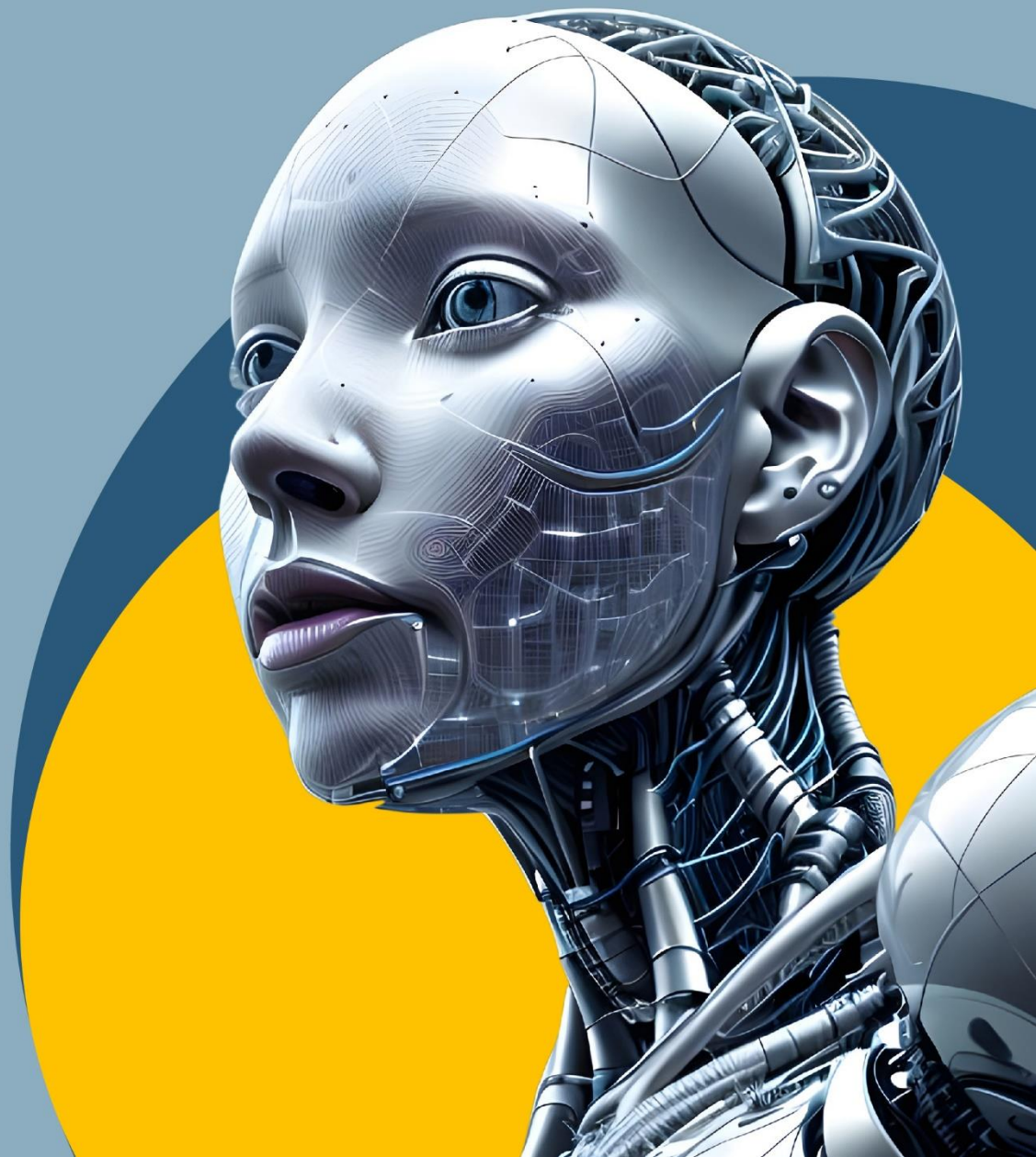
CHANGING
全景軟體

IEC 62443 與物聯網整合
機器身分管理的關鍵角色

全景軟體 邱志成 Frank Chiu



Every Machine Needs an Identity

Every Identity Must be Managed

不信任的世界中數位信任的角色

The Role of Digital Trust in an Untrusting World

機器身分認證，開啟物聯網資安新時代

IoV車聯網、AMI智慧電表、EVSE充電樁、工業自動化及控制、半導體應用設備

IoV 車聯網

ISO 21434

使用機器憑證進行雙向認證，確保車輛與後台系統的安全通信。

AMI 智慧電表

IEC 62056/62351

使用身份驗證技術驗證電表和電力公司系統的身份，以預防數據被篡改。

EVSE 充電樁

OCP/ISO 15118

確認充電樁和電動車的身份，以抵禦非法充電行為，並透過加密技術保護充電樁和電動車之間的通訊資料，以避免竊聽和竄改。

工業自動化及控制系統

IEC 62443

為了解決一系列應用上所遇到的資訊安全問題。包括用於製造和加工廠設施、建築環境控制系統、地理位置分散的業務 、石油生產管道和分配設施以及其他行業和應用。

