RA Ecosystem Partner Solution
# CRYPTO QUANTIQUE® QuarkLink

Solution Summary

Crypto Quantique's® QuarkLink is an IoT security and device management platform that enables easy and scalable end-to-end security for IoT, automating secure firmware provisioning, device onboarding and enrolment, and certificate management, proving zero-touch security from hardware to application whilst giving customers full control of security assets. Out-of-box support is now available for the RA family of MCUs.

Features/Benefits

- Zero-touch device attestation, onboarding and enrolment, based on hardware root of trust

- Enables production programming in a non-secure environment with firmware encryption, **no HSMs or key injection required in manufacturing**

- Certificate management and revocation with automatic renewals, **no external CA required**

- Platform agnostic and flexible deployment, can be hosted on-prem or in the cloud, providing full control of keys and firmware and a fully functional private PKI

- Data encrypted from device to application – not visible to any intermediate cloud
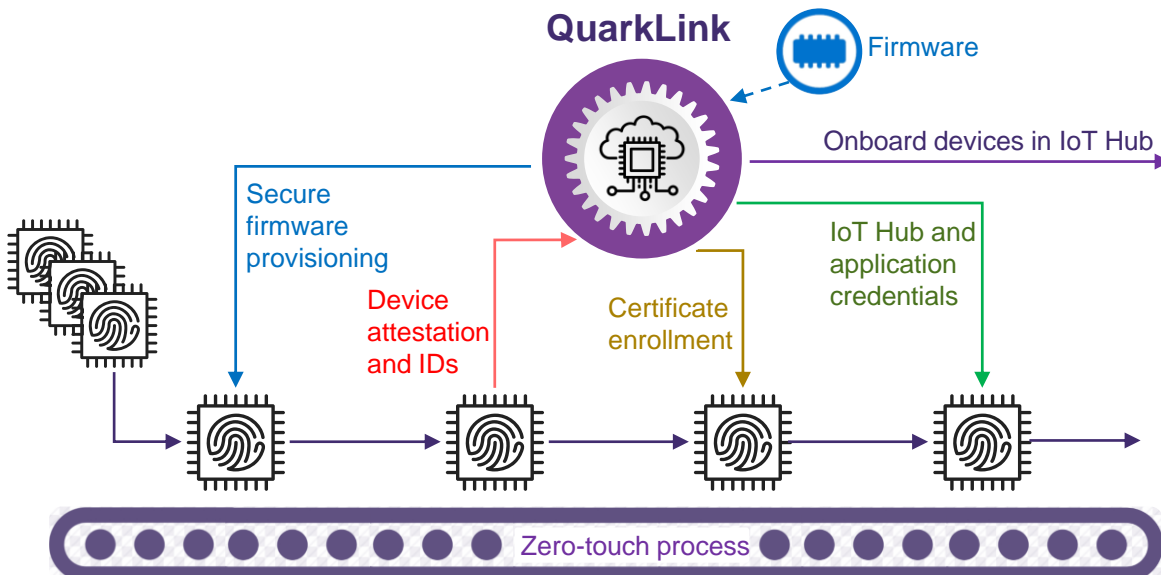
Target Markets and Applications

- Automotive
- Industrial IoT
- Smart Cities

- Smart Homes
- Smart Sensors
- Consumer Electronics

www.cryptoquantique.com

2021.02

Quantum Driven Cybersecurity

Foundational end-to-end cyber security based on unforgeable 'Quantum Safe' hardware root of trust

Q:Architecture: seamless end-to-end IoT security

QDID: the world's first unforgeable Root of Trust

Inherently secure against side-channel attacks

Unforgeable device Identity prevents counterfeiting

Multiple uncorrelated keys with no key injection

QuarkLink: Universal Security Platform

End-to-end security architecture

PKI management, certificate renewal and revocation

Supports QDID and existing third-party Roots of Trust

Crypto Quantique's® Q:Architecture uses hardware and software to combine cutting-edge technologies on quantum-physics and cryptography, delivering strong and easy-to-use IoT security. Q:Architecture redefines the concept of security for the IoT by creating a seamless bridge between the silicon, device, and cloud platform worlds.

Crypto Quantique's® ground-breaking technology radically simplifies the process of generating an immutable hardware root of trust in an IoT edge node, solves the issue of secure provisioning and onboarding an IoT edge node in an untrusted environment, and plugs the gaping device security hole that currently exists in the IoT ecosystem.

The core product is a Hardware Security as a Service (HwSaaS) for managing IoT security, taking advantage of the unique feature afforded by the Quantum Driven Identity (QDID), which generates multiple uncorrelated secret keys internally to the semiconductor device. This unique feature means that there is **no need for a HSM to secretly inject the keys** during manufacture/provisioning of the end product.

At the same time, we recognise the need to hugely improve the security available with existing MCUs/CPUs and roots of trust. Therefore, **QuarkLink can support existing PUFs and other Roots of Trust**, in addition to the QDID, for true end-to-end security, and to provide secure firmware provisioning, authenticated onboarding, and easy key and certificate life-cycle management.

WHY DO WE EXIST?
We envision securing the connected world with zero-trust where the user is in control of their security and privacy of their devices and can create/maintain their own security credentials per device automatically.
Our mission is to provide seamless, end-to-end, zero-trust security for onboarding and managing the IoT,
Our systems are designed to secure devices from birth to death,
We support customers from design to manufacture to deployment and operations.

HARDWARE SECURITY AS A SERVICE
Our radical quantum tunnelling based Silicon IP enables connected devices to originate multiple tamper-proof, unforgeable cryptographic keys on demand, that can never be compromised for the life of the device.
Combined with our advanced cryptographic key provisioning and lifecycle management platform we offer economic cybersecurity from Cloud to Chip.
Our solution reduces the cost of implementing a hardware root of trust.
Our core technology is quantum safe by design.
We are pioneers in cryptography, electrical engineering and quantum physics.