



Keeping data confidential for
ever with Quantum Security



The case for Quantum Key Distribution

Enabling unhackable communications with the
XG Series

www.idquantique.com

| The value of big data security

In a digital world, data is our most highly valued asset. It informs every business decision and is the oil that keeps the engine of commerce running. The exponential growth in data volume and availability that we've experienced over the past twenty years has introduced both complexity and risk.

Increased adoption of cloud services, remote working and the expansion of the Internet of Things has pushed data to the virtual edge of modern network infrastructure.

Evolving data protection regulations have introduced new challenges related to data privacy, sovereignty and longevity.

Overshadowing all of this complexity is a constantly evolving threat landscape, where cyberattacks are becoming increasingly persistent and sophisticated.

The cost of a data breach

According to the Ponemon Institute's annual report, the average cost of a data breach in 2020 was \$3.86 million. This figure includes costs of detection, escalation, notification and remediation but also factors in broader post-breach implications:



Revenue
Loss



Reputational
damage



Breach
of Privacy



Legal
action



Loss
of IP



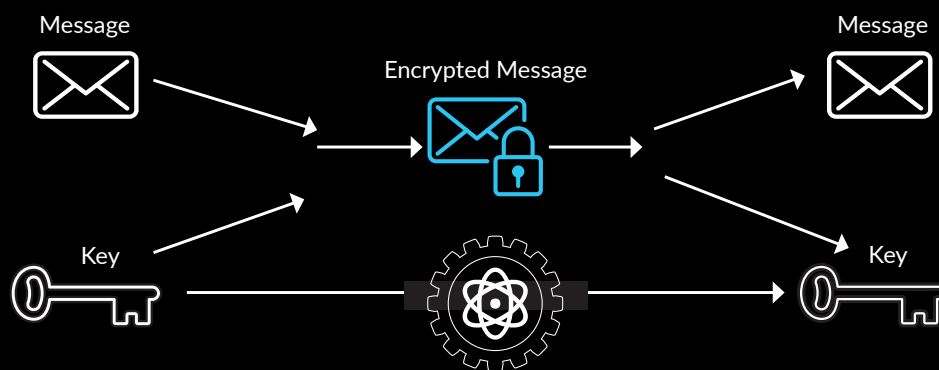
Loss of data
sovereignty

| What is QKD?

Quantum Key Distribution (QKD) is a technology that uses quantum physics to secure the distribution of symmetric encryption keys. It solves the problem of key distribution by allowing the exchange of provably secure cryptographic keys between remote parties over optical fiber networks with absolute security, guaranteed by the fundamental laws of physics.

Observation leads to perturbation

Key information is carried on quantum particles of light down an optical fiber link. According to the principles of quantum physics, unlike classic communication, with a secured quantum channel, any attempt to intercept the data will cause a disruption in the transmission, leading to errors that can be detected by legitimate users.



Key Advantages



QKD offers the ultimate in long-term cybersecurity



It solves the problem of secure key exchange once and for all



Its effectiveness is not impacted by future technological advances



It will form the basis of the world's future quantum internet

| Who needs QKD?

Any organisation or industry that relies on secure key exchange to protect sensitive data as it moves across private or public network infrastructure. Ensuring the authenticity, integrity and privacy of data is essential for all organisation, but especially for those that deal with sensitive, personally identifiable data; those that operate in IP-rich environments, or those that operate in highly regulated sectors:



| The XG Series

The XG Series is the first comprehensive range of QKD solutions designed for commercial applications in production environments. QKD uses quantum physics to secure the distribution of symmetric encryption keys. It solves the problem of key distribution by allowing the exchange of provably secure cryptographic keys between remote parties over optical fiber networks with absolute security, guaranteed by the fundamental laws of physics.

Your use case is covered

The XG Series covers a wide range of applications and allows you to select the solution that really fits your infrastructure. Whether you need to secure short or long distances, with high or lower speed, in any kind of network topologies, such as point-to-point, relay, ring, hub and spoke, star, meshed, we got you covered.



Cerberis XG



Clavis XG



Short/medium range	↔	Long range
Standard key rate	🔄	High key rate

Designed for complex topologies (ring, hub and spoke, meshed, star)
Controlled and monitored centrally

Our QKD systems are also available for research centers and universities through the XGR Series dedicated platforms.

| XG Series: 4th Generation QKD

The XG Series represents the 4th generation of QKD solutions commercialised by ID Quantique. Since the development of its first QKD solution in 2007, ID Quantique has been dedicated to a program of continuous improvement and innovation.

Key Benefits



Proven and highly reliable technology



Designed for complex and large-scale deployments



Extensive Network and Key Management software suite



Interoperability with major encryption vendors

But also...