半導體應用設備

SEMI E187

確保機器和雲端的身份驗證，以抵禦非法入侵，同時透過加密技術保護機器和雲端之間的通訊資料，避免竊聽和竄改。

機器憑證與機器信任根

IEC 62443機器身分管理的關鍵角色

- **機器憑證管理**

  機器憑證管理包含 憑證申請、撤銷、更新、查詢、下載、同步等功能，可有效管理設備的合法性。

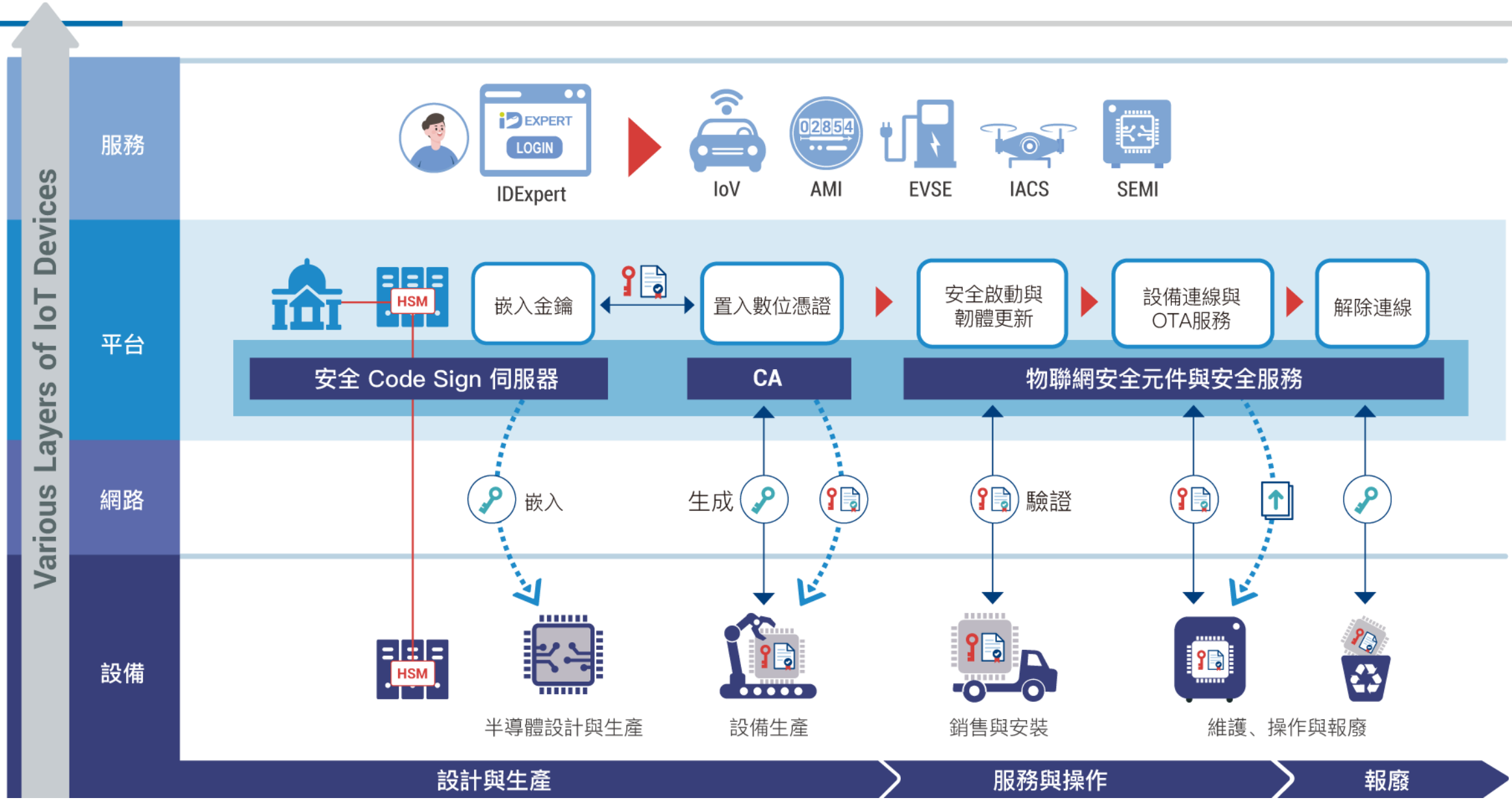
- **機器信任根**

  1. 引入英飛凌的安全晶片，包括 OPTIGA™ TPM 和 OPTIGA™ Trust M。
  2. PUF技術，介紹其獨特的物理特徵生成機器唯一身份識別碼的能力。

融入零信任方法的思維，將每個晶片視為零信任環境中的一個主體，應用 **身份驗證** 和 **授權** 的概念。

憑證管理設備的認證及生命週期

CHANGING



機器硬體信任根- 安全晶片
(root of trust，RoT)

1.物聯網安全的獨特需求:

- 物聯網安全不能僅仰賴軟體解決，需要更強大的硬體信任根。

2.安全晶片 與 IEC 62443:

- 安全晶片在IEC 62443標準下，為工控系統提供卓越的可信賴性。
- IEC 62443重視身份驗證和數據保護，而安全晶片在此扮演關鍵角色。

3.硬體式安全保護:

