QuarkLink for Industrial PCs

Version 1.00

Table of Contents

1 文章範圍 2
2 產業生態鏈的現況 2
3 關鍵安全技術介紹 2
4 QuarkLink 產品介紹 3
4.1 QuarkLink Agent 介紹 5
5 使用案例說明 7
6 總結 8
7 修訂紀錄 9

1 文章範圍

本文主要介紹 Crypto Quantique QuarkLink SaaS 設備安全平台如何用於採用 Linux 的產業電腦的應用領域上。

2 產業生態鏈的現況

在各種應用的情境裡, 方案系統會透過一個完整的產業鏈提供的服務來組成, 當中主要有硬體設計, 軟體開發, 系統整合, 系統運營. 各自分工提供產業需求.硬體設計製造商負責生產硬體與硬體啟動程序, 軟體開發商負責軟體功能設計, 系統整合商則負責整合軟硬功能成為系統, 而系統運營商則負責系統運營與維護. 其中產業電腦則是所有應用的基底, 所有的應用程式或是邊緣應用都須要有硬體的平台來執行.

在既有產業的安全方案考量目前幾乎都以 IT 端為思考方向, 但是近年來為了確保整個系統的安全, 開始導入從 OT 端或是設備端將安全元素設計到產品中, 由於設備安全的實現需要從最低階的硬體端開始進行, 因此這個導入流程是一件非常複雜且繁瑣的事情, 且大部分公司由於產業屬性的因素, 在安全技術與資源的投入相對的薄弱, 因此如何幫助產業從硬體設計開始導入透過信任根, 零信任, 零接觸機制, 一直到安全平台的整合, 使運營服務公司有安全的服務提供給最終用戶, 則是 Crypto Quantique QuarkLink 平台可以幫助客戶快速簡單達成的完整解決方案.

3 關鍵安全技術介紹

目前市面上有許許多多的不斷進化的安全技術, 但是如何有效的設計到產品中, 則是一門專業的知識, 且市面上常見的方案與技術以 IT 方案居多, 實則談到設備安全的則非常罕見, 但是設備又是整個系統的一環, 因此 Crypto Quantique 專注於設備安全的解決方案, 提供給客戶更完整的安全方案並可與其既有的 IT 安全方案進行整合, 提供更全面的保護.
由於要讓設備方案達到安全的過程必須應用到多樣且複雜的安全機制和技術, 還需要配合設備採用的不同的 MCU/CPU/MPU 提供的功能特性,以及考慮到該晶片支援的啟動程式與作業系統的種類.

因此本節主要說明 Crypto Quantique QuarkLink 採用哪些關鍵技術來建立信任鏈以達到產品安全.

- 零信任, 零接觸機制
  - 零信任是一種 IT 的安全概念, 其要求放棄隱性信任的傳統觀念, 所以原則就是從不信任，始終驗證. 而零接觸則是要求避免掉所有人員操作可能發生的風險, 透過將這兩種概念導入到設備安全鏈的建立, 可以讓整個系統的安全從最底層進行保護.
- 安全連線機制
  - 透過 TLS 通訊協議建立安全的連線機制, 達到加密從第三方傳輸的資料, 進行身份驗證, 確保交換資訊的各方是他們聲稱的身份, 以及資料未被偽造或竄改, 以此確保裝置與 QuarkLink 之間的通訊是安全的
- 信任根的建立 (TPM, HSM)
  - 透過裝置的 TPM 與 QuarkLink 的 HSM 各自生成信任根, 並透過相互的認證流程, 確保整體安全系統的源頭是可被信賴.
- 設備認證, 證明, 憑證發放

- 透過 Crypto Quantique 提供給裝置的 agnet SDK 以及與 QuarkLink 通訊所需的基本訊息, 當裝置初始啟動後會開始與 QuarkLink 通訊, 並完成一段交握程序以取得相關身分與憑證. 並以此為基礎進行後續所有的設備管理功能.

