



Press Release

Geneva, October 7th 2021

Telefonica, Fortinet and ID Quantique (IDQ) have jointly demonstrated the first Quantum-Safe IPVPN connection suitable for offering a fully managed datacenter interconnection service

Telefonica is actively preparing a new generation of connectivity solutions that can resist highly sophisticated cyber-attacks made possible with the development of quantum computers. These quantum computers, once sufficiently powerful, may be able to break current public-key cryptography schemes based on prime number factorisation, such as the widely used RSA algorithm.

There is a new breed of encryption services that leverage quantum physics principles, designed with the objective of being quantum-safe, and thus ensuring long-term data security in case information is stolen today and decrypted later using quantum computers.

These services may be proposed as a quantum-safe evolution of current B2B services (e.g. SD-WAN connectivity) or point to point encrypted critical connectivity scenarios but also for different use cases improving the security of operator infrastructure (e.g. network management traffic or 5G Multi Access Edge Computing – MEC deployments).

Quantum Key Distribution (QKD) is a highly innovative key exchange technique, which can ensure quantum-safe security today. It is a technology that exploits a principle of quantum physics – observation causes perturbation – to exchange cryptographic keys over optical fibre networks with ultimate security. A Quantum Random Number Generator (QRNG) embedded in the QKD system provides keys that are produced in an absolutely random way. Once the key exchange is validated, the keys can be used to encrypt data, and encrypted messages will remain confidential.

Telefonica, Fortinet and ID Quantique have successfully demonstrated the combined solution of FortiGate IP Virtual Private Network (IP-VPN) service and IDQ QKD, using a standardised ETSI interface, to provide a Quantum-Safe IP encryption solution over a real deployment scenario consisting of a 20 km span. This Proof of Concept shows the resilience of the solution against different kinds of attacks, such as eavesdropping attempts, along with operational and integration procedures for the service. This is also a testament to Fortinet's continuous FortiGate innovations, including purpose-built security processing units (SPUs) to accelerate both networking and security functions and enable Security-Driven Networking.

Fortinet's FortiGate firewalls receive quantum keys generated by IDQ's [Cerberis³ QKD system](#) using the standardised ETSI Key Delivery Application Programming Interface (API). Integration of these quantum keys with the existing key derivation function ensures seamless interworking with the FortiGate platform. The combination of the FortiGate high-end appliances and VMs with IDQ's QKD provides long-term security for critical data transported over VPN's relying on IPsec protocol.

QKD related technologies are taking advantage of the quantum properties of optical media, and they are one step on the research path towards a future Quantum Internet. This pilot is part of Telefónica's QKD encryption activities, in which the company is being very active from the point of view of innovation with the clear objective of continuing to have secure networks in the future.

“

This PoC results from our sustained collaboration with IDQ within the EU research ecosystem, such as OpenQKD project, and with Fortinet on the commercialisation of security services. The PoC demonstrates the commitment of Telefonica to provide their customers with the best connectivity at any moment at any place, ensuring their privacy and safeguard of sensitive information, and to prepare and protect them for the advent of the quantum internet.

Jesus Folgueira - Transport Network Senior Manager, Telefónica

“

As a leading security provider, Fortinet has been continuously innovating to deliver a best in class security platform to our service provider and enterprise customers, enabling an industry-leading Security-Driven Networking approach that deeply weaves security into networking to future proof customer investments. Working with Telefonica and IDQ, Fortinet continue to lead and accompany service providers and enterprises in securing their networks, data, and services today, for tomorrow's quantum reality and risks.

John Maddison, CMO and EVP Products at Fortinet

“

We are very excited by this achievement with Fortinet and Telefonica. Sensitive data is increasingly in danger from the growing threat of cyberattacks and more and more companies, especially banks and governments are highly concerned by this issue.

Axel Foery, EVP Quantum-Safe Security at ID Quantique

ID Quantique is acknowledging funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857156.

About Fortinet

Fortinet (NASDAQ: FTNT) makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. This is why the world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 530,000 customers trust Fortinet to protect their businesses. And the Fortinet NSE Training Institute, an initiative of Fortinet's Training Advancement Agenda (TAA), provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone.

Learn more at www.fortinet.com, the [Fortinet Blog](#), or [FortiGuard Labs](#).

About Telefonica

Telefónica is one of the largest telecommunications service providers in the world. The company offers fixed and mobile connectivity as well as a wide range of digital services for residential and business customers. With more than 367 million customers, Telefónica operates in Europe and Latin America. Telefónica is a 100% listed company and its shares are traded on the Spanish Stock Market and on those in New York and Lima.

Learn more at www.telefonica.com.

About ID Quantique

Founded in 2001 as a spin-off of the Group of Applied Physics of the University of Geneva, ID Quantique is the world leader in quantum-safe crypto solutions, designed to protect data for the future. The company provides quantum-safe network encryption, secure quantum key generation and Quantum Key Distribution solutions and services to the financial industry, enterprises and government organisations globally.

IDQ's products are used by government, enterprise and academic customers in more than 60 countries and on every continent. IDQ is proud of its independence and neutrality, and believes in establishing long-term and trusted relationships with its customers and partners.

For more information, please visit www.idquantique.com.

For more information, please contact:

Catherine Simondi – VP Marketing & Communications

catherine.simondi@idquantique.com or +41 (0) 22 301 83 71