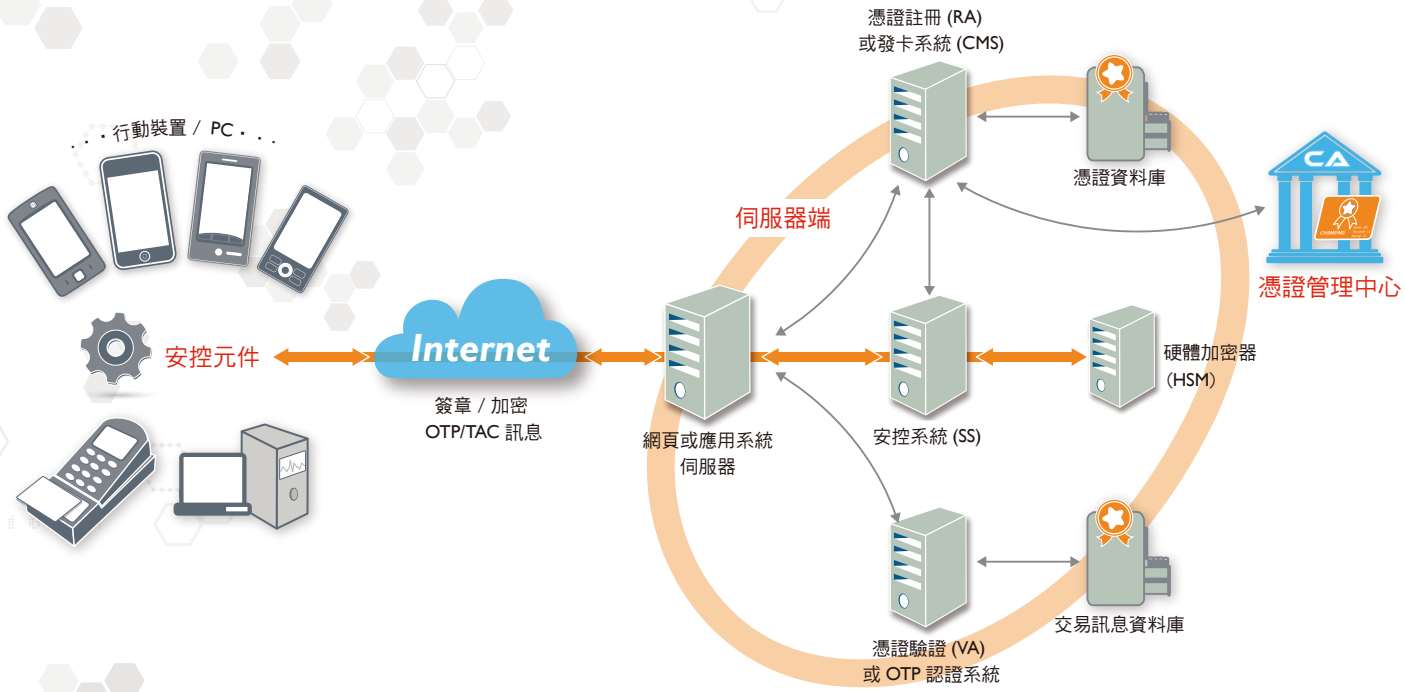
CHANGING 全景軟體

SS 簽章加密安控伺服系統

Secure Server



“安控系統 (SS) 可搭配硬體加密器 (HSM) 運作

– 提供應用系統加解密、簽驗章等機制”

- 保護私密金鑰的安全性
- 加速簽驗章、加解密運算過程
- 提昇整體應用系統效能

- 安控系統 (SS) 提供產生並儲存本系統所需之金鑰對、產生憑證簽發需求資料 (CSR), 並匯入憑證管理系統 (CA) 所簽發之憑證。
- 安控系統 (SS) 提供訊息簽章及加密功能，透過安控元件的整合，系統開發人員可透過此一介呼叫本系統進行訊息簽驗章及加解密。
- 安控系統 (SS) 支援 PKCS7、W3C、XML 簽章加密等國際標準格式。
- 安控系統 (SS) 可支援符合 PKCS#11 規範的硬體安控模組，如：SafeNet(Eracom、Luna) 、THALES(nShield)、Utimaco、AEP、IBM4758、AR Privateserver 等。

SS 簽章加密安控伺服系統
Secure Server

金鑰產生及匯入
- 提供各種金鑰之產生、備份、復原、銷毀；金鑰之查詢、停用、刪除；金鑰權限控管等功能。
- 金鑰匯入功能（Load Keys）—DES、3DES 對稱式金鑰可透過客戶所提供之 AB 碼單或 AB 母卡匯入業務所需金鑰。

多種應用程式 API
- 提供內含 TCP/IP 通訊功能之 API，連結金鑰加密系統執行業務性功能；包括 Win32 動態聯結函式庫 (DLL)、ActiveXJava、Solaris 動態聯結函式庫 (.so) 及 Linux 動態聯結函式庫 (.so) 等介面。

系統管理功能
- 提供 Web-Based 之管理操作介面。
- 具備系統重新啟動、系統設定修改、系統狀態監看、歷史記錄查詢等功能。

系統私鑰之保護與交易紀錄
- 本系統之各項金鑰存放於硬體裝置中 (HSM)，以提供系統私鑰安全上的加強保護；系統更可設定由兩位以上之系統管理人員共同持有金鑰管理權力，提供分散授權與多人授權之機制，以增加金鑰安全性。
- 本系統中的金鑰可與應用系統進行鎖定，應用系統不得使用未經授權的金鑰。
- 系統可記錄任何使用金鑰進行加密、解密之交易紀錄，交易紀錄資料包含操作之應用系統、使用之目的金鑰、時間與交易資料主體等，並提供交易紀錄之查詢、備份功能。
- 訊息加密功能本系統可透過應用系統安控元件進行整合，系統開發人員可透過此一介面呼叫本系統進行訊息簽驗章及加解密之動作。
- 本系統支援各式 DES/3DES/AES 加密模式，包括 ECB、CBC、CFB、OFB 等國際標準格式。

支援硬體安控模組 (HSM)
- 利用硬體安控模組 (HSM) 達成加速加解密運算之目的，可充分滿足同時處理大量交易加解密運算時所需之系統效能，本系統可支援符合 PKCS# 11 規範的硬體安控模組。
- 多台 SS 能夠進行串連，具備 HA 機制，能提供自動故障轉移 (Fail Over) 與負載平衡 (LoadBalanc e)，並保持硬體加密器間之金鑰同步。

帳號管理
- 本系統提供管理者帳號管理相關的功能，可以新增帳號或修改帳號權限設定，管理者可採用憑證智慧卡登入系統之功能與多人授權、控管之功能。

系統稽核紀錄
- 訊息接收回覆以及系統操作設定皆有系統紀錄功能，可提供日後稽核之用。
- 應用系統界接函式本系統提供 COM,Java,DLL 等界接函式庫，供其他應用系統界接使用。並在系統中能限制能連結的 IP 清單，以確保系統的安全。

CHANGING 全景軟體
www.changingtec.com
新竹總公司 300新竹科學園區園區二路48號2樓 TEL:03-5630688 FAX:03-5630618
台北辦公室 100台北市博愛路150號5樓 TEL:02-23700337 FAX:02-23700446