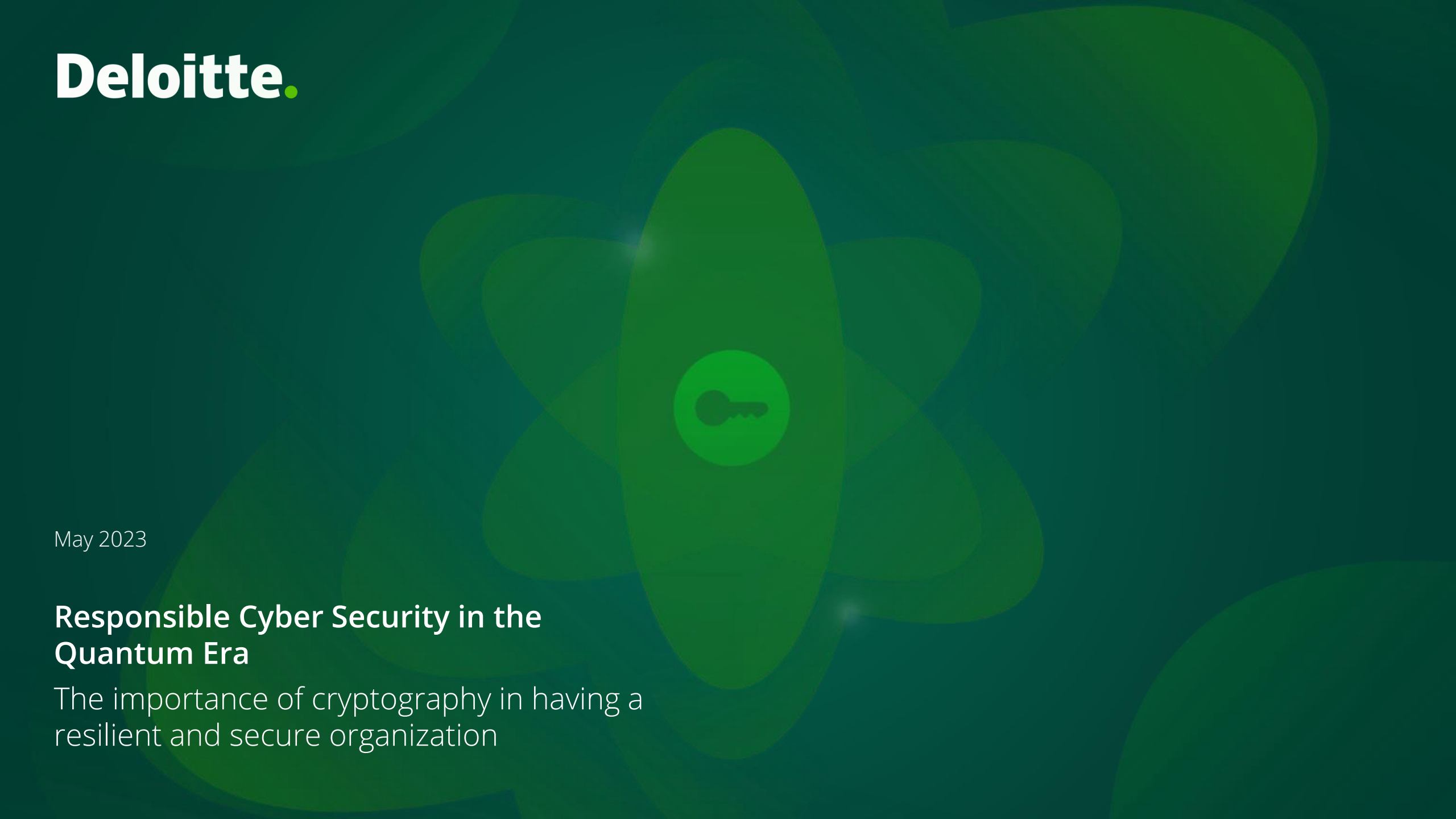
Deloitte.



May 2023

# Responsible Cyber Security in the Quantum Era

## The importance of cryptography in having a resilient and secure organization

# Cryptography is crucial to the heart of your business

The quantum threat adds yet another layer of complexity to the existing challenges of managing and implementing cryptography. As a responsible business it is essential to put this in perspective, to strive for clarity and minimize confusion.

Quantum technology is still in its early stages but gaining momentum, expected to positively impact the global economy and many industries.

