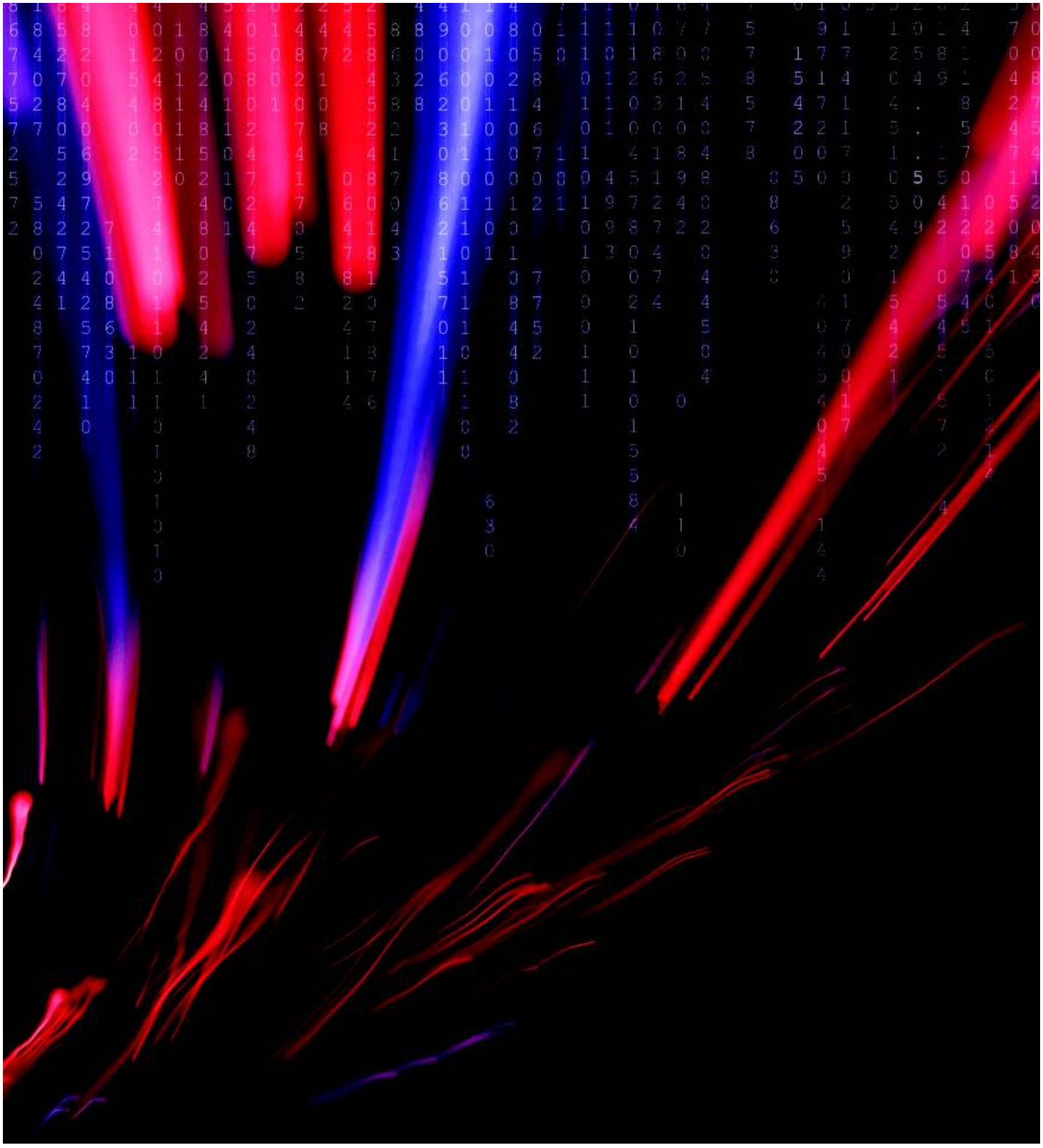

QUANTUM-SAFE CRYPTOGRAPHY

High performance network encryption for long-term data protection
Quantum key generation and quantum key distribution

IDQ
FROM VISION TO TECHNOLOGY

SWISS QUANTUM

Governments and enterprises need to store and transmit large amounts of confidential data securely, both nationally and on a global scale. Whether the data relates to state secrets, confidential client information, real-time banking transfers or other applications, a top priority is to protect such data against ever more technologically advanced cyber-attacks and the growing threat of leaks. The best way to ensure the confidentiality and integrity of data-at-rest and data-in-transit is through encryption.

