

essendi xc

Post Quantum Cryptography – Was Unternehmen heute tun können

Sarah Zügel | 10.10.2023

essendi ist
ISO 27001
zertifiziert*

*Der Hersteller essendi it GmbH ist
ISO27001 zertifiziert.

- 1 **essendi it** – Why we know about PQC
- 2 Quanten Computer und **Post Quantum Cryptography** (PQC)
- 3 **Herangehensweisen** – Umgang mit dem Thema PQC heute
- 4 PQC: **Warum wichtig?**
- 5 PQC: **Marktdurchdringung**
- 6 **Handlungsempfehlungen**
- 7 Was wird sich in **Zukunft verändern?**
- 8

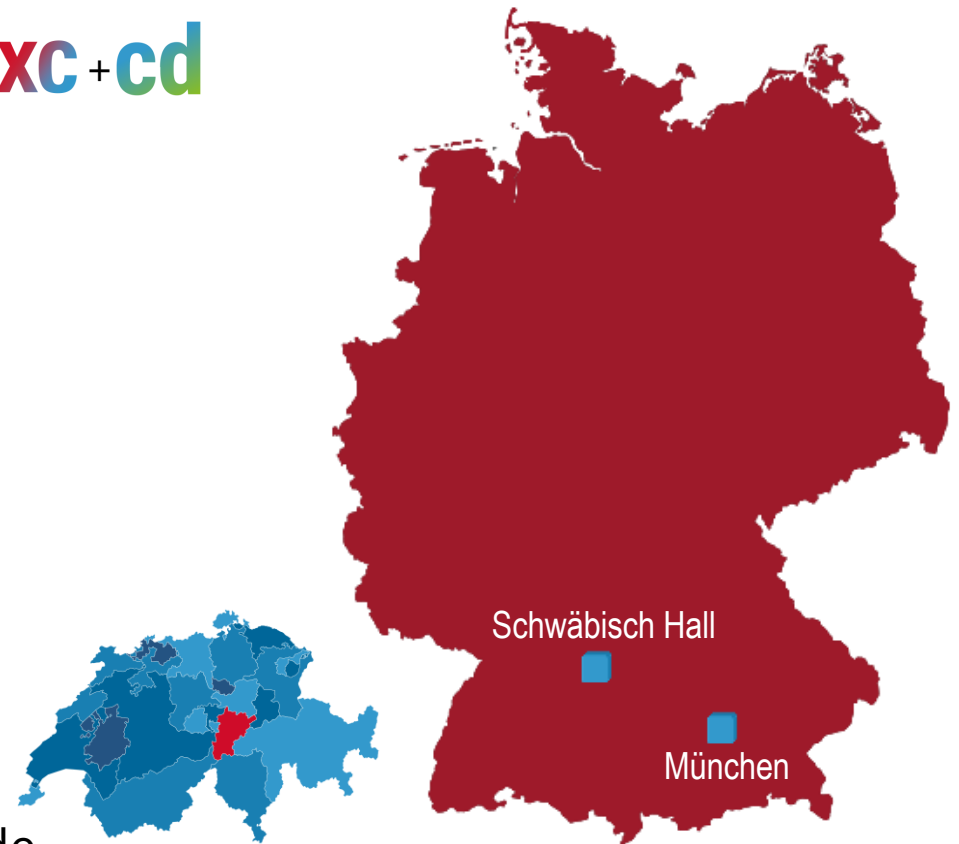


Welcome



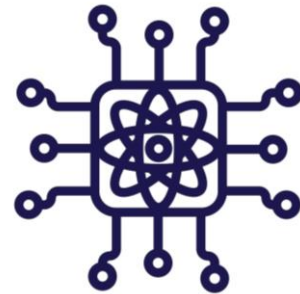
- IT-Security, Management digitaler Zertifikate, digitale Identitäten, Krypto, PKI; Produktfamilie **essendi xc**
- Individuelle Software-Lösungen und Beratung für versch. Branchen
- 70 Mitarbeiter an 2 Standorten
 - Business-Analysten (IREB®)
 - Wirtschaftsinformatiker
 - Software-Ingenieure / -Entwickler (ISAQB®)
 - Testmanager (ISTQB®)
 - **IT Security Experten**
 - Projektmanager – auch agil (PMI®, IPMA)
 - DHBW-Studenten, Auszubildende (IHK)
- Gründung im Jahr 2000, familiengeführt, EU-company
- Tochterunternehmen: essendi it AG, Schweiz  
- Webseiten: <https://xc.essendi.de> und <https://essendi.de>

