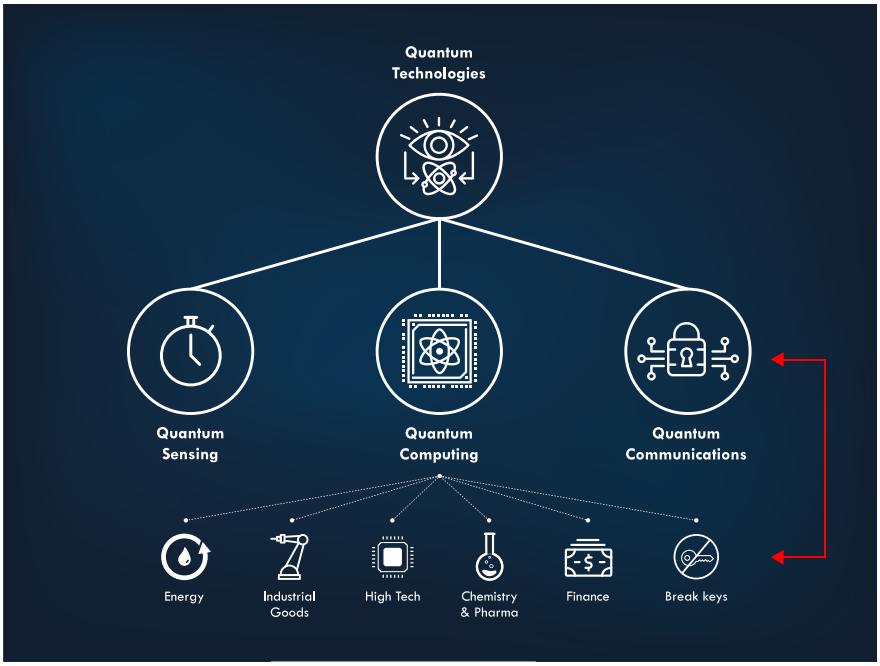
The world leader in
Quantum-Safe Security and
Quantum Randomness

QUANTUM-PROOFING YOUR ORGANISATION

No need to change your whole infrastructure
Just add the Quantum layer

THE VALUE OF QUANTUM TECHNOLOGIES

Quantum technologies are set to revolutionize the world we live in. Progress in quantum computing, quantum sensing and quantum communications will allow unprecedented achievements which will greatly benefit mankind. Indeed, quantum computing's exponential computational power will create a world of opportunities, across almost every aspect of modern life. Some of the most notable examples are finance, machine learning, pharma and medical research.



However, with great opportunities also come significant challenges. A quantum computer's ability to solve complex problems like factorization means that it will also have the power to break keys – the same keys that we rely on to protect our cryptographic systems.

Fortunately, where a challenge lies, there is also a solution. In order to protect the great opportunities quantum technologies will offer, there is a need for its quantum counterpart, quantum communications, that will be able to protect the integrity, security and authenticity of data in the quantum era. This is even more important in a world where businesses embrace digitization and the fact that with an expanded business digital surface comes an equally expanded risk. It is therefore crucial, as organizations build their own growth strategy through digitization, to include an equivalent cybersecurity component.

This is why a Quantum strategy, irregardless of when quantum techs will reach their full potential, is absolutely crucial in order to prepare its organization and seize the opportunities that will come.

WE HELP YOU BUILD A TRUSTED FUTURE

Data is an organization's most precious asset, it's the root of almost all business decisions and often represents a company's competitive advantage – it can't be outsourced. Making data secure is therefore paramount.

Getting prepared must be considered as a journey. Every step completed adds a layer of trust and preparedness. Organizations should assess their existing infrastructure. ID Quantique and its partners help targeting needs and applications with quantum-ready solutions.

A cybersecurity posture tells a lot about a company: are you passive or proactive? Data security is a never-ending marathon. Adding quantum gives you a step ahead in this race.

PREPARING YOUR IT INFRASTRUCTURE FOR THE POST-QUANTUM ERA

Quantum Technologies are creating a world of opportunities across almost every aspect of modern life. We help you build a trusted future by preparing your organization now. Data security is a never-ending marathon. Adding quantum gives you a step ahead in this race. Getting prepared must be considered as a journey where every step completed adds a layer of trust and preparedness.

01 ACKNOWLEDGE THE IMPACT OF QUANTUM COMPUTING ON CRYPTOGRAPHY

Even if we do not know when a universal quantum computer will be available, the first step is to acknowledge its impact on today's cryptography.

The "download now, decrypt later" attack vector means that encrypted sensitive data can be downloaded today & analyzed offline when a quantum computer appears. What you need to keep in mind today is the time to migrate and upgrade current security systems, data lifetime, and the existing risks

02 CONDUCT A RISK ASSESSMENT

Quantum computing will have a different impact on every type of hardware, software, or IoT firmware. A rigorous inventory and assessment of all these assets is therefore strongly advised, with a special attention on public-key infrastructure and data center interconnectivity.

