CRYPTO QUANTIQUE

QuarkLink for Industrial PCs

Version 1.0

Table of Contents

1 Scope

This article introduces how Crypto Quantique's QuarkLink SaaS device security platform is used with industrial PCs running Linux.

2 Definition of an Industrial Ecosystem

An industrial IoT ecosystem includes hardware design, software development, system integration, and system operation. Each division of labor provides industry needs. The device manufacturer is responsible for producing hardware and hardware startup programs, the software developer for software functionality, the system integrator for integrating software and hardware into a system, and the system operator for ongoing operation and maintenance.

Applications run on industrial computers and security considerations are usually focused based on these IT systems. However, in recent years, there has been increasing demand for security to be designed into devices categorized as operational technology (OT). Since the implementation of device security needs to start with the lowest-level hardware, the process is complex and due to the conservative nature of industry, investment in security technology and resources is relatively poor.

Crypto Quantique's aim is to help industrial companies understand and implement the concepts of security-by-design for IoT devices and networks. This includes the adoption of root-of-trust technologies and zero-trust methodologies, starting from the initial hardware design. Only through this approach, which extends to the integration of the security platform, can companies to provide secure services to end users.

Crypto Quantique's QuarkLink platform is a Sofware-as-a-Service (SaaS) product that supports embedded system developers, system integrators, and end customers in achieving the highest level of security across all aspects of IoT implementation, and throughout each system's operating life.

3 Security Functions

There are many evolving security technologies on the market, but how to effectively design them into products is technically challenging. The most common technologies are IT-focused. Device level security that integrates with existing IT-level technologies is required to provide comprehensive protection across OT and IT infrastructure.

Since the process of making solutions secure requires the application of diverse and complex security mechanisms and technologies. it is also necessary to match the functional features provided by the different MCUs/CPUs/MPUs used in the devices, as well as to consider the booting programs and the OS supported by the chip. Therefore, this section explains what key technologies QuarkLink uses to establish a chain of trust to achieve product security:

- Zero-trust, zero-touch mechanism

  Zero-trust is an IT security concept that abandons the traditional concept of implicit trust. The principle is to never trust and always verify. Zero-touchrequires avoiding the risks that may occur in all human operations. The two concepts are introduced into the establishment of the device security chain, which can protect the security of the entire system from the lowest level upwards.

- Secure connection mechanism

  Establish a secure connection mechanism through the TLS communication protocol to encrypt data transmitted from a third party and perform identity verification to ensure that the parties exchanging information are who they claim to be. The mechanism must also ensure that data has not been forged or tampered with, thereby ensuring that the device and its communication are secure.

- Establishment of a root-of-trust (TPM, HSM)

  The device's trusted platform module (TPM) and QuarkLink's hardware security module (HSM) each generate a root-of-trust, and through mutual authentication processes ensure that the overall security system is trustworthy.

- Equipment attestation, verification, and certification issuance

  Through the agent provided by Crypto Quantique to the device and the basic information required to communicate with QuarkLink, when the device is initially started, it communicates with QuarkLink and completes a handshake to obtain relevant identities and credentials. Based on this, all subsequent processes and device management functions are executed.

- Enable/run chip secure boot, sign and update customer images (operating systems, applications)

  The secure boot function provided by the chip itself is used to verify whether the program files loaded during the entire process are authorized and prevent unauthorized programs from running, thereby enhancing system security. These program files include boot programs, operating systems, and applications.

4 QuarkLink Overview

When system integrators or software developers adopt industrial computer products and integrate them with cloud or remote services to provide solutions for customers, they must ensure service quality and system security. They must also facilitate innovation in application services while ensuring devices can generate unique identities and authenticate credentials. This ensures that devices and services operate and communicate in a secure environment.

If such a system is developed in-house, the software development, architecture design and integration of the various functions is highly complex. Another key security challenge is how to implement a zero touch/trust mechanism that aims to eliminate security breaches due to human error. This is another time-consuming and labor-intensive task.

Currently, the common operating systems in the industry are Windows, Linux, and RTOS for hardware resource management and application development. However, currently only Windows provides device security certification and protection. Therefore, if a non-Windows operating system is used, in addition to the development of applications, developers need to add the necessary functions for device security. It is common to use an open-source package/ library to generate a key and send it to a third-party certificate authentication unit to obtain relevant certificates and manage related equipment through the certificates.