xc + cd

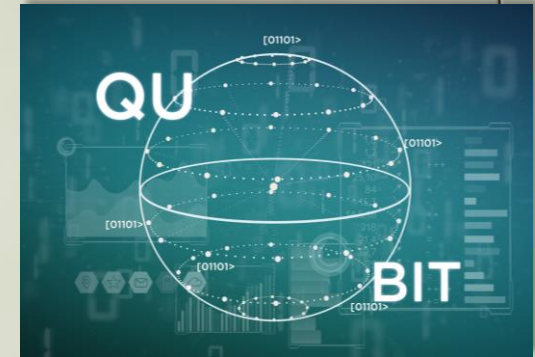
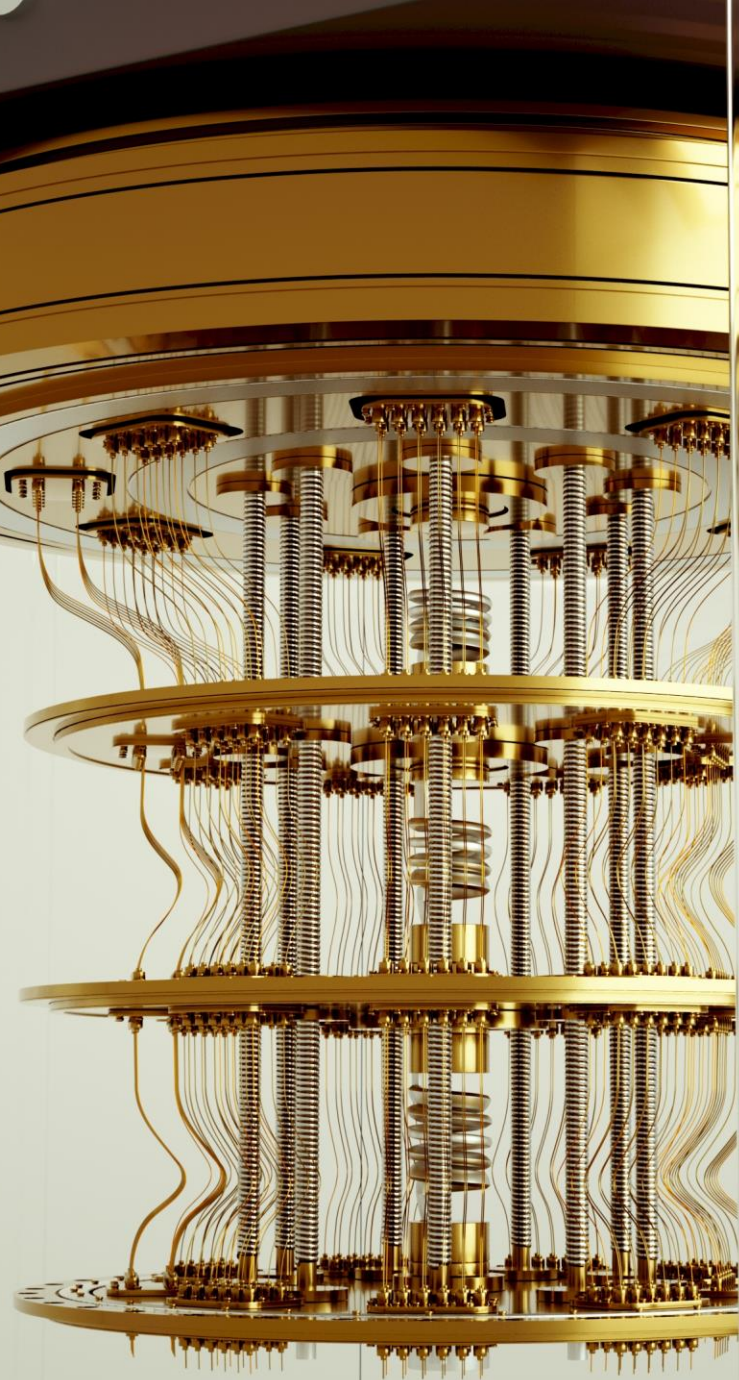


Post Quantum Cryptography & Safety

PQ C



QUANTUM COMPUTING



**Wo stehen wir heute?
Was wird kommen?**

Unter Post-Quanten-Kryptografie versteht man kryptografische Verfahren, **von denen angenommen wird, dass sie auch mit Hilfe eines Quantencomputers nicht zu brechen** sind. Im Gegensatz zur Quantenkryptografie können diese Verfahren auf klassischer Hardware implementiert werden.

