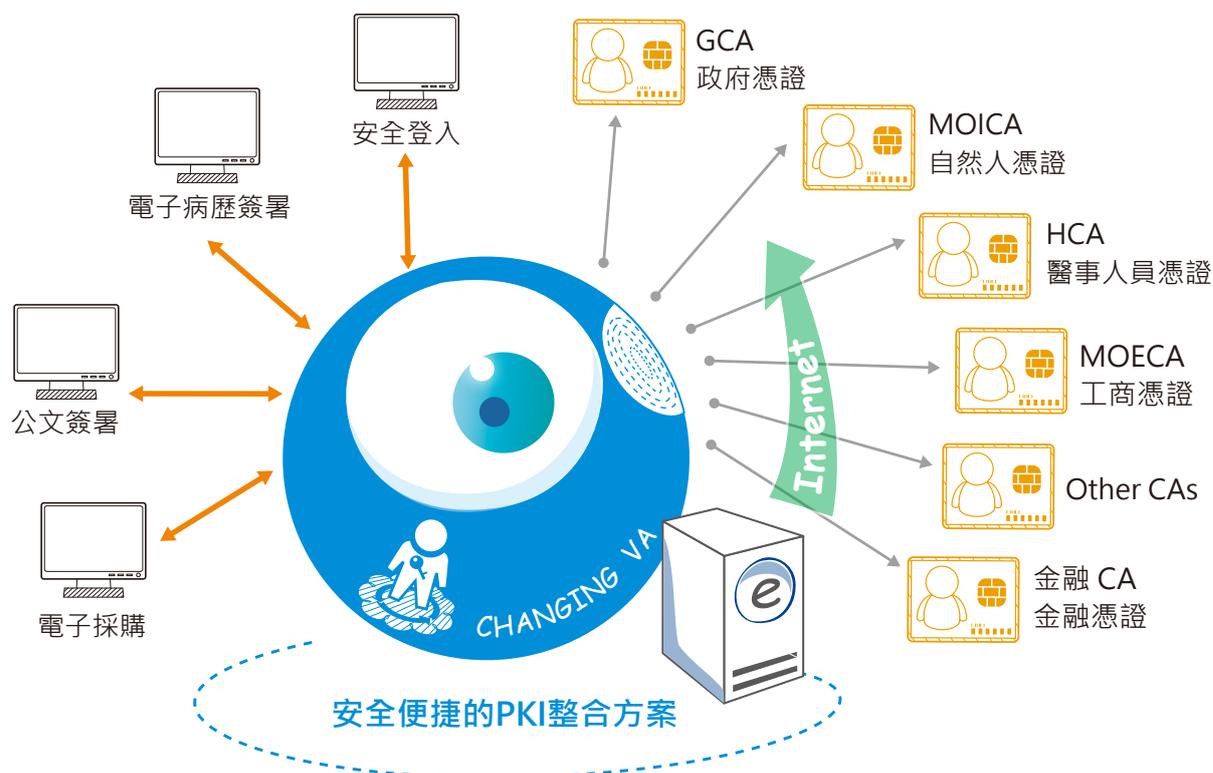


# VA 全景多憑證驗證系統

## Validation Authority

SafeTran VA 6.0



本產品為一數位簽章之驗證伺服器，可提供入口網站及應用系統作為多種數位憑證之驗證機制，並利用搭配的跨瀏覽器安控元件組成理想的 PKI 運作流程。而透過 PKI 相關標準的支援，本產品能夠有效管理公共憑證管理中心（Public CAs）所發出之憑證撤銷清單（Certificate Revocation List，CRL）及線上憑證狀態查詢（Online Certificate Status Protocol，OCSP）功能。

### 提供簽驗章功能

- 支援 PKCS#7 協定之簽驗章格式。
- 支援 RSA 1024/2048 bits 之金鑰長度。
- 支援 SHA1、SHA256 雜湊函數。
- 支援政府自然人憑證、機關憑證之驗證。
- 支援 PKCS#12 協定。
- 支援 PKCS#11 協定。

### 憑證合法性驗證

- 能指定接受多個註冊單位所簽發的憑證。
- 能確認憑證所屬註冊單位、憑證機構與持有者符合設定的驗證規則。
- 不同應用系統可使用不同驗證規則。

## 提供憑證 CRL( 憑證撤銷清單 ) 及憑證鏈管理及驗證功能

- 支援設定下載排程。
- 支援新增、修改、刪除 CRL 及憑證鏈下載網址。



- 能管理國家發展委員會政府機關憑證中心、內政部自然人憑證中心、經濟部工商憑證中心、衛生福利部醫事人員憑證中心、金融憑證、中華電信憑證、財團法人憑證簽發之 CRL 及憑證鏈。
- 依客戶需求 VA 可安裝於 Windows、IBM AIX、Solaris、Linux、Unix 等作業系統。支援 MSSQL、Oracle、MySQL、MariaDB、PostgreSQL、Sybase、DB2 等資料庫。
- 符合國家發展委員會 GCA 政府憑證管理中心「公鑰憑證處理安全檢查表」之憑證驗證項目。

## 提供客戶端安控元件，以供客戶端下載使用

- 可透過 PKCS#11 標準安控界面，呼叫使用者插入於晶片卡讀卡機中的內政部自然人憑證 (MOICA)、商業司工商憑證 (MOEACA)、國家發展委員會組織及團體憑證 (XCA)，讀取並解譯憑證相關資料 ( 包括「版本」、「序號」、「簽章演算法」、「發行者」、「有效起止期限」、「主體」、「公開金鑰長度」、「金鑰使用方式」、「身分證末碼或統一編號」...等相關訊息 ) 之功能。
- 提供密碼檢核、密碼變更、數位簽章、資料加密與解密等功能。
- 支援的作業系統：
  - Windows 2012/2016/2019 Server 及 Windows 8/10 等 32/64 位元
  - Mac OS 10.13/10.14/10.15
- 支援多瀏覽器使用：  
IE/EDGE/Chrome/Firefox/Safari
- 提供客戶端環境偵測之網頁與元件安裝程式，以方便使用者進行安裝。
- 可支援 1024 及 2048 位元憑證 ( 政府憑證 (GCA)、內政部自然人憑證 (MOICA)、商業司工商憑證 (MOEACA)、組織及團體憑證 (XCA) )，及支援前項憑證之內定演算法 (SHA1 或 SHA256) 進行憑證驗證作業。
- 簽章演算法支援 RSA2048 搭配 SHA256 演算法或 RSA1024 搭配 SHA1 演算法。