Apart from the myriad of business opportunities the quantum era will bring about, it also reveals a fundamental threat to the backbone of today's digital trust. The new paradigm of quantum computing  will be able to break the mathematical difficulty underlying many of currently used cryptography.

While the risks of quantum computing are real and imminent, high-impact other attack scenarios show there is a more immediate need to pay attention to cryptography management. These cases highlight the trust we put in cryptography to protect the organisation's sensitive data.

The time to act is now. By investing in robust cryptography, we protect our businesses and our digital infrastructure from the threats of today and tomorrow. Taking action today allows us to ensure that our data remains secure and that we are prepared to face the challenges of the quantum era.

Itan Barmes
Quantum & Cryptography Security Leader

# What's inside


1 Introduction
Understand the relevance 4

2 Our approach
What steps to take 7

3 Our capabilities
How we can help 9

4 Client stories
Learn from our experience 15

5 Contact
Reach out to us 17

# Understanding quantum and cryptography in the digital age

## Quantum computing

Quantum computing is a new computing paradigm that leverages the principles of quantum mechanics to perform computations.

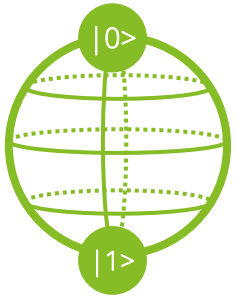
Quantum mechanics is a theory that describes the behaviour of matter and energy on a small scale, such as photons, atoms and molecules.

By utilizing the unique properties of quantum mechanics, such as superposition, entanglement, and quantum interference, quantum computers can perform complex computations that are far beyond the capabilities of classical computers.

## Bits and qubits

Qubits play a similar role in quantum computing as bits play in classical computing, but they behave very differently.


Classical bits are **binary** and can hold only a position of 0 or 1




Qubits can hold a **superposition** of all possible states

## Cryptographic algorithms

The trusted internet relies on cryptographic algorithms and the digital economy depends on its trust.

Cryptographic algorithms are embedded in the enterprise internally as well all as the organization's products and services. They help safeguard sensitive personal and financial information and verify the integrity of internet transactions, as well as the identity of users and systems.

- Digital identities - Cryptography provides the tools to associate a digital identity to people and devices
- Public-key infrastructure - The backbone of trust of the internet. Digital certificates are used to create secure communication channels and to prove authenticity and integrity of data.
- Encryption of sensitive data - Cryptography is used to encrypt sensitive data, whether it is personal health data or state secrets. Protecting data is often mandated by various regulations and a lack of compliance is associated with big fines.
- Blockchain technology - Cryptocurrencies, Decentralised Finance and Web3 all use cryptography to enable a decentralised governance system.

## The quantum threat to cryptography

The mathematical complexity of breaking the cryptography algorithms used today is beyond the capability of the fastest classical (super)computer.

However, with access to quantum computing capabilities, cybercriminals and nation-state actors can gain the ability to crack all currently standardized and widely used public-key cryptography algorithms. Even though the technology is not yet mature, attackers could conduct “harvest now, decrypt later” attacks, collecting and storing encrypted data today with the goal of decrypting the data in the future.

# 8 reasons to improve cryptography management

## For today, tomorrow and towards the quantum era

**Spearhead the change to a quantum-safe world**
With quantum computing on the horizon, your customers and partners are expecting you to keep their data secure and mitigate risks. Are you prepared to lead the way?

**Secure the products and services you sell**
Are the products, you are selling today, quantum-safe? Discover how future-proof your products and services really are.

**Prevent outages of critical business services**
You accidentally forgot to renew a security certificate. The result? Your primary service is offline for several hours. How simple mistakes can have big ramifications.

**Mitigate cyber risk**
OWASP lists Cryptographic Failures as the #2 risk that often leads to sensitive data exposure or system compromise. How do you prioritize cryptography in your cyber transformation?

**Comply with current and future regulations**
With the quantum era on the horizon, regulators are pushing for stringent measures. What's the impact? Understand the impact on your organization.

**Define who is responsible for quantum security**
Quantum and cryptographic security, who is responsible - and for what - in your organization? Proper governance is crucial in the current and future cyber landscape.

**Evaluate the impact of quantum computing**
Researchers claim to have found a way to break encryption using quantum computers. Should you be worried? Understand the impact of quantum computing on your organization.

**Secure your cloud transformation**
You are planning, or in the middle of, a cloud transformation. How to ensure your keys, certificates and secrets are secure? It's time to rethink your machine identity (PKI) management.