- 啟用/運行晶片安全啟動, 針對客戶映像檔(作業系統, 應用程式)進行簽名與更新
  - 啟動晶片本身提供的安全啟動功能用於驗證在啟動過程時, 過程中加載的程式檔是否經過授權, 防止未經授權的程式運行, 從而增強了系統的安全性, 這當中的程式包含了 bootloader, OS 以及應用程式, 由此進行整個系統的第一環保護.

4 QuarkLink 產品介紹

當系統整合商或是軟體開發商採用了工業電腦產品並與雲端或是遠端服務整合提供方案給客戶使用時, 為了確保服務品質與系統安全性, 除了應用服務的創新外, 還會針對相關的通訊方式與設備進行身分識別化的產生以及憑證的認證, 以確保設備或是服務都是在安全的環境下運作.

這樣的系統如果要自行開發則會牽扯到上述的各項技術的軟體功能開發以及管理架構設計與整合的難度, 除了這些功能性開發因素以外, 其實還有另外一個安全問題, 也是很大的原因就是來自於人為的程序介入, 因此如何做到一個zero touch/trust的機制也是一個耗時耗力的工作.

目前業界最常採用的作業系統不外乎是 Windows, Linux, RTOS來進行資源的管理與應用程式的開發. 但是目前也只有Windows提供了設備安全的認證與保護, 因此如果採用非Windows的作業系統進行開發的業者除了應用程式的開發外就需要自行另外設計與設備安全相關的功能.

常見的就是採用openssl套件產生金鑰並送到第三方憑證認證單位取得相關憑證,透過憑證管理相關設備.

如此做法有許多的問題需要深入考量, 例如如何確保金鑰的產生/安全保存/管理, 如何與第三方單位整合, 如何在過程中避免人為的洩漏, 如何設計一個管理系統管理所有的憑證鍊...等等. 這都是一個需要投入大量人力資源與技術的工程.

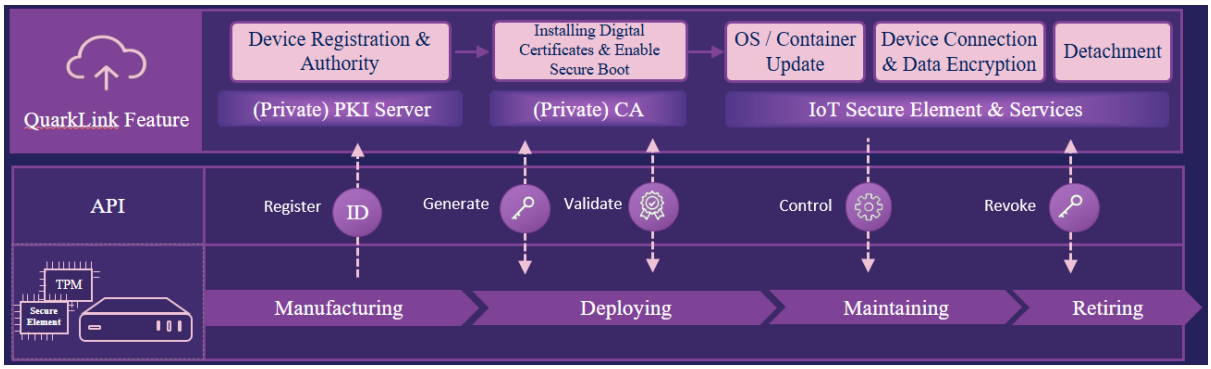
除此之外, 硬體設備本身提供的安全啟動程序如何整合到安全架構中, 如何讓每個佈建到各設備執行的作業系統或是應用程式都是安全的, 而沒有被有心人重新編譯和竄改，並另外產出含有惡意病毒的程式檔，誘騙使用者下載安裝以進行不法行為. 因此在軟體程式碼開發完成後，如何幫軟體程式加上公司專屬的數位簽章，宣告此程式是正版的、沒有被竄改過的, 這些都是需要開發設計.

然而並非所有公司都有資源進行這類工程, 因此Crypto Quantique提供了一套完整的解決方案協助客戶完成以上工作, 讓客戶可以專心於公司產品上面, 加速進入市場的時間與資源的有效利用.