You need to understand the risks involved in order to be able to act accordingly and prioritize.

PREPARING YOUR IT INFRASTRUCTURE FOR THE POST-QUANTUM ERA

03 FEED YOUR SECURITY SYSTEMS WITH QUANTUM RANDOMNESS

Using Quantum Random Number Generation (QRNG) instantly strengthens current cryptographic systems.

Quantum Random Number Generators have the advantage over conventional randomness sources of being provably secure: elementary components can be easily monitored to detect any failure or attacks, environmental perturbations can be ruled out by simple health checks, guaranteeing QRNG always produce high quality entropy.

05 BUILD YOUR ORGANISATION'S CAPACITY IN QUANTUM TECHNOLOGIES

The impact of quantum technologies on our lives will be tremendous. You need to have a global understanding of the stakes and keep up with what is going on in order to seize potential opportunities.

This can be done by training existing staff and employing people with a background in quantum physics or mathematics. Look at the various workshops available that can be tailor-suited to fit your organisation's needs.

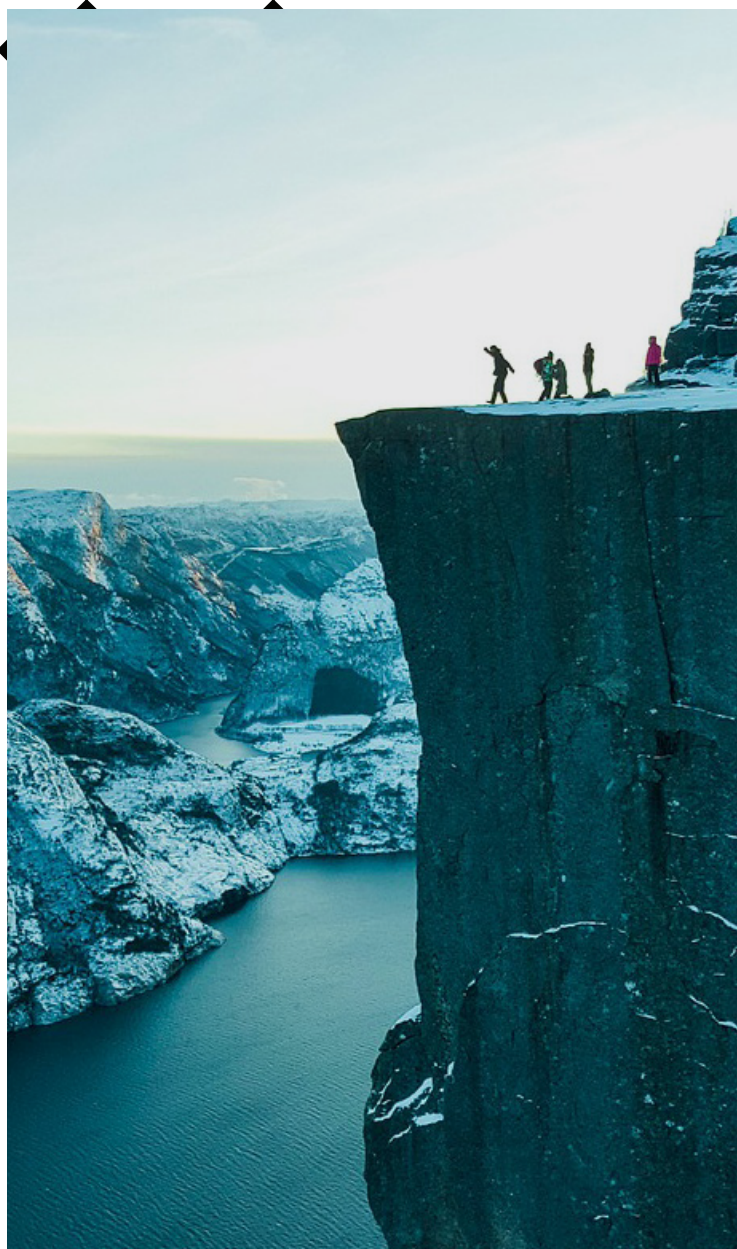
04 PURSUE CRYPTOGRAPHIC AGILITY

Organizations must ensure they are crypto-agile in order to minimize the disruption of their infrastructure when changes are needed. It is all about planning to render the transition as smooth and flexible as possible.

A future quantum-safe infrastructure requires different types of tools, adapted to the security target. A few examples:

- Guarantee the authentication and integrity of your solutions through the transition to new quantum-safe signatures
- Make sure your encryption systems are flexible and upgradable to quantum security
- Implement a so-called hybrid solution, relying on a mixture of standard solution and QRAs (when available)
- Add a QKD component to your infrastructure for long-term privacy needs
- Handle large sensitive data exchanges between several locations with QKD as an extra layer, complementing and enhancing your existing infrastructure.

