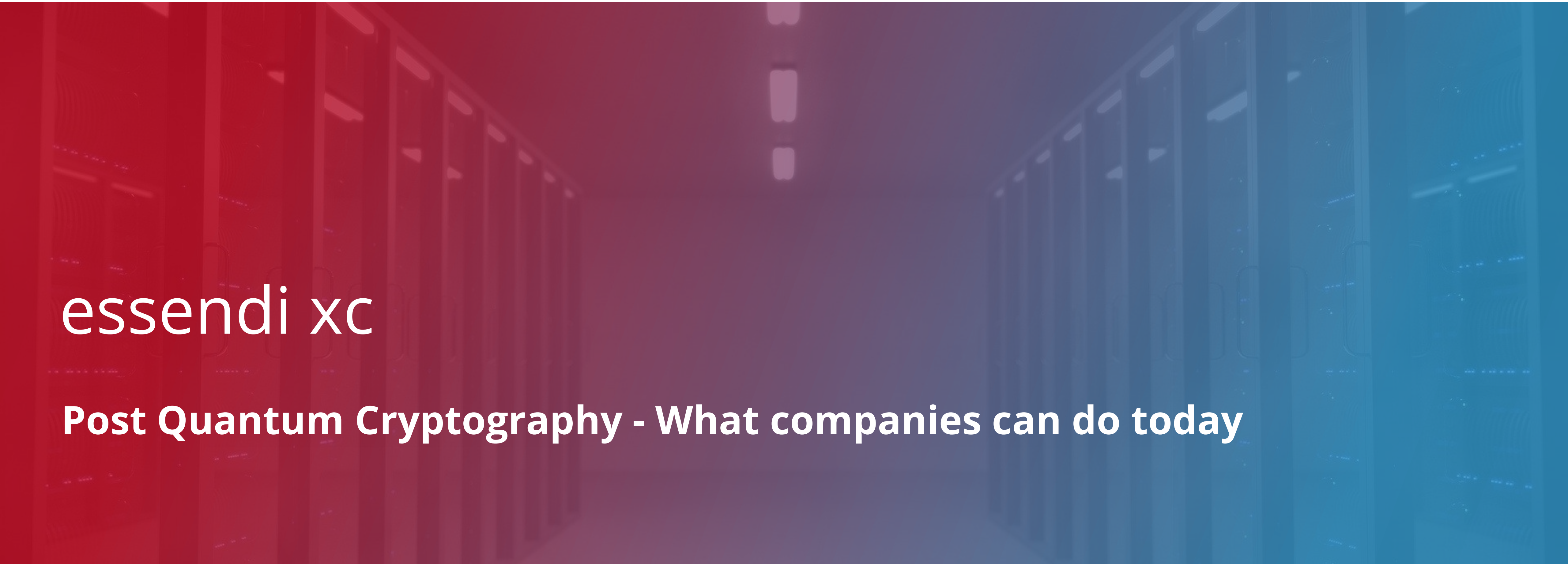


essendi xc

Post Quantum Cryptography - What companies can do today

Agenda

1. **essendi it** - Why we know about PQC
2. Quantum Computer and **Post Quantum Cryptography** (PQC)
3. **Approaches** - dealing with the issue of PQC today
4. PQC: **Why important?**
5. PQC: Market **penetration**
6. **Recommendations for action**
7. What will change in the **future**?

Allianz für Cyber-Sicherheit
Teilnehmer

SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

essendi it Group

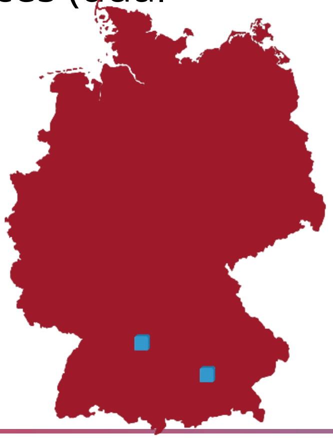
IT security, digital certificate management, digital identities, cryptography, PKI; product family **essendi xc**