QuarkLink 是 Crypto Quantique 通用物聯網安全平臺，它使用先進的加密技術與硬體信任根集成，以提供配置、管理和監控，以實現輕鬆的可擴展性和可靠的安全性。
它提供了以下的基本功能

- 安全連接：QuarkLink 是一種基於軟體服務的 IoT 安全平台，可以安全地將 IoT 設備轉連接到應用服務的伺服器或是雲端.
- 先進的密碼技術：QuarkLink 使用先進的密碼技術，可以與任何根信任 (root-of-trust) 進行整合，實現 IoT 設備的端到端安全
- 設備生命週期管理：QuarkLink 可以輕鬆管理所有設備的憑證的生命週期

- 軟體更新：QuarkLink 可以將各種映像注入 IoT 設備，並進行加密和簽名，從而支持實現安全配置、身份驗證以及監控、更新等管理活動
- 設備註冊：一旦設備被配置和識別，QuarkLink 就會對它們進行驗證，並提供證書和憑證以實現安全的註冊
- 金鑰, 憑證管理：QuarkLink 提供了證書管理功能，使客戶可以全面控制安全資產
- 硬體設備支援：QuarkLink 支援多種不同的硬體設備與模組,包含MPU或MCU類型



接下來說明QuarkLink 如何透過安全的機制與流程確保從系統的硬體身分的建立, 安全啟動功能開啟以及各層軟體安全保護, 延伸至整體的安全鏈的建立與管理.

QuarkLink的實現原理乃透過設備在生產階段執行provision程序將設備先註冊於QuarkLink, 且 QuarkLink 會產生憑證給設備, 以此為雙方未來溝通的依據, 這個過程都是在TLS協議的保護下進行, 確保過程是安全的, 當設備通過這個程序後, 便可開始使用QuarkLink提供的所有功能.

除了 QuarkLink 這個平台功能外, 設備端會有一個agent的腳色存在, 這個agent的腳色主要就是與 QuarkLink進行通訊, 其會運行在兩個階段, 一個是在設備生產階段, 用以生成裝置身分與 QuarkLink溝通取得憑證, 另一階段則為應用程式內需要包含, 用以定時與 QuarkLink 溝通確認是否有新版軟體需要更新或是憑證是否需要更新來管理設備的安全與應用.

由於產業需求與使用情境不同, QuarkLink 針對產業的需求分成兩個類型, 第一類是針對硬體設備設計製造商, 第二類則是針對軟體開發與系統整合商, 主要是因為這兩類廠商的產品與安全考量完全不同, 因此 QuarkLink 才會特別針對這兩類廠商進行差異化的定義.

針對硬體設備設計製造商, QuarkLink 提供了零接觸/零信任的裝置身分生成流程並整合了信任根的技術以取代現有的可預測且風險極高的序列號與 MAC address 的方式來識別設備與管理後續維護流程. 除此之外更可以防止產品遭到仿冒以及做到客戶使用設備的真實性驗證. 另外經過這個流程的設備也可以符合各式針對設備安全定義的安全法規, 例如 CRA, ISO62443 等.

而對於軟體開發與系統整合商, QuarkLink 確保使用者使用了唯一身分的安全設備之外, 也可透過 QuarkLink 提供的 UI 或是 API 來與使用者既有的方案或是應用平台進行整合. 而 QuarkLink 針對這類客戶提供了以下的功能: 設備硬體安全啟動功能的制能, 設備註冊與管理, 設備憑證或生命週期管理, 客戶專案管理, 軟體(包含作業系統以及應用程式)映像檔管理, 軟體簽名, 以及軟體安全 OTA. 客戶可以依需求整合各項功能到既有的後台系統, 如此大大縮短開發時間並且可以直接使用安全的設備進行產品開發與研究.

4.1 QuarkLink Agent 介紹

QuarkLink agent 的主要工作就是讓硬體設備上的軟體可以與 QuarkLink 進行溝通, 所以 QuarkLink agent 有幾個重要的工作要進行.

