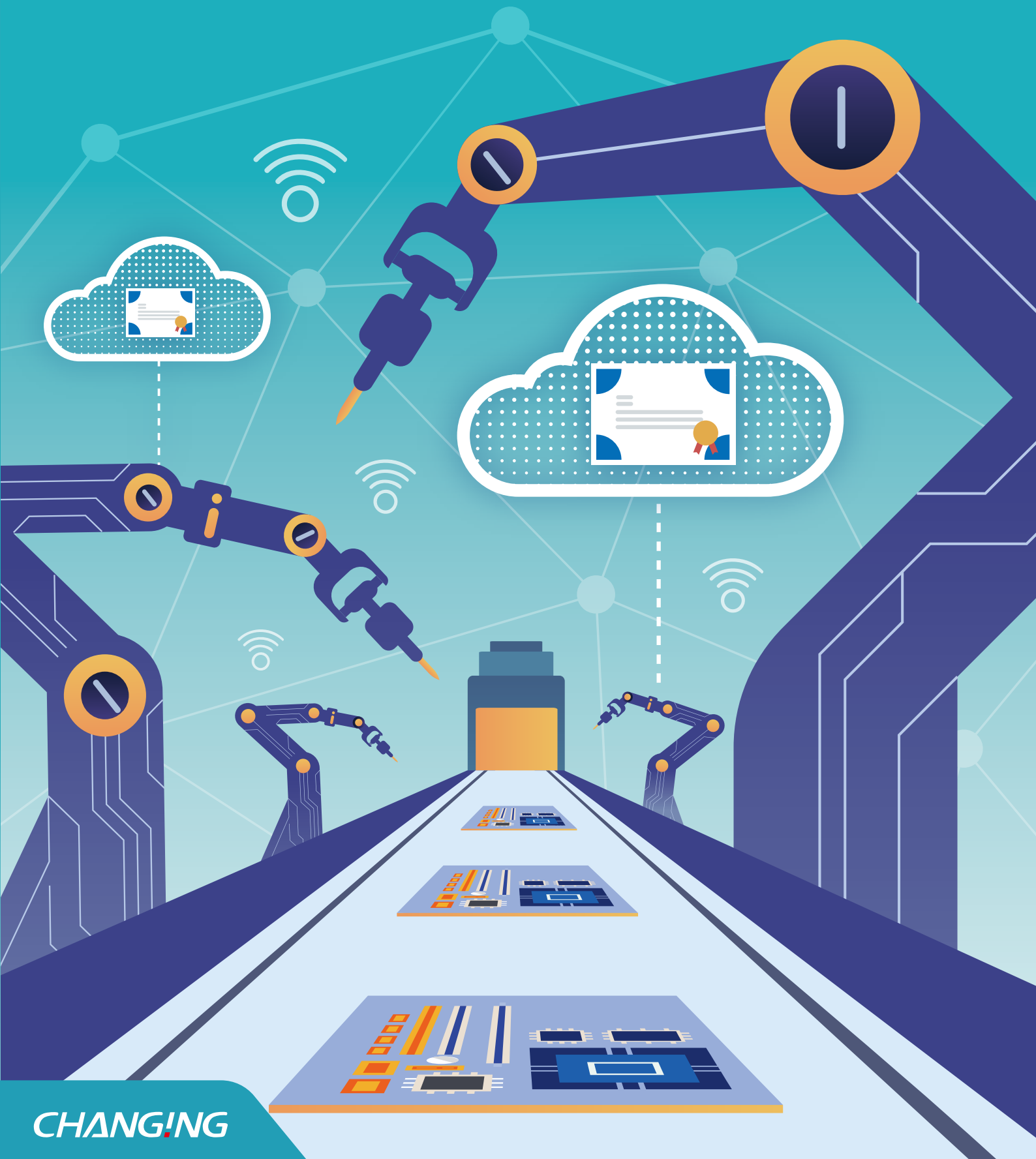
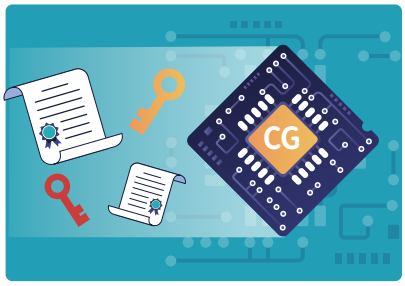
IoT 時代
設備安全認證的關鍵服務



