鑰於 oauth 認證時將身分證字號及 authorization code 進行加密回傳。

檢查碼驗算:

以 A 碼單為例，將 A 碼做為本文進行加密，加密金鑰也為 A 碼。使用碼單上的加密模式(ECB/CBC)進行 AES 加密，不需 PADDING。驗算得到的結果取末四碼即為檢查碼。

金鑰 AB 碼計算:

將 A 碼與 B 碼做 XOR 計算，即可取得 AES 金鑰

碼單交換規則:

金鑰有效時間	一年
金鑰命名規則	TDCC_OPENAPI_AES_｛銀行代碼｝_｛西元年｝
金鑰更新時間	每年 1 月 1 日 00:00:00 生效
金鑰交換方式	每年 12 月集保會提供下一年度之 AB 碼單，請合作單位先行匯入，並於 1/1 後切換為新的金鑰進行解密。

例如：集保與第一銀行 2020 年度的金鑰名稱為「TDCC_OPENAPI_AES_007_2020」，於 2021/1/1 00:00:00 後則切換為「TDCC_OPENAPI_AES_007_2021」之金鑰。

身分證字號加密範例

加密金鑰	B639AF7DC503C1F45E56198851D02DFECF837D73EBFAC5D8D1897035964C88F7
加密演算法	AES-256
加密模式	CBC/PKCS5Padding
IV	TDCCOPENTOBANKIV
IV（HEX）	544443434F50454E544F42414E4B4956

本文	A123456789
本文(HEX)	413132333343536373839
密文(HEX)	1764AF1A366F32AC869453C86FB2BBA6

二、 JWE 加密憑證公鑰

集保提供憑證公鑰給予本公司，本公司於回傳 OpenAPI 資料時，使用此金鑰將本文加密金鑰使用 RSA-OAEP-256 演算法進行 JWE 加密。

資料加密演算法:

金鑰加密演算法

RSA-OAEP 2：RSA-OAEP-256 3：RSA-OAEP-384 4：RSA-OAEP-512 5：RSA-OAEP-224

本文加密演算法

A128CBC-HS256 2：A192CBC-HS384 3：A256CBC-HS512 4：A128GCM 5：A192GCM 6：A256GCM

乙、 特別條款

壹、 本案設備維護工作應由得標廠商承擔。

貳、 得標廠商同意履行以下情事：

一、 應本公司業務需要，得標廠商對於所開發之應用軟體同意本公司使用並重製於本公司所購置之機器中，本公司不另行付費。

二、 本公司如因業務需要對得標廠商所提供之程式或文件得作適當之修改。

三、 得標廠商應依本公司業務需要，配合修改應用軟體之程式和文件。

四、 得標廠商所提供之程式及文件，無條件供本公司存查，惟不得公開予無關之第三者。於維護期間所開發應用程式與交付軟體，得標廠商應善盡義務執行資訊安全檢查是否內藏惡意程式，並出具相關資安檢測證明文件，本公司不另行付費。

五、 得標廠商不得於提供之設備上做任何不當作業之行為及植入非法或足以損害正常作業與保密之功能，否則如致本公司遭受損害，應由得標廠商負賠償責任。於保固及維護期間得標廠商須配合本公司定期資安檢測作業或電腦資訊安全評估作業，例如弱點掃描、滲透測試、源碼檢測等，所檢測出之風險弱點項目，應配合本公司要求於期限內進行修正完成，本公司不另行付費。

六、 得標廠商於上線前應配合本公司要求進行相關檢測，並提交相關無弱點檢測文件。如應用軟體程式應於上線前通過源碼檢測、系統及設備應於上線前通過弱點掃描、對外網頁版應用系統應於上線前通過滲透測試，本公司不另行付費。

七、 依上述規定之弱點檢測如因市場工具未能支援無法提出相關檢測文件，得標廠商應出具資訊安全聲明書。

八、 得標廠商依本契約提供本公司服務時，如使用開源軟體，應依該開源軟體之授權範圍，授權本公司利用，並以執行檔及原始碼共同提供之方式交付予本公司使用，得標廠商應於上線前交付開源軟體清單（包括但不限於開源專案名稱、出處資訊、原始著作權利聲明、免責聲明、開源授權條款標示與全文）。