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.

Quelle: BSI

Quelle: 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 (Abruf: 23.09.2023)

3 Herangehensweisen

3

Umgang mit dem Thema PQC in Großkonzernen heute*:

abwartend

- Argumentation: noch keine **Standards für Algorithmen** vorhanden, man kann noch nicht genau sagen, wie PQC aussehen wird, **Dynamik** in diesem Bereich erwartet
- Beschäftigung mit dem Thema geplant für den Zeitpunkt, wenn Standards vorhanden sind

interessiert

- Das Thema wird kommen;
- **Wissen sammeln**
- **Operationalisierung später**

Let's do a POC together

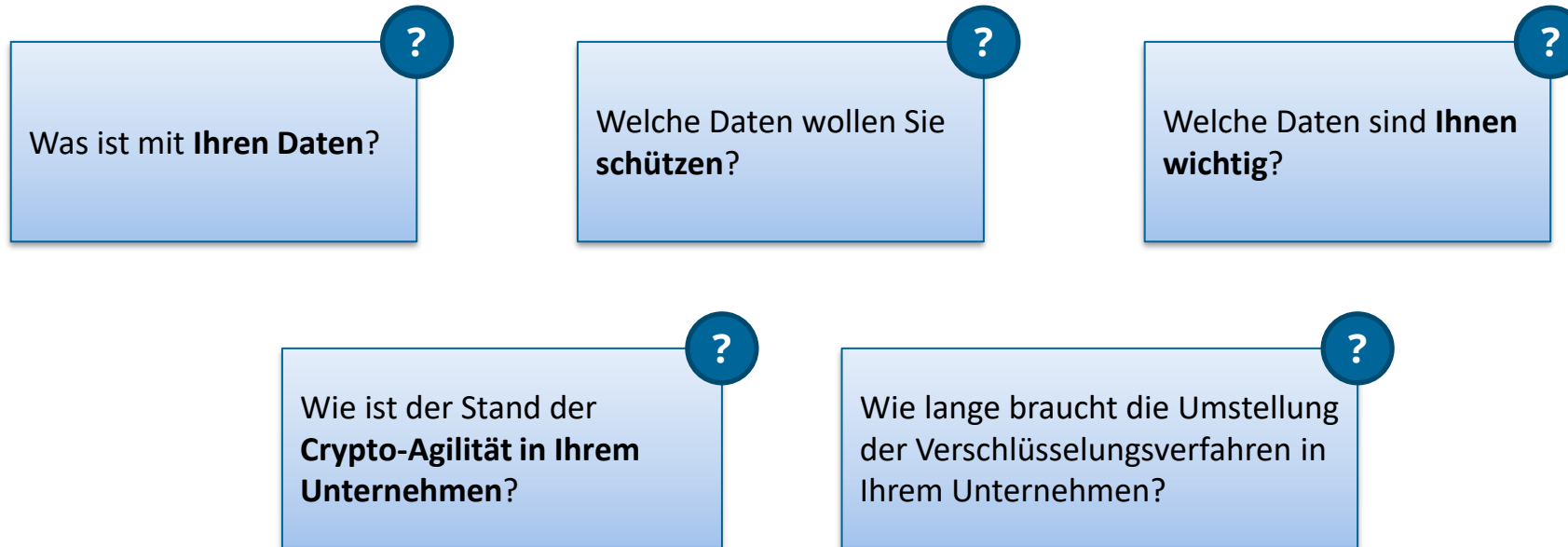
- Haben das Thema **heute** schon auf der **Tagesordnung**
- Beobachten aktuelle Entwicklungen, z.B. NIST Wettbewerb **aktiv**
- Durchführung eines **POC** zur aktiven **Gewinnung von Erkenntnissen**, um darauf basierend eine **Handlungsstrategie** für den eigenen Konzern festzulegen

*Aktuelle Erkenntnisse aus der gemeinsamen Zusammenarbeit / Research-Tätigkeit mit der HSLU

Warum wichtig?

