

# Quanten- technologie und Cybersicherheit

Innovationsnetzwerktreffen

08.10.2024

Dr. A. Schüttpelz

[www.thalesgroup.com](http://www.thalesgroup.com)



## Thales: Partner mit europäischen Wurzeln und starker globaler Präsenz



**77.000**  
Beschäftigte



**68** Länder  
weltweit



**€1 Mrd.\***  
Eigenfinanzierte  
F&E



**€18,4 Mrd**  
Umsatz 2023

## 3 Kernmärkte, in denen Thales Sicherheit und Vertrauen schafft



UNTERNEHMEN



REGIERUNGEN



INSTITUTIONEN



STÄDTE

Cybersecurity in IT- und Industrieanwendungen  
Verschlüsselungssysteme für zivile und militärische Anwendungen

# Bedeutung Schutz kritischer Infrastrukturen

## > Umfeld

- vernetzte Sensoren (Internet of Things – IoT)
- zentrale Informationsverarbeitung in Cloudstrukturen
- Echtzeitsteuerung & -überwachung industrieller Prozesse und Komponenten

## > Bedrohungen

- 'Klassische' Bedrohungen: Ausnutzung bekannter Angriffsvektoren
  - unzureichende Authentisierung,
  - Ausnutzung von SW-Sicherheitslücken,
  - Phishing,
  - Unerlaubter Zugriff erlaubt wahlweise Eingriffe oder Einschleusen von Schadsoftware
- Neue Bedrohungen, Schwerpunkt:
  - AI zur Ausnutzung von Schwachstellen: z.B. durch Codegenerierung
  - Angriffe mit Quantencomputern – v.a. Brechen aktueller Kryptoalgorithmen: Authentizität und Vertraulichkeit
  - Kombination Quantencomputer mit AI: z.B. AI-assisted zur Fehlerreduktion von Quantencomputern beim Einsatz zum Brechen von Verschlüsselung



# Standardmaßnahmen

## > Rahmenwerk / Standards - Übersicht

- ▶ Rechtlichen Rahmen kennen und berücksichtigen
  - NIS-2 Network and Information Security (NIS) Directive: Unternehmen & Institutionen, ab 2025
  - CRA Cyber Resilience Act: IT-Produkte Hersteller & Betreiber, ab 2027
- ▶ ISMS | BCMS aufsetzen und pflegen
  - ISO27001 Informationssicherheitsmanagementsystem (ISMS) | Sicherheitsmechanismen
- ▶ Schutz von IT & OT durch Informationssicherheit nach „Stand der Technik“
  - IEC 62443 Cybersicherheit für industrielle Netze und Systeme
  - BSI Grundschutzmethodik & Grundschutzkompendium

## > Operative Maßnahmen

- ▶ Sicherheitsbewertungen, Assessment, Pentests
- ▶ System- und Schwachstellenmanagement
- ▶ Systemüberwachung: Erkennung und Reaktion



**Mit Berücksichtigung der Vorgaben lässt sich aktuell ein hohes Schutzniveau erreichen!**

⇒ Prüfen und Umsetzen!

⇒ Ggf. Unterstützung holen

Allerdings gibt es noch ‚neue‘ Bedrohungen



# Neue Maßnahmen gegen neue Bedrohungen

## > Einsatz von AI

- AI erfasst Normalzustände gut (basiert auf Identifikation von Ähnlichkeiten / Korrelation)
- AI kann daher Abweichungen identifizieren => Angriffserkennung, vorbeugender Schutz (Schwachstellenerkennung)

## > Post-Quanten-Kryptographie

- Identifikation der verwendeten Systeme, die kryptographische Algorithmen verwenden (=> das sind üblicherweise viele)
- Einführung PQC-Verfahren bedenken: Kritikalität festlegen, Anpassungsoptionen identifizieren, Umsetzung planen und angehen
- Berücksichtigung Krypto-agilität: d.h. Anpassbarkeit an neue Verfahren gewährleisten

⇒ Vorbereitung hilft für zukünftige Bedrohungen gewappnet zu sein!

