EVIDEN

EVIDEN
MINDSHARE
2024

Securing the Digital Future:

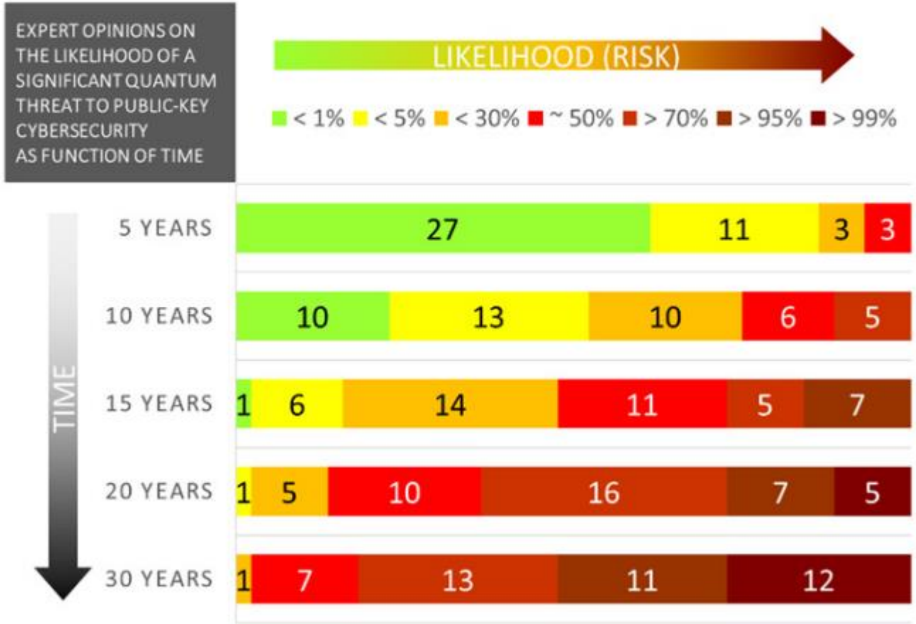
The Role of Post-Quantum Cryptography Consulting

Anastazija Zivkovic,
Global Cybersecurity Consultant,
Global PQC Consulting Lead,
PhD in PQC Candidate

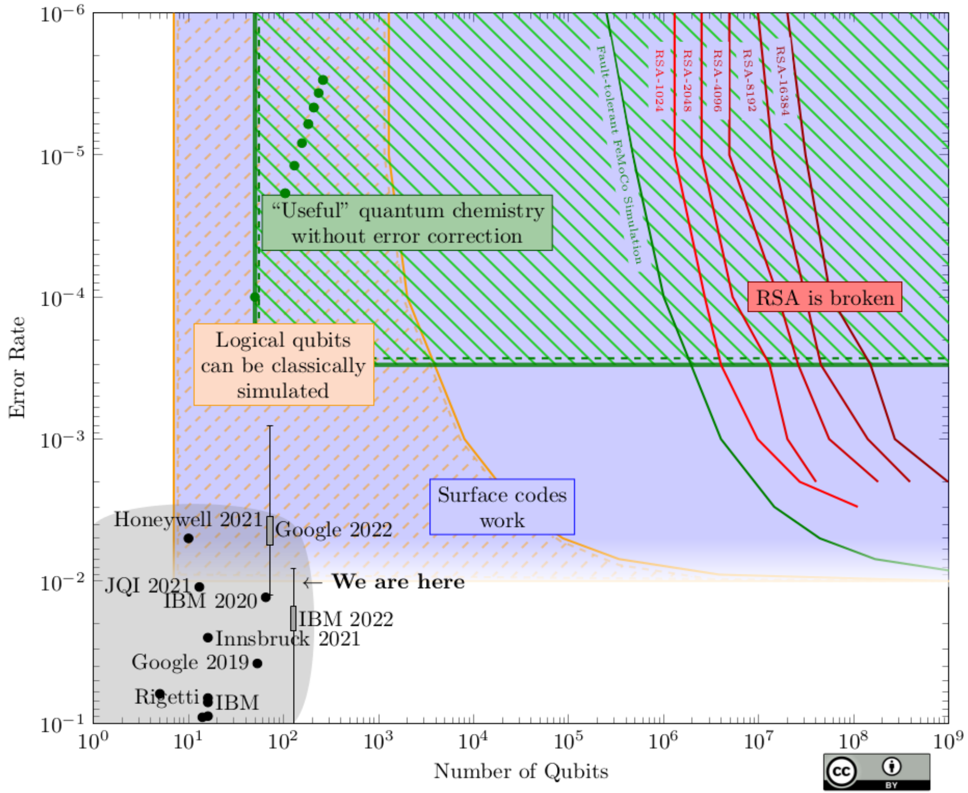
The Quantum Threat

Are you ready?

