ARISTA | IDQ

Driven by PSNC

Quantum-Safe Security

Preparing for tomorrow's quantum era

- **No need to change your whole infrastructure**
- **Just add the Quantum Layer**

Today, we are on the edge of a quantum revolution. The advent of quantum computers in the next decade will give mankind access to unparalleled processing power with all the advantages that this brings, however this also creates challenges as they will render much of today's cybersecurity useless.

What impact will quantum computers have on today's cryptography?

The security of public key cryptography is based on mathematical complexity. RSA algorithms, Diffie Hellman Key exchange protocols and Elliptic curve cryptography all include an element of calculation that is near impossible for conventional computers to crack. Quantum computers will change this dynamic, as they can solve these complex problems incredibly quickly, **rendering today's cryptographic defenses ineffective.**

What can be done today to secure tomorrow's infrastructure?

Coming to grips with the quantum threat is not a matter of if, but when. Security conscious organizations are not waiting until the threat becomes a reality before doing something about it. For many, this process begins with an internal audit of the current cybersecurity stance and the development of a roadmap towards quantum resilience. **Introducing crypto-agility today can help streamline the onboarding of advanced quantum-safe technologies as they become available.**

Quantum computers have been described as the greatest ever threat to the future security of public key infrastructure.

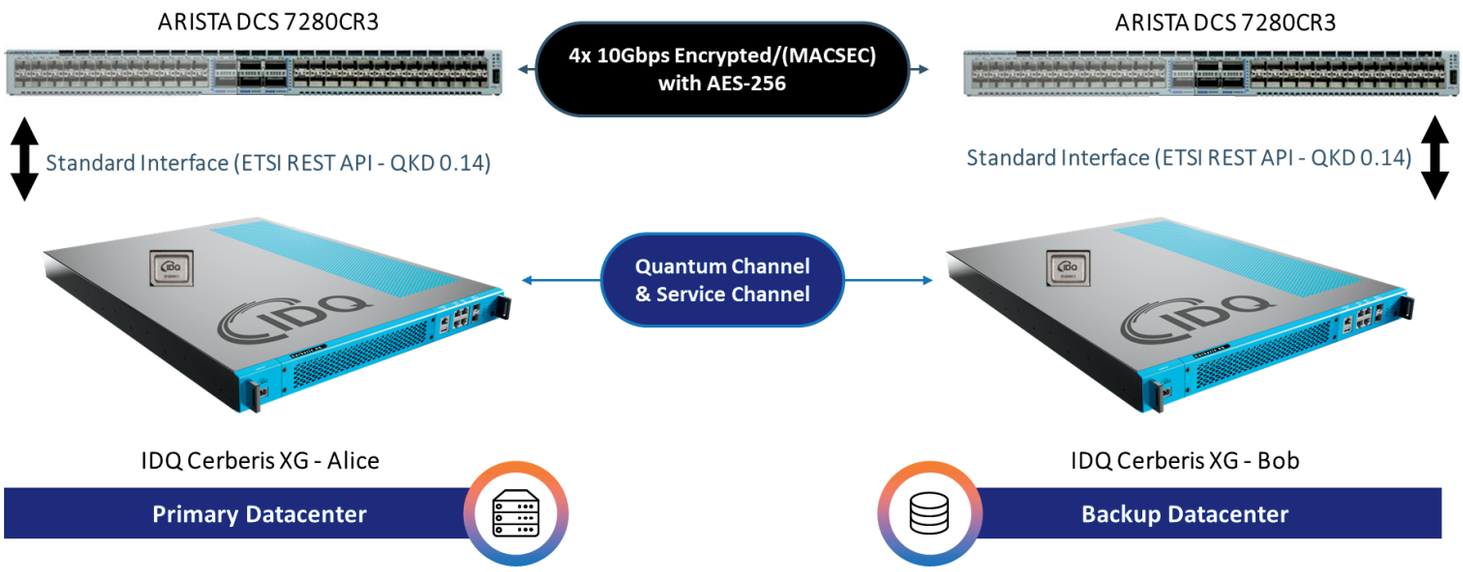
Quantum Key Distribution (QKD) provides quantum-safe key exchange. Combined with Arista's encryption solutions, it ensures the highest level of security

How can Quantum Key Distribution enhance traditional cybersecurity?

Cryptographic systems are only as strong as their weakest link. For many, this is the secure exchange of encryption keys that form the basis of public key cryptography. **QKD is already being used to enhance classical encryption technologies, to provide provably secure key exchange**.

Thanks to one of the principles of quantum physics (observation causes perturbation), any attempt to intercept or observe the keys during exchange leads to transmission errors that can easily be detected by the intended recipient.

Adding a QKD layer to your most sensitive links ensures a quick start towards quantum-safe security.



ARISTA
www.arista.com

IDQ
www.idquantique.com