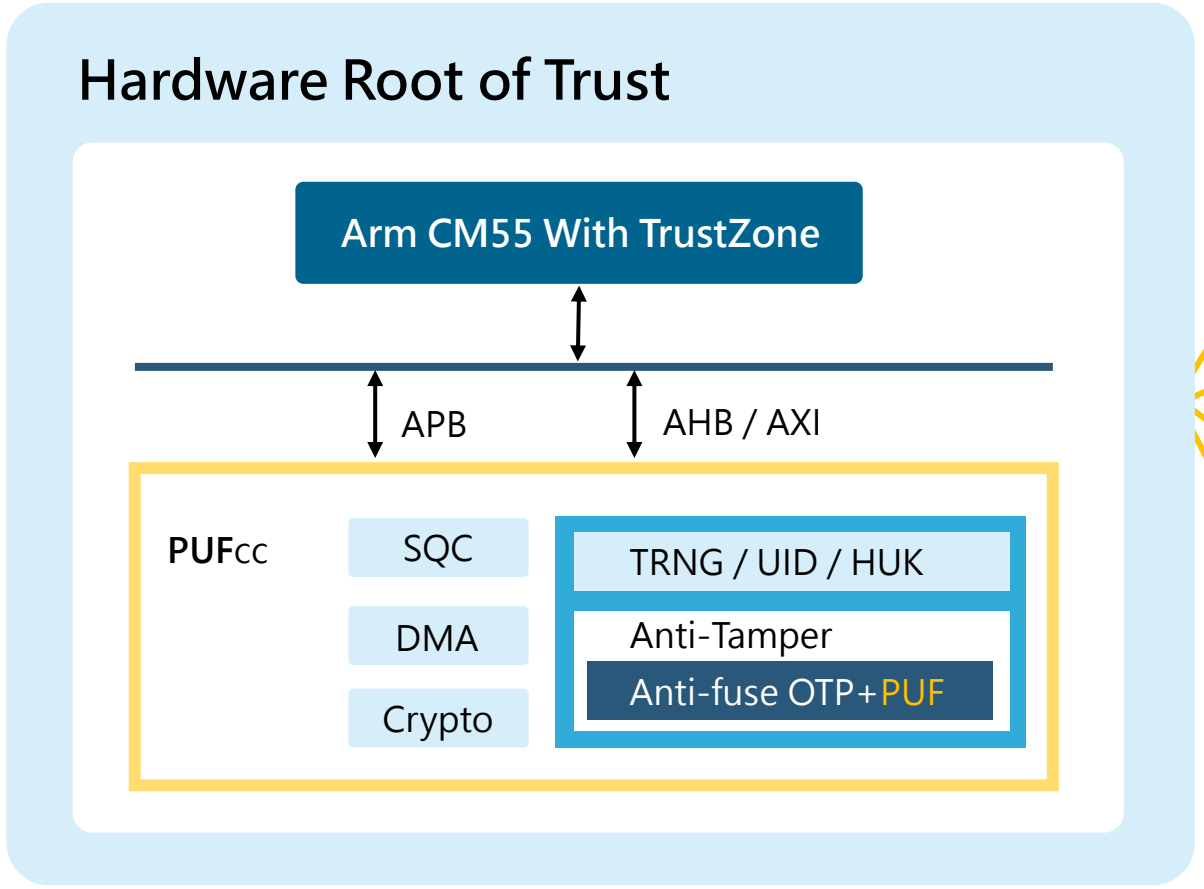
- 通過 Common Criteria EAL6+認證，確保卓越的硬體安全性。
- 具有獨立的微處理器和儲存區域，內部安全儲存密鑰，加密/解密在晶片內部執行，極難被竊取。

4.物聯網安全全方位概覽:

1. **強化身份驗證:** 安全晶片確保只有受信任的應用程式和機器能夠訪問系統，提升整體安全性。
2. **硬體式數據保護:** 利用硬體式安全機制，確保敏感資料免受未授權存取，為系統提供全面的保護。

