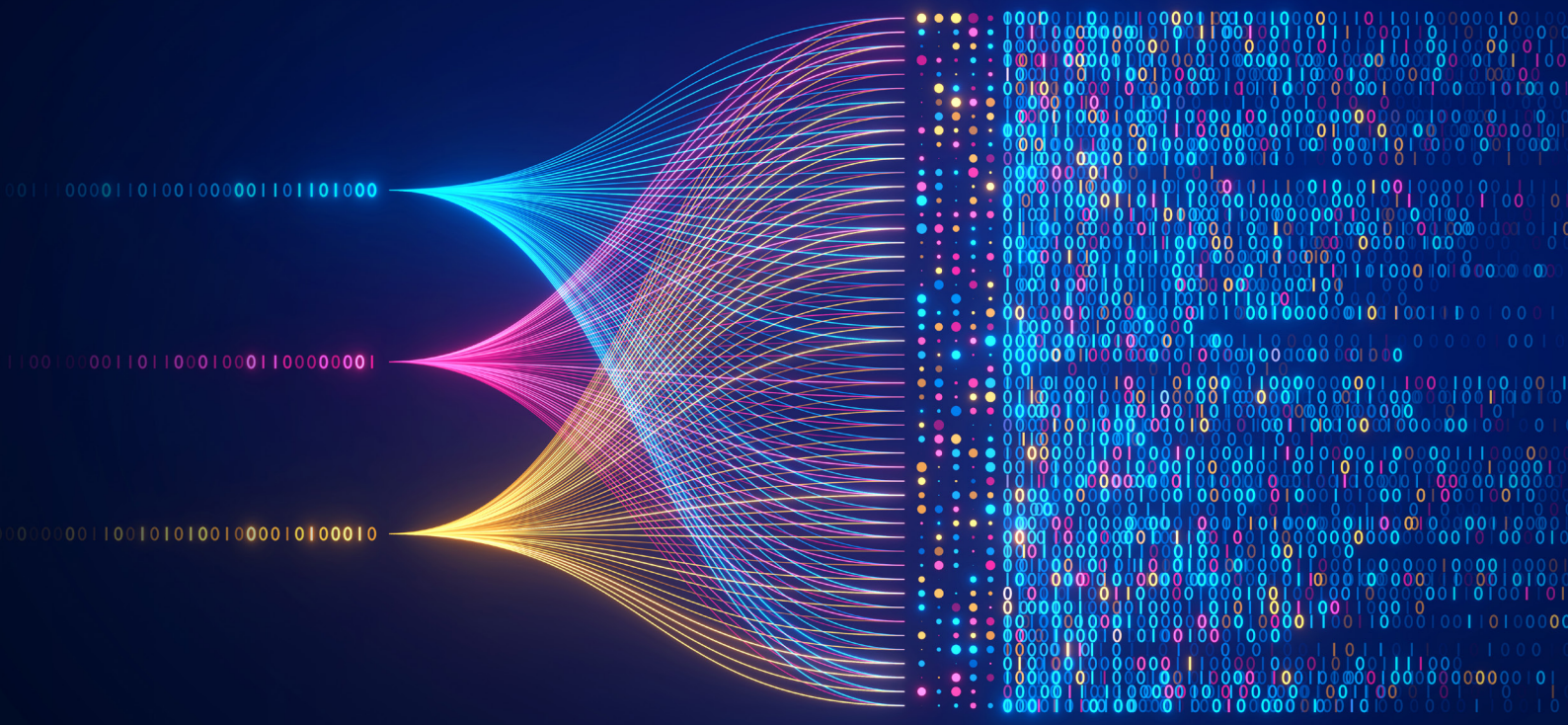
EVIDEN

Post-quantum migration guide

The essentials
Revised edition 2024



Management summary

Does the notion of a hacker penetrating your corporate network and reading your encrypted emails while accessing your company's most sensitive data disturb you? This scenario is more realistic than one might think, when cryptographically relevant quantum computers will be available one day. At that point all crypto systems based on RSA, Diffie-Hellman, or ECC can be easily attacked. These cryptographic mechanisms represent the current security bedrock and are used billions of times in web browsers, email clients, smartphones, VPN solutions and operating systems.

Fortunately, it's not that far yet. While quantum computers already exist, current models are far too weak and noisy to break any real cryptographic system. But the technology is significantly progressing and therefore the need for quantum-resistant alternatives is becoming more and more obvious. Such "postquantum cryptography" (PQC) methods already exist. After years of academic research, some of these are now ready for standardization. CRYTSTALS-Kyber (key exchange) and CRYSTALS-Dilithium (digital signatures) are currently considered the most promising schemes.

Independently from post-quantum cryptography, so-called quantum key distribution protocols (QKDs) have been developed. QKD protocols are based on quantum mechanics themselves and can't be broken with quantum computers. However, the QKD technology is still in its infancy and not suited to replace current key exchange systems in typical corporate or government IT environments. For this reason, QKD is not covered in this document.

Now that post-quantum cryptography is becoming ready for practice, migration to it represents one of the most significant challenges in the IT world. Protocol designers, cryptography vendors, system integrators, and administrators are facing a major task for the years to come.

One obvious challenge is that post-quantum methods require more computing resources than the currently utilized RSA, Diffie-Hellman, and ECC schemes. Proposed PQC methods use public and private keys that are significantly longer than the ones of current systems while the overall performance is lower. This can be especially challenging for platforms with limited resources such as smart cards and smart tokens.

Because the currently proposed post-quantum cryptographic algorithms are not as mature as their conventional counterparts, experts agree that more analysis is needed. For the same reason, the need for crypto agility, the ability to rapidly transition to an alternative method without making significant changes to the environment, is crucial. Organizations that will be able to implement changes between cryptographic algorithms in running systems will be best prepared for the risks of a particular algorithm being broken in the future.

Migration strategies that include shutting down all classical cryptographic systems and starting all the post-quantum alternatives at once are, of course, not realistic. Instead, it is recommended to plan a phased migration project which may include hybrid crypto methods (i.e., a combination of pre- and post-quantum algorithms) for a transition phase. Eviden recommends to structure such a project as follows:

1. Project setup
2. Crypto inventory creation
3. Understanding of your risks
4. Organization and policies impact assessment
5. Executive sponsorship buy-in
6. Migration execution

This guide outlines the major steps of making your corporate IT environment quantum-resistant and illustrates how the major challenges can be solved. Moreover, it will show what Eviden can do for your enterprise or your authority in order to enable a smooth transition to the post-quantum world. Feel free to contact us for further information.