1. 啟動硬體裝置的網路功能
2. 擁有 QuarkLink 的 URL 與 root 憑證
3. 產生硬體裝置的身分, 金鑰並安全地儲存它們
4. 使用硬體設備的身分註冊到 QuarkLink
5. 檢查 QuarkLink 上是否有韌體需要更新
6. 執行軟體更新過程

因此硬體設備設計製造商或軟體開發與系統整合商會在設備設計生產或是產品應用程式開發中使用到 QuarkLink agent 的功能. Crypto Quantique 會提供完整的 image 或是以程式庫的方式讓使用者進行整合與使用.

以下我們針對不同的應用情境說明 agent 的工作程序.

硬體設備設計製造商: 協助客戶建立設備身分與保存於安全儲存器, 客戶可以於生產線上進行該程序, 並與硬體功能測試的流程整合.
以下以 Adlink I-Pi SMARC I.MX8M Plus 為例:

- 設備準備:

Adlink I-Pi SMARC I.MX8M Plus with TPM
SD card *1
PC with monitor
USB2UART cable

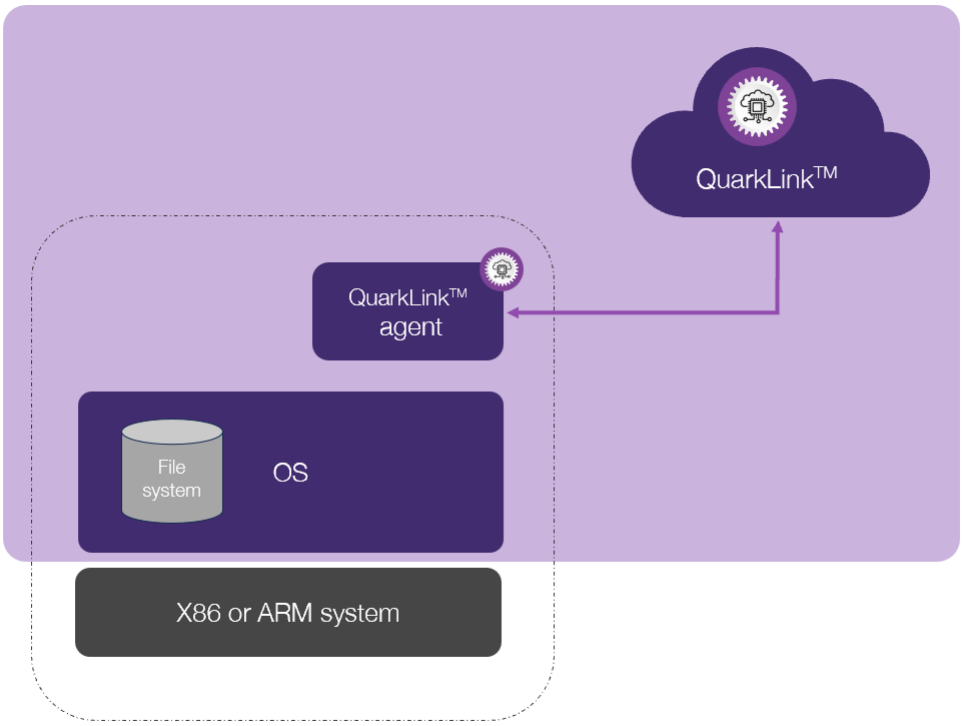
- 軟體準備:

QuarkLink server
QuarkLink agent for manufacturing
Terminal tool
燒錄工具 (dd command, uuu tool, disk writer tool)

- 執行步驟:

1. 使用 USB2UART 連接 PC 與 I-Pi SMARC I.MX8M Plus
2. 使用燒錄工具安裝 QuarkLink agent for manufacturing 到 SD card
3. PC 開啟 terminal tool,設定 baud rate.
4. PC 開啟 Browser, 連上 QuarkLink server
5. 設定 I-Pi SMARC I.MX8M Plus 為 SD card boot, 插入 SD card, 然後 power on.
6. QuarkLink agent for manufacturing 會自動完成所有工作, 並可以在工作最後觀察 terminal tool 產生了 device ID
7. 確認 QuarkLink server 也同樣顯示了 device ID

軟體方塊圖: (QuarkLink server and QuarkLink agent for manufacturing)