機器硬體信任根–MCU Trust Zone + PUF

不限何時與何地:
具有高度延展性，可在任何時間、任何地點實現攻不可破的信任根基。



01 PUF技術的應用
利用PUF（物理不可複製功能）的天生密碼(晶片指紋)作為金鑰，用於加密存儲機要資訊。

02 高品質的熵提供
PUF 中的 TRNG 能為 TrustZone 提供高品質的熵以執行各種安全功能。

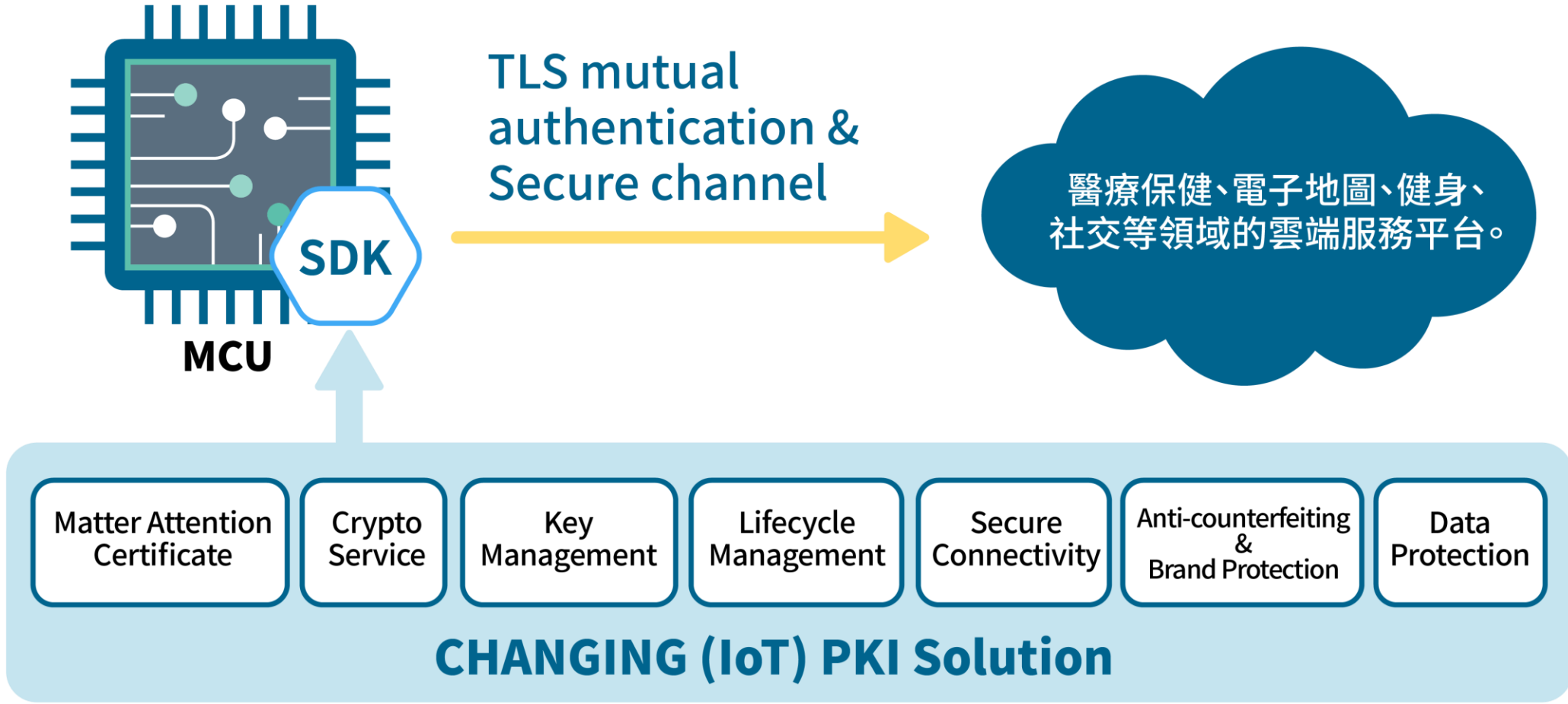
03 PUF + ARM TrustZone的整合
PUF+ARM TrustZone實現安全信任根、安全存儲和安全系統。

04 原生且唯一的金鑰
利用矽晶圓的原生特性產生金鑰，無需額外整合安全晶片，或在不安全的軟體環境中生成金鑰。

全景設備整合(TPM/SE/TrustZone)安控元件

CHANGING

穿戴裝置PKI安全解決方案



機器安全保護及TLS傳輸安全通道

全景IoT解決方案

CHANGING

設備設計階段	設備生產階段	設備維護、操作與報廢階段
在物聯網設備建置硬體信任根，搭載安全功能 - 以確保裝置身分認證、完整性和安全連線	IC 燒錄包括金鑰保護、韌體簽章及設備認證發放	設備連線認證、連線安全通道、韌體 OTA 安全更新
設備認證與安全通道功能 • 驗證設備的身分 • 使用 TLS 雙向認證及加密通道 • 進行資料簽署以確保資料完整性和不可否認性 **安全啟動與韌體更新功能** • 使用安全晶片的信任根 (RoT) 進行設備韌體完整性檢查 • 使用加密和簽署安全存儲設備，保障機密性與完整性，防止竄改 **設備中的硬體信任根 (Root of Trust) 設計** For 物聯網裝置製造商 : • TrustM 安全模組 • Linux TPM 安全模組 For IC 設計公司: • MCU Trust Zone + PUF IP	**KMS 金鑰管理系統** • 整合憑證管理系統 • HSM (硬體安全模組) 整合 **IC 燒錄：Code Sign 韌體及驗證系統** • IC 燒錄簽署和韌體燒錄 • 驗證管理 **IC 燒錄：憑證發放及驗證管理系統** • IC 生產憑證發放和燒錄 • 驗證管理 IC 程式生產的兩種方式: • 設備商工廠自建燒錄設備和系統 • 全景有配合的燒錄廠商,設備商可以外包燒錄	**設備憑證 PKI 基礎架構** • CA 憑證管理系統 • RA 憑證註冊系統 • VA 憑證驗證系統 **Over-The-Air (OTA)** • 設備身分驗證 • 建立安全通訊通道 • OTA 軟體簽章 • 更新驗證 • 還原機制

全景IoT安全晶片解決方案

將完整的資安防護，導入智慧物聯網

採用 Infineon 安全晶片，
提供物聯網裝置 Root of Trust 資安防護，有效保護安全通道及加密雲端資料。

6大防護機制

專業規格安全晶片

使用 Infineon High-end Security Controller，並通過 Common Criteria Certified EAL6+的認證，安全晶片裡的密鑰及憑證均無法被取出或複製。