⇒ Beispiel und nähere Infos folgen



Quantum<sup>BW</sup>

IT BUSINESS CLUB



Bundesministerium  
für Bildung  
und Forschung

**Thales Deutschland: Aktive Teilnahme an Forschungsprojekten und Netzwerken der relevanten Akteuren**

# Beispiel Herausforderungen KRITIS & Quantencomputer

## > Vernetzung von IoT-Geräten => Identitätsmanagement & Authentifizierung & Verschlüsselung

- Beispiel: Absicherung der Überwachung & Steuerung, z.B. Pumpen in Kraftwerken (Stichwort: Schadsoftware)
- Hohes Sicherheitsbedürfnis: Technologien zur Authentisierung und Verschlüsselung
- Absicherung mit Public Key Infrastrukturen (PKI)
- Spezielle Bedürfnisse im KRITIS Umfeld: Sehr hohe Anzahl an Geräten, Ressourcen auf IoT beschränkt, Edge Devices – Hoher Durchsatz/Last der PKI bei gleichzeitig hohem Schutzniveau

## > Spezielle Herausforderung: Quantentechnologie und Post-Quantenkryptographie

- Absicherung der Kommunikation und der Authentisierung in kritischen Infrastrukturen: Elliptische-Kurven-Kryptographie (z.B. Elliptic-Curve Diffie-Hellman)
- Gilt heute noch als sicher mit Einsatzempfehlung >2029
- Jedoch existieren Quantenalgorithmien (Shor), die diese brechen können
- ⇒ Geheime Schlüssel können berechnet werden
- ⇒ Kommunikation abhören oder Zugriff auf die industriellen Steuerungen erhalten – mit entsprechend weitreichenden Folgen
- ⇒ Schutz durch Post-Quantenkryptographie: inzwischen NIST Standards verfügbar – Grundlage für Implementierungen

# Public Key Infrastructure - PKI

## > Was ist das?

- Erzeugt, verteilt und annulliert digitale Zertifikate, die von einer gemeinsamen Vertrauensquelle erzeugt werden

## > Digitales Zertifikat verknüpft einen öffentlichen Schlüssel mit Identität

⇒ Im Prinzip ein Ausweis (ID-Card)...

- ...aber mit Schlüssel: ermöglicht digitale kryptografische Operation
- Zertifikat: öffentlicher Schlüssel & weitere Informationen (z.B. Schlüsselinhaber und erlaubte Schlüsselverwendung)

## > Private/Public Key Verfahren – Asymmetrische Kryptographie

- Asymmetrische Kryptographie: Schlüsselpaare
- Gewährleistung der Integrität: Identifikation, Authentisierung => Signaturverfahren
- Gewährleistung der Vertraulichkeit: Verschlüsselung => Verschlüsselungsverfahren

## > Zertifikate für Geräte

- Alltag und essentiell für den Schutz, z.B. signierte SW, Trusted-Boot-Plattform, Netzwerkkommunikation (TLS), ...



# HSM als Krypto-Komponente einer PKI



## > Hardware Sicherheitsmodul (HSM)

- › Führt sämtliche kryptographischen Operationen in Hardware aus
- › Sehr schnell: Hardwarebeschleuniger geeignet für hohe Lasten, großen Durchsatz
- › Sehr sicher: keine Verarbeitung kritischer Daten im Prozessor/Software
- › Wird über standardisierte Schnittstellen angesprochen – lässt sich flexibel an PKI anbinden

## > Aktuelle Anwendungsforschung: HSM mit Post-Quanten-Kryptografie

- › Post-Quanten-Algorithmen: NIST Kyber, Dilithium, Classic McElliece
- › Implementierung auf FPGA => flexibel für Anpassungen, Krypto-agilität