九、 得標廠商提供本公司使用之軟硬體應為合法，如有第三者主張得標廠商提供本公司使用之軟硬體有侵犯智慧財產權時，本公司同意儘速以書面通知得標廠商，得標廠商應負責為本公司提出抗辯或和解談判，所有經法院判決確定或成立和解應由本公司負擔之費用、損害賠償及本公司因此所支付之費用（含委聘律師酬金）、所受之損害等均由得標廠商負擔。

十、 得標廠商應訂定其聘僱人員之相關管理規定，並於契約履行期間應提供開發、維護（修）之服務人員名冊（含公司簽章）及經得標廠商之員工簽署之「保密同意書」至本公司備查，且對其操守行為負責，如有異動時亦同。

十一、得標廠商因履行契約應辦事項所知悉一切有關本公司及本公司客戶等相關資料及內容，僅得揭露於本契約目的範圍內有接觸需要之得標廠商員工，得標廠商及其聘僱人員均應保守秘密不得洩漏，並採取必要之安全措施，否則如致本公司遭受損害應由得標廠商負賠償責任；契約經終止、解除或期限屆滿後亦同。

十二、得標廠商因履行契約應辦事項所應負之損害賠償責任以直接實際損害為限。但有關人身傷害（包含死亡）、物之毀損、專利權及著作權之損害、得標廠商之故意或重大過失造成之損害賠償則不在此限。

十三、得標廠商同意金融監督管理委員會、中央銀行、中央存款保險公司、農業部農業金融署等機關或依農業金融法第七條規定之機關及本公司或委託獨立第三方單位進行辦理本契約相關事項之稽核。得標廠商應提供本契約之應辦事項相關資料或報告，配合金融檢查或稽核，並於期限內提供相關資料或報告。

十四、得標廠商履行契約不得違反法令強制或禁止規定、公共秩序及善良風俗，對本公司經營、管理及客戶權益，不得有不利之影響，並應遵守農業金融法、銀行法、洗錢防制法、個人資料保護法、消費者保護法、中華民國銀行商業同業公會全國聯合會訂定之相關業務規章或自律公約及其他法令之規定。得標廠商應本於善良管理人之注意義務辦理本契約事宜，契約如有履行不能或履行困難之虞者，應即通知本公司。

十五、得標廠商應建立標準作業程序，執行消費者權益保障、風險管理、內部控制及內部稽核制度，除應建立消費者爭端解決機制，包含解決時程、程序及補救措施外，另應提供聯絡窗口及電話詢答服務。

十六、得標廠商若有違反契約約定情事發生，除契約另有約定外，本公司得於通知得標廠商後終止或解除契約，本公司於主管機關命為終止或解除契約時亦同。

十七、得標廠商履行契約應辦事項，對外不得以本公司名義為之，亦不得進行不實廣告，若違反致本公司受損，應負賠償責任。

十八、得標廠商不得將本契約或基於本契約所生之權利義務，全部或一部分轉讓或複委託予其他第三人，但經本公司事先書面同意者不在此

限。

十九、經本公司事先書面同意之複委託，其範圍及限制、條件均不得超出本契約；得標廠商應確認分包商具備資訊安全措施、遵循本公司資訊安全管理制度並簽署保密協議，如因分包商之不當行為致本公司發生損害時，得標廠商應與分包商負連帶損害賠償責任。

二十、得標廠商及分包商應擬定本契約項目之服務水準(SLA)：

(一)如無法訂定本契約項目之服務水準時，須擬定補償性控制措施。

(二)違反本公司資訊安全要求或因人員疏失等原因，導致發生資安事件或未達本公司資訊安全要求之服務水準時，應依契約所定罰則計付違約金予本公司，若因此造成本公司相關損害，得標廠商應依契約內容負賠償責任。

(三)因本契約作業項目之性質、產品內容或服務，得標廠商無法提供服務水準或補償性控制措施時（如訂閱制服務、客制化套裝軟體、商業應用軟體、電腦週邊設備採購等），雙方之權利義務得依雙方協議內容另定之。