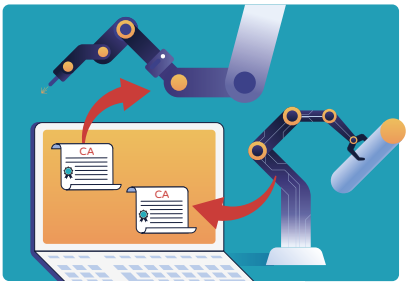
CHANGING

全景 IoT 安全解決方案

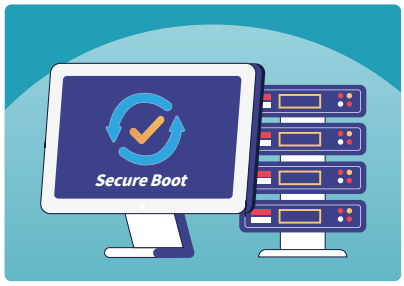
可於設備各個生命週期階段，提供不同的安全保障，包括設備密鑰的產出與管理、憑證管理以及 IoT 安全服務，將機器身分管理融入全面的資訊安全防禦體系，為物聯網及供應鏈環境建立「零信任網路架構」，以因應內外網邊界逐漸模糊的現況，幫助確認設備合法性，預防設備軟體平台遭竄改及軟韌體的不合法更新，並保障 TLS 傳輸安全通道與加密敏感資料，確保設備間資料傳輸的安全，在享有物聯網帶來便捷生活的同時，也能安全無虞。