Individual software solutions and consulting for various industries

essendi it GmbH, Germany

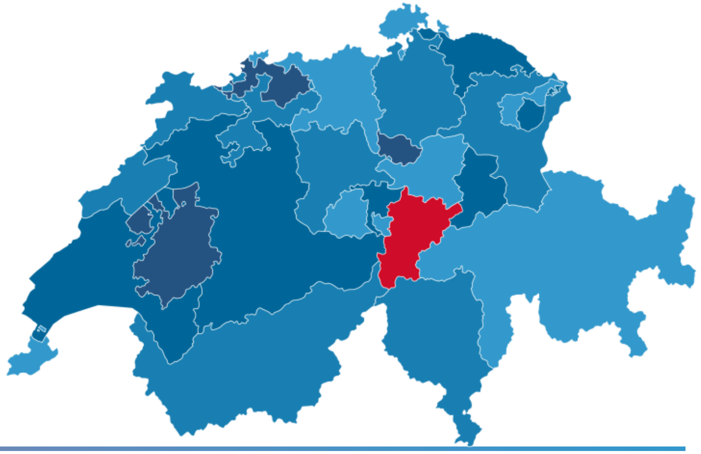
- 70 employees at two locations
  - Business analysts (IREP®)
  - Software engineers / developers (ISAQB®)
  - Testmanager (ISTQB®)
  - Projektmanager, incl. agile (PMI®, IPMA)
  - Students, trainees and apprentices (dual system Germany)
- Founded: 2000, family-run
- ISO 27001 certified

SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig



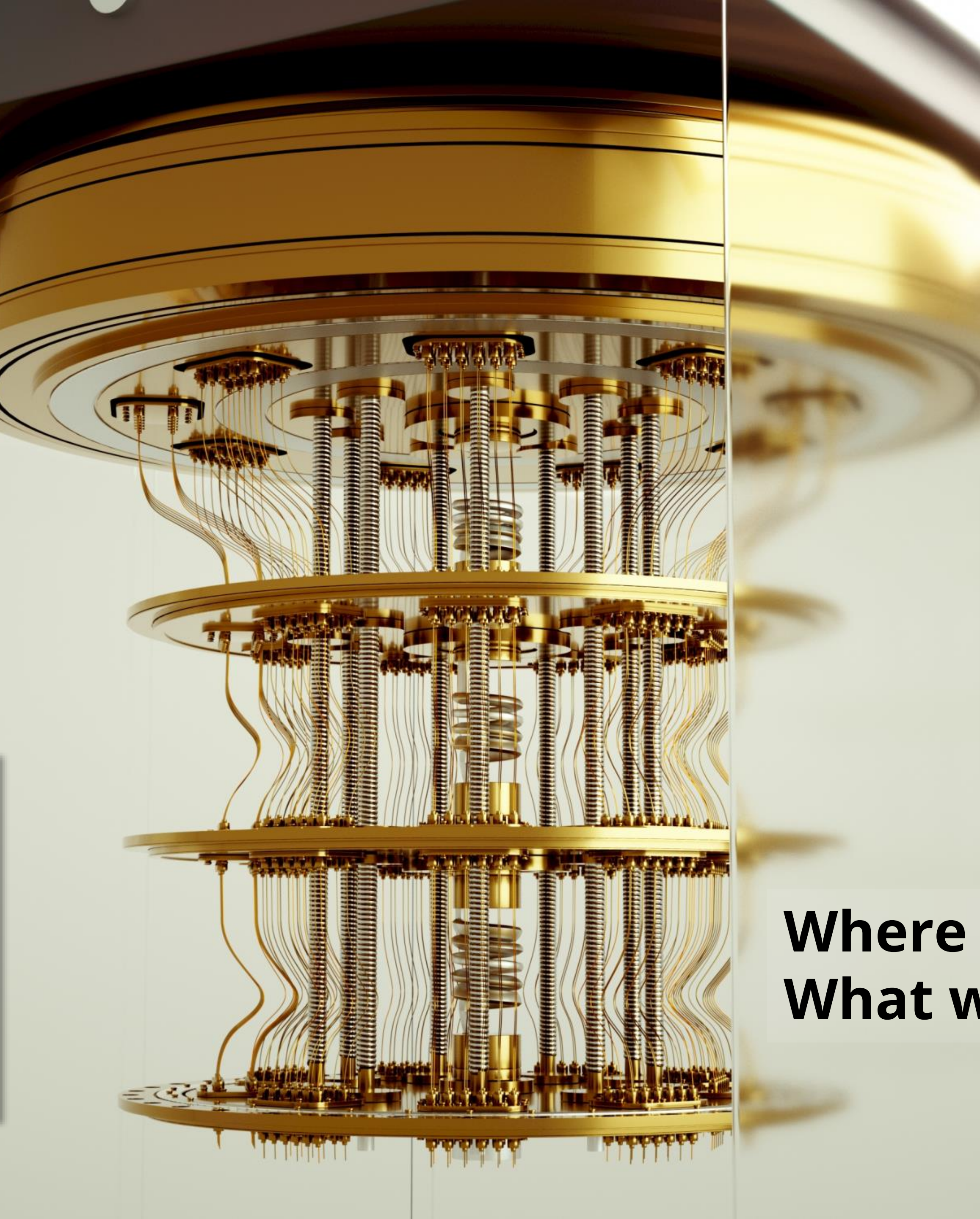
essendi it AG, Switzerland

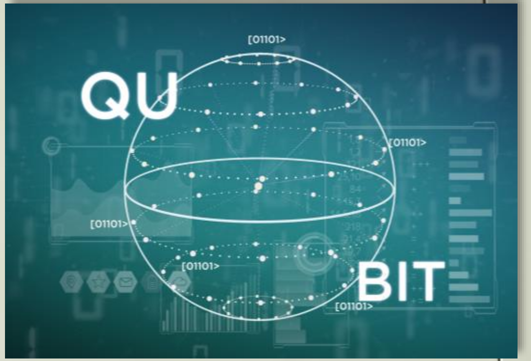
- Member of the essendi it Group, subsidiary of essendi it GmbH
- Specialised in processing international enquiries
- Founded in February 2022, family-run



Post Quantum Cryptography & Safety

PQC





Where do we stand today?
What will come?

Post Quantum Cryptography

Post-quantum cryptography refers to cryptographic schemes that are **assumed to be unbreakable even with the help of a quantum computer**. In contrast to quantum cryptography, these algorithms can be implemented on classical hardware.

Source: BSI

Source: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Post-Quanten-Kryptografie/post-quanten-kryptografie_node.html (retrieved: 23.09.2023)

3 Approaches

Dealing with the issue of PQC in large corporations today*:

waiting

- Reasoning: **standards for algorithms** do not yet exist, it is not yet possible to say exactly what PQC will look like, further **dynamics** expected in this area
- Plan to deal with the topic when standards are in place

interested

- The issue will come;
- **Collect knowledge now**
- Operationalise later

Let's do a POC together

- Have the topic **on the agenda already today**
- **Actively** monitor current developments, e.g. NIST competition
- Conduct a **POC** to actively **gain knowledge** in order to define a **strategy for action** based on this knowledge for the own group

*Current findings from the joint collaboration / research activity with the HSLU

Post Quantum Cryptography

Why important?

- Keeping **today's protected communication data secure and locked away in the future** (relevant in the field of medicine, the military or business secrets, among others).
  - Avoid / prevent "*harvest now, decrypt later*": Encrypted data of a present-day communication is stolen, stored and decrypted later when there are better possibilities
- **Maintaining the ability to act - time factor**: massive amount of time needed to change the encryption process in the company. Be ready for the new reality in good time. The more complex the organisation & infrastructure and the more diverse the communication channels, the more time-consuming.
  - Experience with switching from RSA 156 to 265: **3-7 years**
  - <u>Upcoming ToDos</u>: get prepared / create inventory (identification of encryption procedures, objects, affected systems, etc.); define of migration scenarios; testing / piloting; complete migration; **new normal**: new encryption procedures in use
- **Be prepared** - attack scenario **"manipulation of encrypted, digital communication**":
  - What if quantities were suddenly changed in an automated production process? For example, in production processes for pharmaceuticals?
- **Certificates everywhere**: Digital certificates and crypto operations, already play an important role in **worldwide digital communication networks,** but often unnoticed. When the quantum computer (or a similar technology) is developed, **every type of digital communication will be affected!**

Post Quantum Cryptography

Why important?

What about **your data**?

What data do you want to **protect**?