Contents

Introduction **4**

Quantum computers 4

Post-quantum cryptography 5

Quantum key distribution 5

Standardisation 6

The road to a post-quantum world 7

Legislation 8

Migration to post-quantum crypto systems **9**

General 9

Requirements for simple migration 9

Steps of the migration process 10

Project set-up 10

Crypto inventory creation 11

Impact, risk, and cost assessment 13

Quantum-migration readiness evaluation 14

Executive sponsorship and buy-in 14

Migration execution 15

Understanding post-quantum cryptography **16**

What Eviden can do for you **17**

Consulting 17

Our crypto products 17

Conclusion 18

Contributors **19**

Introduction

Quantum computers

Quantum computers represent a completely new way of building computer systems. Contrary to conventional IT devices, they are based on the priciples of quantum mechanics, which allows for designs that are not possible in traditional architectures. Quantum computers are a promising future technology. Among other things, they can be used for the following applications:

- Quantum computers can support research in chemistry and thereby curb global warming[1];
- Quantum computers are able to solve various problems in drug development[2];
- Quantum computers can increase the performance of autonomous vehicles[3];
- Quantum computers can be used for artificial intelligence[4];

There are also interesting applications of quantum mechanics in cryptography. These include quantum random number generation (QRNG), which can be used to generate secret keys, and quantum key distribution (QKD), which is provably secure against many attacks.

Apart from this, quantum sensors for radar, navigation, imaging and particle detection represent a promising technology for the future. They significantly outperform conventional sensors in terms of sensitivity, spatial resolution and time resolution and can be used in areas such as medicine and engineering.

And then, quantum computers can break current crypto systems, including RSA, Diffie-Hellman and others.

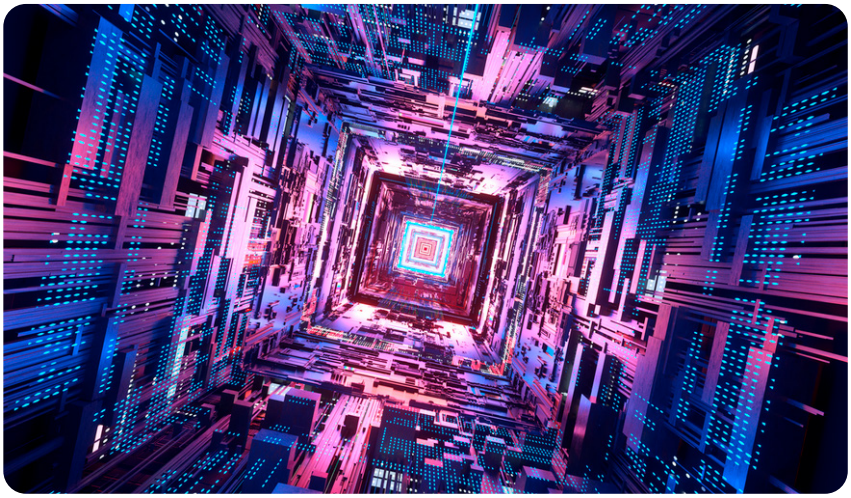
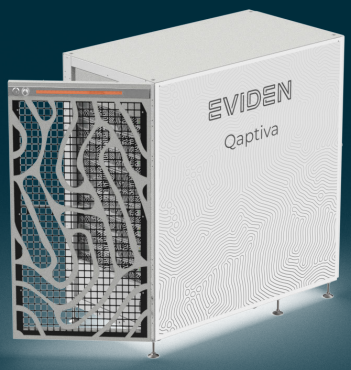


Figure 1: Quantum computers are a promising technology for the future. Among other things, they can be used to break certain crypto methods.

Did you know that Eviden:

- offers Qaptiva, a comprehensive NISQ computing environment to optimize, compile, and emulate code on noisy and noiseless qubits or run code on a QPU;[5]?
- sells appliances that emulate hundreds of qubits?
- can help you adopt quantum computing technology?
- enables development of quantum algorithms on any device with myQLM, python package?



1. https://www.weforum.org/agenda/2019/12/quantum-computing-applications-climate-change/
2. https://pharmafeatures.com/drug-discovery-quantum-computing/
3. https://www.newsweek.com/ibm-using-quantum-computing-help-automotive-industry-solve-ev-traffic-problems-1637827
4. https://www.researchgate.net/profile/V-Moret-Bonillo/publication/265642441_Can_artificial_intelligence_benefit_from_quantum_ computing/links/54f0b8090cf2b36214aae3a2/Can-artificial-intelligence-benefit-from-quantum-computing.pdf
5. https://atos.net/en/solutions/high-performance-computing-hpc/quantum-computing-qaptiva

Post-quantum cryptography

As we have explained in our "Introduction to post-quantum cryptography" whitepaper[6], there are serious threats to IT security posed by quantum computers. Imagine that a hacker is capable of penetrating almost any corporate network or connecting to the same private network as your employees and spying on it. Assume that the same hacker can read all encrypted emails and network communications that they encounter, as if they were plain text. Finally, imagine that this attacker can hijack every protected WWW and VPN connection within reach.

All this might happen one day, because it is expected that there will be quantum computers being capable of factorizing large prime number products. In this paper we will qualify such machines as "cryptographically relevant quantum computers". Devices of this kind could be used to break several important cryptographic algorithms, including RSA and Diffie-Hellman, two systems that are used billions of times in web browsers, connected objects, email clients, smartphones, ATMs, etc. A dystopian digital apocalypse would become reality.

Fortunately, we're not there yet. Although quantum computers already exist, current models can at most decompose two-digit numbers into their factors. To threaten current asymmetric systems such as RSA or Diffie-Hellman, they would have to manage a similar operation with a 700-digit number. This will not be feasible to do today or tomorrow. Nevertheless, numerous organizations are currently conducting intensive research on quantum computers, which results in constant performance improvements.

For the reasons mentioned, it is imperative to research viable alternatives to RSA, Diffie-Hellman and other systems that are vulnerable to cryptographically relevant quantum computers. Fortunately new methods already exist, and they are grouped under the term **post-quantum cryptography**.