However, with the advent of the quantum era when the massive computational power of quantum computers will render much of today's encryption unsafe, it is essential for enterprises and governments to deploy “quantum-safe” solutions already today.

IDQ's quantum-safe cryptography solutions are designed and built for such quantum-era security, with the goal to protect mission-critical data which has long-term sensitivity and value.

Quantum Key Generation

The key is the cornerstone of secure cryptosystems. Today, best security practices are based on the Kerckhoff principle: the assumption that an attacker has in-depth knowledge of the cryptographic algorithm (such as AES), and that the security of the system therefore resides primarily in the secrecy and quality of the encryption key. And yet is surprising in today's world just how weak many of these keys are - either by design or by negligence. To provide any security the key must be:

- Unique
- Truly random (unpredictable)
- Stored, distributed and managed securely

While these attributes – uniqueness and randomness – are easy to assume, they are actually complex to ensure and even more complex to test. ID Quantique’s Quantis Random Number Generator (QRNG) range uses the fundamental and provable randomness of quantum mechanics as a source of true randomness Such quantum processes provide instantaneous and inexhaustible entropy for use in the generation of encryption keys or random seeds. Quantis is one of the most trusted RNGs in the market, with certifications from different countries and in multiple industries.

Quantis QRNGs serve as a hardware source of trust for cloud or distributed environments, with both Linux and Windows operating systems. They provide true randomness for crypto applications in Virtual Machines (VMs), Virtual Private Networks (VPNs), HSMs, storage encryption and others.

Quantum Safe Encryption

IDQ’s Centauris encryption platform provides high-performance network encryption for data-in-transit. Centauris products encrypt high throughput traffic up to 100Gbps on local and storage area networks for data back-up and recovery, as well as on fully meshed global networks for international operations.

With the Centauris encryptors there is no trade-off necessary between security and performance. Full network performance is maintained so that time-sensitive applications may be accessed remotely from different countries or branches without delay or latency. Easy installation and “set and forget” functioning ensure that the encryption does not place an additional burden on the network.

Security certifications ensure both physical protection of the appliances (tamper-proofing and detection), and best-practice processes (such as separation of duties) for the secure remote provisioning and easy daily management of global networks.

Centauris encryptors can be deployed today and upgraded to quantum cryptography through the addition of the Cerberis Quantum Key Distribution (QKD) server in the coming years. This guards against the presence of eavesdroppers and ensures provable forward secrecy as well as investment protection far into the future.

BY COMBINING THE BEST OF QUANTUM AND CLASSICAL ENCRYPTION, IDQ'S SOLUTIONS PROVIDE LONG TERM PROTECTION FOR SENSITIVE DATA IN TRANSIT

Why Encrypt?

In a digital age and global environment data no longer resides securely within a limited physical perimeter. Increasingly data is required to transit many kilometers, even international borders, to serve real time applications in other locations and countries. Data on third party leased lines must be protected, but even on dedicated or private networks such data is not secure - the ease with which hackers can intercept data on Ethernet or optical fiber cables is now well publicised.

With the aid of a cheap optical tap criminals can download and analyse in real time gigabits of Ethernet & Fibre Channel information in locations where the optical fibers are readily accessible, such as in splice chambers, under manholes and in telecom stations. While the interception and analysis technologies available to hackers are becoming cheaper and better, at the same time data protection regulations and the penalties for data breaches are also increasing worldwide. There has never been a better time to invest in encryption.

Why Quantum-Safe?

The security of today's public key cryptography rests primarily on the assumption that certain mathematical functions are complex to calculate, or decode, without access to computing power beyond the realms of today's classical computers.

However, with the advent of massively powerful quantum computers in the next decade, such assumptions will no longer hold. Much of today's encryption will be vulnerable. Moreover, information which has been downloaded today may be decrypted offline in the next years (Store now, decrypt later).

