Press Release

Geneva, February 27th 2020

ID Quantique partners with Fortinet to commercialize a quantum-safe VPN solution

ID Quantique (IDQ), the world leader in quantum-safe security solutions, integrates with the Fortinet Security Fabric to provide long-term security for critical data transported over Virtual Private Networks.

ID Quantique and Fortinet, a global leader in broad, integrated and automated cybersecurity solutions, will provide a dedicated commercial-grade interface to IDQ's latest generation of Quantum Key Distribution (QKD) system. Fortinet's flagship next-generation firewall, FortiGate, will offer a dedicated interface for quantum keys based on the ETSI key delivery standard. FortiGate is a key part of the Fortinet Security Fabric, which has an open architecture and interfaces to enable technology partners in Fortinet's Open Fabric Ecosystem to develop integrated solutions for comprehensive cybersecurity.

"Combining secure Layer 3 encryption with QKD will provide the best VPN security for data in motion. We are very excited by this new partnership with Fortinet and being part of the Fortinet Open Fabric Ecosystem", says Grégoire Ribordy, CEO and co-founder of ID Quantique. *"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."*

This joint solution will be the first commercially available quantum-safe VPN platform built on a standardized interface. QKD – also known as quantum cryptography – is added as an extra layer of security on top of the encryption taking place at Layer 3 to protect data in transit.

The key use cases of this joint solution will be for deployments of Quantum-Safe L3 VPNs in Data Center Interconnection (DCI) and 5G backbones. Using QKD on VPNs will provide immediate protection to data in the face of today's brute force attacks, ensure that data with a long shelf life is protected against future attacks and will safeguard high-value data in a post-quantum computing world. Typical targeted customers are governments, financial service companies, healthcare organizations, cloud and 5G service providers and commercial enterprises worldwide.

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 fiber networks with ultimate security. A Quantum Random Number Generator (QRNG) embedded in the QKD system provides keys that are produced in an absolute random way. Once the key exchange is validated, the keys can be used to encrypt data and encrypted messages will remain confidential. QKD is widely predicted to be a vital tool for securing highly sensitive data transport from all forms of cyberattack, including the threat of quantum computers that could render current public key cryptography useless. Distributing encryption keys in a quantum state ensures that all tapping attempts are detected as any attempt to intercept traffic disturbs photons, introducing coding errors and alerting operators.

Fortinet's FortiGate firewalls will receive quantum keys generated by IDQ's Cerberis3 QKD system using the standardized ETSI Key Delivery API. An internal dual key-agreement (combination of quantum keys with the internal exchanged dynamic keys) will be used to assure seamless interworking with the FortiGate platform. The combination

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

of the FortiGate high-end appliances and VMs with IDQ's QKD will provide long-term security for critical data transported over Virtual Private Networks (VPN's).

"Practical quantum physics can be used by threat actors to steal encrypted data and make current public key cryptography obsolete." says John Maddison, CMO and EVP Products at Fortinet. *"As a leading security provider to service providers and enterprises, Fortinet teaming up with ID Quantique to integrate the FortiGate with their innovative quantum key distribution solution will allow our joint customers to build a secure encryption foundation for today and the quantum future."*

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 organizations globally. IDQ's quantum random number generator has been validated according to global standards and independent agencies, and is the reference in highly regulated and mission critical industries – such as security, encryption, critical infrastructure and IoT – where trust is paramount.

Additionally, IDQ is a leading provider of optical instrumentation products, most notably photon counters and related electronics. The company's innovative photonic solutions are used in both commercial and research applications.

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.

Contact info:
Catherine Simondi
VP Marketing & Communications
catherine.simondi@idquantique.com
+41 (0) 22 301 83 71