- Quantum computers can break current encryption
- RSA and ECC -> vulnerable to quantum attacks
- Experts predict major risks in the next decade
- **Urgent need for quantum-safe security**

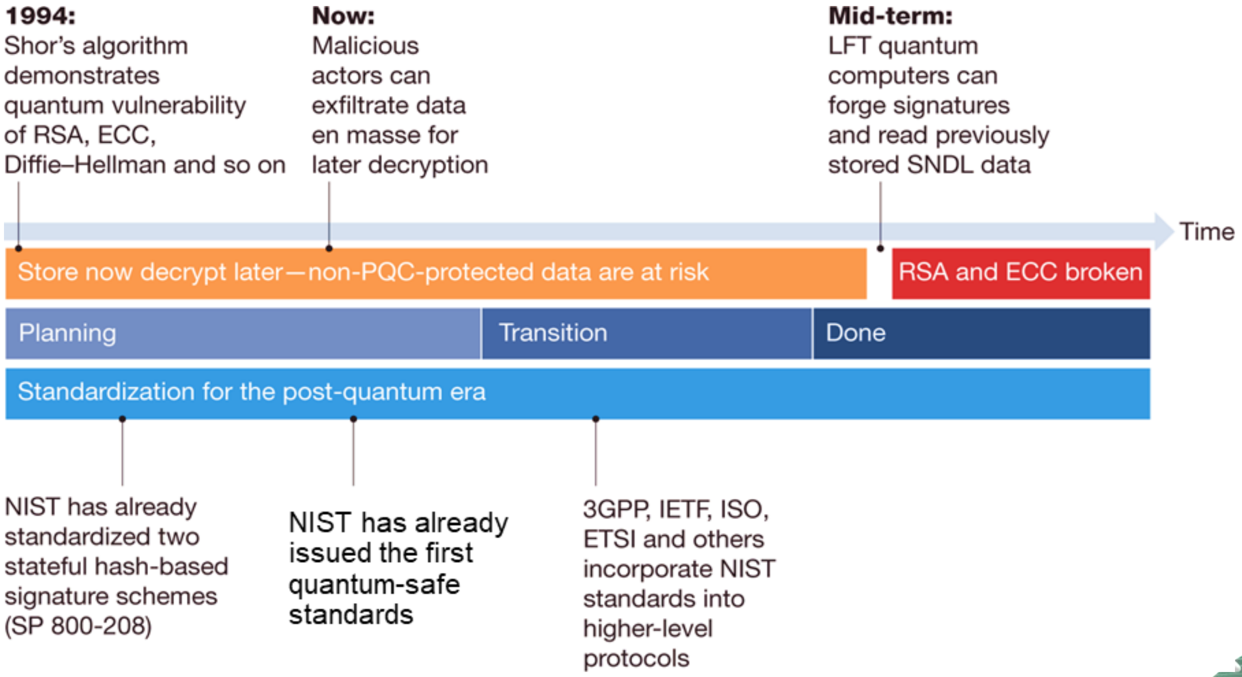


Numbers reflect how many experts (out of 44) assigned a certain probability range.


Error Rate
10^{-6}
10^{-5}
10^{-4}
10^{-3}
10^{-2}
10^{-1}
Number of Qubits
10^{0}
10^{1}
10^{2}
10^{3}
10^{4}
10^{5}
10^{6}
10^{7}
10^{8}
10^{9}
"Useful" quantum chemistry without error correction
Fault-tolerant FeMoCo Simulation
RSA-1024
RSA-2048
RSA-4096
RSA-8192
RSA-16384
RSA is broken
Logical qubits can be classically simulated
Surface codes work
Honeywell 2021
Google 2022
JQI 2021
IBM 2020
← We are here
IBM 2022
Innsbruck 2021
Google 2019
Rigetti
IBM

Introduction to the Post-Quantum Cryptography

Why PQC Matters?