There are many issues that require in-depth consideration in this approach, such as how to ensure the generation/safety storage/management of keys, how to integrate with third-party solutions, how to avoid human leakage in the process, how to design a management system to manage all security chains, etc. This is a project that requires a lot of human resources and technology.

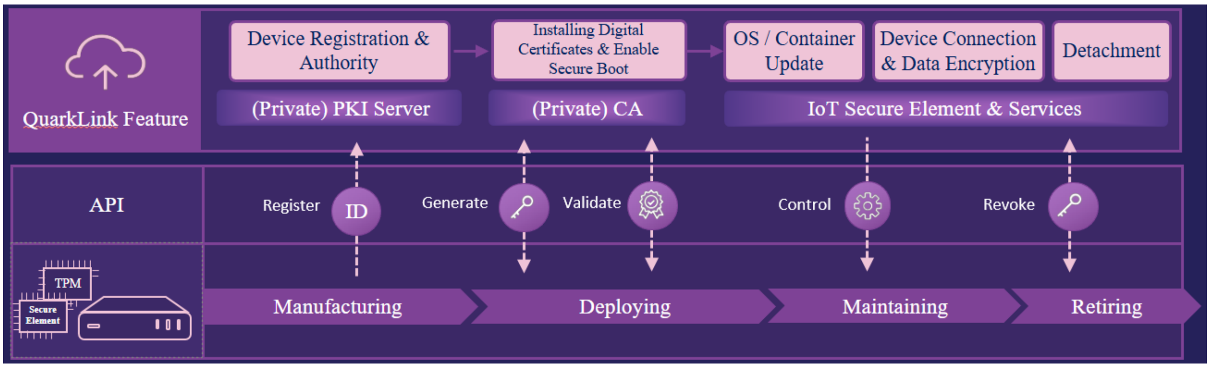
The developer must also integrate the secure boot program provided by the hardware device into the security architecture. This is to ensure that every operating system or application deployed to each device is safe and has not been recompiled and tampered with. Such tampering may include generating additional program files containing malicious viruses, tricking users into downloading and installing them to enable bad actors to commit illegal activities. Therefore, after the software code is built, developers need to add a company-specific digital signature to the program to declare that it is genuine and tamper-free. This adds further design and development work.

QuarkLink helps customers with all the above tasks, and allows them to focus on differentiating their products, accelerating time-to-market market, and making the most effective use of resources.

QuarkLink is a universal IoT security platform that uses advanced cryptography integrated with a hardware root-of-trust to provide provisioning, management, and monitoring with easy scalability and robust security.

It offers the following basic functions

- Secure connection: QuarkLink is an IoT security platform based (software-as-a-service) that securely connects IoT devices to application servers or the cloud.
- Advanced cryptography: QuarkLink uses advanced cryptography and can be integrated with any root-of-trust to achieve end-to-end security for IoT devices.
- Device lifecycle management: QuarkLink makes it easy to manage the lifecycle of credentials for all devices.
- Software updates: QuarkLink can inject various images into IoT devices and encrypt and sign them to support management activities such as secure configuration, authentication, monitoring, and updates.
- Device Enrollment: Once devices are provisioned and identified, QuarkLink authenticates them and provides certificates and credentials for secure enrollment.
- Key and certificate management: QuarkLink provides certificate management functions, allowing customers complete control of security assets.
- Hardware device support: QuarkLink supports a variety of different hardware devices and modules, including MPU, MCUs, and Linux distributions.



QuarkLink uses security mechanisms and processes to ensure the establishment and management of system hardware identities and the activation of secure boot functions, as well as various layers of software security protection. Its functions extend to the establishment and management of the entire security chain.

The implementation of QuarkLink is carried out as follows. During the device production stage, the device generates an identity and registers with QuarkLink through the provisioning process. QuarkLink generates a certificate for the device as the basis for future communication between the two parties. This process is carried out securely using the TLS protocol. Once the device is verified, the other QuarkLink features can be used.