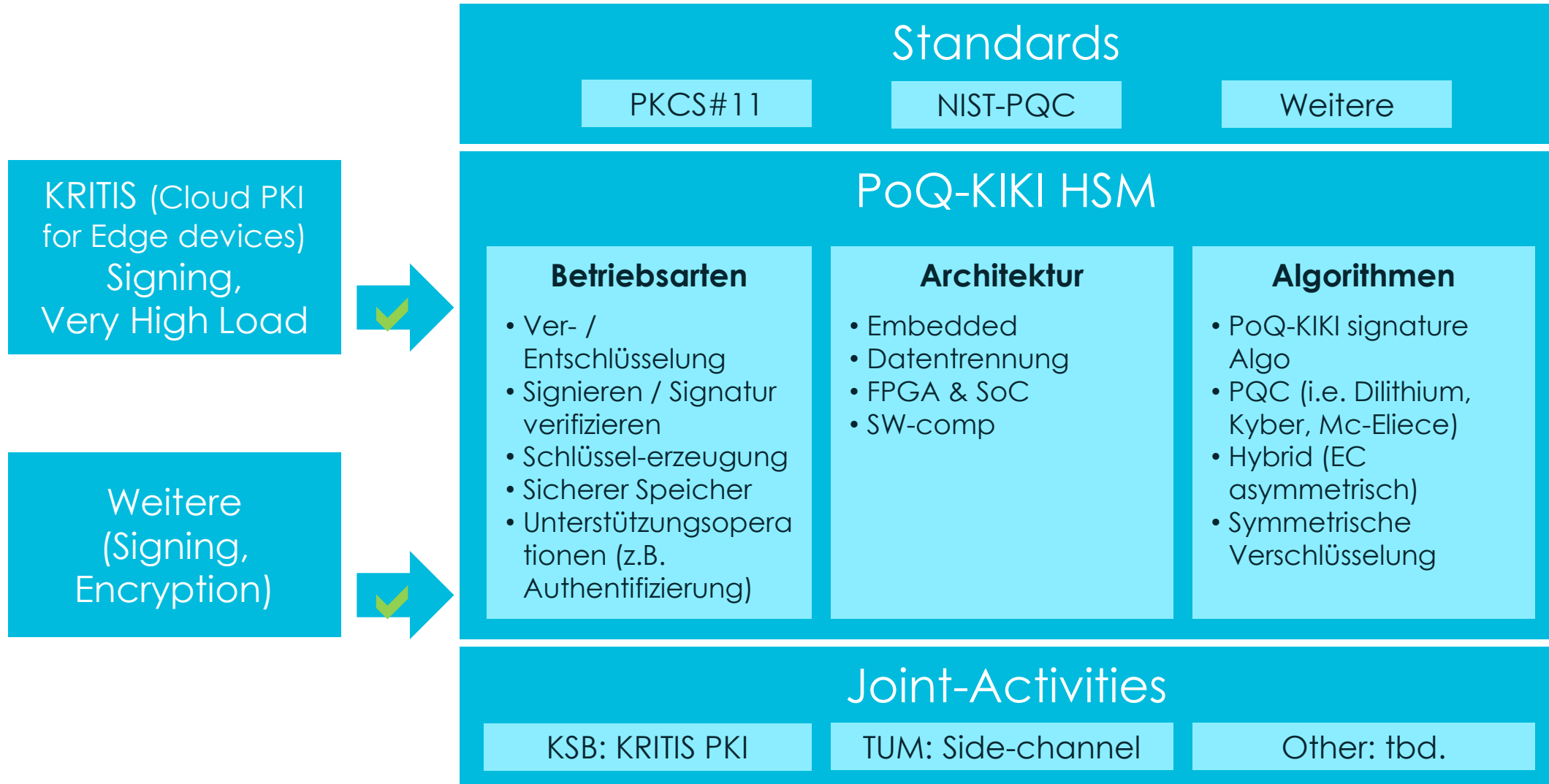
## > „Post-Quanten sichere PKI für die Cloud-Anbindung in kritischer Infrastruktur - PoQ-KIKI“

- › BMBF gefördertes Vorhaben im Rahmen „Post-Quanten-Kryptografie in die Anwendungen bringen“
- › Weitere Informationen:
  - <https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/poq-kiki>
  - <https://www.thalesgroup.com/de/countries-europe/deutschland/news/postquantensichere-kryptografie-zur-absicherung-von-kritischen>





# PoQ-KIKI HSM Ansatz



# Zusammenfassung

## > Zusammenfassung

- › Kritische Infrastrukturen
- › Bekannte & neue Bedrohungen
- › Bekannte & neue Maßnahmen
- › Bsp.: aktuelle F&E zum Schutz vor Angriffen mit Quantencomputern

## > Empfehlungen

- › Bewusstsein über aktuelle Gefährdungen und Umsetzung Schutz Stand der Technik als Grundlage
- › Bewusstsein neue Bedrohungen und Prüfung wie diese in den Systemen zukünftig berücksichtigt werden
- › Wissen, wo im System Kryptografie, Wissen um PQC
- › Update/Upgradefähigkeit gewährleisten, Krypto-agilität berücksichtigen





# Thank you

[www.thalesgroup.com](http://www.thalesgroup.com)