二十一、得標廠商資訊安全責任：

(一)得標廠商須遵守本公司現有各項系統管理作業規定及安全管理規範。

(二)得標廠商於契約履行期間，如得標廠商人員異動時（完成階段性任務或離職等情形），得標廠商應會同委託單位將其借用之設備、軟體或其他物件返還予本公司，並移除相關作業權限。

(三)得標廠商不得任意複製或攜出本公司非對外公開之業務資料。本公司所提供之資訊資產及資料等，得標廠商均應於契約終止、解除或期限屆滿時返還予本公司，並刪除或銷毀因執行本契約而儲存持有之個人資料檔案，且不得以任何形式留存備份。得標廠商履行契約相關事務之資料處理流程及傳輸方式，應依本公司資料安全管控規定辦理。

(四)如需使用自攜資訊設備，應經本公司檢核同意後始得使用，且不得連接本公司內部網路。

二十二、本契約應辦事項若有重大異常、缺失或發現疑似資訊安全或個人資料外洩等異常事件或事故時，得標廠商應立即以口頭、電話等方式通知本公司，並配合本公司相關程序辦理異常排除及通報事宜，如必要應提供駐點服務。並於處理完成後，提供相關報告。

二十三、得標廠商所提供之程式若有採用第三方套件(非得標廠商自行開發之程式)，應明列於系統維護手冊中，且交付驗收前應確認無已知公

開的風險；於保固及維護期間內若採用之第三方套件經揭露弱點風險，須配合本公司要求於期限內完成修正，本公司不另付費。

二十四、於專案建置或維護期間內，為解決第三方套件經揭露弱點風險之修正，其解決方法、範圍、期限，得標廠商應協助評估及處理，如係非得標廠商單方修正程式得以解決者(如需作業系統、資料庫、產品升級或原廠產品已終結等)，則不受前款規定限制，雙方得另議處理方法。

二十五、得標廠商應提供第三方認證證明或公正第三方之驗證報告，如資訊安全管理國際標準要求或資訊安全管理系統國家標準（ISO/CNS 27001）有效證書；得標廠商若無法提供時，應配合本公司辦理資訊安全訪視作業。

二十六、得標廠商應配合本公司於系統軟硬體換版時，協助辨識複雜度及影響範圍，提供風險影響評估報告與上線及復原計畫操作手冊。

二十七、得標廠商禁止使用中國廠牌資通訊產品、軟體(如應用軟體、系統軟體、開發工具、客製化套裝軟體、APP 及電腦作業系統等)、硬體(包括具連網能力、資料處理或控制功能者皆屬廣義之資通訊設備)及資通訊服務。

二十八、得標廠商所屬人員倘因參加本案系統建置、維護，致本公司蒙受損害，得標廠商應與其所屬人員負連帶賠償責任。

二十九、得標廠商應遵循相關法令法規及其他適當資訊安全國際標準。

三十、　履約期間遇資安事件時，得標廠商應辦理事項：

(一)知悉發生資安事件之通報並採取適當應變措施

得標廠商知悉發生資安事件應於2小時內通知本公司（或接獲本公司通知2小時內），並採取適當之應變措施。逾時未完成，本公司得請求得標廠商按逾時時數，每小時支付契約總價款0.1%之違約金，逾時未達1小時者以1小時計。

(二)完成損害控制或復原作業

得標廠商應於知悉資通安全事件後72小時(重大資安事件為36小時)內完成損害控制或復原作業。逾時未完成，本公司得請求得標廠商按逾時時數，每小時支付契約總價款0.1%之違約金，逾時未達1小時者以1小時計。

(三)調查及處理資安事件

得標廠商完成損害控制或復原作業後，應於1個月內送交調查、處理及改善報告（或因應本公司所訂期限及指示事項提供協助調查處理相關事宜）。逾期未完成，本公司得請求得標廠商按