In addition to the platform function of QuarkLink, there is an agent role on the device side. This comprises two stages. One is in the equipment production stage, which is used to generate device identities and communicate with QuarkLink to obtain credentials; the other is to obtain credentials for connecting to servers or hubs. The application then regularly communicates with QuarkLink to see if there is a new version of the software that needs to be updated or if the certificate needs to be updated to manage secure updates of the application running on the device.

QuarkLink serves the needs of hardware device designers/manufacturers, as well as software developers and system integrators.

For hardware device designers and manufacturers, QuarkLink provides a zero-touch, zero-trust device identity generation process. It also integrates root-of-trust technology to replace existing predictable and high-risk serial number and MAC address methods for identifying devices.

QuarkLink subsequently manages the device maintenance process. In addition, it can prevent product counterfeiting and verify the authenticity of the equipment used by customers. Through these functions, QuarkLink helps ensure compliance with various safety regulations defined for equipment security, such as CRA, ISO62443, etc.

For software developers and system integrators, QuarkLink provides devices with unique identities and provides the following functions for these customers: device hardware secure boot function enablement, device registration and management, device certificate and life cycle management, customer project management, software image (including operating system and application/container) management, software signing function, software OTA function. Customers can integrate various functions into the existing back-end system according to their needs, which greatly shortens development time and can directly use secure device for function development and research.

4.1 QuarkLink Agent

The main job of the QuarkLink agent is to enable hardware devices to communicate with the QuarkLink platform. Its functions are to:

1. Activate the network function of the hardware device.
2. Have the URL and root credentials of QuarkLink.
3. Generate hardware device identities and keys and store them securely.
4. Register to QuarkLink using the ID of the hardware device.
5. Check software updates form QuarkLink.
6. Execute the software update process.

Hardware device designers/manufacturers and software developers and system integrators can use the QuarkLink agent in device design and production and product application development. Crypto Quantique provides a complete image or a program library for customers to integrate and use.

This assists customers in creating device identities and records for storage. Customers can perform this process on the production line and integrate it with hardware functional testing.

The following takes Adlink I-Pi SMARC IMX8M Plus as an example:

- Equipment preparation:

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

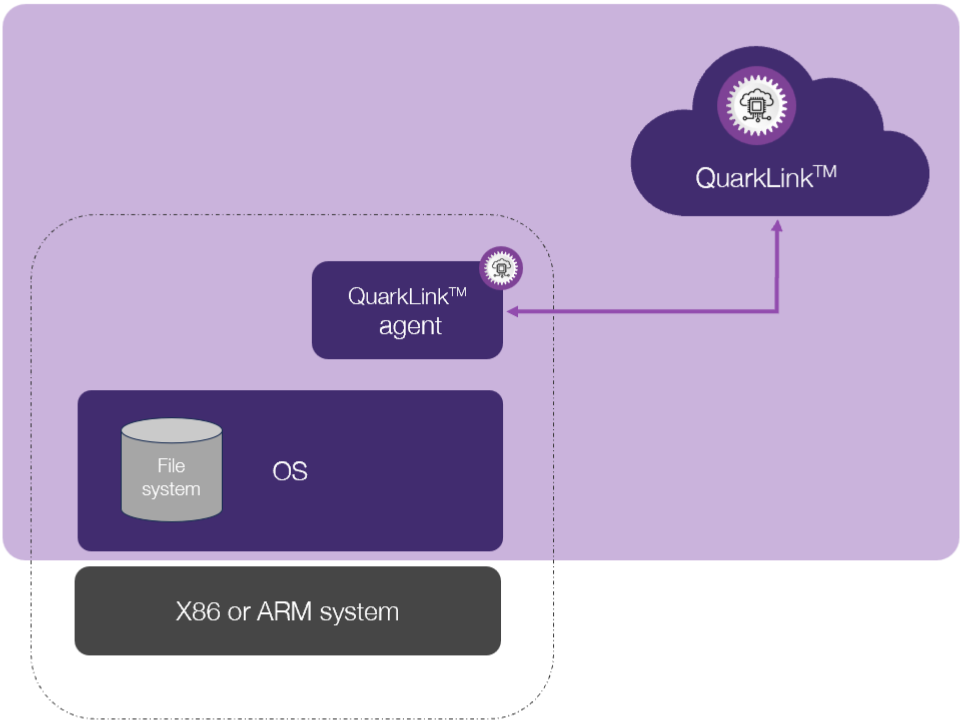
- Software preparation:

