零信任產品功能與服務項目之規格說明

一、 產品功能合規

應符合「金融業導入零信任架構參考指引」，能保護重要資通系統，並配合現況應用需求之適宜產品功能與服務；具備資安院要求之身分鑑別、設備鑑別、信任推斷三大核心功能，並提供資安院零信任三階段驗證(含送驗中)之證明文件。

二、 廠商具備資訊安全管理（如 ISO 27001)或個人資料隱私管理（如 ISO 27701、BSI 10012)等認證尤佳。

三、 零信任架構遠距辦公及系統維運管理之特定資訊人員，包括但不限於「身分」與「設備」功能、保護重要資通系統如等級 I 及等級 II。

四、 身分鑑別功能

1. 採用多因子驗證機制，降低帳號密碼遭破解、竊聽等風險。採用包含綁定實體載具(如 FIDO、動態密碼產生器、晶片卡、綁定手機且具數字配對 APP 等，排除簡訊、語音及電子郵件 OTP)的多因子驗證機制。以符合金管會零信任架構指引身分 1.1、1.2 項次要求。
2. 對外部使用者(如服務供應商或跨機構協作)提供或採用不低於內部使用者信賴等級之身分鑑別機制。以符合金管會零信任架構指引身分 1.3 項次要求。
3. 如具多元身分鑑別機制且有互通之必要，其信賴等級應具一致性之標準。以符合金管會零信任架構指引身分 1.4 項次要求。
4. 完成身分鑑別後，除依角色屬性存取控制(RBAC)落實最小授權原則外，並具基於屬性存取控制(ABAC)機制，可將每個工作階段(Session)之動態屬性(如時間、地點等)納為授權審核條件，動態撤銷、限縮存取授權或即時告警。配合現況應用需求，使用者直接透由瀏覽器登入存取閘道(包含中繼閘道，多種網路服務和功能)進行身分驗證，並得依帳號權限顯示可連線之重要資通系統，以達最小授權原則，如具授權存取的網頁資源，內、外網 RDP 微軟遠端桌面應用程式連線、ANCHOR 特權管理平台連線等。以符合金管會零信任架構指引身分 1.5 項次要求。

五、 設備鑑別與設備健康管理功能

1. 具有效盤點且可唯一識別(如 TPM 等)納管設備機制，並對其安全要求(如病毒碼、作業系統狀態等)之判斷及應處機制；對未納管設備具有即時偵測及風險控管(如強制隔離)機制，若設備未達標準可顯示不合規等，病毒碼如 Symantec、Windwos 作業系統狀態等。以符合金管會零信任架構

指引設備 2.1 項次要求。

2. 具納管設備合規檢測及弱點管理機制(如未更新或具已知資安漏洞)，可持續監控不合規設備並及時採行風險控管措施(如強制更新、修補弱點、強制隔離或即時告警等)。例如對設備鑑別、設備健康度等條件資訊作為信任分數之推論依據，若設備未達標準可顯示不合規等，即不具備連線重要資通系統之授權。以符合金管會零信任架構指引設備 2.2 項次要求。
3. 對外部設備(如 BYOD、服務供應商或跨機構協作等)，應建立不低於內部設備防護基準之管控措施；或限制需經由可控之合規中繼閘道存取。配合現況應用需求，設備經由存取閘道除了 Web-based 應用程式連線存取重要資通系統之外，包含中繼閘道(多種網路服務和功能)存取，如具授權存取的網頁資源，內、外網 RDP 微軟遠端桌面應用程式連線、ANCHOR 特權管理平台連線等，若設備未達標準可顯示不合規等。存取受保護重要資通系統，並利用反向代理技術。以符合金管會零信任架構指引設備 2.3 要求。
4. 可將設備之動態屬性(如是否納管及合規、設備位址、或是否屬外部設備等)納為每個工作階段(Session)之授權審核條件，動態撤銷、限縮存取授權或即時告警；或具備隔離機制，可即時偵測並阻斷未合規設備之連線；或於資源存取路徑限制須經可控之合規中繼閘道存取。配合現況應用需求，如具中控管理界面，可檢視每個工作階段之授權審核條件，亦可動態撤銷連線、設定即時告警，且支援包含中繼閘道(多種網路服務和功能)存取，如具授權存取的網頁資源，內、外網 RDP 微軟遠端桌面應用程式連線、ANCHOR 特權管理平台連線等，若設備未達標準可顯示不合規等。以符合金管會零信任架構指引設備 2.4 項次要求。
5. 整合或收容事件日誌，建立定期審查及異常行為之偵測、告警及回應機制，如集中收容於 SIEM 平台並與資安監控機制(SOC)整合等。以部分符合金管會零信任架構指引設備 2.6 項次要求。

六、 信任推斷功能

1. 根據身份鑑別、設備鑑別、設備健康度與信任分數進行動態授權與風險屬性評估，未通過評估者自動阻斷存取。
2. 整合系統能力，提供 API 模組可與既有系統或第三方資安產品整合。

七、 部署與平台支援

1. 支援 Windows HyperV 虛擬化平台及地端部署。
2. 支援 API 模組介接、監控側錄等功能模組擴充及自動化開發，或付費客

製化。

3. 跨平台支援 Windows 與 Mac OS 作業系統，或付費客製化。

八、 零信任方案授權需求：包括但不限於身分鑑別授權 10U、設備鑑別與設備健康管理授權 10U、信任推斷、零信任系統等。

九、 零信任作業系統、資料庫及相關商業軟體授權需求

廠商若所需搭配作業系統、資料庫及相關商業軟體，皆須提供合法授權，並提供相關授權證明文件。如：Microsoft Windows Server 2022 Standard + 5 CAL、Microsoft SQL Server Standard + 5 CAL、相關商業軟體授權文件等。

十、 零信任硬體設備需求

1. 廠商應包含提供記憶體增購及安裝：
   (1)DELL R650 擴充記憶體：4 組 32GB 2RX8 DDR4 RDIMM 3200MHz 16Gb BASE ，HTPJ7。
   (2)DELL R450 擴充記憶體：8 組 16GB 2Rx8 DDR4 RDIMM 3200MHz，M04W6。
2. 本司只提供 Windows HyperV 環境資源佈建零信任軟體。除此之外，廠商應包含提供其他額外系統之所需的相關硬體設備與建置服務，例如若需從外網 VPN 透過 Gateway 設備設定 SAML 協定服務，應包含提供 Gateway 設備一台如 FortiGate 120G(含內建 VPN、SAML 協定)或 PA 440(含內建 VPN、SAML 協定)皆含等級以上。

十一、廠商交付系統應提供相關掃描報告如弱點掃描、滲透測試，確保無惡意程式及後門程式。依掃描結果評估為中風險以上之弱點應於 2 個月內修補或完成補償性控制措施，評估為低風險應訂定適當措施及完成時間等。

十二、維運服務與保固二年

1. 保固期自驗收日起二年。
2. 教育訓練到場。
3. 每季定期維護到場包含漏洞修補、版本升級、技術支援、諮詢等。
4. 事件通報、技術支援等包含電話、eMail 或到場等服務。
5. 服務時間週一至週五 09:00-18:00。
6. 其他系統整合需求可按情況付費客製化。

十三、本案所需憑證（如 TWCA）由本公司另行採購，投標廠商無須提供。

十四、付款方式

驗收合格後月結 30 日一次付清。

十五、依照廠商資格、產品功能合規、服務與保固等項採最有利標，未符合規格說明者視為無效標；若產品功能及服務項目未通過驗收，依相關規定辦理。

以上。