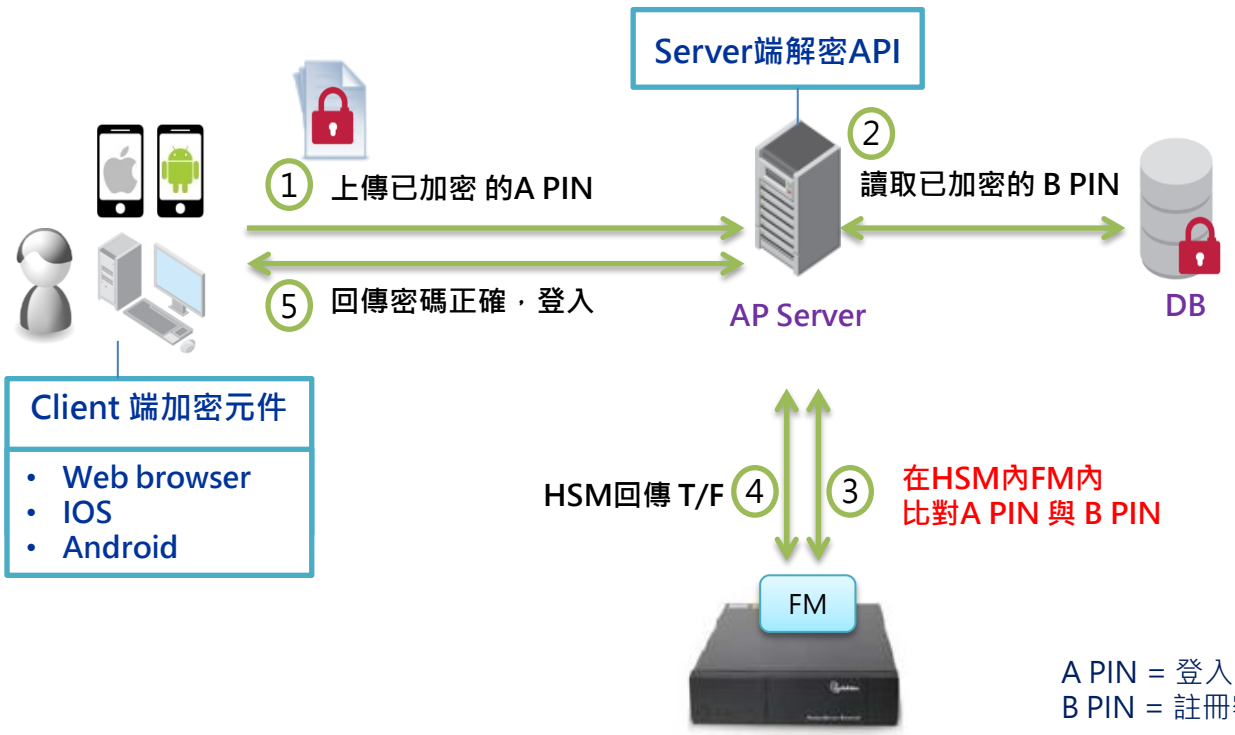
E2EE (End-to-End Encryption)點對點加密方案

因應銀行公會「金融機構辦理電子銀行業務安全控管作業基準 」第九條交易面之安全設計九、 應用於法人客戶之高風險交易且未依據無法否認傳送訊息與無法否認接收訊息之訊 息傳輸安全設計使用數位簽章者，應遵循下列必要措施：

(七) 傳輸敏感資料時，應提供端點對端點加密機制(如 end-to-end encryption, E2EE)，於客戶端輸入資料時立即加密，傳送至金融機構端符合 FIPS 140-1 Level 2(含)以上之硬體安全模組(如 HSM)內進行解密，以避免中間人(Man In The Browser、Man In The Middle)竊取；傳輸固定密碼者須於硬體安全模組內 進行驗證。

(資料來源：金管會 105 年 8 月 16 日金管銀國字第 105 00193690 號函)

聯宏科技提出E2EE解決方案，流程圖如下：



產品特色

聯宏科技提出E2EE點對點加密方案，採用銀行現有SafeNet ProtectServer HSM (Hardware Security Module)之設備符合FIPS 140-2 level 3 ，透過HSM之 FM (Functionality Module)韌體開發，將固定密碼或敏感性資料於HSM內進行加/解密運算，主要確保加密資料與金鑰安全，讓重要資料能於HSM內部進行處理，防止資料外洩風險，能有效避免中間人攻擊。

點對點(End-to-End)加密方案

銀行端目前提供客戶服務採「網頁版」與「行動App」兩種方式，均有交易與登入安全考量

聯宏提供：

- Client端加密元件：網頁版(IE 6.0 / Firefox 2.0/Chrome4.0/Safari latest two)、Android 5.0、iOS 7以上
- Server端解密API ：提供API程式供AP Server(應用伺服器)讀取資料，於硬體密碼模組(HSM)進行資料比對
- FM韌體：加密資料於硬體密碼模組(HSM)內解密演算

聯宏科技股份有限公司
PAYSECURE TECHNOLOGY CO.,LTD.
114 台北市內湖區內湖路一段91巷17號10樓之1
TEL：+886-2-2657-1187 FAX：+886-2-2657-1205