Therefore governments and enterprises need to start investing in "quantum-safe cryptography" - including key distribution solutions such as QKD - which can withstand quantum computers. All governments and enterprises should envisage a move to quantum-safe security as an integral part of their risk management planning, and new investments in infrastructure and security should taken in accordance with such a plan.

Benefits of IDQ Solutions:

- Quantum-safe crypto solutions for long-term data protection
- Swiss engineered and developed
- True quantum random number generator (QRNG) for secure key generation
- Quantum key distribution (QKD) for provable security of key exchange and forward secrecy
- Full range of interoperable high-performance network encryptors, with option to upgrade to “quantum cryptography”

ID Quantique

ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services. IDQ products and solutions are trusted by the financial industry, enterprises and government organisations in over 60 different countries. IDQ's vision is to secure mission-critical data which has long-term sensitivity and value both into and beyond the quantum-era.

Founded in Switzerland in 2001 as a spin-off of the University of Geneva, IDQ has retained its Swiss identity and its edge in transforming innovative technologies into secure commercial and government solutions. Since the world's first installation of quantum cryptography for the Swiss government elections in 2007, IDQ has continued to break records in the development of new technologies.

CLASSICAL AND QUANTUM CRYPO SOLUTIONS FROM IDQ: SWISS SECURITY AT ITS BEST

LONG TERM DATA PROTECTION FROM IDQ WITH UNPARALLELED PERFORMANCE AND FLEXIBILITY

IDQ's quantum-safe key generation, key distribution and high performance encryption solutions allow users to implement security policies now, which will protect data into and through the quantum era.

Centauris CN8000 Multi-link Encryption

Designed to cost-effectively secure the most demanding of networks, the CN8000 encrypts native Ethernet, MPLS and Fibre Channel protocols with a total throughput of up to 100Gbps. Each CN8000 supports 10 different links in point-to-point or multipoint mode. It is transparent to network equipment and has no performance impact on high-availability architectures such as data center or back up environments. "Set and forget" functioning ensures easy and low cost management. The CN8000 also supports multi-tenancy - with different end users, certificates and differeniatedt access rights per card - for support of service/cloud provider environments. A quantum RNG ensures high quality entropy for very secure encryption keys, and the CN8000 supports Quantum Key Distribution (QKD) for long term data protection.

Centauris Dedicated Layer 2 Encryptors

The Centauris range of dedicated layer 2 encryptors provide organisations with high performance Ethernet, Fibre Channel and SONET/SDH encryption up to 10Gbps to secure sensitive data in transit. Compatible with the CN8000, the Centauris dedicated encryptors also work in point-to-point, hub-and-spoke and fully meshed modes on any layer 2 network architecture without impacting network performance. Selected Centauris encryptors include the Quantis QRNG and support QKD.

Cerberis Quantum Key Distribution (QKD) server

QKD uses the intrinsic laws of quantum mechanics to secure the exchange of the encryption keys between different encryptors. The quantum principle that measurement introduces perturbation is used to ensure that there is no eavesdropper or interception attempt on the key exchange. In addition the use of quantum keys ensures forward secrecy of all communications. The Cerberis QKD server comes as a stand-alone server, or as a rackable ATCA blade. It can be added to optical fiber data center links to ensure long-term data protection by providing quantum keys to Centauris encryptors and other third party encryption devices.

Quantis QRNG Appliance

The Quantis Appliance is a network-attached device, which securely generates and delivers high quality random numbers for crypto applications. The random numbers generated by the Quantis Appliance are used for different applications: to generate high-quality cryptographic keys for encryption or authentication; to seed deterministic PRNGs and provide additional randomness for commercial Hardware Security Modules (HSM); or to provide entropy for online gaming and mathematical simulations
The Quantis Appliance serves as a hardware source of trust for cloud or distributed environments on both Linux and Windows operating systems (eg. such as in the use of OpenSSL for Linux crypto functions).

ID Quantique SA
Chemin de la Marbrerie
1227 Carouge - Geneva
T+41 22 301 83 71
T+41 22 301 83 79
info@idquantique.com
www.idquantique.com