IDQ

SWISS QUANTUM

Redefining Security

Use Case: Telecom Service Provider

Securing tomorrow's post-quantum threat environments

Launching the first 100G Ethernet encryption with Quantum Key Distribution

Customer name : British Telecom (BT)

Industry: Telecom Service Provider

Country: United Kingdom

Business need	Solution	Results
Increase their customers' backbone capacity and secure tomorrow's post-quantum threat environments.	100G Ethernet protection from Gemalto (CN9000 series) with Quantum Key Distribution (QKD) from ID Quantique	Successful implementation of 100G encryption with Quantum Key Distribution protection

Business need

British Telecom (BT) is one of the leading communications companies, serving the broadband, phone, TV and mobile needs of customers in the UK and in more than 170 countries.

As challenges to secure data-in-motion increase and requirements for big data intensify, BT was looking for a solution to provide greater capacity and quantum-safe encryption today to secure tomorrow's post-quantum threat environments.

In today's world, telecom service providers need 100G transport technology in their networks in order to handle increased data traffic and bandwidth consumption. But speed isn't everything. The key question is: how can data in motion be effectively protected when travelling across todays' global networks?

Indeed, protection of data-in-transit is an area that is often overlooked by organizations keen to secure their local networks. The unfortunate truth is that links between secure areas, where data is travelling across publicly accessible optical fibres, represent a significant risk. That risk environment will only increase as data rates get higher and it becomes possible to intercept and capture more data in less time.

For BT, securing sensitive personal, financial and government data for the long term is critical.

The rise of quantum computers means that in the future many current encryption algorithms will become obsolete and insecure. Because the security of today's public key cryptography rests primarily on the assumption that certain mathematical functions are complex to calculate, or decode, without access to computing power beyond the realms of today's classical computers. With the advent of massively powerful quantum computers in the next decade, such assumptions will no longer hold. And the danger today is real, knowing that information which is downloaded today may be decrypted offline in the next years (download now, decrypt later).

Solution

Just as governments and enterprises are starting to invest in "quantum-safe cryptography" - including key distribution solutions such as QKD which can withstand quantum computers. BT decided to consider offering a move to quantum-safe security to their customers as an integral part of their risk management planning.

BT worked closely with IDQ and partner Gemalto, the world leader in digital security, to test a new solution. The solution chosen by BT was SafeNet High Speed Encryptors developed by Senetas Corporation which are fully field-upgradeable to support IDQ's Quantum Key Distribution (QKD) systems. The QKD systems are added as an additional layer of security to the layer 2 encryptors to ensure that they are quantum safe.

Ensuring forward-secrecy for the most sensitive information, QKD works on the intrinsic and proven principles of quantum physics – i.e. that the generation of the quantum key is truly random, and that any interruption or eavesdropping of the data will perturb the system and can thus be detected. Each quantum key is independent and uncorrelated, and automatically updated every minute. Unlike classical encryption based on mathematical algorithms, QKD will not be compromised by mathematical progress or the continued increase in computing power and it is not vulnerable to passive attacks. Such passive attacks are potentially the most dangerous as they are most often not even detected.

As organizations upgrade their networks bandwidths to meet increasing demand for voice, video, virtualization and mass data, securing these assets from cybercriminals and other unauthorized access is essential. ID Quantique's Quantum Key Distribution system, integrating a built-in Quantum Random Number Generator (Quantis), combines with Gemalto's newest addition to its proven high speed encryption solution, the SafeNet Ethernet Encryptor CN9100. The CN9100 encrypts traffic at Layer 2 at native speeds of 100 Gbps with latency under 2 microseconds and provides unmatched performance and security to protect data and sensitive communications across large-scale, high-capacity networks.

Results

Successful demonstration and testing at BT, ensuring readiness of the solution for quantum-safe 100G Ethernet encryption.

Protection against the threat vector of "download now, decrypt later"

> *"With the expertise of IDQ and Gemalto, we demonstrated a world leading 100Gbps Ethernet transport with full quantum encryption at our highly influential BT innovation week in June 2017 and we plan to take them into Proof of Concept trials. The technology is world leading and we are excited to continue to showcase it."*
>
> Andrew Lord
> Head of optical research at BT

Disclaimer: The information and specification set forth in this document are subject to change at any time by ID Quantique without prior notice.