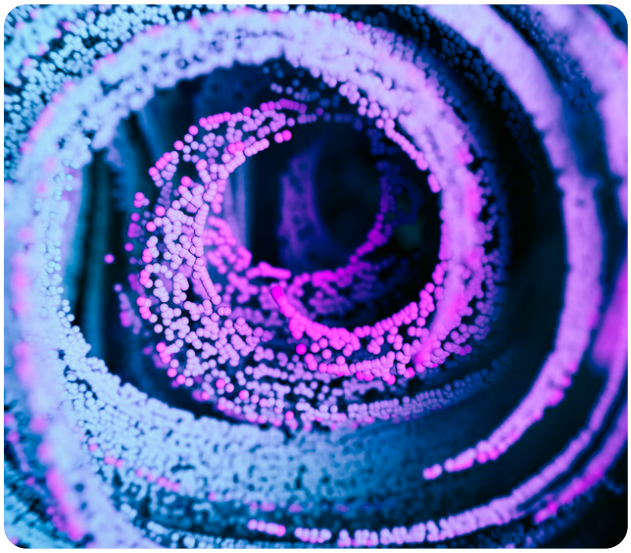
So far, post-quantum cryptography methods are rarely used in practice, and there is not a large historical research base to draw from. However, significant progress is being made. Several post-quantum methods have recently emerged as viable RSA and Diffie-Hellman alternatives with which we can venture into the new epoch.

This guide focuses on the migration path to post-quantum cryptography. It outlines the major challenges of making your corporate IT environment quantum-resistant and illustrates how these challenges can be solved. Moreover, it will show what Eviden can do for your enterprise or your authority in order to enable a smooth transition to the post-quantum world.

Quantum key distribution

Quantum key distribution (QKD), sometimes referred to as quantum cryptograpy, is another quantum-safe cryptographic technology. QKD protocols are based on quantum mechanics themselves and can't be broken with a quantum computer. However, it is important to note that QKD requires dedicated hardware and is limited by factors such as distance and the need for line-of-sight communication. In addition, QKD doesn't cover all functional use cases of asymmetric cryptography, and it lacks maturity in practical deployments.

It is generally expected that the use of QKD will be limited to high-end military and national security communication conducted in dedicated networks. A position paper published by the ANSSI (France), the BSI (Germany), the NLNCSA (Netherlands) and the SNCSA (Sweden) confirms this view.[7] This means that QKD is not relevent for a current post-quantum migration project. For this reason, QKD is not covered in this document.



6. https://www.cryptovision.com/en/download-access

7. https://cyber.gouv.fr/sites/default/files/document/Quantum_Key_Distribution_Position_Paper.pdf

Standardization

In 2017, the US National Institute of Standards and Technology (NIST) launched a competition pitting post-quantum cryptographic methods against each other.[8] Experts from all over the world were invited to submit suitable algorithms to a selection process where the best methods would be identified and standardized. This competition included both signature algorithms and encryption/key-exchange methods. The final result was to be a portfolio of reliable post-quantum crypto schemes suitable for different purposes based on diverse mathematical foundations.

NIST admitted 69 of the submitted methods into the competition. In July 2022, after three rounds of evaluation, four winners were announced: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+. The two CRYSTALS methods are expected to become the preferred algorithms for the next decades with CRYSTALS-Kyber being used for key exchange and CRYSTALS-Dilithium for digital signatures.

The NIST jury also identified four additional candidates (later reduced to three, as one algorithm proved unsecure) for further analysis and evaluation in a fourth round. Depending on the results of this process, more winners might be announced in the near future.

Of the numerous algorithms in the competition, only few signature methods proved both secure and practicable. On top of that, these methods generate relatively long signatures that are costly to verify. In 2022, the NIST therefore launched an additional post-quantum competition for signature methods only, with a particular call for the submission of algorithms with short and easy-to-verify signatures.[9]

Currently, 40 methods are being scrutinized in a first round.

It is anticipated that the winning algorithms from these post-quantum competitions will be incorporated in numerous standards and products worldwide. For instance, the German Federal Office for Information Security (BSI) and the French IT security agency (ANSSI) are expected to adapt the NIST recommendations accordingly.

The Internet Engineering Task Force (IETF), the Internet's standardization body, will likely adopt the NIST competition winners, too. In addition, the IETF has published two "Requests for Comments" (RFCs) specifying post-quantum procedures that didn't take part in the NIST competitions, namely the signature schemes XMSS (RFC 8391)[10] and Leighton-Micali (RFC 8554)[11].

8. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
9. https://csrc.nist.gov/projects/pqc-dig-sig/round-1-additional-signatures
10. https://www.rfc-editor.org/rfc/rfc8391.html
11. https://www.rfc-editor.org/rfc/rfc8554.html

The road to a post-quantum world

It is not possible to make serious predictions about when quantum computers will be available, so assumptions have to be made. The National Security Agency (NSA), the United States' cybersecurity authority, mandates that the owners and operators of national security systems start using post-quantum algorithms no later than 2035.[12] The German BSI operates on the working hypothesis that pre-quantum crypto methods will become insecure in the early 2030's.[13]

All currently available post-quantum methods differ from RSA and Diffie-Hellman in major respects. Most significantly, the keys of post-quantum algorithms are often considerably longer than the keys of conventional schemes. For instance, the public keys of CRYSTALS-Kyber and CRYSTALS-Dilithium are several times larger than the ones of RSA and Diffie-Hellman (see Figure 2). Other proposed post-quantum algorithms even require hundreds of thousands of public-key bits more. The situation is not much different when it comes to private keys. In addition, many key generation, signing and verification operations become less performant when post-quantum cryptography is used.

Most experts recommend **hybrid cryptographic mechanisms** for a transition phase. A hybrid cryptographic mechanism combines a pre-quantum public key algorithm, such as RSA, and a post-quantum method, such as CRYSTALS-Dilithium, such that an attacker needs to break both schemes to be successful. This combination provides protection from both quantum computers and potential weaknesses in post-quantum algorithms.

If hybrid schemes are used, two approaches can be employed. The **composite approach**, on the one hand, provides for a hybrid signature (consisting of two signatures) to be stored in one signature field. The composite approach has the advantage that the existing formats, which are almost all designed for just one signature only, do not have to be changed. The **non-composite approach**, on the other hand, provides for two signature fields being used when a hybrid scheme is employed. The non-composite method usually requires the message format to be extended, as most specifications are based on the assumption that only one signature is utilized.

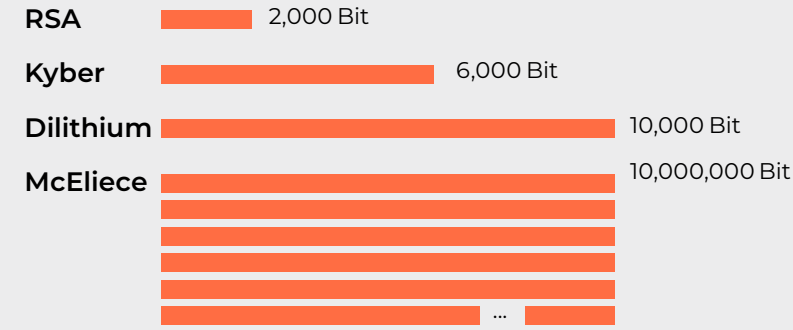


Figure 2: The public keys of most post-quantum algorithms are longer than the ones of conventional crypto systems such as RSA.