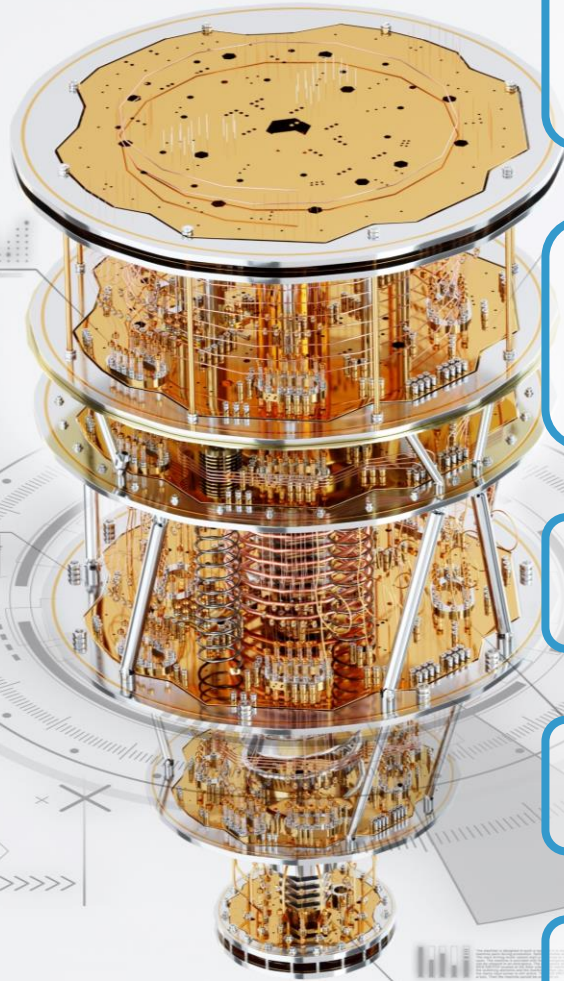
- **Geschützte, heutige Kommunikationsdaten** auch **in Zukunft sicher und verschlossen** halten (relevant u.a. im Bereich der Medizin, des Militärs oder von Geschäftsgeheimnissen)
 - „*Harvest now, decrypt later*“ vermeiden / verhindern: Verschlüsselte Daten einer heutigen Kommunikation werden abgegriffen, gespeichert und später, wenn es bessere Möglichkeiten gibt, entschlüsselt
- **Handlungsfähigkeit bewahren – Faktor Zeit:** massiver Zeitaufwand für die Umstellung des Verschlüsselungsverfahrens im Unternehmen. Rechtzeitig bereit sein für die neue Realität. Je komplexer die Organisation & Infrastruktur und je vielfältiger die Kommunikationswege, desto zeitaufwändiger.
 - Erfahrungswerte beim Switch von RSA 156 auf 265: **3-7 Jahre**
 - Anstehende ToDos: Vorbereitung / Bestandsaufnahme (Identifikation von Verschlüsselungsverfahren, -objekten, betroffenen Systemen etc.); Definition von Migrationsszenarien; Testing / Pilotierung; Komplet-Migration; **New normal:** Neue Verschlüsselungsverfahren im Einsatz
- **Vorbereitet sein** – Angriffsszenario „**Manipulation verschlüsselter, digitaler Kommunikation**“:
 - Was wäre, wenn in einem automatisierten Produktionsprozess plötzlich Mengen verändert werden? Zum Beispiel bei Produktionsprozessen für Medikamente?
- **Zertifikate überall:** Digitale Zertifikate und Krypto-Operationen, spielen bereits heute schon eine wichtige Rolle in **digitalen Kommunikationsnetzen weltweit**, jedoch oftmals unbemerkt. Wenn der Quanten Computer (oder eine ähnliche Technologie) entwickelt sein wird, **wird jede Art der digitalen Kommunikation betroffen sein!**

Warum wichtig?



Nutzen Sie die Zeit heute!

PQC – Marktdurchdringung & Verbreitung



Definition / Suche nach neuen **Industrie-Standard Algorithmen**
(Bsp. NIST Wettbewerb, geplante Laufzeit bis 2025)



Umsetzung & Integration der neuen Algorithmen in **Hersteller Lösungen**, Krypto-Infrastrukturen und Zieldevices
(Bsp. CAs, HSMs sowie Server, Clients etc.)