1994:
Shor's algorithm demonstrates quantum vulnerability of RSA, ECC, Diffie–Hellman and so on

Now:
Malicious actors can exfiltrate data en masse for later decryption

Mid-term:
LFT quantum computers can forge signatures and read previously stored SNDL data

Time

Store now decrypt later—non-PQC-protected data are at risk

RSA and ECC broken

Planning

Transition

Done

Standardization for the post-quantum era

NIST has already standardized two stateful hash-based signature schemes (SP 800-208)

NIST has already issued the first quantum-safe standards

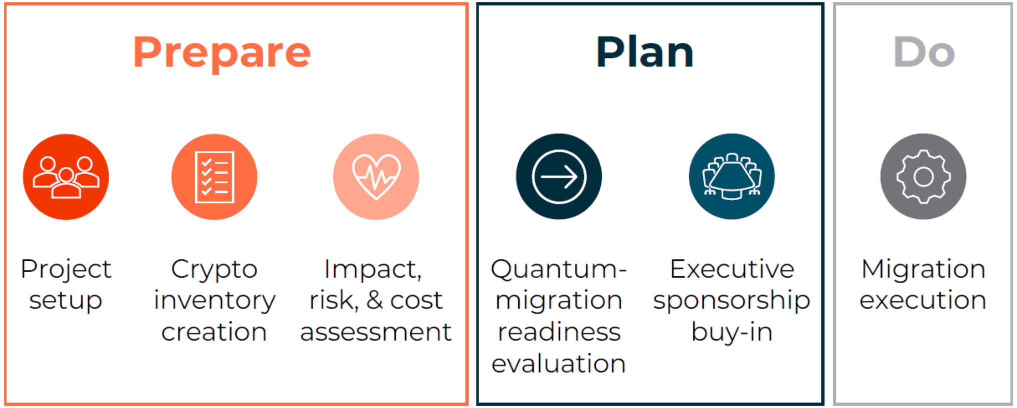
3GPP, IETF, ISO, ETSI and others incorporate NIST standards into higher-level protocols

The Need for PQC Consulting

How to Create Order in Quantum-Caused Chaos?

What to Discuss?

- Assessment Strategies
- Frameworks
- Regulations
- Current Market



Prepare

Project setup

Crypto inventory creation

Impact, risk, & cost assessment

Plan

Quantum-migration readiness evaluation

Executive sponsorship buy-in

Do

Migration execution

1 Economical Advantage
PQC Migration Preparedness

- Hot Governmental Agenda Topic, due to the fact countries that will be the first to develop quantum technologies, will have vast advantages in terms of productivity, economic growth, health, sustainability, and national security and resilience.
- Country Level PQC Preparedness strategies: US (CISA, DHS, NIST), UK (DSI&T), Germany (BSI), France (ANSSI) or EU Level (ENISA).
- Evolving standardization of PQC Algorithms (first standards are already here)

2 Investments in the PQC Market, Research

- Growing demand for advanced security solutions due to an increasing number of data breaches, Global investment and competition are increasing (rapid pace & scale).
- Quantum cryptography as a solution: quantum cryptography is gaining attention as an effective solution due to its use of quantum mechanics principles to secure data transmission, making it highly resistant to hacking attempts.
- Rising adoption of quantum cryptography: organizations seek quantum cryptography solutions to enhance their data security & protect against cyber threats

3 Protection of strategic digital assets of countries, businesses ahead of time

- More data is being produced, it's critical to **control** it at every step (in rest, in transit and in use) and in any location (On premise, in the cloud…)
- Geopolitical tensions accelerating information & trade war, industrial espionage, etc.
- There are announcements of the BSI and the NSA that PQC will be required by frameworks and by the law within a decade.

ISO 27005 Risk Assessment integrated with PQC Risk Frameworks

Overview

Service Summary

ISO 27005 standard expand the risk management methodology of the information security management system created according to ISMS-ISO 27001 standard. Atos facilitates organizations Risk Assessment activities and establish initial context to identify, Analyze and evaluate risks for treatment.

Business Value

Cybersecurity Risk Assessment Service provides you with a systematic approach which enables your organization to identify and understand your information security risks. It allows Business organizations to prioritize, choose risk treatment options and implement relevant and appropriate controls to effectively and efficiently prevent security incidents. It enables risk-based compliance.