逾期日數，每日支付契約總價款0.1%之違約金，1日以24小時計，逾時未達24小時者以1日計。

(四)前開違約金之累計總額以契約總價款之20%為上限。本公司並得自契約總價款、履約保證金或保固保證金中扣抵。如違約金總額達契約總價款之20%時，本公司得通知得標廠商終止或解除契約之部分或全部，且不補償得標廠商所生之損失。

參、 報價

得標廠商以新臺幣為報價基礎，且分別依下表列出價格：

單位：元

項次	名稱	規格	數量	單價	金額
一	開放銀行第二階段集保TSP介接系統建置		1式		
合計					

*以上報價應依規格內容報價（含稅）。

肆、 交貨、安裝及測試

一、 得標廠商須於簽約次日起1個月內交付經本公司簽認之工作說明書，如逾所訂期限，得標廠商須依照下列公式計付違約金予本公司：

違約金 = 契約總價款 * 0.1% * 逾期日數

二、 得標廠商應須於簽約次日起6個月內完成本案設備之開發、測試作業，並提出經本公司簽認之系統功能測試報告書，如逾所訂期限，得標廠商須依照下列公式計付違約金予本公司：

違約金 = 契約總價款 * 0.1% * 逾期日數

如逾期超過前述約定期限1個月仍未完成開發或測試時，除仍應依前述規定計付違約金外，本公司得通知終止或解除契約之部分或全部，並沒入履約保證金。

三、 前開違約金之累計總額以契約總價款之20%為上限，本公司得自契約總價款或履約保證金中扣抵。

伍、 驗收與付款

得標廠商於簽約次日起6個月內完成本案，交付相關文件後，由本公司派員辦理驗收，驗收合格後，支付契約總價款。

應交付相關文件如下：

項次	文件名稱	形式	份數
1	產品光碟	光碟	2
2	測試報告書 1.系統功能測試報告書（經本公司簽認）。 2.應用系統功能測試報告書(所有功能都成功)。 3.集保個案測試通過。	書面及光碟	2
3	操作手冊(含安裝、維護說明)	書面及光碟	2
4	教育訓練計畫及教育訓練簽到表	書面及光碟	2
5	弱點掃描報告、APP檢測報告、滲透測試報告 原碼檢測報告（依本公司規定低/中/高風險都必須修正）	書面及光碟	2
6	系統架構書、資料庫檔案說明書、備援作業程序書	光碟	2
7	原始程式碼、程式規格書	光碟	2

陸、 維護及保固

一、軟體：

得標廠商於完成全案正式驗收之次日起，負責維護及保固1年，本公司不另行付費；保固期滿，本公司得視實際需要與得標廠商簽訂維護契約，其每年維護費率為須維護標的之契約價款之10%，得標廠商不得拒絕簽約。若本公司要求簽訂維護契約而得標廠商未於保固期間屆滿前與本公司簽訂維護契約，則保固期間自動延長至維護契約生效日止。

二、得標廠商於維護及保固期間須依下列事項進行維護：

(一)應於本公司營業日上午9時至下午5時提供技術維修服務，以維護本案設備之正常運作。

(二)應於通報後1小時內回應，並透過電話服務協助系統問題之判斷、偵錯與故障排除，如有進一步到場鑑定維護之必要，須於4小時內到場服務，本公司不另行付費。

(三)維護期間交付應用程式過版時，得標廠商須檢附程式源碼檢測報告或資安相關檢測證明，確認完成後，才允進行應用程式過版作業，本

公司不另行付費。

(四)得標廠商違反前開各款約定之服務水準時，每違反1次，本公司得按契約總價款之0.1%計收懲罰性違約金，並得自契約總價款、履約保證金或保固保證金中扣抵。

(五)上開懲罰性違約金之累計總額以契約總價款之20%為上限，如累計總額達契約總價款之20%時，本公司得通知得標廠商終止或解除契約之部分或全部，且不補償得標廠商所生之損失。

柒、 得標廠商應提供本案相關教育訓練4小時及辦理技術移轉並詳列於服務建議書，本公司不另行付費。

捌、 得標廠商應對本案契約內容充分瞭解，並應依本公司之解釋切實執行辦理。