# Our approach consists of three phases

## 1 Discover and Assess

We help you to understand the impact of quantum computing and the importance of cryptography. By benchmarking and conducting assessments, we provide insight in the maturity of your organisation in different areas.

## 2 Design and Transform

We design the cryptography blueprint for the quantum era and guide your organization in its transformation. We give cryptography a place in the organization and provide access to our market-leading cryptographic expertise.

## 3 Manage and Operate

We deliver crypto-as-a-service, providing organizations with (semi-) managed monitoring, tooling & automation. We offer flexibility, scalability, and cost-effectiveness while you focus on your core business activities.

Cryptography is the foundation of digital trust and quantum computing is set to disrupt that foundation. It's time for organizations to stay ahead of the curve and adopt quantum-resistant cryptographic methods to protect their organization's sensitive data.

# Overview of our capabilities

## 1. Quantum & cryptography transformation

Systematically enhance your cryptographic capabilities and prepare your organization for a future with quantum computing.

**Deloitte helps organisations with a holistic perspective on the quantum threat and the necessary tools & methods for achieving strong cryptography management.**

## 2. Machine Identity (PKI) transformation

Maintain the trustworthiness and authenticity of machine identities in your digital environment by modernizing and streamlining your Public Key Infrastructure (PKI).

**Deloitte helps organisations deal with the complexity of modern IT environments and the increasing sophistication of cybercriminals targeting machine identities.**

## 3. High-value cryptographic key management

Secure and manage your most valuable assets that are used for data encryption and decryption, authentication, and digital signatures.

**Deloitte helps organisations innovate and develop new solutions securely and quickly, while being able to demonstrate compliance and security.**

# 1. Quantum & cryptography transformation

## Kickstart the transition towards a quantum-secure organisation today

**What does it encompass?**

Quantum & Cryptography Transformation is a comprehensive service offering that includes the implementation of quantum-resistant cryptographic systems to safeguard against emerging threats, as well as the enhancement of existing cryptographic capabilities to ensure security against current risks.

We help organizations future-proof their cryptographic systems, so they remain secure even as quantum computing advances.

Through our structured approach, we asses the current cryptographic infrastructure, identify improvements and develop a customized roadmap for improved security against both current and future threats. We guide you in the transformation and provide ongoing support and management of cryptographic systems.

**Why is it important to start now?**

**Future-Proofing**
Quantum computing has the potential to break current cryptographic algorithms, making it imperative to enable crypto-agility and to implement quantum-resistant cryptographic systems to safeguard against emerging threats.

**Compliance**
With the increasing number of industry regulations and data protection laws, organizations need to ensure that their cryptographic systems are compliant, and failure to do so could result in significant financial and reputational damage.

**Security**
Even without the threat of quantum computing, current implementations of cryptographic systems can be vulnerable due to misconfigurations and other improper implementations. Organizations need to ensure that their data is secure against today's risks.

OFFERING IN FOCUS

**Quantum Security Lab**
An interactive workshop that will allow you to kickstart the transition towards a quantum-secure organization.

Together we will:
1) Uncover the latest developments and insights regarding the quantum threat.
2) Discover and assess what your organization needs in order to kickstart your quantum transition.

**The outcome**
- Balanced understanding of the quantum threat
- Clear view of the drivers to take action
- Targeted plan with initiatives that your organisation should prioritise


Interactive workshop


2-5 participants


4 hours


Fixed fee

# 1. Quantum & cryptography transformation


## Capabilities

We mobilize, manage, and deliver a structured and prioritized program of work to help you transform to improved governance, quantum security, vigilance, and resilience.

### 1 Identify

Pinpoint top risks, align investments, develop an executive-led cyber risk program

### 2 Protect

Take a measured, risk-prioritized approach to defend against known and emerging threats

### 3 Detect & Monitor

Develop situational awareness and threat intelligence to detect & monitor harmful behaviour

### 4 Respond & Recover

Have the ability to recover from and minimize the impact of cyber incidents

 | 

OFFERING IN FOCUS

**PKI Maturity Assessment**
Gain insight in the security and operational efficiency of your Public Key Infrastructure (PKI). Get an understanding of how mature your current capabilities and identify areas of improvement.