CodeSign 服務

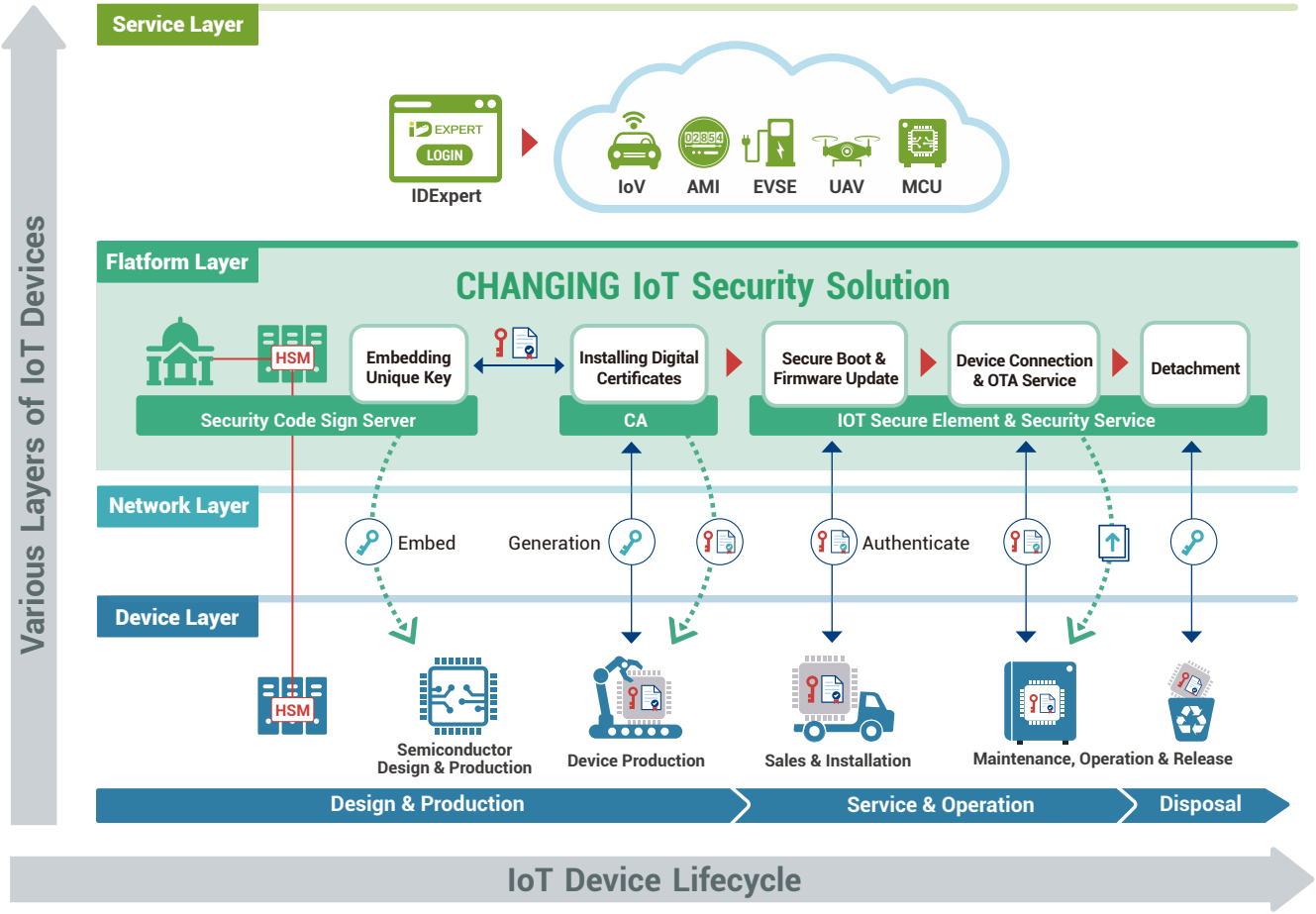


CA 設備憑證管理



IoT 安全服務

架構圖



CodeSign 服務

金鑰簽章加密控管

搭配硬體保密模組 HSM (Hardware Security Module) 運作，在晶片的安全區域大量嵌入唯一私鑰，實現安全晶片加解密及簽驗章功能。

- 使用私鑰簽章，保障機敏資料完整性及不可否認性，防偽造和竄改。
- 使用公鑰驗章，確保韌體安全更新，系統也能安全啟動。

HSM Cluster 金鑰管理

智慧查詢 Cluster 所設定的 Master 或 Slave Slot 的金鑰清單，資訊包含金鑰狀態、名稱、類型、啟用及停用日期，並可使用金鑰名稱進行模糊查詢，使用者可彈性運用。且支援 RSA、ECDSA、DES、3DES、AES 等加密演法，因應不同的安全等級。

HSM 統合管理

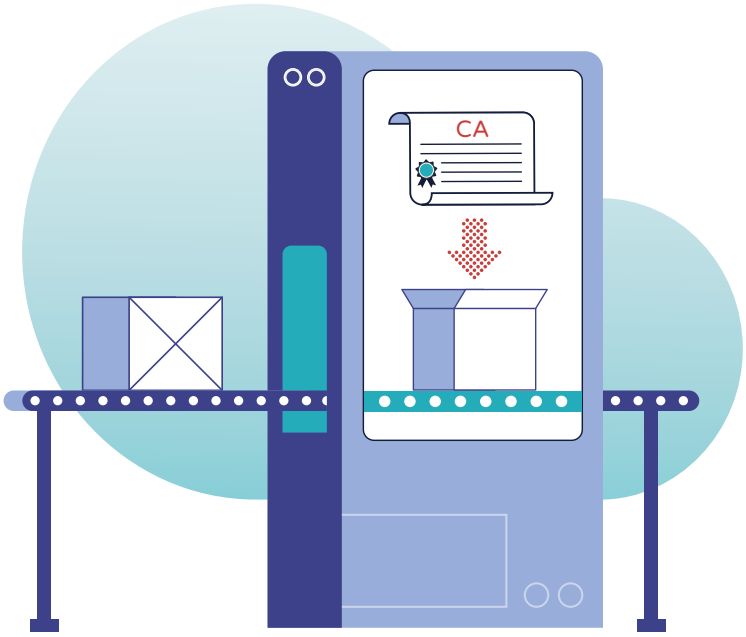
可進行 HSM 連接、同步等操作，並可於系統內填入 HSM 資訊，包含名稱、廠牌、IP、Slot 等，方便建置及管理。