Several hybrid cryptographic network protocols are currently being standardized. Among the most important ones are hybrid variants of S/MIME, OpenPGP, TLS, and IKEv2. Public Key Infrastructures (PKI), including X.509 digital certificates, are likewise being adapted.

Unfortunately, there are different opinions about the use of hybrid crypto mechanisms.[14] While the German BSI and the French ANSSI clearly recommend the implementation of this approach, other IT security authorities advise against it. The EU organizations ETSI and ENISA allow the use of hybrid systems, but they don't state a recommendation for or against them. Hopefully, further analysis will lead to eventual agreement amongst the experts.

Migration to post-quantum methods will become easier if the crypto algorithms used in an IT system are easily interchangeable. This paradigm is known as **crypto-agility**. Ideally, a crypto solution allows for changing the algorithms used by mouse click. In addition, it should be possible to introduce new crypto methods without having to recompile the code.

The migration to post-quantum cryptography is inextricably linked to the crypto-agility paradigm. Only with crypto-agile solutions, a simple and fast switch to quantum-proof methodes becomes possible. Undoubtedly, consumer demand will drive crypto-agile development, while manufacturers will strive to meet this shift in focus. Standards, benchmarks, and certifications all will evolve. Post quantum migration plans will heavily depend on the crypto agility of the components involved.

12. https://fedscoop.com/nsa-sets-2035-deadline-for-adoption-of-post-quantum-cryptography-across-natsec-systems/
13. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.html
14. https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

Legislation

The migration to post-quantum cryptography is a hot governmental topic in many countries. It is expected that nations that adapt quantum technologies early will have advantages in terms of productivity, economic growth, health, sustainability, and national security and resilience. Among others, the state authorities in the USA (CISA, DHS, NIST), UK (DSI&T), Germany (BSI), France (ANSSI) an EU Level (ENISA) Country occupy themselves with PQC preparedness strategies.[15]

There are especially many activities of this kind in the USA. For instance, in 2021 the U.S. Department of Homelands Security together with the NIST published a guideline, "Post-Quantum Cryptography".[16]

In 2022, U.S. president Biden signed the Quantum Computing Cybersecurity Preparedness Act[17], which encourages federal government agencies to adopt technology that will protect against quantum computing attacks. U.S. government agencies were required to provide a full inventory of active cryptographic systems by May 2023.

15. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.html
16. https://www.dhs.gov/quantum
17. https://www.forbes.com/sites/forbestechcouncil/2023/01/25/what-the-quantum-computing-cybersecurity-preparedness-act-means-for-national-security/#:~:text=7535%2C%20the%20Quantum%20Computing%20Cybersecurity,and%20deploy%20quantum%2Dresilient%20cybersecurity

Migration to post-quantum crypto systems

General

Now that new standards are within reach and crypto vendors are adapting their products, it is time for enterprises and authorities to occupy themselves with post-quantum cryptography, as well. The current outlook dictates migration to PQC methods within the next ten years. A phased project dealing with this task should be planned. Considering that large organizations typically use dozens, if not hundreds, of crypto applications, a considerable amount of resources will be required.

It is important to note that not all cryptographic implementations are affected by cryptographically relevant quantum computers in the same way. Symmetric algorithms, such as AES and Triple-DES, do not need to be replaced by new cryptographic systems. Instead, it is sufficient to use these ciphers with appropriate key lengths. 256 bits are expected to withstand even the most powerful cryptographically relevant quantum computers.

In many systems, 256-bit keys are already in use. When this is not the case, hardware and software implementations often allow for a key-length change by mouseclick. If this is not supported, the program code needs to be changed. However, it is not necessary to introduce a completely new encryption technology to make symmetric cryptography quantum-proof.

Things are different with RSA and Diffie-Hellman, as they will have to be replaced by completely different algorithms. This is also true for other asymmetric crypto systems, including Fiat-Shamir, DSA, and systems based on elliptic curves (ECC).

As not all applications of asymmetric cryptography can be attacked the same way, the following distinctions should be made:

1. Encryption and key exchange: Asymmetric algorithms used for this purpose can not only be attacked at the time their of use, but also much later (store now, break later). For instance, an attacker may try to decipher an encrypted email that was sent years earlier. Because of this threat, the transition to post-quantum encryption should be made as soon as possible.

2. Data signatures: Signed payload data may be subject to a "store now, break later" attack, too. For example, an attacker might want to tamper with signed information that was created years earlier. However, data can be resigned with a post-quantum scheme at a later stage, if necessary.

3. Authentication signatures: Signatures used for authentication, as utilized by protocols such as TLS and IKE, are verified immediately. If the signature is correct, the signer is granted access, otherwise they are rejected. Signatures of this kind have no value at a later stage. For this reason, the migration of authentication signature schemes is less time-critical than the applications mentioned previously.

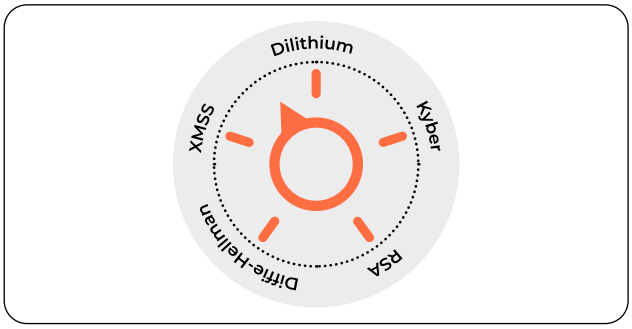


Figure 3: Crypto implementations should allow for easily changing the algorithms used. This concept is referred to as crypto agility.

As mentioned above, some experts recommend hybrid crypto mechanisms for a transition phase. If you follow this advice, your IT systems not only must be made post-quantum ready but also be prepared for hybrid crypto use. In many cases, this will prove challenging, as it is often easier to replace an algorithm than to introduce the support of several algorithms at the same time.