建立安全可靠的連線

裝置透過 Bluetooth、WiFi、LoRaWAN、SIGFOX或NB-IoT連線，建立符合國際資安標準的加密安全通道，確保資料傳輸隱密、完整且正確。

標準客製化服務

有多年實務經驗的專業團隊，根據客戶的產業特性及需求，提供最新產業資安標準的解決方案，亦可協助整合公有雲及私有雲的資料安全儲存。

保護資料+裝置合法性

藉由裝置唯一ID及憑證確保裝置的合法性，並提供符合國際資安標準的對稱式及非對稱式加解密功能，保護裝置內的資料。

Secure Boot

裝置啟動時，自動檢查裝置Firmware是否遭竄改，檢查正確後才允許裝置啟動。

Firmware自動安全更新

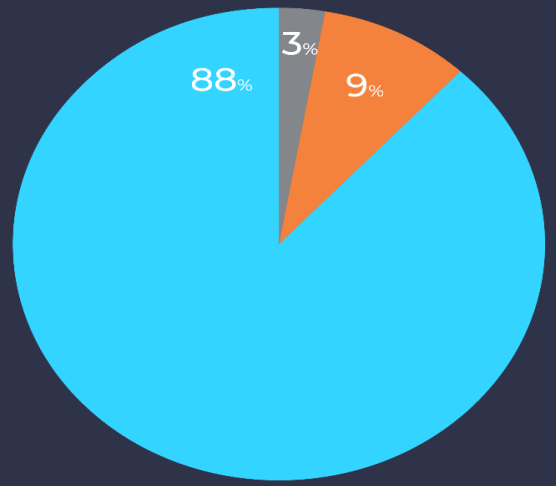
Firmware發布皆由憑證簽署 (Code Sign)，更新時檢查Code Signed Firmware合法性及正確性。檢查正確後，Firmware則透過OTA (Over the Air) 進行更新。

設備憑證管理平台

DEVICE

Device Status

Online Offline No Certificate

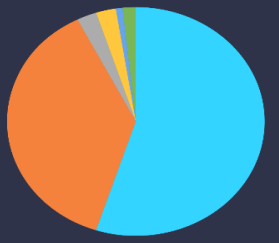


88%	3%	9%
Online Device	Offline Device	No Certificate

CERTIFICATE

Certificate Template Issue

Device_01 Gateway Admin
Device_02 User Server

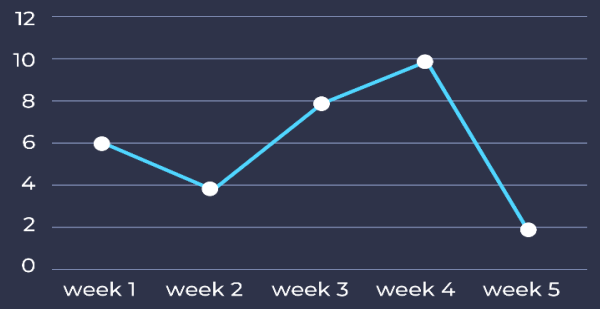


Certificate Status

125	9	1
Active Certificates	Issue in Last 7 Days	Revoke in Last 7 Days

3	5	8
Expired in 48 H	Expired in 7 Days	Expired in 14 Days

Certificate Issue (Weekly)



Certificate Revoke (Weekly)