There is no universal primitive, which would provide perfect security for all applications. Implement the ones you need.



QUANTUM RISK ASSESSMENT

In the 40 years that asymmetric encryption technology has been in use, there has never been a threat to cryptography of this scale. There will be massive upheaval and disruption. A quantum risk assessment should be part of the current risk assessment to consider what steps you should be taking to be secure in a post-quantum world.

01

What is a quantum risk assessment?

The concept behind a quantum risk assessment is to provide an organisation with an understanding of the extent of its quantum-related cybersecurity risk; plus, a timeframe in which quantum-enabled threats are likely to emerge.

02

What are the benefits of a quantum risk assessment?

It helps organisations to take a proactive approach to quantum risk management or mitigation, enabling the development of a roadmap to a quantum-safe state that would include the implementation and validation of quantum-safe solutions as a part of the normal life-cycle management, rather than as a response to a crisis. A quantum risk assessment should just be added to the traditional risk assessment.

03

What does a quantum risk assessment encompass?

Knowing what systems are doing cryptographic signing or encryption, with a clear listing all the applications, systems and devices across the organization detailing the type of cryptography and algorithms in use is essential. The goal is eventually to evaluate exposure to attack, the sensitivity of information that is being protected, and to determine if the system will need to be replaced by more agile tools.

04

Why run a quantum risk assessment?

The lack of urgency concerning cryptography is one of most significant problems facing most enterprises as they consider what steps they should be taking to be secure in a post-quantum world. In reality, in the 40 years that asymmetric encryption technology has been in use, there has never been a threat to cryptography of this scale. There will be massive upheaval and disruption and that is why it is urgent to assess now!