Requirements for simple migration

It is expected that migration to post-quantum cryptography will become easier when the crypto technology used in an organization meets the following requirements:[18]

- The operator understands all compliance requirements.
- The operator has an inventory of all crypto assets.
- A Certificate Lifecyle Management (CLM) in place.
- A Key Management System (KMS) is used.
- Crypto algorithms are not hard-coded. Instead, the applications used are crypto-agile.
- The operator is prepared to use crypto algorithms that are slower and use longer keys than the ones in place.
- Crypto libraries are kept up-to-date, software that is no longer supported is phased out.

18. Paul van Brouwershaven, PKI Consortium Chair, at the PQC Conference in March 2023

Steps of the migration process

Migration to post-quantum cryptography in your organization should follow a structured approach. The ETSI report on migration strategies[19] recommends the typical steps of such a project. In alignment with this guidance, Eviden has developed a detailed migration scheme. This business- and practice-oriented process consists of six key steps:

1. Project setup
2. Crypto inventory creation
3. Understanding of your risks
4. Organization and policies impact assessment
5. Executive sponsorship buy-in
6. Migration execution

Project set-up

To begin with, a company or authority planning to migrate to post-quantum cryptography must start with an initial analysis. Such an analysis usually includes the impact and potential damage of security incidents caused by quantum-prone components, as well as the threat of downtime and compliance breaches. Budgeting should also be an issue in this step.

The results of the analysis will help the organization to better understand the quantum threat and its impacts on the IT infrastructure. They need to be presented to the management in order to obtain the necessary support. If the management agrees, a larger migration project is launched.

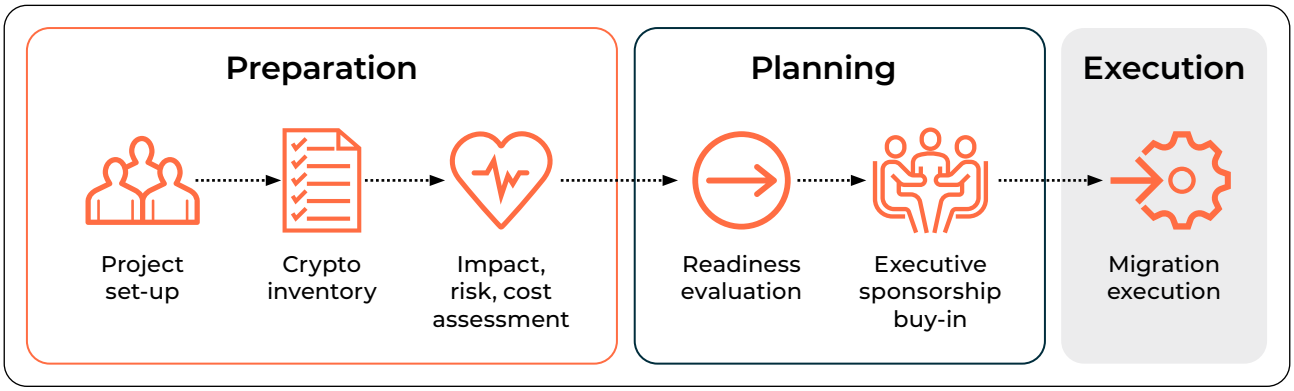


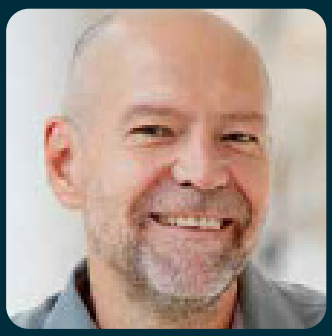
Figure 4: Eviden's post-quantum migration scheme

"Post-quantum migration is a major task for the years to come. A crypto inventory yields valuable insights for organizations and often shows risks that need to be addressed right now."

Simon Ulmer, Eviden

19. https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

Why we should hurry	... carefully
• Possible quantum technology breakthrough • Migrating will be long and complex • Some data need long-term protection • Attackers are storing data now to decrypt it later	• No standards yet • Network protocols are not ready yet • Migration will be hard • Lack of skills • Interoperability challenges • No security certification available yet



"Post-quantum algorithms differ from conventional crypto schemes in many subtle details. Post-quantum Migration therefore requires considerable expertise and experience."

Markus Hoffmeister, Eviden

Crypto inventory creation

Before the actual migration to post-quantum cryptography can take place, it is essential to know where cryptography is used within the organization. Determining the full scope of crypto-enabled applications or infrastructure components can be daunting. Typical applications using cryptography include PC operating systems, web-browsers, VPN solutions, IP telephones, and smartphone apps. In many cases, users are not even aware that cryptography is being utilized.

To address this challenge, a catalog of all cryptographic applications and infrastructure components needs to be compiled. Such a crypto inventory will contain concise information about each component using cryptography, including:

- Component manufacturer
- Hardware or software solution
- Component purpose
- Cryptographic algorithms used (asymmetric and symmetric, although the latter are less exposed)
- Keys and key stores
- Digital certificates
- Protocols
- Cryptographic providers and libraries

In addition, a crypto inventory should detail infrastructure components, such as a Public Key Infrastructure (PKI) and include certificate policies and certification practice statements.

The level of detail that each assets record in a crypto inventory must observe should strike a clear balance between full exhaustivity and the capacity to start the migration in time. Operational constraints may warrant a continuous improvement approach that includes updating or adding new information to the inventory over time when applied.

Eviden and their partners provide tooling that support the generation and maintenance of a crypto inventory. Despite the automation potential, some tasks may still have to be done by hand as they require institutional knowledge and understanding of IT and business aspects of an organization. Identifying the components that use cryptography may not be readily available to inventory scans and could be overlooked.

As not all assets might be discovered at once, crypto inventory creation and update should be a continuous process in the organization and never be stopped. Additionally, every new application project has the potential to change the crypto inventory by starting or stopping to use cryptography, changing its infrastructure layers or modifying its risk profile.

Figure 5: Eviden and its partners use tools that support the creation and maintenance of a crypto inventory.

Did you know that Eviden Strategic Cybersecurity Advisory teams have developed a methodology for this “first level business risk analysis”?

Learn more in “What Eviden can do for you” at the end of document.

Impact, risk, and cost assessment

In this step, every entry of a crypto inventory must be assessed with respect to its impact on the organization and the risk associated if it isn't made quantum-resistant in time. Impact considerations should include a review of contracts, and ideally contracts should include a mention if a solution is, or must be, made quantum-ready.

On the other hand, the risks of using post-quantum cryptography need to be considered. Switching to post-quantum algorithms might lead to incompatibilities and result in unexpected downtime and service interruption. Additionally, migration risks of invalid implementation must be taken into account.