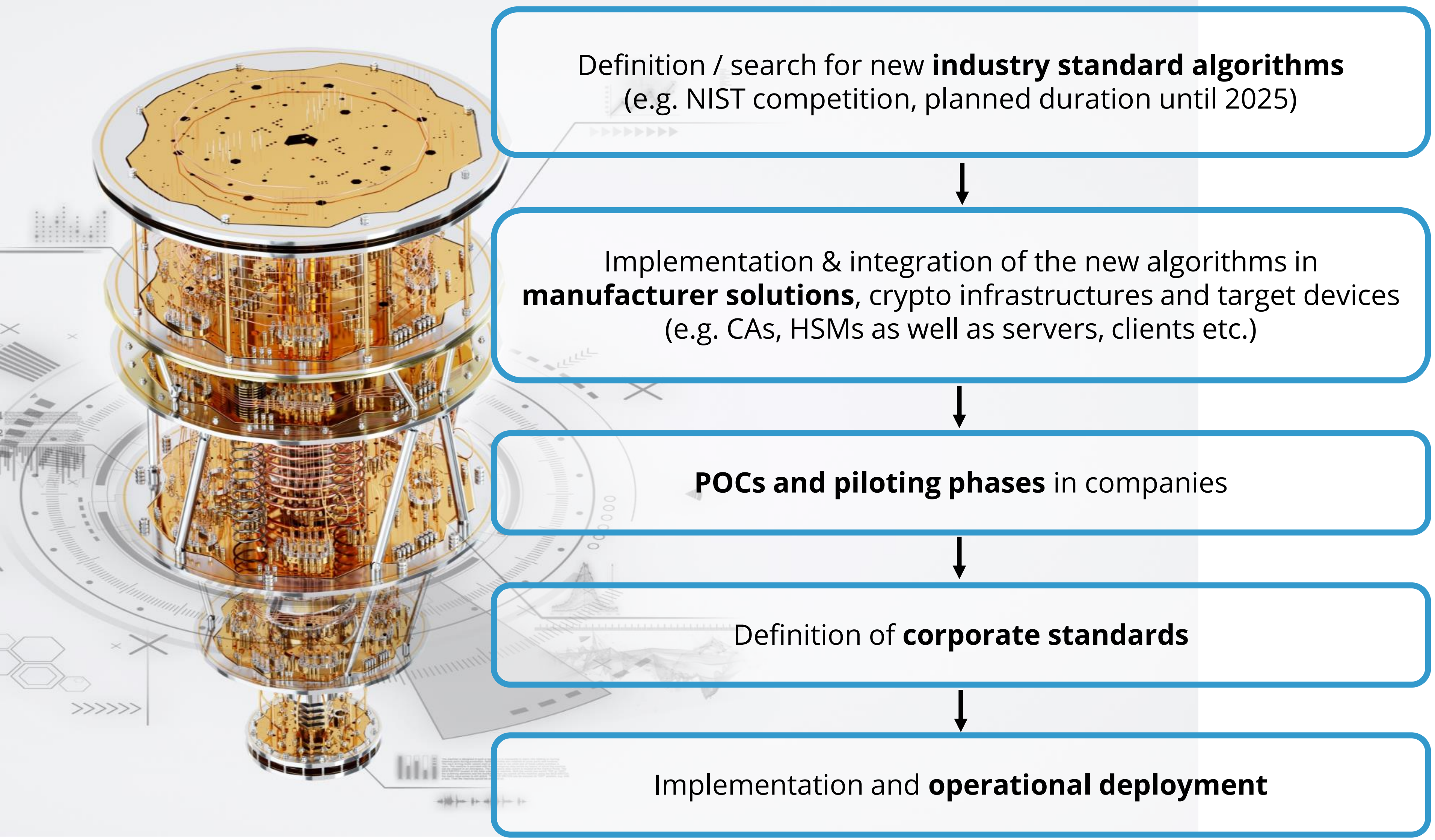
What data is **important to you**?

What is the state of **crypto-agility in your company**?

How long does it take to change the encryption procedures in your company?

Make use of the time today!

