**Crypto Quantique** (based in London) has developed **Q:Architecture** - a scalable architecture for quickly and securely connecting IoT devices to the cloud.

**Q:Architecture** has two complementary elements:

**1. QDID** is hardware IP that generates random, unique, unforgeable identities and cryptographic keys on-demand in silicon.

a. It does this by measuring quantum effects in chips produced using standard CMOS processes. (Other technologies may do this in compound semiconductors.)

b. Keys do not need to be stored and can be reconstructed on-demand.

c. It eliminates the need for key injection and its associated cost, complexity, and security compromise. (Key injection is the alternative process for creating a Root-of-Trust in IoT devices).

**2. QuarkLink** is a universal IoT security platform for connecting devices to in-house or cloud servers. Originally designed to work with QDID, it is also available as a standalone product to be used with other Roots-of-Trust. Its unique feature is its breadth of capability in one tool. It provides:

a. Secure provisioning, including cryptographic keys and firmware.

b. Automated secure onboarding to any platform and simultaneously to multiple platforms. AWS, Microsoft and Mosquito are supported now, with more to follow.

c. Security monitoring, including firmware encryption, signing and secure updates over-the-air, and certificate and key renewal and revocation.

QuarkLink can be set up in minutes by engineers without specialist IoT security knowledge. Thousands of end-point devices may then be connected to servers through cryptographic APIs, with just a few keystrokes that initiate an almost instantaneous, automated process.