Objectives

- Provide assurance the organization Business Information Security practices
- Demonstrate value of the Information Security Management System - ISMS to Management
- Comprehensive approach to integrate ISMS, PIMS and BCMS
- Establish foundation for company compliance practices.

Activities

- Assessment planning & kickoff
- Scope definition
- Risk assessment activities
- Interviews
- Evidence collection & review as basis for risk information, i.e. threat catalogue, vulnerabilities, control effectiveness, etc.

Phases - Deliverables

I	• Project planning & charter • Scope document
II	• Assessment documents based on organization requirements
III	• Risk Assessment and treatment plan Report
IV	• Executive summary report

Risk Assessment Frameworks vs PQC Risk Assessment Frameworks

Old Topics – New Buzzwords?

NIST SP 800-30
ISO/IEC 27005
OCTAVE
NIST CSF
Mosca's model
Crypto agility

- focuses on risk of technology
- focuses on information security
- focuses on operational and organizational view
- focuses on known threats
- focuses on risk from quantum timeline
- CARAF focuses on... **CRYPTO AGILITY**

Crypto Agility:

-> an organization's or system's capacity to quickly adjust to modifications in the cryptographic technologies and protocols it employs.

PQC Risk Assessment Frameworks – Mapping Table

What is really new?

ISO 27005	PQC Specifics
Establishing the context	Mosca Theorem: x+y < z; x + y > z
Risk identification	There PQC specific threat, but impacts remain similar – data loss or disclosure
Asset Inventory (Asset Management Process)	Assets protected by current classic encryption tools, algorithms
Risk analysis	CARAF Risk = Timeline * Cost (it is not a proper risk definition)
Risk Evaluation (compare risk vs risk limit acceptance, tolerance criteria)	Risk acceptance criteria should be driven by Country or Regional Preparedness Strategy (EU ENISA), French ANSSI as part of input to business risk acceptance of PQC Impact
Risk treatment	Risk Treatment is not yet fully available – migration roadmap is in fact evolving risk treatment plan. Quantum-Safe Algorithm are being developed
Communication & Consultation Risk Review & Monitoring	Risk Monitoring relies on PQC Disruptive Trends, Technologies monitoring

PQC Risk Assessment Frameworks – Mapping Table

What is really new?

ISO 27005	CARAF* - Crypto Agility Risk Assessment Framework	GRI - A Methodology for Quantum Risk Assessment or Mosca's Quantum Risk Assessment (QRA)
Establishing the context	n/a	Phase 1: Identify and document information assets, and their current cryptographic protection. Phase 4: Identify the lifetime of your assets "x", Phase 4: Identify the time required to transform the organization's technical infrastructure to a quantum-safe state "y".
Risk identification	Phase 1: Identify threats	Phase 3: Identify threat actors and estimate their time to access quantum technology "z".
Asset Inventory (Asset Management Process)	Phase 2: Inventory of assets	GRI is Phase 1 and partially Phase 4
Risk analysis	Phase 3: Risk estimation	Phase 5: Determine quantum risk by calculating whether business assets will become vulnerable before the organization can move to protect them. (x + y > z)
Risk Evaluation (compare risk vs risk limit acceptance, tolerance criteria)		N/a: Lack of clear definition risk acceptance criteria, x + y > z is a general risk limit which an organization must adopt.
Risk treatment	Phase 4: Secure assets through risk mitigation	Phase 6: Identify and prioritize the activities required to maintain awareness, and to migrate the organization's technology to a quantum-safe state.
Communication & Consultation Risk Review & Monitoring	Phase 5: Roadmap	Phase 2: Research the state of emerging quantum computers and quantumsafe cryptography. Estimate the timelines for availability of these technologies. Influence the development and validation of quantum-safe cryptography.

POC Migration Recommendations

Key Approach to the PQC Migration

EVIDEN

France ANSSI views on the Post-Quantum Cryptography transition March 25, 2022 Post-quantum transition roadmap (gradual transition)

3-phase roadmap:

Phase 1 (today): Mandatory pre-quantum security, optional PQC, no claimed quantum resistance..

Hybridization to provide some additional post-quantum defense-in-depth to the pre-quantum security assurance. This phase should last until after NIST's first standards are announced and it is planed to last until after 2025. Note: NIST has already announced first standards (!).