CHANGING

符合IEC62443標準的半導體IC安全燒錄生產

工廠生產燒錄 Code Sign 韌體及驗證管理系統

1.半導體IC安全燒錄：

- 實施安全燒錄技術，確保半導體IC在生產過程中的安全性。
- 針對韌體的寫入過程進行監控和保護，防範未授權的存取和潛在的威脅。

2.Code Sign及驗證管理：

- 韌體的Code Sign，確保其來源合法，防範惡意修改。
- 配備驗證管理系統，確保僅信任的韌體能夠在半導體設備上執行，降低風險。

工廠機器生產憑證簽發及驗證管理系統

1.機器生產憑證簽發：

- 提供安全的憑證簽發機制，確保僅合法的機器能夠參與生產流程。
- 使用先進的加密技術，防止憑證被冒用或篡改。

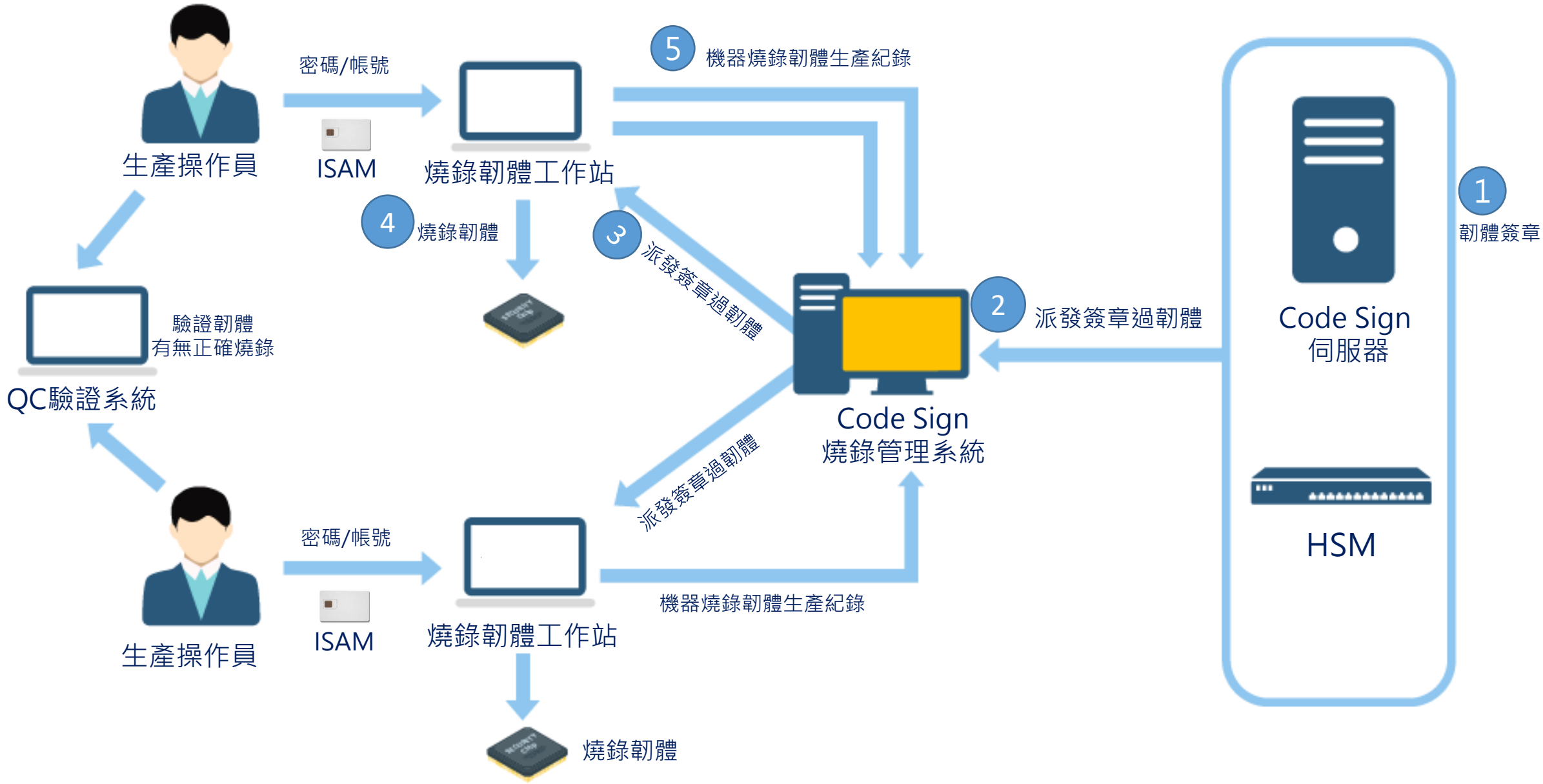
2.驗證管理系統：

- 建立嚴格的機制，驗證機器生產憑證的有效性和合法性。
- 整合強固的身分驗證，確保僅受信任的機器參與各生產階段，提高整體系統的安全性。

3.多層次生產保障：

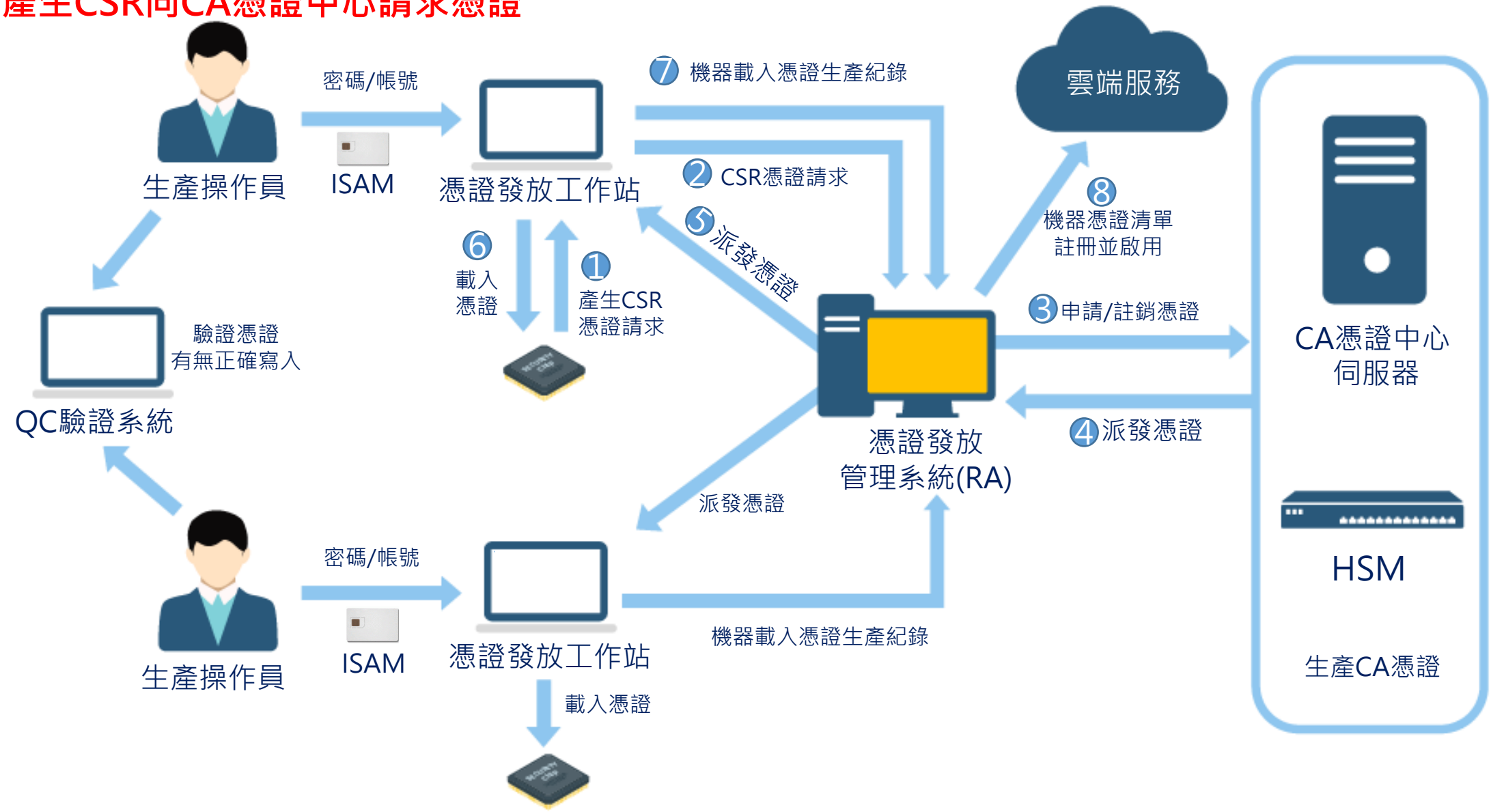
- 將憑證簽發和驗證納入多層次的安全保障，以應對不同攻擊向量。
- 定期更新驗證機制，以確保對新型威脅的即時應對。