CodeSign 程式碼數位簽署

對軟體或程式碼進行數位簽署，使用者可驗證程式碼的真實性 (來源) 及完整性，並防止篡改。

- 支援 ActiveX、Jar、exe、dll、img、bin、apk 等檔案的 Code Sign 作業。
- 整合客戶端 SignTool，進行 firmware Code Sign 作業。
- 可批次 Code Sign 或單次上傳 Code Sign。
- 支援第三方 CA 憑證或自簽憑證。

CA 設備憑證管理



申請設備憑證，鑑別設備的合法性

透過設備的憑證管理系統 (Certification Authority) 滿足設備商在 IoT 設備出廠前的憑證載入需求，以設備唯一 ID 及憑證，保障設備佈署的合法性。

CA 憑證中心批次產製憑證，統一處理，便捷快速

向雲端服務註冊 CA→ 私鑰放置於 HSM 負責簽發憑證 → 批次產製憑證。

提供 API，幫助設備生產流程順暢且安全

- 生產工作站 API：接收憑證相關檔案，並將憑證載入 IC 晶片，同步將憑證資料傳送至憑證生產管理系統。
- QC 工作站 API：驗證憑證是否有正確寫入。

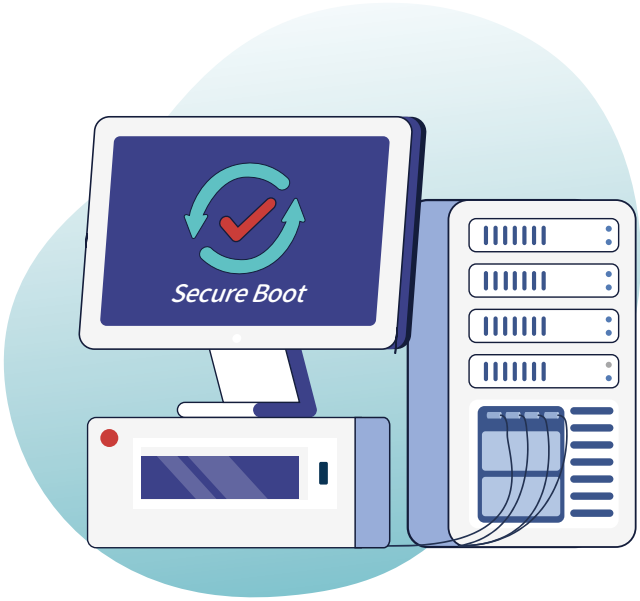
IoT安全服務

雙向認證及 TLS 安全通道

利用設備憑證進行設備雙向認證，互相驗證憑證有效性，裝置透過 Bluetooth、WFi、WANGOX 或 NBT 連線，建立設備之間傳送資料的加密安全通道，確保資料傳輸隱密、完整及可靠性，符合國際標準。

硬體安全晶片

採用通過 Common Criteria EAL6+ 認證的英飛凌 OPTIGA™ TPM 以及 OPTIGA™ Trust M 安全晶片，擁有獨立的微處理器和儲存區域，可與設備終端作業系統、應用軟體的執行環境進行物理隔離，具高度安全性，其安全啟動、存取、儲存等核心功能將有效抵禦駭客的攻擊。