For performing a post-quantum risk assessment, it is not necessary to reinvent the wheel. Instead, it is possible to add a post-quantum part to a general risk assessment according to ISO 27005, NIST SP 800 30, or OCTAVE.[20] In addition, several post-quantum specific risk-assessment frameworks are currently developed and tested:

- CARAF (Crypto Agility Risk Assessment Framework),[21]
- Mosca's Quantum Risk Assessment,[22]
- Wells Fargo PQC Risk Model.[23]

Based on these frameworks, Eviden has developed its own method, the PQC Risk Based Awareness Assessment (RBA2), which includes the following steps:

- Establish the Context: Identify PQC use cases, objectives, and assets
- Risk Identification: Identify PQC threats vulnerabilities, controls, sovereignty levels
- Risk Analysis: Determine likelihood and impact for the given timeline
- Risk Evaluation: Calculate PQC priority score
- Risk Treatment: Develop recommendations action plan for PQC non-compliance risk mitigation

Figure 6: The steps of a quantum risk assessment as applied by Eviden

Did you know that Eviden Strategic Cybersecurity Advisory teams have developed a methodology to help you create, maintain, and continuously improve your crypto inventory?

Learn more in "What Eviden can do for you" at the end of document.

20. https://www.sisainfosec.com/blogs/comparison-between-iso-27005-octave-nist-sp-800-30-sisa-blog/
21. https://academic.oup.com/cybersecurity/article/7/1/tyab013/6289827
22. https://globalriskinstitute.org/publication/gri-quantum-risk-assessment-report-part-1/
23. https://www.youtube.com/watch?v=sP0DsBZWpLs

Quantum-migration readiness evaluation

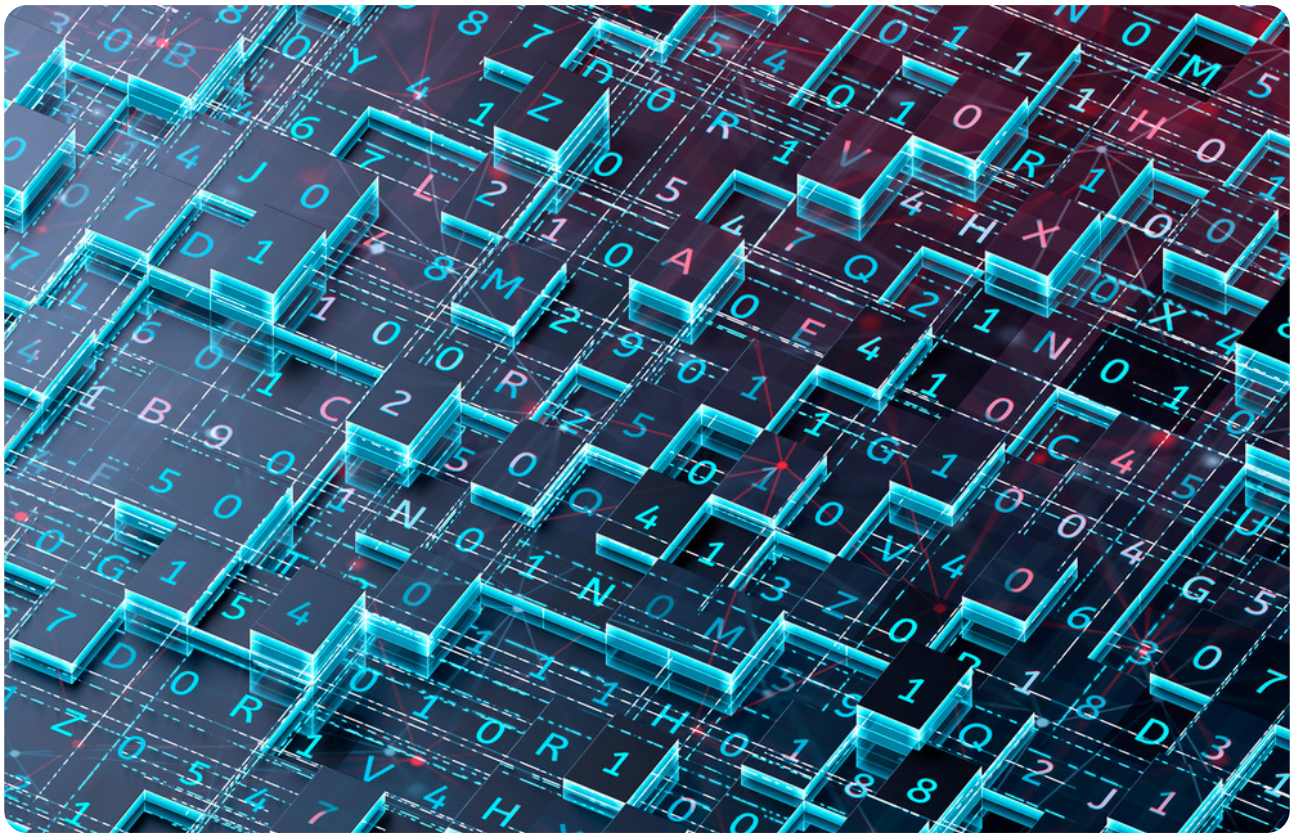
Migrating applications listed in the crypto inventory will have varying degrees difficulty. To produce a meaningful overview, it is recommended that systems be classified according to the quantum migration readiness evaluation scheme:

1. **PQC-ready:** The application already supports (asymmetric) post-quantum methods or sufficient (symmetric) key lengths.
2. **Crypto-agile:** The application is not PQC-ready but is designed to support crypto-agility.
3. **PQC readiness plan:** The application is not crypto-agile but the vendor has a PQC readiness plan.
4. **Readiness option:** There is no PQC readiness plan for this application yet, but there is potential for one in the near future.
5. **No readiness option:** The application might never be PQC ready.

Since creating a crypto inventory and assessing it according to different criteria is a comprehensive task, it is recommended to have such a catalog checked assessed by a third party. External validation of quantum migration readiness evaluation strategies will become a standard procedure. It is highly likely these audits will be required by legal regulations and governed by evaluation standards. Standardized evaluation schemes and certificates for the successful implementation may evolve. However, these developments are still in their infancies.

Executive sponsorship and buy-in

After having completed the previous steps, it is necessary to reinvolve the management of your organization. At this juncture, you will need to explain the executives why post-quantum migration is necessary and what risks appear if this process is delayed. In addition, you need to provide a budget planning for the migration project. After evaluating this information, the management board will be well prepared to decide how to proceed with the migration project.



Migration execution

Now that the challenges and risks of post-quantum migration are understood, and the project is planned and budgeted, execution can finally begin. Since it is impossible to perform all replacements at once, prioritization is necessary.

