



Redefining Security

Use Case: Telecom Service Provider

Securing Smart Factories' critical data over a 5G network

Integrated Quantum Key Distribution and Encryption



Customer: SK Telecom (SKT)

Industry: Telecom Service Provider

Country: South Korea



Business need



Securing a 5G network for smart factories' critical data

Solution



Encryption and Quantum Key Distribution from Clavis³⁰⁰ QKD platform

Results



High-speed, stable and secure data connectivity over a 5G network

Business need

Established in 1984, SK Telecom (SKT) is the largest mobile operator in Korea with nearly 50 percent market share. As the pioneer of all generations of mobile networks, the company launched the fifth generation (5G) network on December 1st, 2018. Through the application of differentiated network technologies and quantum-safe cryptography, SKT is determined to offer 5G services with the highest level of speed, stability and safety. Moreover, building on its unrivaled competitiveness in mobile connectivity, SK Telecom is also leading the new ICT ecosystem by driving innovations in areas such as media, security and commerce.

By combining 5G and IoT, companies can transform standard manufacturing factories into smart factories. SK Telecom joined with 18 other companies and organisations to launch an alliance (5G Smart Factory Alliance (5G-SFA)) aimed at creating a universal solution compatible with smart factories while leveraging 5G networks.

A customer of SKT, an auto parts manufacturer – Myunghwa Industry – based in Ansan has implemented a smart factory using IoT devices and robots. The factory generates a large volume of confidential data transmitted over the 5G network to reach the SKT Cloud – for example IP information, such as design documents, are sent to robots and machines.

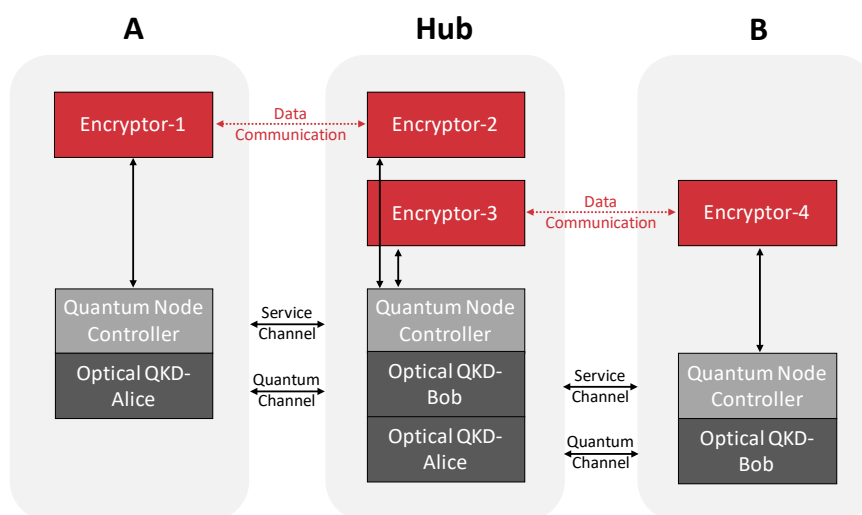
Therefore, the customer was looking for fast and secure access to the SK Telecom commercial 5G Service to connect their new smart factory. The customer site is connected with fibre optics to SKT 5G Network Point of Presence.

Solution

In order to best address this customer security need, SKT has secured the 5G network connectivity with the latest quantum safe technology using quantum cryptography (Encryption and Quantum Key Distribution) between the customer premises and SKT 5G network (for validation purposes). The latest Clavis³⁰⁰ connected to the 5G backbone optical networks carries out both the data encryption and quantum key distribution functions.

The Clavis³⁰⁰ is a complete modular cryptographic solution that performs QKD in a point to point configuration, as well as key relay to allow distribution over longer distances. The keys can be supplied to up to 80 separate encryptors, either to external encryptors or to integrated high speed encryption blades. In this case the setup was based on the integrated encryptor of the Clavis³⁰⁰.

The 5G design includes a Distribution Unit located on the customer site in Ansan (A) while the 5G Central Unit (CU) is located at the SKT Network in Sungsoo (B). Since the 5G DU to CU connectivity is using a fibre optic network, it was possible to combine QKD with the encryption on the 5G Mid-Haul Network.



The two 5G nodes are connected through a network Point of Presence defined as a Hub (H) for the encryption and QKD design as shown on the diagram explaining the components of this use case.

The Clavis³⁰⁰ was also used in the Hub site with 2 encryption and QKD modules connected to the two remote encryption and QKD modules. The design is optimised and generates savings since one single chassis acts as a Hub connected to two remote nodes. The design was optimised even further by using WDM for the data and service channel hence reducing the number of fibres used between the Hub and the remote site.

Results

While adding encryption and Quantum Key Distribution to their 5G network access thanks to the latest Clavis³⁰⁰, SK Telecom was able to leverage their brand-new 5G Network combined with IoT to propose a fast and secure Smart Factory solution. This solution combines the latest technology available ensuring high-speed, stability and security for the customer data connectivity.

While first applying quantum cryptography communication technology to the Ansan-Sungsoo section of its 5G network, SK Telecom was able to demonstrate the first encrypted 5G access combined with quantum key distribution to his smart factory customer. CEO Park Jung-ho said he is *“determined to provide the highest level of network security and stability at all times, [and that] SK Telecom will continue to work closely with companies across the globe to secure the best technologies.”*