Phase 2: Mandatory pre-quantum security, optional PQC with claimed quantum resistance.
Hybridization to provide post-quantum security assurance while avoiding any pre-quantum security regression.

Phase 3 (probably not earlier than 2030):
Optional standalone PQC with claimed quantum resistance.

Source: anssi-technical_position_papers-post_quantum_cryptography_transition.pdf

ETSI TR 103 619 v.1.1, CYBER: Migration strategies and recommendations to Quantum Safe schemes

Stage 1 - Inventory compilation

- Starting and end states of migration
- Inventory compilation
- Business process requirements for stage 1
- Appointment of a migration inventory manager & Allocation of budget for inventory compilation

Stage 2 - Preparation of the migration plan

- Creation of the migration plan
- Migration issues
- Considerations for migration impact on hardware-based security environment
- Key management during migration
- Trust management during migration
- Isolation approaches during migration
- Access to non-QSC protected resources after migration
- Business process requirements for stage 2

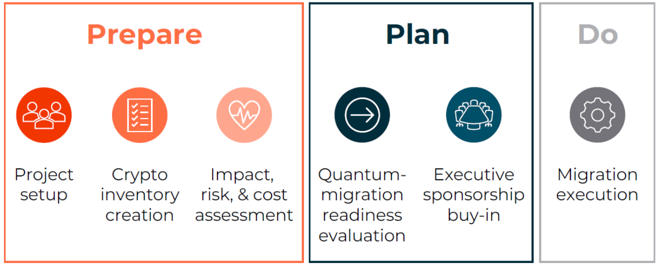
Stage 3 - Migration execution

- Migration management
- Mitigation management
- Business process requirements for stage 3

Annex A: Migration checklist

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

Eviden PQC Steps of the migration process


Prepare
Plan
Do
Project setup
Crypto inventory creation
Impact, risk, & cost assessment
Quantum-migration readiness evaluation
Executive sponsorship buy-in
Migration execution

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

Post-quantum cryptography - PQC migration guide - Atos

Eviden’s PQC Risk Based Awareness Assessment (RBA²)
-> GRI & ISO 27005

PQC Asset Inventory

Identify and document information assets, and their current cryptographic protection.

Identify assets being subject of current encryption in view of the below:

x = data value time

y = migration time

z = threat timeline

Disruptive Resilience PQC/AI, etc. Trends Update

Research the state of emerging quantum computers and quantum-safe cryptography.
Estimate the timelines for availability of these technologies. Influence the development and validation of quantum-safe cryptography issues.

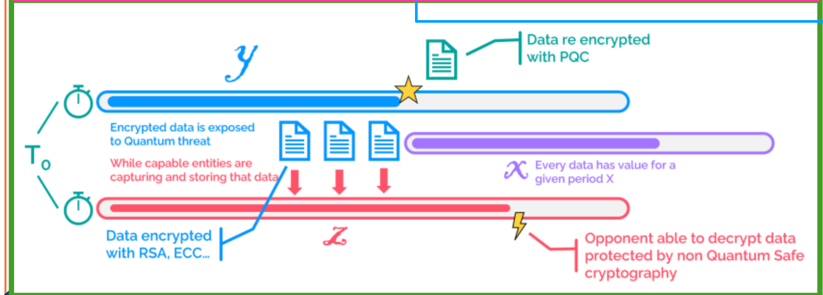
Threat Timeline “z”

Identify threat actors, and estimate their time to access quantum technology “z”.

Timeline Data Value “x” Quantum Safe State “y”

Identify the lifetime of your assets “x”, and the time required to transform the organization’s technical infrastructure to a quantum-safe state “y”

Establish the context

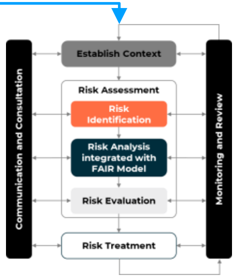


y
Data re encrypted with PQC
T0
Encrypted data is exposed to Quantum threat
While capable entities are capturing and storing that data
x
Every data has value for a given period X
Data encrypted with RSA, ECC...
z
Opponent able to decrypt data protected by non Quantum Safe cryptography

PQC Risk Impact Assessment x+y > z

Determine quantum risk by calculating whether business assets will become vulnerable before the organization can move to protect them. (x + y > z)

Z = PQC Risk: For every data type where **x + y > z**, then worry now



PQC Risk Treatment Strategy / Roadmap

Identify and prioritize the activities required to maintain awareness, and to migrate the organization’s technology to a quantum-safe state.

