IDQ

Redefining Security

Use Case: Utilities

Future-proof datacenter interconnection

Integrated Quantum Key Distribution and Layer 1 Encryption

Customer: Services Industriels de Genève (SIG)

Industry: Utilities

Country: Switzerland

SIG

Business need	Solution	Results
Adding an extra layer of security on top of current encryption to protect critical data for the next decades	ADVA's FSP 3000 Layer 1 encryption combined with IDQ's QKD for secure datacenter interconnect	Long-term security and privacy of critical data over optical network

Business need

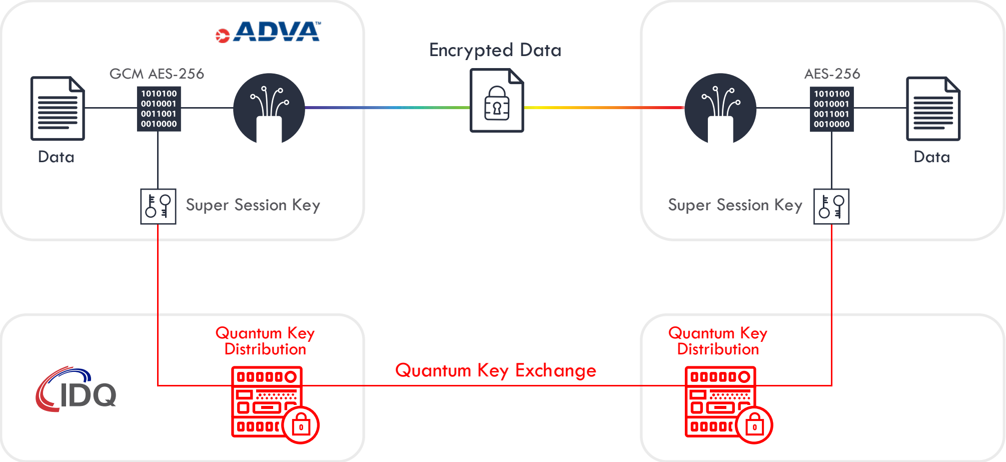
SIG (Services Industriels de Genève), the Geneva Canton Utility company, uses two main datacenters to run private cloud applications processing sensitive data. Although network encryption was already implemented between the two datacenters, SIG wanted to protect critical information for the next decades when quantum computers will be powerful enough to break current public key encryption standards. This expected game-changing disruption creates a necessity to future-proof current cybersecurity solutions. By anticipating and learning to use existing solutions, SIG wanted to prepare itself before one discovers that it is too late to guarantee data protection for the next 5 to 10 years.

Solution

SIG decided to implement the state-of-the-art in terms of cryptography, aka quantum cryptography, in order to reduce the attack surface of the fiber optical network.

In order to best address this need, SIG combined ADVA FSP 3000 product running AES-256 encryption with ID Quantique Cerberis^3 Quantum Key Distribution (QKD) securing the symmetric key exchange between the two datacenters. The latest production release of IDQ QKD system and ADVA's FSP 3000 scalable optical transport product (Release 19.1.1) supports the ETSI standard interface for the quantum key exchange (REST API QKD 014) between QKD and encryptors.

QKD 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 a proven optimum random way.



Once the quantum key exchange is performed, the quantum key XOR with the standard session key generates a super session key, which is used by the ADVA encryption equipment. Thus, the network security certification remains valid and becomes future-proof is even improved thanks to the ITS (Information-Theoretic Security) nature of QKD.

The ADVA encryptors define the key rotation period, generate key requests to the QKD Node and the encryption key is updated automatically securely without any human intervention.

In the unlikely event of QKD Key unavailability due to an incident, the ADVA encryptors continue to operate using standard encryption keys so that there is no service interruption on the encrypted data link.

Results

The combination of the FSP 3000 ConnectGuard™ Optical Layer 1 encryption with IDQ's QKD provides long-term security for critical data transported over optical networks. QKD – also known as quantum cryptography – is a highly innovative key-exchange technique, which can ensure quantum-safe security today.

"We have been working with ADVA for many years" says Grégoire Ribordy, CEO and co-founder of ID Quantique. "Combining secure Layer 1 encryption with QKD will provide the best security for data in motion. 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. We are honored to work with SIG and ADVA on this QKD secured datacenter interconnection project"

"SIG now benefits from the state-of-the-art quantum cryptography solution between their two main datacenters ensuring long time privacy for our critical data" says Olivier Gudet, head of SIG Network infrastructure.

"QKD is a method to secure the key exchange against quantum computer attacks. We were the first to implement the ETSI key delivery API on a commercial high-speed optical networking product. Through our partnership with ID Quantique, we can leverage their technology and expertise to provide a new level of long-term security in data transport." says Jörg-Peter Elbers, Senior Vice President of Advanced Technology, Standards & IPR, ADVA.

Disclaimer: The information and specification set forth in this document are subject to change at any time by ID Quantique without prior notice.