QuarkLink server
QuarkLink agent for manufacturing
Terminal tool
Burning tools (dd command, uuu tool, disk writer tool)

- Steps:

1. Use USB2UART cable to connect PC and I-Pi SMARC I.MX8M Plus
2. Use the burning tool to install QuarkLink agent for manufacturing to SD card
3. Open the terminal tool on the PC and set the baud rate.
4. Open Browser on PC and connect to QuarkLink server
5. Set I-Pi SMARC I.MX8M Plus to SD card boot, insert SD card, power on.
6. QuarkLink agent for manufacturing will automatically complete all the work, and you can observe the device ID generated by the terminal tool at the end of the work.
7. Confirm that the QuarkLink server also displays the device ID

Block Diagram of software: (QuarkLink server and QuarkLink agent for manufacturing).



The QuarkLink platform enables software developers and system integrators to assist customers in establishing device credentials and activating chip security functions (such as secure boot), confirm whether the equipment is genuine and whether it has been manipulated, and implement complete equipment safety life cycle management. They can also assist customers with image signatures to meet CRA or other industry regulations, such as ISO62443.

The following takes Adlink I-Pi SMARC I.MX8M Plus as an example:

- Equipment preparation:

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

- Software preparation:

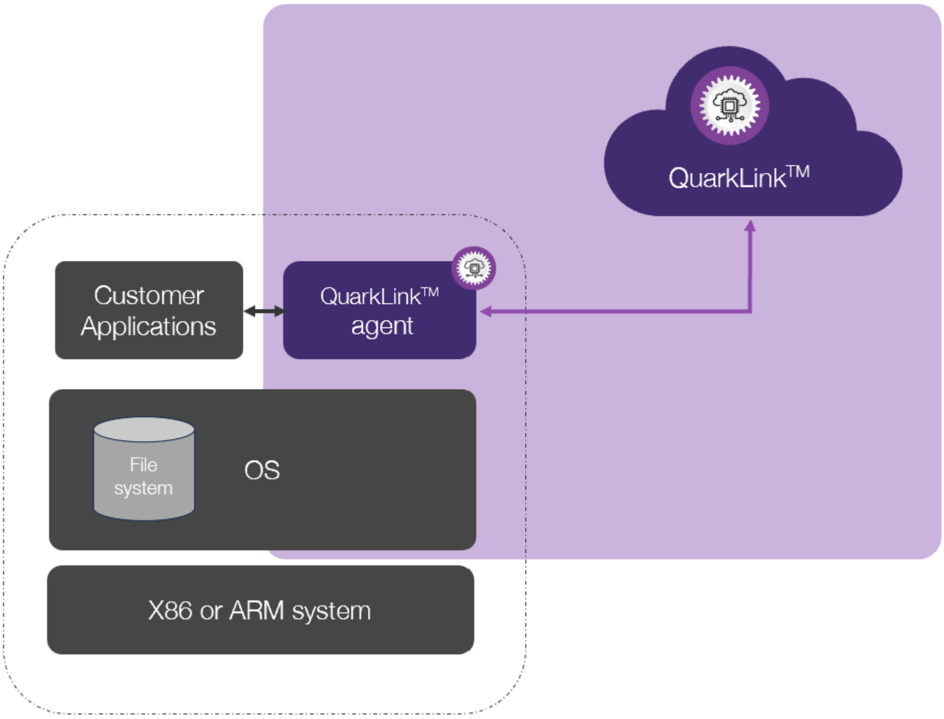
QuarkLink instance
QuarkLink agent for QuarkLink instance
Customer image
Burning tools (dd command, uuu tool, disk writer tool)

- Steps:

1. Use the burning tool to install QuarkLink agent for QuarkLink instance to SD card.

2. Open Browser on PC and connect to QuarkLink instance.
3. Upload customer image to QuarkLink.
4. Set I-Pi SMARC I.MX8M Plus to SD card boot, insert SD card, power on.
5. QuarkLink agent for QuarkLink instance will automatically complete all the work and download the signed customer image.
6. Set I-Pi SMARC I.MX8M Plus as eMMC boot, and you can see the customer image boot up.
7. Customer application can communicate with QuarkLink by QuarkLink agent.