Migration to quantum-safe controls.

Action Plan / Roadmap

Ensure you have a current, thorough organizational inventory which includes details of embedded cryptography that may exist in a variety of products;

- Monitor your environment for threats, and ensure that you conduct regular risk assessments;
- Conduct a quantum risk assessment as part of or subsequent to the regular risk assessment process;
- Understand your telecommunications and security vendors’ posture on quantum computing, which of their products will be affected and their preparations to manage this risk;
- Evaluate quantum readiness as part of your current procurement processes for network and security systems; and ask your current vendors to discuss the state of their quantum planning;
- Work with an informed partner to track developments in quantum computing and quantum safe solutions, and to establish a roadmap to quantum readiness for your organization.

WEEKS TBD	WEEKS TBD	WEEKS TBD	WEEKS TBD

Basic schedule: TBD weeks +/- customer maturity or specifics TBD weeks: assumption: customer is available for the project, key expert plus supporting consultants

PQC Cybersecurity Risk Assessment - Mutual Cooperation to Succeed

Risk Assessment Exemplary Deliverables:

- Identification of Client's business decisions and business value protection for risk assessment is to be performed.
- Decision: What methodology to choose: Clients or Atos. Discussion, Feedback, Final Decision
- Conduction of risk assessment according to agreed methodology
- Collecting evidence supporting risk information
- Iterative approach on agreeing contents of Risk Assessment and Risk Treatment Report
- Final Presentation of Risk Assessment Results
- Optional adjustments after feedback from Presentation meeting to key Client's Stakeholders
- Decision on eventual further support in Risk treatment recommendations implementation or completion the activities

Client 's Exemplary Responsibilities:

- Appoint single point of contact for the project duration
- Identify respective stakeholders and operational coordinators for specific domains of Client's organization
- Organize logistics for meetings arrangements and assure all required people are attending the meeting and after meetings supervising timely providing information on action plan.
- Provide asset inventory based on which risk assessment will be conducted
- Create or modify missing, not relevant, outdated information in asset inventory impacting results and completeness of risk assessment
- Appoint owners(s) for conducting risk assessments
- Be available for Risk Assessment Training
- Conduct Risk Assessments under Eviden guidance
- Participate in Risk Treatment Planning

Eviden – Post-Quantum Cryptography

Helping Customers Prepare Their Migration

Raising PQC awareness

Communication

- Dedicated website
- Whitepapers
- Migration Guide
- articles

Presentations & Talks

- 16+ talks at major events since 2018 in multiple languages, across the globe and online

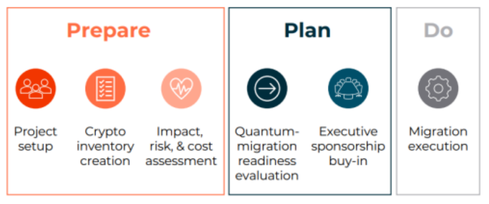
Crypto-Agility
McEliece
Dilithium
Kyber
DH
RSA
Switch to another crypto method should be possible at the touch of a button.

PQC migration Services

PQC Journey Preparation

- PQC Education - Risk Based Awareness & Assessment
- PQC Risk assessment report ith recommendations
- PQC Risk Awareness Maturity Assessment (QuRisk)
- PQC Migration Roadmap Elaboration
- Crypto Inventory (infra, data, keys)

PQC Journey Implementation


Prepare
Project setup
Crypto inventory creation
Impact, risk, & cost assessment
Plan
Quantum-migration readiness evaluation
Executive sponsorship buy-in
Do
Migration execution

PQC ready Products

Q4 2023

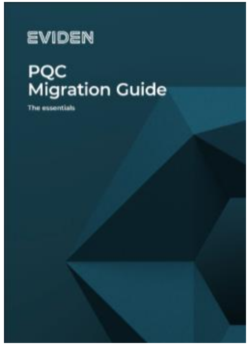
- Public Key Infrastructure servers (IDnomic PKI)
- Email & file encryption (Cryptovision Greenshield)
- Hardware Security modules (Trustway HSM)