Together we assess the following areas:

1) Strategy & governance
2) Architecture & principles
3) Policies, operational procedures & controls
4) Technology & tooling
5) Use cases & templates
6) Key & certificate lifecycle management

**The outcome**

- Report with valuable insights into security posture and areas for improvement

# 2. Machine Identity (PKI) transformation

## Secure your machines, transform your PKI and empower your business

**What are machine identities and how does PKI relate to it?**

Machine Identity Management is the process of managing digital certificates and their associated keys, devices, workloads, applications, containers, and other entities in a digital environment. This process is responsible for maintaining the trustworthiness and authenticity of machine identities in a digital environment.

In many organizations a key application for Machine Identity Management is Public Key Infrastructure (PKI). PKI ensures that the authenticity of any machine, a human or machine is attempting to connect to, may be verified

**Why is it important to start now?**

**Security**
A transformation can enhance the security of your Public Key Infrastructure, reducing the risk of data breaches, certificate outages, and other security incidents.

**Efficiency**
There is an increase in certificate use cases and because of that PKIs are becoming larger and more important. Outdated or inefficient PKI systems can be time-consuming and costly to manage, resulting in productivity losses and increased overheads. A PKI Transformation can streamline the system, reduce management overheads and increase efficiency.

**Future Proof**
As more devices and applications become connected to the internet, the need for machine identities will continue to grow. Implementing PKI now can help you future-proof your infrastructure and ensure that you can securely manage machine identities at scale. Starting now helps to stay ahead of the curve and secure your digital assets for years to come.

# 3. High-value cryptographic key management

## Ensure the safety of high-value cryptographic keys in confidential transactions, systems and information

**What does it encompass?**

Cryptographic keys play a critical role in securing sensitive information. High-value cryptographic keys are involved in data encryption and decryption, as well as user authentication.

If a cryptographic key is compromised, it can lead to a catastrophic breach of an organization's security infrastructure. Concurrently, having secure and effective key management in place allows organizations to innovate and develop new solutions securely and quickly, while being able to demonstrate compliance and security.

High-value Cryptographic Key Management refers to the full lifecycle of processes, systems, and people that are needed to safely generate, store, protect, and manage cryptographic keys.

**Why is it important to start now?**

### Enhanced Security

Ensures the secure management of an organization's most valuable cryptographic keys, minimizing the risk of key loss, theft, or compromise.

### Innovation and Agility

Allows organizations to develop new solutions quickly and securely, while providing the agility to respond to emerging threats and changing business requirements. This enables organizations to innovate and remain competitive in their respective markets.

### Compliance

Ensures that an organization's cryptographic key management practices are compliant with industry standards and regulations (e.g. PCI-DSS). This helps organizations avoid financial penalties and reputational damage that may result from non-compliance.

**OFFERING IN FOCUS**

### Managed Services

We offer managed solutions to outsource your key management capabilities including sound processes and procedures for repeatable and high quality execution.

### Offline Root Certificate Authority

Ensures maintaining the root private key of a trusted root CA, which is offline hosted, while you maintain full control of your key stack.

### Fully Outsourced Key Management

Focus on your core operations while ensuring your most valuable assets are kept safe and secure by outsourcing all aspects of key management.

### Key Management Tooling

Supports the end-to-end key management process including planning, documentation and execution. Provides a full audit trail and inventory of sensitive resources and keys.

# Having the right expertise on board is crucial

As quantum computing continues to advance, the need for organizations to prioritize quantum security has never been more urgent. Many organizations acknowledge the importance and are already assigning a quantum security lead to manage this topic for success in this challenging transition.

The quantum and cryptography transformation is an ongoing journey to ensure that organisations stay up to date with latest developments in the quantum security and cryptography field.

A Quantum Security Officer (QSO) needs to have real domain knowledge but also needs a strategic view, management buy-in and the ability to connect different business units within the organization. Moreover, the QSO will set priorities and deal with governance structures.

In addition, someone that understands quantum security can identify and implement quantum-resistant encryption methods that can protect sensitive data. This is particularly important as quantum computing and technology continues to evolve rapidly, and new threats and vulnerabilities may emerge.

# Learn from our experience

## 1. Quantum & cryptography transformation

Deloitte helped a Global Healthcare Manufacturing Company in kickstarting their transformation to a quantum-secure organization.

**Relevant key activities**

- Conduct a quantum security lab with key stakeholders, engaging participants with practical, interactive exercises.
- Provide insights into the latest developments and emerging trends regarding the quantum threat.
- Identify and assess the requirements necessary to kickstart the organization's quantum transition.
- Identify key obstacles and goals to drive the agenda forward.
- Foster teamwork and idea sharing.