PQC - Market Penetration & Dissemination



Definition / search for new **industry standard algorithms** (e.g. NIST competition, planned duration until 2025)

Implementation & integration of the new algorithms in **manufacturer solutions**, crypto infrastructures and target devices (e.g. CAs, HSMs as well as servers, clients etc.)

POCs and piloting phases in companies

Definition of **corporate standards**

Implementation and **operational deployment**

New, today **unknown factors** have to be included and create **dynamics**

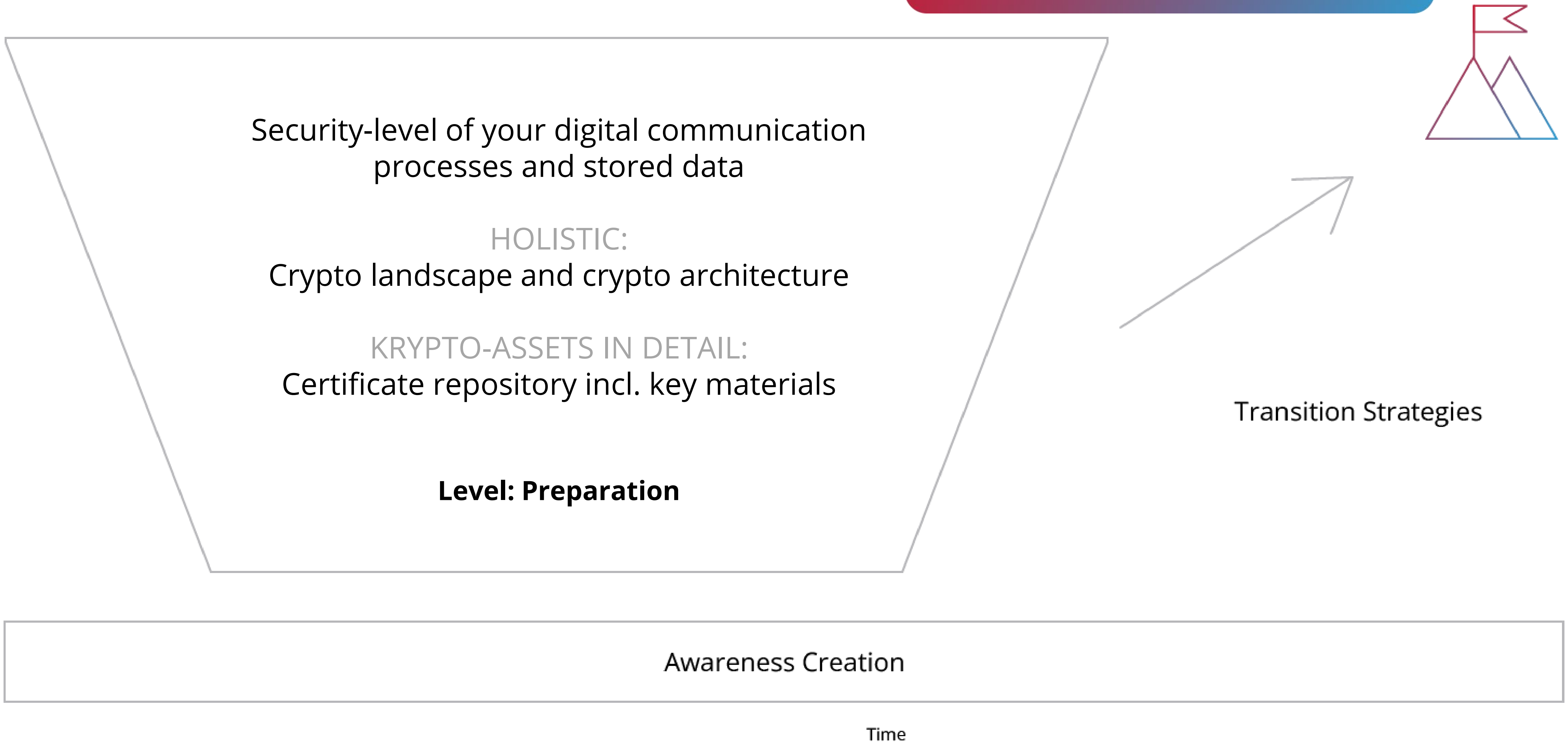
(Ex. Feb 2023: AI cracks an algorithm classified by NIST as quantum-save
Detail: CRYSTALS-Kyber public key encryption and key encapsulation mechanism)