Cryptography Research

- Crypto agility by design
- Smartcard, tokens & chips integration

Eviden PQC References – Documents and Press Releases

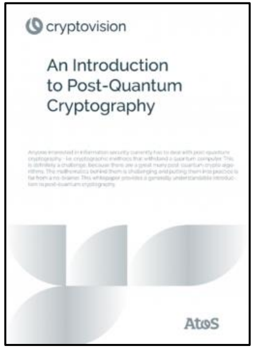
- **Upgrading our Cybersecurity Products**
  - Eviden Trustway HSM : Press Release
  - Eviden IDnomic PKI and Cryptovision Greenshield : Press Release
- **Raising awareness**
  - A solution webpage to consolidate communication
  - Main Whitepaper explaining what PQC is - An introduction to Post-Quantum Cryptography
  - Specific White paper - Trustway R&D and the Post-Quantum Cryptography
  - Specific White paper - Trustway: A cryptographic hybridization to ideally prepare for post-quantum migration
- **PQC Migration guide**
  - 1st document PQC Migration Guide – The essentials
  - Download available here: https://atos.net/en/lp/post-quantum-cryptography-pqc-migration-guide
  - Video : https://youtu.be/5cSNk7q-12o



EVIDEN

PQC
Migration Guide

The essentials

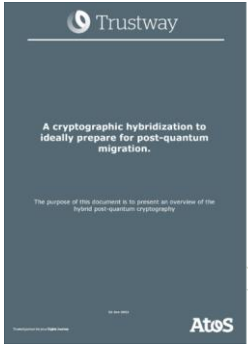


cryptovision

An Introduction
to Post-Quantum
Cryptography

Anyone interested in information security currently has to deal with post-quantum cryptography - i.e. cryptographic methods that withstand a quantum computer. This is definitely a challenge, because there are a great many post-quantum crypto algorithms. The mathematics behind them is challenging and putting them into practice is far from a no-brainer. This whitepaper provides a generally understandable introduction to post-quantum cryptography.

Atos



Trustway

A cryptographic hybridization to ideally prepare for post-quantum migration.

The purpose of this document is to present an overview of the hybrid post-quantum cryptography

Atos

Trustway Proteccio

Trustway R&D and the Post-Quantum Cryptography

The purpose of this document is to present an overview of the Post-Quantum cryptography and the on-going contest organized by the NIST to define the future of the PQC

Atos

References

Further Reading

- Banerjee T & M.A. Hasan: Energy Consumption of Candidate Algorithms for NIST PQC Standards http://cacr.uwaterloo.ca/techreports/2018/cacr2018-06.pdf
- BSI TR-02102-1: Technical Guideline: Cryptographic Mechanisms: Recommendations and Key Lengths https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf
- Craig Gidney, Martin Ekerå: How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits https://www.researchgate.net/publication/333338015_How_to_factor_2048_bit_RSA_integers_in_8_hours_using_20_million_noisy_qubits
- National Cyber Security Center: White paper: Preparing for Quantum Safe Cryptography https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography
- NIST IR.8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf
- NIST SP.800-56C Rev 2, Recommendation for Key-Derivation Methods in Key-Establishment Schemes https://doi.org/10.6028/NIST.SP.800-56Cr2
- ETSI TR 103 619 V1.1.1 (2020-07) CYBER; Migration strategies and recommendations to Quantum Safe schemes https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf
- NIST CSWP.04282021, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms https://doi.org/10.6028/NIST.CSWP.04282021
- CARAF: Chujiao Ma, Luis Colon, Joe Dera, Bahman Rashidi and Vaibhav Garg. “CARAF: Crypto Agility Risk Assessment Framework.” Journal of Cybersecurity, Dr. Michele Mosca & John Mulholland https://globalriskinstitute.org/publication/a-methodology-for-quantum-risk-assessment/
- Joseph, D., Misoczki, R., Manzano, M. et al. Transitioning organizations to post-quantum cryptography. Nature 605, 237–243 (2022). https://doi.org/10.1038/s41586-022-04623-2

EVIDEN MINDSHARE 2024

Thank you!

Questions?

Anastazija Zivkovic

Consultant, Global Cybersecurity Consulting,

Post-Quantum Cryptography Consulting Lead,

PhD in PQC Candidate

anastazija.zivkovic@eviden.com

Follow Eviden Digital Security:
eviden.com