Typically, organizations target the infrastructure with critical priority. This is especially true for the PKI, because standardized post-quantum algorithms will need to be deployed there first before any certificate-based application can be made post-quantum ready.

The schedule for the replacement should be administered based on the following criteria:

- State of the art of quantum computers: Currently, it seems unrealistic that quantum computers capable of breaking current crypto systems will become available before 2030. However, advances in this technology should be monitored and, if necessary, the migration process should be accelerated.
- State of the art of post-quantum cryptography: Although post-quantum cryptography has made considerable progress in recent years, there will be new developments. For example, none of the three digital signature algorithms chosen by the NIST solves all issues, and therefore new ones are being evaluated in a new competition. With the advent of new methods, the project plan might have to be amended.
- Dependence from infrastructure: Some crypto solutions rely on a user management or procurement system. Asymmetric crypto systems usually use digital certificates provided by a PKI. It is evident that components can only be updated if the infrastructure it relies on has been migrated. Conversely, stand-alone systems, such as a component using symmetric cryptography without external key management, can be addressed independently from any infrastructure.
- PQC readiness: Of course, only PQC ready components can be migrated.
- Risk: Components with a high risk of being attacked or with a high damage potential are prioritized. The riskiest items should be migrated first, then followed by less critical components.

It is clear that resources required for the actual migration need to be planned. Staff must be provided and trained. Ongoing managing migration projects should also include monitoring the current state of quantum computer technology and the PQC readiness of the systems in the crypto inventory. Ideally, a crypto inventory will be updated during the migration, as well as when new applications are introduced.

Every new addition to the crypto inventory, should lead to restarting steps 3 to 6 (understand risk, organization and policies impact assessment, executive sponsorship buy-in, and migration execution) for the newly added scope.

Understanding post-quantum cryptography

Eviden is aware that post-quantum cryptography will only succeed when developers, consultants, IT managers, administrators, and IT executives all come to grips with it. This leads to a challenging situation, as the mathematics behind post-quantum cryptography is complex and differs significantly from the principles that have prevailed in cryptography to date. For instance, understanding CRYSTALS-Kyber and CRYSTALS-Dilithium is more difficult than comprehending systems like RSA and Diffie-Hellman.

Because this degree of crypto literacy is not widely prevalent, Eviden is actively involved in many activities that aim to help explain post-quantum cryptography to non-specialists in many diverse ways. Eviden has developed explanatory models for post-quantum cryptography based on cartoons and everyday analogies. The comic illustrations, which are distinctive worldwide, have been published in whitepapers and magazine articles[24] and are presented with audience acclaim at leading security events across the globe.

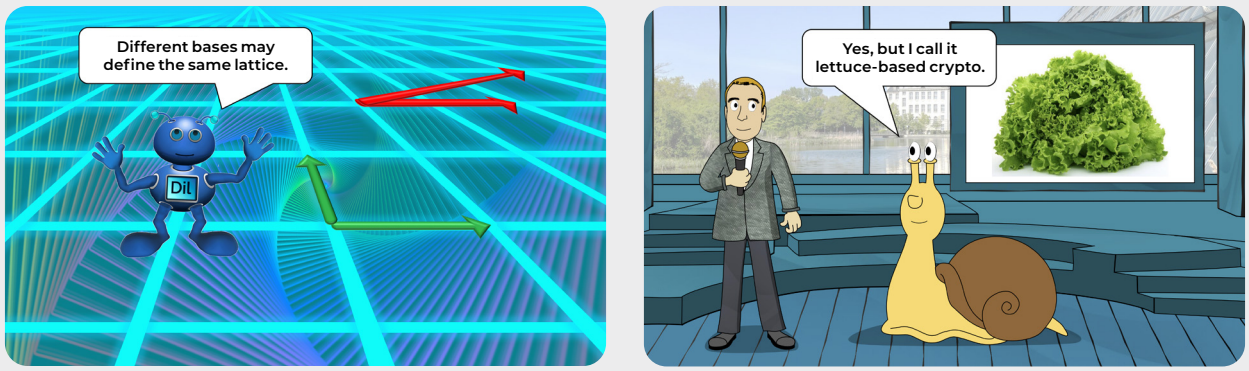


Figure 7: Eviden explains post-quantum cryptography with such graphics, which are also understandable for non-mathematicians.

Figure 8: Eviden employees speak about post-quantum crypto at conferences and exhibitions worldwide.

24. https://www.cryptovision.com/wp-content/uploads/2021/06/VAULT_Post-Quantum-Cryptography_062021.pdf

What Eviden can do for you

Consulting

Eviden is a leading specialist in post-quantum migration consulting. We stand for a comprehensive, step-by-step approach to your post-quantum migration, supported by our quantum-resistant cybersecurity products. Among other things, we support you in the following tasks:

- Develop your “first level business risk analysis” aiming at assessing the extent of the program,
- Create, maintain, and continuously improve your crypto inventory,
- Assess quantum-migration risks based on Eviden’s PQC Risk Based Awareness Assessment (RBA2) framework,
- Check the quantum readiness of your crypto solutions, choose alter-natives if necessary,
- Raise awareness in your organisation through presentations and publications.

Eviden is involved in several European post-quantum research and development projects. Our customers benefit from strong partnerships with leading encryption and auditing technology companies.

Our crypto products

IDnomic PKI
IDnomic PKI is a powerful, multi-purpose PKI software suite, compliant to highest security standards. IDnomic PKI is crypto-agile in design and capable of issuing hybrid certificates (composite and non-composite). It enables a smooth migration path from conventional crypto systems to post-quantum algorithms. IDnomic PKI can be easily extended with other Eviden solutions that enable user-side key management, complex workflows and other features.

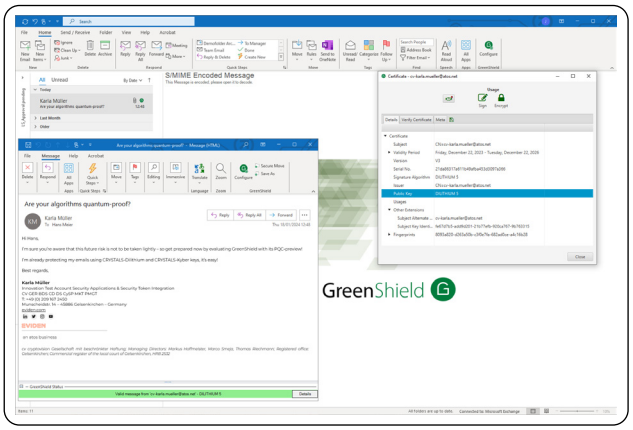


Figure 9: cryptovision GreenShield encrypts and signs emails and files. It features a PQC Preview Module, which enables the use post-quantum algorithms.