POCs und Pilotierungsphasen in Unternehmen



Definition von **Unternehmensstandards**



Umsetzung und **Operativer Einsatz**

Neue, heute **unbekannte Faktoren** müssen mit einbezogen werden und sorgen für **Dynamiken**

(Bsp. Feb 2023: KI knackt einen von NIST als Quantum-safe eingestuften Algorithmus
Detail: CRYSTALS-Kyber public key encryption and key encapsulation mechanism)

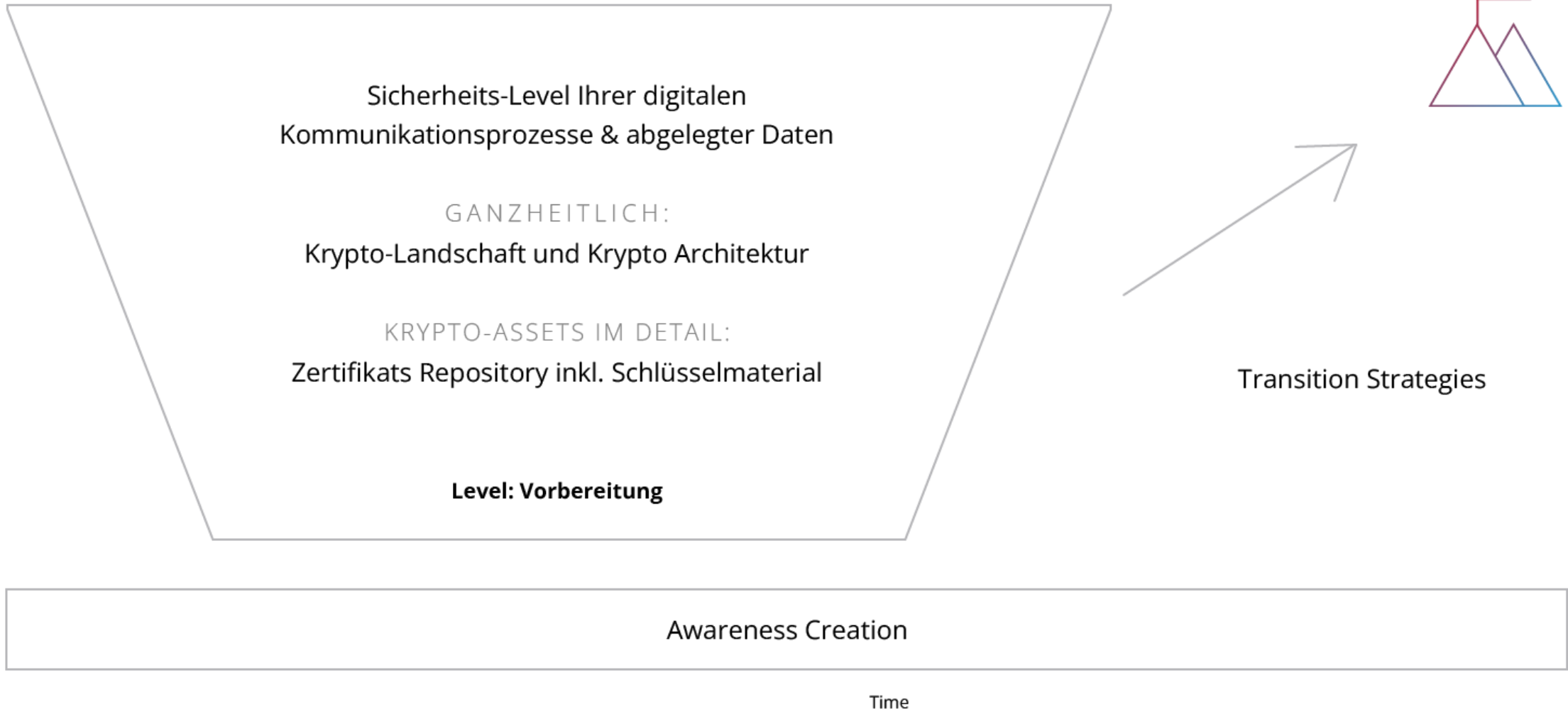
Be prepared



Handlungsempfehlungen (1/2)

Unterstützung benötigt? Unser Team hilft Ihnen gerne. Fragen Sie nach unserem **essendi-Leistungsspektrum**.