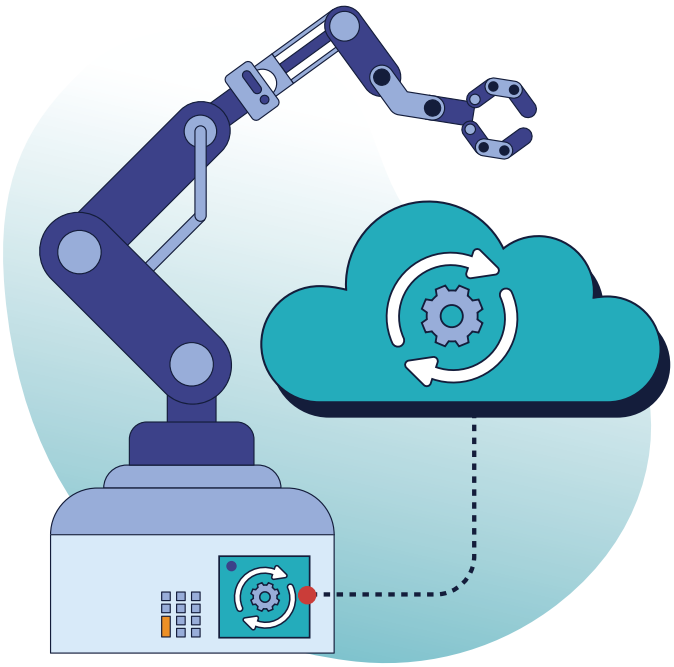


裝置安全啟動

安全晶片展現信任根的安全防護，提供設備軟韌體完整性檢查功能，滿足裝置安全啟動 (Secure Boot) 需求，裝置啟動時，會自動檢查裝置韌體 (firmware) 是否遭竄改，檢查正確後才允許裝置啟動，提高設備的安全可靠度。

系統 OTA 線上升級

透過網路將新版本的軟體或系統更新推送到終端設備，在 OTA (Over-The-Air) 升級過程中，終端設備無需連接到電腦或使用 USB 線連接，經由網路接收到更新包，即可自動完成升級，能快速、簡便完成系統或軟體更新，同時可降低終端使用者及服務提供者的維護成本。



OTA 保障連線安全

OTA 線上升級服務全程採用全景設計的安全機制，包括 Transport Layer Security (TLS) 交互身分驗證、OTA 更新流量經由全景 OTA Server 管理及傳遞，每個透過 OTA server 傳入及傳出的 HTTP 或 MQTT 訊息，都會經由身分驗證及授權，此外，設備韌體可在 OTA 更新之前進行數位簽署，確保其來自可靠的來源，且未遭竄改。

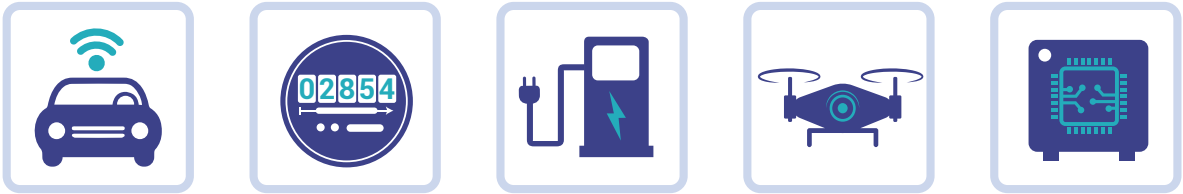
符合國際資安標準

協助設備製造商在設計、生產產品的同時，將資安的合規性納入考量。

- 美國聯邦物聯網網路安全法
- 國際工控資安標準 IEC62443
- 歐盟執委會資安韌性法草案

多元應用

在物聯網服務中，應用 MFA 多因素認證可提高使用者身分的安全性，防止未經授權的訪問及資料洩漏。



IoV 車聯網　AMI 智慧電表　EVSE 充電樁　UAV 無人機　MCU 應用設備

授權經銷商

CHANGING
全景軟體股份有限公司
www.changingtec.com
TEL : +886-3-563-0688
30844 新竹科學園區新竹縣園區二路48號2樓