



Press Release

Geneva, 1st November 2017

ID Quantique Celebrates 10-Year Anniversary of the World's First Real-Life Quantum Cryptography installation

10 years ago the State of Geneva in Switzerland installed quantum cryptography to protect its elections. It was the first ever deployment of a commercial quantum cryptography system. A decade later Geneva is still using the system to protect the integrity of its elections.

10 years ago in October the State of Geneva and ID Quantique SA (IDQ), the world leader in quantum-safe security solutions, installed the world's first commercially available quantum cryptography system. The Geneva government was a pioneer in the use of quantum technology in 2007, using it to secure the network linking Geneva's ballot counting center (where the votes are counted) to the government repository (where votes are stored) in order to ensure integrity of the data and the election results. The system is still used to secure every federal and cantonal election annually in the State of Geneva.

Dr Grégoire Ribordy, CEO and co-founder of ID Quantique, stated: "IDQ and the State of Geneva made history in 2007 with the world's first real use of quantum cryptography. The State of Geneva took a pioneering role at the time in recognizing the need for strong security solutions to underpin the integrity of our direct democracy. Since then quantum cryptography has been deployed by governments and enterprises worldwide. With the very real threat that emerging quantum computers pose to many current mathematics-based cryptographic primitives, we expect that market demand for Quantum Key Distribution (QKD) will only increase. However, it will take time for public perception to catch up – enterprises seem continually surprised that QKD not only exists as a robust and stable solution, but that it has been in use for over a decade now..."

Quantum cryptography combines AES 256-bit Ethernet encryption with Quantum Key Distribution (QKD). QKD uses the inherent properties of quantum mechanics to guarantee that the key which is used to encrypt the data is both truly unique and has not been intercepted by any adversary. This is based on the proven principles of quantum physics- namely, 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. This is the cornerstone for secure encryption, which is then used to guarantee the integrity, authenticity and confidentiality of the data exchange.

On 21st October 2007 the Geneva government used IDQ's hybrid quantum cryptography solution, which combines state of the art Layer 2 encryption (Centauris Ethernet Encryptors) with the Cerberis Quantum Key Distribution (QKD) servers. The solution secures a point-to-point Gigabit Ethernet link used to send ballot information for the federal and cantonal elections from the central ballot counting station to the Geneva government data center.

Typically sealed ballot boxes are brought from the polling stations to the central counting station where they are opened and counted alongside the already delivered mail votes. Counting is done manually according to strict procedural norms. Geneva law dictates that any citizen can attend the ballot counting procedure to ensure the authenticity of the results. However in the modern world this principle has been reinterpreted- the Electoral Commission carries out close surveillance of the counting and the data entry, and the authenticity and integrity of any subsequent data transfer is then guaranteed by the highest level of encryption.

Unlike many of today's "conventional" cryptographic primitives which rely on mathematical complexity for security, QKD will not be compromised by mathematical progress or by the continual increase in computing power and emerging quantum computers. It thus ensures true future-proofed information theoretically secure distribution of the encryption key.

> Discover the full use case [here](#).

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 and online gaming- where trust is paramount.

IDQ's products are used by government, enterprise and academic customers in more than 60 countries and on every continent. As a privately held Swiss company focused on sustainable growth, 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 <https://www.idquantique.com/>.

Contact Info:

Catherine Simondi – Marketing Director at ID Quantique
catherine.simondi@idquantique.com or +41 22 301 8371