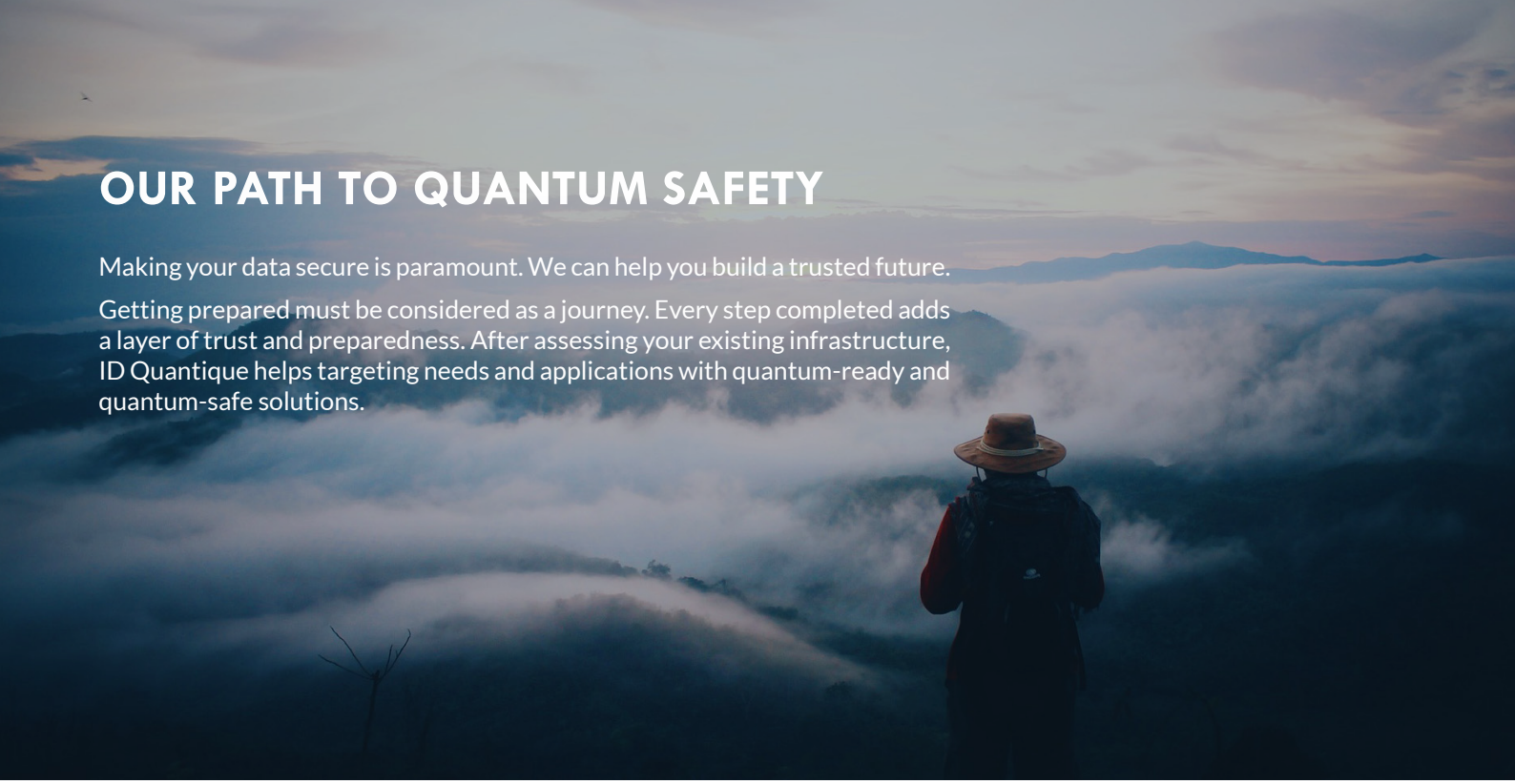
05

What if I do not have time or budget right now?

Focus on understanding the exposure to your more important, business-critical set of applications and on what allows you to run your daily business. That's the first step to getting started towards quantum readiness.

Questions? Meet our partner.

evolution



OUR PATH TO QUANTUM SAFETY

Making your data secure is paramount. We can help you build a trusted future.

Getting prepared must be considered as a journey. Every step completed adds a layer of trust and preparedness. After assessing your existing infrastructure, ID Quantique helps targeting needs and applications with quantum-ready and quantum-safe solutions.

01

Apply Quantum Random Number Generation

Good random numbers that can generate strong keys based on true randomness are the cornerstone of security.

Hardware-based QRNGs are the perfect solution, providing full entropy and inherent security while instantly strenghtening current infrastructures thanks to the fundamentals of quantum physics.

Additionally, it allows organisations to be ready to upgrade to post-quantum algorithms when they are available with software over-the-air updates.

VIEW OUR USE CASES

02

Ensure crypto-agility with Quantum-ready encryption

Planning for quantum-safe cryptography today can be tough. However, assuming organisations work on a 5-10 year upgrade cycle of their security systems, they must act now in order not to be left behind with major risks.

Crypto-agility is essential. Planning ahead of the quantum era is one thing, being ready to upgrade is another. IDQ and its partners work to ease the transition period and simply add the Quantum layer on top of organisations' existing infrastructure.

VIEW OUR USE CASES

03

Upgrade to Quantum Key Distribution

Quantum Key Distribution (QKD) is a technology designed to distribute the keys generated by QRNG securely to different locations. The technology offers proven secrecy of encryption keys and let organizations reach long-term confidentiality while maximizing trust.

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

VIEW OUR USE CASES

INTEGRATED SOLUTIONS
JUST ADD QKD ON TOP

ID Quantique works with different network encryption solutions which may be upgraded with QKD to be Quantum-Safe.

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

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. Simply use QKD as an overlay while improving your TCO and your ROI.

What do we cover?

- **Ethernet VPN** — MACsec
- **OTN/WDM encryption**
- **SSL VPN** — SSL / TLS
- **MPLS VPN**
- **IP VPN** — IPSec

Supported / PoC Vendors

IDQ · HITACHI · ABB · ADVA™ · FORTINET · THALES

LEARN MORE

AT WHAT STAGE ARE YOU?

I NEED MORE INFO

NEED A WORKSHOP ON QUANTUM TECHNOLOGIES

ID Quantique offers tailor-made workshops to introduce the added value quantum technologies can bring to your organization.

Contact us

NEED A QUANTUM RISK ASSESSMENT

Our partners can guide you through the whole process and help you build a roadmap to match your needs and priorities.

Contact EvolutionQ

LET'S MOVE ON!

READY TO IMPLEMENT QRNG

IDQ's QRNGs are available in several form factors, with different levels of performance and certifications.

Have a look at the Quantis family

READY TO UPGRADE TO QUANTUM-READY NETWORK ENCRYPTION

Get started with quantum technologies by making sure your organisation is crypto agile and ready to upgrade to quantum-safe security when the time is right.

> Turnkey solutions
> Integrated solutions

READY TO IMPLEMENT QKD

IDQ's QKD systems are commercially available today and have already been deployed in production environments in various industries.

Our products

START YOUR

QUANTUM JOURNEY

TODAY &

MAKE AN IMPACT

IN YOUR ORGANISATION.

KEEP LEARNING

More on Quantum Computing & its impact

More on QKD Technology

White Paper: What's the Q in QRNG?

White Paper: Understanding Quantum Cryptography

STAY CONNECTED

Subscribe to our newsletter

Follow us on LinkedIn

Follow us on Twitter

ID Quantique

Switzerland • South Korea
United States of America

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.