CardOS
CardOS is a high-security focused, multi-functional smart card operating system, providing all functions to cover different applications via contact-based and contactless interface. CardOS will support post-quantum algorithms in the near future.

Evidian IAM
Evidian IAM is a suite of products that protect companies from attacks by unauthorized users. Evidian IAM supports numerous security protocols and crypto mechanisms. These will embrace the post-quantum signature and encryption standards currently defined by the NIST in the near future.

cryptovision Greenshield
Eviden‘s cryptovision GreenShield is a software solution for encrypting and signing emails and files. It is approved for the exchange of classified information (EU restricted, NATO restricted, German VS-NfD) and accredited by the German BSI and the EU-Council. Cryptovision GreenShield is fully crypto-agile. It features a PQC Preview Module, which enables post-quantum and composite signatures with CRYSTALS-Dilithium, and post-quantum encryption with CRYSTALS-Kyber.

IDnomic Certificate Monitor
IDnomic Certificate Monitor enables the complete discovery of your fleet of digital certificates. It is therefore ideal to create a crypto inventory. In addition, it provides a centralized Interface to manage the certificate lifecycle, and it enables automatic renewal of digital certificates.

Trustway
The Trustway Proteccio product line consists of several certified Hardware Security Mo-dule (HSM) appliances. Trustway Proteccio has integrated the post-quantum signature schemes CRYSTALS-Dilithium (signature algorithm), CRYSTALS-Kyber (key exchange mechanism) and will be released in first half of 2024.

The VPN solution, Trustway IP Protect, will support CRYSTALS-Kyber (Key exchange mechanism) between two Trustway IP Protect VPNs.

Conclusion

Eviden is an expert in the fields of quantum computing and crypto-graphy. Based on this unique expertise, Eviden is your ideal partner in all questions of post-quantum cryptography. Eviden's cryptography products, including HSMs, email encryption software, smart cards, and PKI systems, are currently made quantum-proof. Some of these solutions have post-quantum algorithms already included.

Most importantly, Eviden supports your organization in the post-quan-tum migration process. We advocate for a comprehensive, step-by-step approach that assists you in achieving your migration goals on time and within budget. We are pleased to provide support with crypto inventory-ing, risk assessment, awareness, product selection, project management, and all other aspects of post-quantum migration.

For more information, please contact: cybersecurity@eviden.com

Contributors

Editor in Chief:
Klaus Schmeh
Chief Editor Marketing
klaus.schmeh@eviden.com

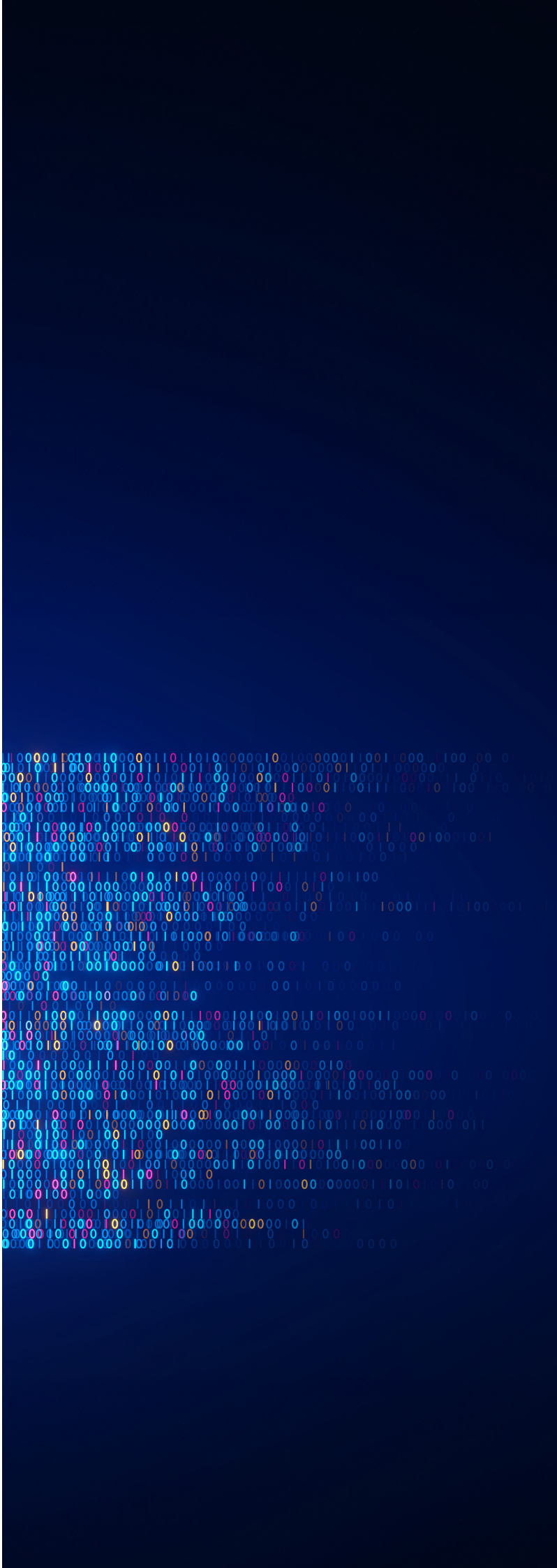
Cryptography, PKI, Certificate Lifecycle Management:
Markus Hoffmeister
BDS Cyberproducts – Digital ID – Strategic Advisor
Managing Director cv cryptovision GmbH
markus.hoffmeister@eviden.com

Crypto Inventories, Certificate Lifecycle Management, Risk Assessment:
Simon Ulmer
Group VP - Head of Digital ID – BDS Cyberproducts
Eviden Scientific Community member
simon.ulmer@eviden.com

PQC Products:
Vasco Gomes
Cybersecurity Products CTO
Digital Security Offerings Technology Lead Eviden Scientific Community member
Cybersecurity Distinguished Expert
vasco.gomes@eviden.com

PQC Risk Assessment:
Sławomir Pijanowski, Ph.D.
Global GRC Practice Leader, Global Cybersecurity Consulting
Eviden Distinguished Expert
slawomir.pijanowski@eviden.com

PQC Organisation and Coordination:
Anastazija Zivkovic
Security Advisor
Global Cybersecurity Consulting
anastazija.zivkovic@eviden.com



Connect with us

eviden.com