工廠生產燒錄Code Sign韌體及驗證管理系統



工廠機器生產憑證簽發及驗證管理系統

IC產生CSR向CA憑證中心請求憑證

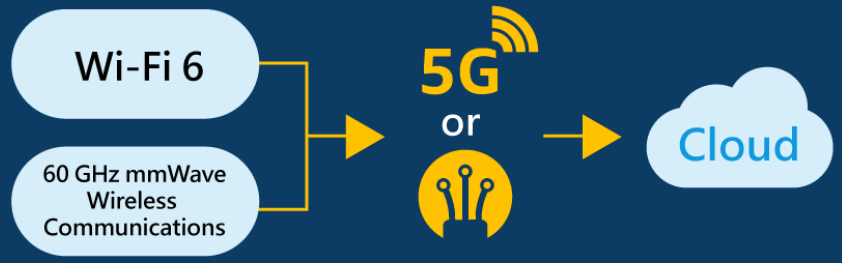


案例分享 - 智慧城市資安防護方案

智慧聯網機器資訊安全防護

- 機器內含安全晶片保護密鑰
- 機器憑證身分認證
- 機器安全啟動
- 機器韌體安全更新

資料網路傳輸安全防護



- TLS雙向認證及加密安全通道
- 機敏資料簽章，資料防竄改及不可否認性
- 上傳檔案簽章加密，檔案資料機敏性及完整性

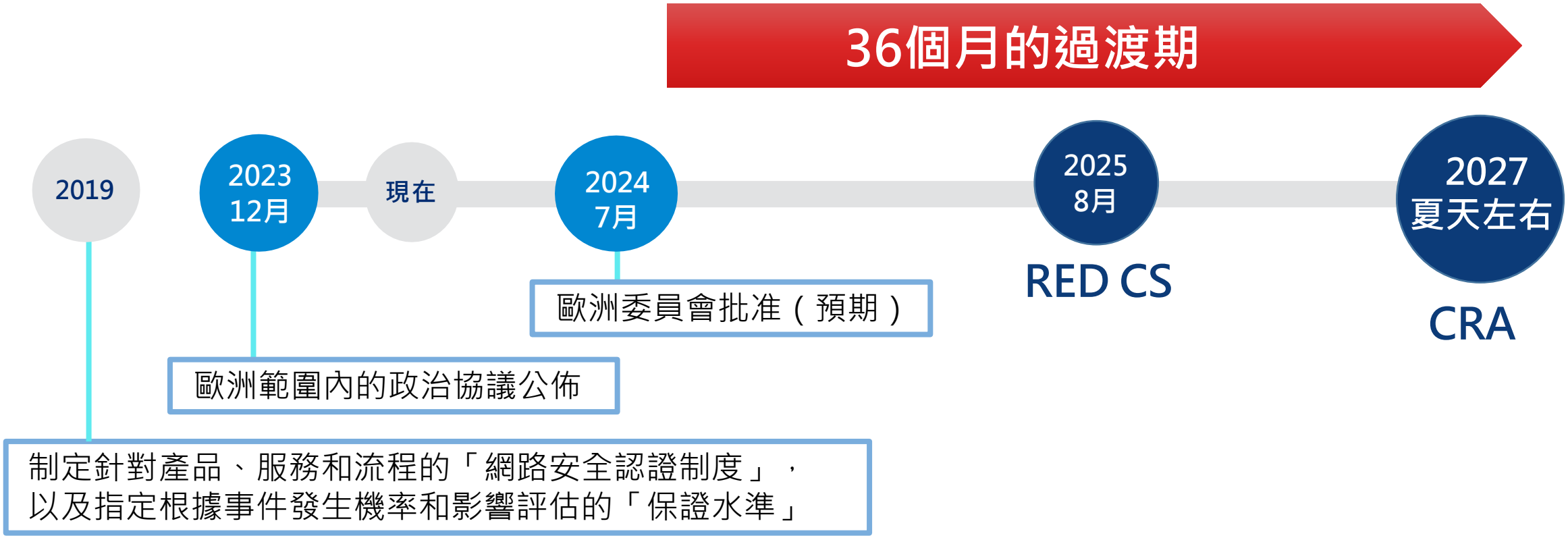
安全晶片　機器憑證

物聯網機器符合國際資安法規及標準

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

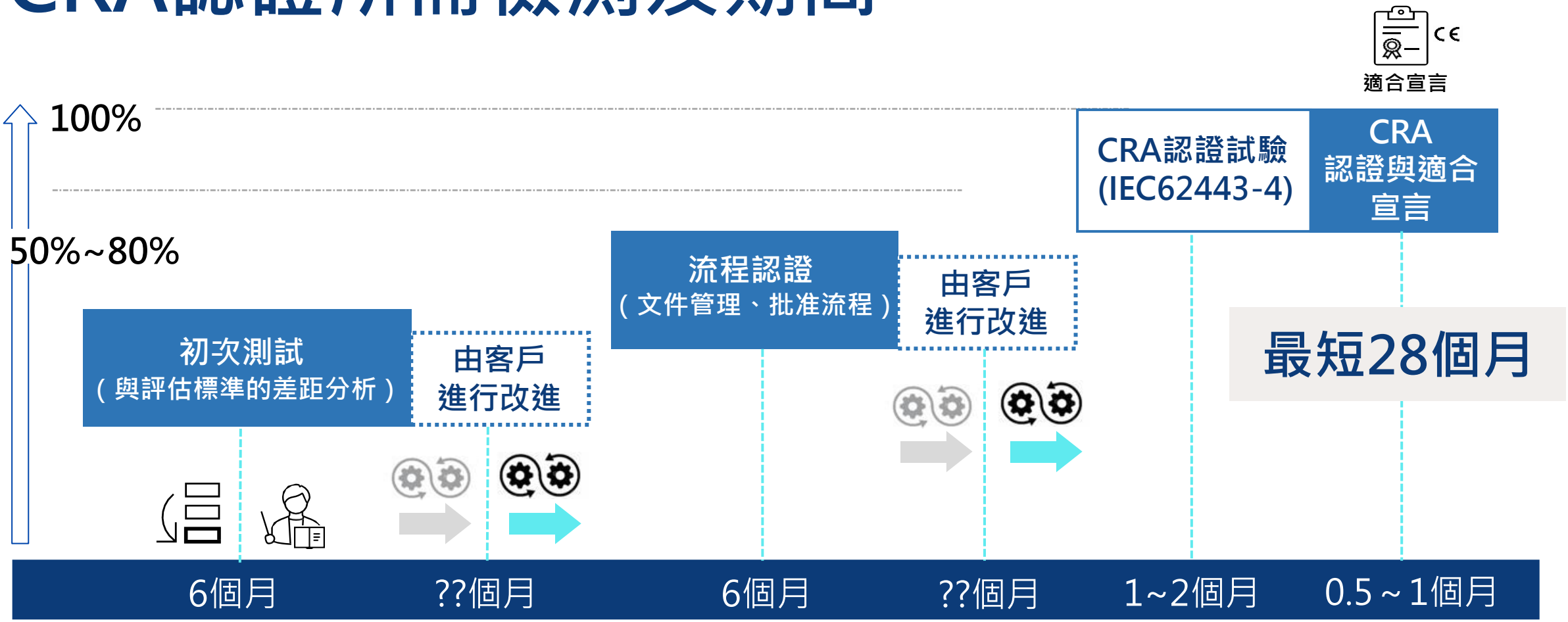
法規類別	法規名稱	主要內容
隱私	一般資料保護規範(GDPR)	歐盟通過於2018年，適用於歐盟境內所有處理個人資料的組織，包括物聯網產品供應商。
	台灣個人資料保護法修正條文	台灣於2020年5月修正，增訂物聯網裝置收集個人資料的相關規定。
資安	美國聯邦物聯網網路安全法 IoT Cybersecurity Improvement Act of 2020	根據NIST的物聯網指引，包括辨識、管理安全弱點、科技發展、身分管理、遠端軟體修補、型態管理等，為聯邦政府設立最低安全標準。 包括通報政府資安環境弱點的指引。