軟體開發與系統整合商: 協助客戶建立設備憑證, 啟動晶片安全性功能(如 secure boot), 確認設備是否為正品, 設備是否被操縱, 並實現完整的設備安全生命週期管理以及協助客戶 Image 簽名以達到 CRA 或其他行業安全法規，例如 ISO62443.
以下以 Adlink I-Pi SMARC I.MX8M Plus 為例:

設備準備:
Adlink I-Pi SMARC I.MX8M Plus with TPM
SD card *1
PC with monitor

- 軟體準備:

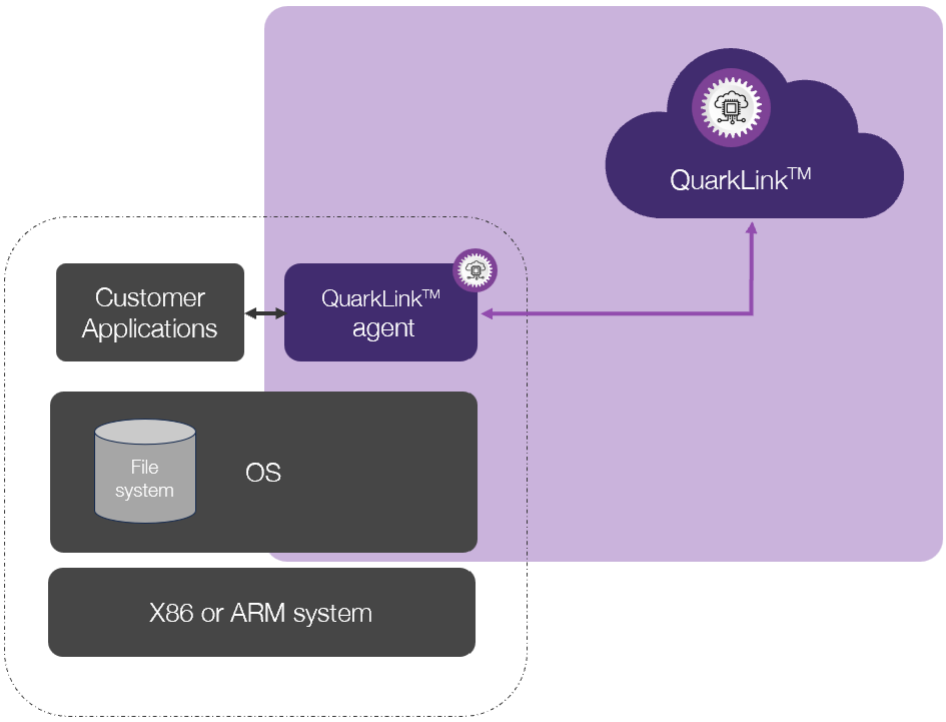
QuarkLink instants
QuarkLink agent for QL instants
Customer image
燒錄工具 (dd command, uuu tool, disk writer tool)

- 執行步驟:

1. 使用燒錄工具安裝 QuarkLink agent for QuarkLink instants 到 SD card
2. PC 開啟 Browser, 連上 QuarkLink instants
3. 上傳 customer image 到 QuarkLink
4. 設定 I-Pi SMARC I.MX8M Plus 為 SD card boot, 插入 SD card, power on.
5. QuarkLink agent for QuarkLink instants 會自動完成所有工作, 並下載 signed customer image 到板端

6. 設定 I-Pi SMARC IMX8M Plus 為 eMMC boot, 即可看到 customer image boot up.
7. 使用者的應用程式開始透過 QuarkLink agent 的功能與 QuarkLink 溝通

軟體方塊圖: (QuarkLink instants and QuarkLink agent for QuarkLink instants)



5 使用案例說明

AI 是目前市場上的顯學, 有林林總總的產品與 AI 相關, AI 伺服器, AI 攝影機, AI 個人助理, AI 醫療診斷, AI 影像識別, 智慧交通, 智慧能源, 智慧工廠…等等. 這些應用都需要有設備在邊緣端執行並且需要常態的更新設備內的軟體功能與模型演算法, 且為了能持續的更新演算法也需要從終端收集與取得更多的現場資料, 而如何確保整個雙向設備通訊與應用是安全的, 單靠目前的 IT 資安解決方案是明顯不足, 因此 Crypto Quantique QuarkLink 所提的設備安全解決方案恰可補足這個漏洞, 讓整個應用的場景與情境是在安全的環境下運行並可以符合各項新的法規規定.
例如 AI Camera 實現了邊緣數據收集並使用本地推論且快速回應緊急情況, 其特點包括：