Block Diagram of software: (QuarkLink instance and QuarkLink agent for QuarkLink instance).



5 Use Case

With the growth of AI, there is a need for equipment to execute algorithms at the edge. The software functions and model algorithms in equipment need to be constantly updated. To continuously update the algorithm, it is also necessary to collect and obtain more on-site data from terminal.

Current IT security technologies alone are insufficient. QuarkLink compensates for these security inadequacies and creates a secure end-to-end OT/IT environment. It operates under a wide variety of conditions and assists with achieving regulatory compliance.

For example, an AI Camera realizes edge data collection and uses local analysis data to quickly respond to emergencies. Its features include:

- Instant alerts and notifications.
- Object detection and recognition.

- Behavioral analysis to identify suspicious activity.
- Local data processing reduces the need for continuous data transfer.
- Smart motion detection.
- Audio analysis.
- Privacy mask.
- Data encryption and security prevent unauthorized access.

The security technical requirements for achieving these functions include:

- Encryption of data in transit and at rest.
- Strong authentication and role-based access control.
- Software updates to patch known vulnerabilities.
- Security update mechanism (secure boot).
- Data integrity and audit trails.
- Privacy mask.
- Artificial Intelligence-driven anomaly detection and response.
- Supply chain security.

These devices use operating systems to manage related resources because of their diverse functions. QuarkLink provides a secure root-of-trust configuration (usually a Trusted Platform Module - TPM) to help customer products achieve security through the above functionality.

Therefore, through QuarkLink, customers' products can achieve:

- Zero contact.
- Unique cryptographic identity and key generation.
- Easy system expansion and integration.
- Automatically generated certificate authorization.
- Easy deployment into manufacturing processes.
- Cost efficiency.
- Easy-to-use certificate management.
- Consistency in operating procedures.

6 Summary

QuarkLink is a security platform for introducing security from the beginning of device production. It can help customers easily activate hardware security mechanisms and easily integrate them into various client existing environments and systems through a simple UI or API. The entire process offers zero-contact security, while greatly reducing the difficulty, resources, and time needed for customers to introduce security mechanisms. This allows customers' products to be launched faster and to comply with various safety regulations.

7 Revision History

CQ QuarkLink for Industrial PCs

Rev.	Date	Owner	Description
1.0	24.09.2024	DC	Final

Legal Notice Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. CRYPTO QUANTIQUE MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Crypto Quantique disclaims all liability arising from this information and its use. Use of Crypto Quantique devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Crypto Quantique from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Crypto Quantique intellectual property rights unless otherwise stated.

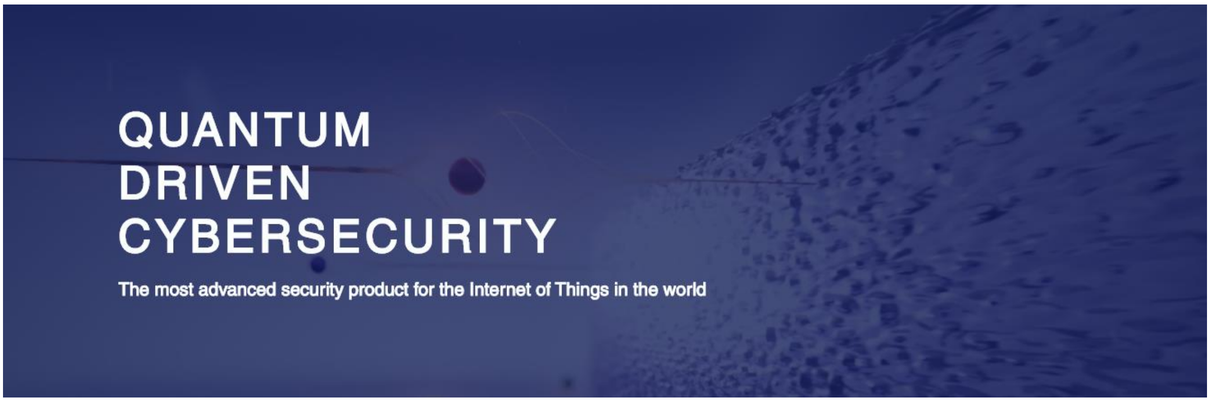
CRYPTO
QUANTIQUE

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