Provably secure key distribution and instantaneous intrusion detection

Small rack footprint

Centrally monitored solution

Trusted security (tamper detection, secure memory module, QRNG chip)

Easy integration in any data center and telco infrastructure

Easy (remote) installation and maintenance

Non-intrusive to data communication channels

The **XG Series** is available now.

Get in touch with our team to find out what it can do for you today.



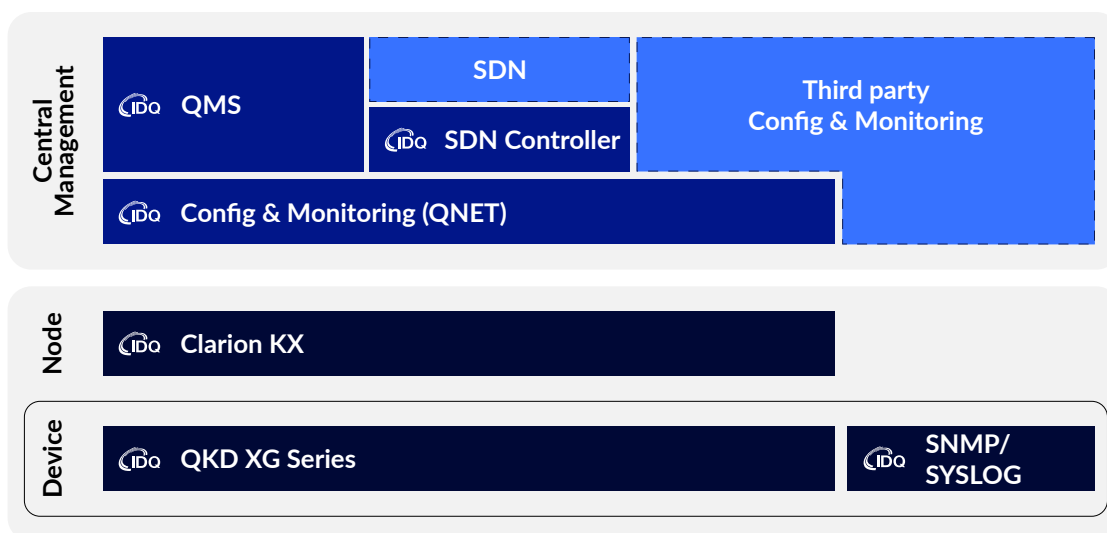
SCAN ME

| The full QKD framework

IDQ's software suite gives you the power to control every aspect of your network. From the design, configuration, and simulation of a complex infrastructure to its operation and monitoring, IDQ's different framework components enable user autonomy with minimal training, helping you reduce the time and effort managing complex networks.

The XG Series is compatible with IDQ's QKD management and monitoring framework, which consists of an Extensive Network and Key Management software suite: Clarion KX. This framework integrates current Software-Defined Network (SDN) QKD ETSI standards as well as IDQ's Quantum Management System (QNET QMS) to facilitate all large QKD deployments. It ensures a seamless integration in existing infrastructure.

- ✓ State-of-the-art Key Management System (KMS): Clarion KX
- ✓ Intuitive dashboard and configurator wizard via the QMS
- ✓ Command line access for easy configuration and monitoring
- ✓ Easy to use QNET API to facilitate integration with Third Party Configuration & Monitoring
- ✓ Support latest SDN standard



| Integrated Solutions

IDQ works with different network encryption solutions which may be upgraded with QKD to be Quantum-safe. Having a joint approach with one of our technology partners protects any kind of investment you have made so far.

Securing your critical assets can be done in various ways, with various techniques. Adding a QKD layer to your infrastructure today ensures you get a quick start towards quantum-safe security.

Overlaying Quantum Key Distribution is simpler than you may think and delivers a number of benefits, including:

- ✓ Securing your organisation in the post-quantum era
- ✓ Reaching long-term confidentiality and aiding data integrity
- ✓ Improving the TCO & ROI of your incumbent encryption solution
- ✓ Acting as a 'value-add', demonstrating your cybersecurity commitments to stakeholders



| Selected case studies

ID Quantique has been pioneering Quantum Cyber Security since 2001. Its successful and proven track record among all kinds of industries has helped our forward-thinking customers position themselves as the market leaders they are today.

QKD networks have been deployed worldwide to secure data for banks and financial institutions, governments, communications networks, critical infrastructure, and medical organizations.

Polish intercity QKD infrastructure

Poznań Supercomputing and Networking Center (PSNC) and IDQ have collaborated to add QKD to the Polish National Research and Education Network Infrastructure. It provides a secure communication infrastructure for digital science, economy and social innovations, with new highly secured services for a number of applications such as telemedicine, medical data transmission, data storage and public services.

This new 380 km-long link will serve as a steppingstone for a country-wide quantum communication infrastructure.

The final goal is to interconnect all High Performance Computing Centers in Poland and to establish common access layers to QKD services.