	美國國家標準技術研究院(NIST)	制定最低安全標準及指引，涵蓋辨識、管理物聯網設備安全弱點、身分管理、遠端軟體修補、型態管理等項目。
	國際工控資安標準 **IEC62443**	IEC 62443目前所涉及應用的產業，除了一般所認知的工控產業，包含能源產業(電力、油、瓦斯、水)、運輸產業(空運、鐵道)、健康產業、數位基礎設施。
	歐盟執委會資安韌性法草案 (Cybersecurity Resilience Act)	規範進入歐盟市場的IoT設備，包括軟體及硬體，要求基於安全設計，設備分級並制定資安規範，實施資安定期檢測與標章取得，以落實「資安零信任」原則。

歐洲法規時間表: 獲得CRA認證所需的時間



為了確保在2027年CRA之後能夠及時完成過渡期，必須在2024年開始進行相應的準備。（或者退出歐洲市場）

CRA認證所需檢測及期間



CRA 要求除了產品安全需求外，還需要遵守流程要求。
取得認證需要大約28至34個月的時間。

在 IoT 環境中，機器身分管理的有效實施不僅是生產安全和效率的基石，也是應對日益複雜的安全挑戰的必然要求。

遵從相關標準，善用 PKI 和密碼學技術，並將機器身分管理融入整體身分和訪問管理，將有助於建立更為穩固的 IoT 安全基礎。

謝謝各位參與，期待未來共同迎接物聯網安全的機會與挑戰。

感謝聆聽

如果您需要更多資訊，歡迎隨時與我們聯繫。

CHANGING
全景軟體