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



- **Bewerten** Sie das **Sicherheits-Level / Sensibilitäts-Level** Ihrer **digitalen Kommunikationsprozesse** und **verschlüsselt abgelegter Daten** – Minimum: Machen Sie sich darüber Gedanken.
 - Auf dieser Basis: Welche Kommunikations-Prozesse / -Devices beinhalten besonders sensible Informationen, die (langfristig) geschützt werden sollten?
- **Übersicht:** Wenn Sie es nicht bereits wissen, machen Sie sich mit Ihrer **Krypto-Landschaft** im Unternehmen vertraut
 - Welche **Krypto-Assets & -Systeme** sind im Einsatz (u.a. **digitale Zertifikate und Schlüsselmaterial**)? Welche **Abhängigkeiten / Interoperabilitäten** gibt es?
 - Wie sieht meine **Krypto-Architektur** aus? Bestehend aus Krypto-Assets s.o, Krypto-Systemen (Hardware Security Module HSMs, Public Key Infrastructures PKIs, Certificate Authorities Cas etc.) und Zielsystemen sowie evtl. weiteren Komponenten
 - Welche **Krypto Prozesse** gibt es?
- **Zertifikats-Repository:** Bauen Sie ein Zertifikats-Repository auf, das eine Übersicht Ihrer digitalen Zertifikate sowie der Krypto-Keys (privater und öffentlicher Schlüssel) enthält
 - **Einsatzbereiche und Nutzung** Ihrer digitalen Zertifikate
 - **Gruppierungsmöglichkeiten** Ihrer digitalen Zertifikate, z.B. nach Usecase
- **“Awareness creation”** innerhalb Ihrer Organisation: Setzen Sie das Thema auf die Tagesordnung. Beschäftigen Sie sich damit.
- Denken Sie über **“transition strategies”** nach (**Zeitfaktor!**)

ISO27001/NIST-relevant



- **Analyse des Status quo**
- Umsetzung der genannten Handlungsempfehlungen
 - Aufnahme der **Krypto Prozesse**
 - Darstellung der vorhandenen **Krypto-Landschaft / Architektur**
 - Erstellung eines Zertifikats-Repositories inkl. Verantwortlichkeiten
 - Analyse der vorhandenen Kommunikations-Prozesse inkl. Schutzlevel
- Definition einer **Transition Strategie**
- **Durchführung eines POCs:** Aufbau von PQC Kommunikationsstrecke in Ihrem Unternehmen (in Zusammenarbeit mit HSLU)
- **essendi xc** Zertifikatsmanagement
 - Erstellung eines **Zertifikats-Repository** und Unterstützung beim Zertifikats-Handling
 - **Automatisierung der Zertifikatsprozesse**
- **essendi cd** – Zertifikate finden
 - Unbekannte **Zertifikate im Rechenzentrum finden**
 - Ausblick: **Validierung** des Repositories

?


Wie kann **essendi** Sie im Bereich PQC unterstützen?

xc + **cd**

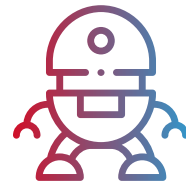
Was wird sich in Zukunft verändern....

...mit Blick auf Kryptografie und digitale Zertifikate?*

- **Hybride Zertifikate** bringen neue Fragestellungen: Wie soll / muss mit diesen umgegangen werden?
- **Vielfältigere Krypto-Schlüssel – komplexeres Handling**
 - Nicht mehr linear
 - Spezifische Einsatzfelder: Sicherheit nur mit Blick auf bestimmte Anforderungen / Usecases etc.
- **Neue Algorithmen**
 - Finale Ergebnisse des NIST Wettbewerbs: erwartet 2025
- **Erhöhte Zeitdauer** und **Performance** in Relation zur Schlüssel- und Signaturgröße: Dauer für die Durchführung der Krypto-Operationen bzw. das Erstellen des Krypto Keys werden zunehmen
 - **Dilithium2** (PQC) generiert ein **Schlüsselpaar** innerhalb von **0.044ms**. **ECDSA** (traditionelle Krypto) benötigt **0.631ms**. Der **Dilithium2 Schlüssel** ist aber **über 20x so gross** wie bei ECDSA.
 - **SPHINCS+-128s-robust** (PQC) benötigt für das Generieren eines Schlüsselpaars **min. 13.769 ms (bis max. 106.087 ms!)**. Der Schlüssel ist dafür nur **halb so gross** wie bei **ECDSA**.
- Neue Herausforderungen - **Anpassungen von Standards erforderlich**: Bsp. Kreditkarten - Das Chip Communication Protokoll hat eine begrenzte Anzahl an Zeichen für Krypto-Keys – die bei PQC Algorithmen überschritten wird. Die Standards müssen angepasst werden.
- **Offene Fragen:**
 - Wie werden die CAs reagieren? Wie und wie schnell werden Geräteanbieter reagieren?


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

Let's start!



Treffen Sie uns!

essendi it auf der it-sa



Besuchen Sie uns!

Das **essendi Team** freut sich auf den **gemeinsamen Austausch** mit Ihnen.

Thank you

Sarah Zügel

essendi it GmbH | Sarah.Zuegel@essendi.de

www.essendi.it