



Post-Quantum Secure Data Transmission Devices

Telecommunication Industry Use Case Carrier-Grade Quantum-Resistant VPN

Quantum computing represents a growing threat for communication security by taking advantage of quantum speed-up to affect standard cryptography of telecommunication deployments using RSA and ECC. Additionally, typical implementations rely on pseudo-random number generation to create cryptographic keys, potentially lowering the security level due to the lack of true randomness.



Telefonica Chile is the biggest fixed-line operator and internet service provider in the country. The Telefónica Group has been in the country since 1989 and accounts for 35% of the market share of mobile telecommunication services.



Problem

Potential vulnerability of user authentication by Quantum computing, and/or use of weak cryptographic keys.



Solution

Post-Quantum enhanced VPN secured with GoQuantum and true randomness.



Successful establishment of the one of the first (or the first) carrier-grade quantum-secure network among Mobile Network Operator in South America.

goquantum.tech





Founded in 2018, GoQuantum is focused on the development of secure connectivity devices using cryptographic algorithms not affected by quantum computers. Our solutions feature quantum random number generators for extra-secure keys as well as custom implementations according to specific data-transport protocol layers (L1 up to L4).

Within the corporate network of Telefonica, GoQuantum deployed a quantum-secure VPN over the standard IP infrastructure, with minimal additional hardware required.

Our solution uses cutting-edge quantum-safe algorithms for encryption, following a crypto-agile philosophy and adding quantum hardware for cryptographic keys based on true randomness.











Quantum Random Number Generator

Base Architecture:	Base Architecture: x86_64 VM + QRNG
Power Usage:	100 mW - Peak - Powered by USB
Interface	USB-3
Physical Format	1 U Rack Format Server



Base Architecture: ARM SBC + QRNG

Secure key generation using quantum-photonic hardware

For creation of crytptograpic keys, our devices integrate Quantum Random Number Generation (QRNGs), which take advantage of quantum states and statistics for true randomness based on the unpredictability of physical photonic detection, over standard pseudo randomness.



goquantum.tech