- 即時警報和通知
- 物體檢測和識別
- 行為分析以識別可疑活動
- 本地資料處理減少了對持續資料傳輸的需求
- 智慧運動偵測
- 音訊分析
- 隱私屏蔽
- 資料加密和安全防止未經授權的訪問

但是在達到這些功能時可能會有那些安全技術要求：

- 傳輸中和靜態資料加密
- 強大的身份驗證和基於角色的存取控制
- 軟體更新以修補已知漏洞
- 安全性更新機制（安全啟動）
- 資料完整性和審計追蹤
- 隱私屏蔽
- 人工智慧驅動的異常檢測和響應
- 供應鏈安全

這些設備基本因為功能多樣因此皆會採用作業系統來管理相關資源, 因此 QuarkLink 提供安全的信任根配置（通常是可信任平台模組 - TPM）透過上述各項特點與好處來協助客戶產品達到安全保障.

因此, 透過 QuarkLink 讓客戶的產品可以達到:

- 零接觸
- 獨特的加密身分和金鑰產生
- 容易擴展與整合
- 自動產生的憑證授權單位
- 易於部署到製造流程中
- 成本效率高
- 容易使用的證書管理
- 一致性操作程序

6 總結

QuarkLink 提供了一個安全的機制從設備生產開始導入安全元素, 並可協助客戶輕鬆啟動硬體安全機制, 透過一個簡易的 UI 或是 API 易於整合入各種客戶端既有的環境與系統. 全程零接觸安全性高, 大大降低客戶導入安全機制的難度,資源與時間. 讓客戶的產品可以更快的上市並且符合各式的安全法規.

7 修訂紀錄

Crypto Quantique QuarkLink for Industrial PCS

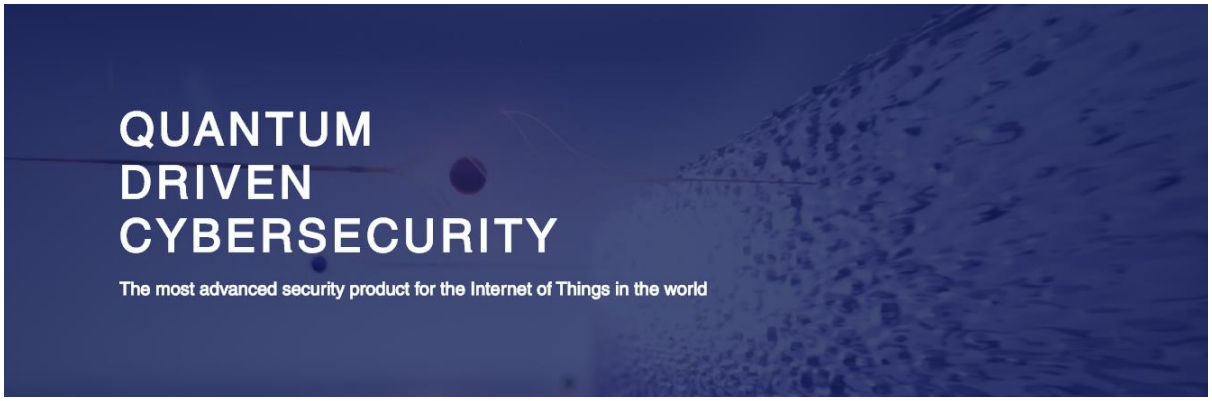
Rev.	Date	Owner	Description
1.0	24.09.2024	DC	Final

CRYPTO QUANTIQUE

United Kingdom

Unit 304-5,
164-180 Union Street,
London
SE1 0LH

General contact email:
info@cryptoquantique.com


QUANTUM
DRIVEN
CYBERSECURITY
The most advanced security product for the Internet of Things in the world