**The outcome**

We provided a comprehensive understanding of the quantum threat, including its potential impact on an organization's cryptographic infrastructure and security posture. Based on this understanding, we determined priorities for action, highlighting the most critical areas that require attention and investment.

Drawing on our expertise and experience, we developed a custom roadmap that outlines key actions and milestones necessary to prepare for the quantum era. This roadmap is tailored to the organization's specific needs, taking into account their unique context, goals, and constraints.

## 2. Machine Identity (PKI) transformation

Deloitte supports a Global Life Insurance Provider in their Machine Identity (PKI) Transformation. The client is a global insurer with a strong reputation for providing reliable and secure insurance products to its customer.

**Relevant key activities**

- Conduct multiple interviews to map out where, and in what way, cryptography was used across the organization.
- Analyse findings, taking into account the long-term business goal of the client. The output of the engagement was a current state assessment and a proposed 3-year roadmap.
- Help with sketching the high-level architecture of various cloud components.
- Help the client to align their technical crypto capabilities with the overall business strategy to ensure a scalable, robust and secure infrastructure.

**The outcome**

With Deloitte's machine identity (PKI) transformation in place, the client has a more secure and reliable way to manage and protect their digital certificates and keys. This helps the client better protect their sensitive data, including customer information, from cyber threats and data breaches, ultimately improving customer trust in the company's products and services.

Overall, Deloitte's support in machine identity (PKI) transformation proves to be instrumental in helping the client enhance their cybersecurity posture and maintain their reputation as a trusted insurance provider.

## 3. High-value cryptographic key management

Deloitte supports a leading Dutch Oil & Gas Corporation in their High Value Cryptography Key Management with consultancy services. The client is a leading Dutch oil & gas company that operated in multiple countries and has a large customer base. The network completes transactions with a total value of over 10 billion per month.

**Relevant key activities**

- Payment card provider, payment security and key management expertise.
- Advice on implementing key technologies like EMV and migrations of cards data.
- Cryptographic consultancy on a broad variety of topics (HSMs, ApplePay, EMV, etc.)
- Owner of custom HSM firmware to support client specific wishes
- Innovation sessions for future technologies

**The outcome**

With Deloitte's high-value cryptography key management advice, the client has taken big steps in their security transition. The client has a more secure and reliable way to protect their technologies, firmware and cryptographic keys. This helps the client to better protect their sensitive data, including trade secrets, financial information, and personal data, from cyber threats and data breaches, ultimately improving customer trust in the company's products and services.

Thanks to Deloitte's support, the client has strengthened their cybersecurity posture and maintain their reputation as a trusted oil & gas provider.

**CONTACT**

# Please reach out to us if you have any questions


## Itan Barmes

Specialist Leader – Quantum & Cryptography Security Lead

+31650098170
ibarmes@deloitte.com



## Niels van de Vorle

Partner – Cyber Lead North South Europe

+31882882186
nvandevorle@deloitte.com



## Marc Verdonk

Partner – Risk Advisory Innovation Lead

+31652615027
mverdonk@deloitte.com

CONTACT

# Read more about quantum & cryptography security

## Quantum computers and the Bitcoin blockchain

An analysis of the impact quantum computers might have on the Bitcoin blockchain

Does Quantum Supremacy, as announced by Google, mark the demise of currently used cryptography? And of Bitcoin in particular? We present a balanced view regarding the risks that quantum computers pose to Bitcoin.

https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html

## Managing the quantum cybersecurity threat

Cryptographic agility in the quantum era

What might organizations face when quantum computers materialize and threaten existing cryptographic algorithms? And what steps can they take to keep their data secure? A new white paper in collaboration with the World Economic Forum (WEF) has the answers.

https://www2.deloitte.com/nl/nl/pages/risk/articles/managing-the-quantum-cybersecurity-threat.html

## Managing cyber risk in the quantum era: a responsible approach

Focus on facts and clarity; embrace change

How can organizations properly prepare for the cyber risk from quantum computing? The quantum computing threat is causing organizations to take a “back-to-basics” approach to manage cryptography capabilities, mitigate risk, and prepare for future cybersecurity challenges.

https://www.deloitte.com/global/en/services/risk-advisory/blogs/managing-cyber-risk-in-the-quantum-era-responsible-approach.html

Deloitte.