Selected nodes will also act as possible cross-border QKD infrastructure nodes, which will open new possibilities for pan-European QKD infrastructure and services.

The National Convergence Network Project

IDQ and SK Broadband are building the first nation-wide QKD network in Korea. It will constitute the largest operational QKD network in the world outside of China.

The National Convergence Network Project will strengthen security and stability, as well as increase the efficiency of the operation and budget of national institutions.

↗ ↖
↘ ↙ 800
kilometers



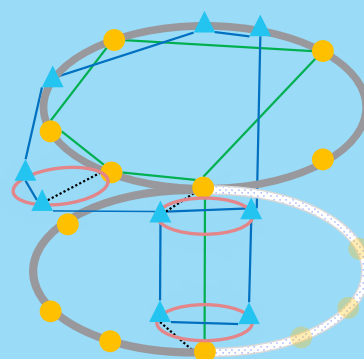
48 government
organizations



Security, stability
& efficiency

[QKD & KMS Network]

- ▲ Gov. regional office
- SKB regional office
- Customer KMS link
- Customer KMS link
- Customer ring
- SKB backbone
- ... Ext. key



| Dispelling the myths of QKD



Myth 1: QKD is not necessary today

Using quantum cryptography now will provide immediate protection to data in the face of today's brute force attacks, ensures that data with a long shelf life is protected against future attacks and safeguard high-value data in a post-quantum computing world.

QKD comes hand in hand with PQC (Post Quantum Cryptography). QKD provides stable long term security on all your fiber network with no impact on speed of encryption. It comes on top of PQC that provides flexibility to deploy over copper and wireless networks, but at the cost of lower performance and a long term security that can be challenged at any time.



Myth 2: QKD is not compatible with conventional cryptography

This couldn't be further from the truth. A security solution is as secure as its weakest link and in network encryption, the current weakest link with respect to the quantum computing threat is the secret key distribution based on public key cryptography. As its name says, QKD is used to distribute encryption keys, whose security is based on quantum physics and is thus guaranteed for the long-term. The security of QKD is based on sound principles, which, if properly implemented, guarantees absolute security for key distribution.



Myth 3: QKD is still unproven as a technology

QKD is a mature technology. It has been commercially deployed by IDQ since 2007 and is used in a wide range of industries, all across the world. Today's 4th generation of QKD has been built from field experience, based on customers' feedback, and is now operating in both country-wide and continental production environments.



Myth 4: QKD is not a standard.

Standardization work on QKD is taking place at an increasing pace. In addition to the ETSI, the ITU, ISO and IEEE organizations have made good progress on quantum communication and QKD. Industry is getting organized for large-scale deployment of this technology.



Myth 5: QKD is difficult to implement

With the 4th generation of QKD now available, integration and management are easier than ever. Available as a 1U rack-mounted device, it acts as an overlay technology and seamlessly integrates with most conventional encryption technologies. As long as your existing infrastructure allows it, having a joint approach with one of our technology partners protects any kind of investment you made so far, and improves your TCO and your ROI.



Myth 6: QKD is not affordable

The latest QKD systems cost less than previous generations, deliver long-term data protection with a lower TCO, and provide a rapid and sustainable return on your investment in cybersecurity. Consider the value of your data and the time you need to protect it, versus the risks. Ask yourself what your cyber security posture is and remember that there is direct correlation between investments in security and the level of protection you get for that money.



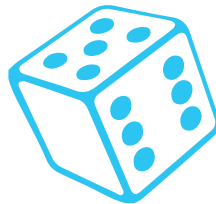
| A legacy of quantum innovation

ID Quantique is the world leader in quantum security solutions. Headquartered in Geneva, Switzerland, it maintains a global footprint through R&D partnerships with leading technology providers and academic institutions.

Founded in 2001 it has established a well-earned reputation for innovation, quality and trust. IDQ maintains its leadership role through continuously developing new products and solutions. With a growing number of patents, it continues to push the boundaries of quantum technology.



Quantum
Cryptography



Quantum Random
Number Generation



Quantum
Sensing

20 YEARS OF EXPERIENCE,
INNOVATION AND TRUST.

Discover the **XG Series**



*Quantum Cybersecurity keeps
data confidential for ever.*

LEARN MORE

[Contact Us](#)

[Request a demo](#)

[Watch video](#)

STAY CONNECTED



[Subscribe to our newsletter](#)



[Follow us on LinkedIn](#)



[Follow us on Twitter](#)



ID Quantique

Switzerland • South Korea • USA

T +41 22 301 83 71

F +41 22 301 83 79

E info@idquantique.com

www.idquantique.com

ID Quantique (IDQ) is the world leader in quantum-safe security 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 to the financial industry, enterprises and government organisations globally.

IDQ also commercialises a quantum random number generator, which is the reference in the gaming and security industries.

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.