Be prepared

Recommendations for action (1/2)

- **Create attention, drill down, define strategies**

Need support? Our team will be happy to help you. Ask for our **essendi service portfolio.**



Security-level of your digital communication processes and stored data

HOLISTIC:
Crypto landscape and crypto architecture

KRYPTO-ASSETS IN DETAIL:
Certificate repository incl. key materials

Level: Preparation

Transition Strategies

Awareness Creation

Time

Recommendations for action (2/2)

- **Evaluate** the **security level / sensitivity level of** your **digital communication processes** and **encrypted stored data** - minimum: give it some thought.
  - On this basis: Which communication processes / devices contain particularly sensitive information that should be protected (in the long term)?
- **Overview**: If you don't already know, familiarise yourself with your corporate **crypto landscape**
  - What **crypto assets & systems** are in use (including **digital certificates and key material**)? What **dependencies / interoperabilities** do exist?
  - What does the **crypto architecture** look like? Consisting of crypto-assets (see above), crypto-systems (Hardware Security Modules HSMs, Public Key Infrastructures PKIs, Certificate Authorities Cas etc.) and target systems as well as possibly other components
  - What are the **crypto processes**?
- **Certificate repository**: Build a certificate repository that contains an overview of your digital certificates as well as the crypto keys (private and public key).
  - **Areas of application and use of** your digital certificates
  - **Grouping options for** your digital certificates, e.g. by use case

! ISO27001/NIST **relevant**

- **"Awareness creation** within your organisation: Put the issue on the agenda. Deal with it.
- Think about **"transition strategies"** (**time factor!**)

essendi - your partner in the field of PQC

essendi it

- **Analysis of the status quo**
- Implementation of the above recommendations for action
  - Recording of the **crypto processes**
  - Mapping of the existing **crypto landscape / architecture**
  - Creation of a certificate repository incl. responsibilities
  - Analysis of the existing communication processes incl. protection level
- Definition of a **transition strategy**
- **Implementation of a POC**: Establishment of PQC communication route in your company (in cooperation with HSLU)

?

How can **essendi it support you** in the area of PQC?

- **essendi xc** certificate management
  - Creation of a **certificate repository** and support with certificate handling
  - **Automation of the certificate processes**
- **essendi cd** – discover certificates
  - **Discover** unknown **certificates in the data centre**
  - Outlook: **Validation of** the repository

xc + cd

What will change in the future ....

... regarding cryptography and digital certificates?*

- **Hybrid certificates** raise new questions: How should / must these be dealt with?
- **More diverse crypto keys** - **more complex handling**
  - No longer linear
  - Specific fields of application: Security only with regard to specific requirements / use cases etc.
- **New algorithms**
  - Final results of the NIST competition: expected in 2025
- **Increased time duration** and **performance in** relation to the key and signature size: duration of crypto operations or creation of the crypto key will increase.
  - **Dilithium2** (PQC) generates a **key pair** within **0.044ms**. **ECDSA** (traditional crypto) takes **0.631ms.** However, the **Dilithium2 key is over 20 times larger than** ECDSA.
  - **SPHINCS+-128s-robust** (PQC) needs **a minimum of 13,769 ms (up to max. 106,087 ms!**) to generate a key pair. The key is only **half as large as** with **ECDSA**.
- New challenges - **adaptations of standards required**: e.g. credit cards - The chip communication protocol has a limited number of characters for crypto keys - which is exceeded with PQC algorithms. The standards need to be adapted.
- **Open questions:**
  - How will CAs react? How and how quickly will equipment providers react?

!

The future will tell. Let's shape it together.

*Current findings from joint collaboration / research activities with HSLU. Subject to change.

Let's start!

Thank you

EU contact

essendi it GmbH

Dolanallee 19
DE-74523 Schwäbisch Hall
xc@essendi.de
xc.essendi.it
Tel.: +49 791 94307011

International contact

essendi it AG

Bahnhofplatz 1
CH-6460 Altdorf
xc@essendi.ch
xc.essendi.it
Tel.: +41 41 874 27 30

Please do not hesitate to contact us if you have any questions or require further information. E-mail: xc@essendi.de