



POST QUANTUM **PRAKTISCHE ÜBERLEGUNGEN**

RESTRICTED

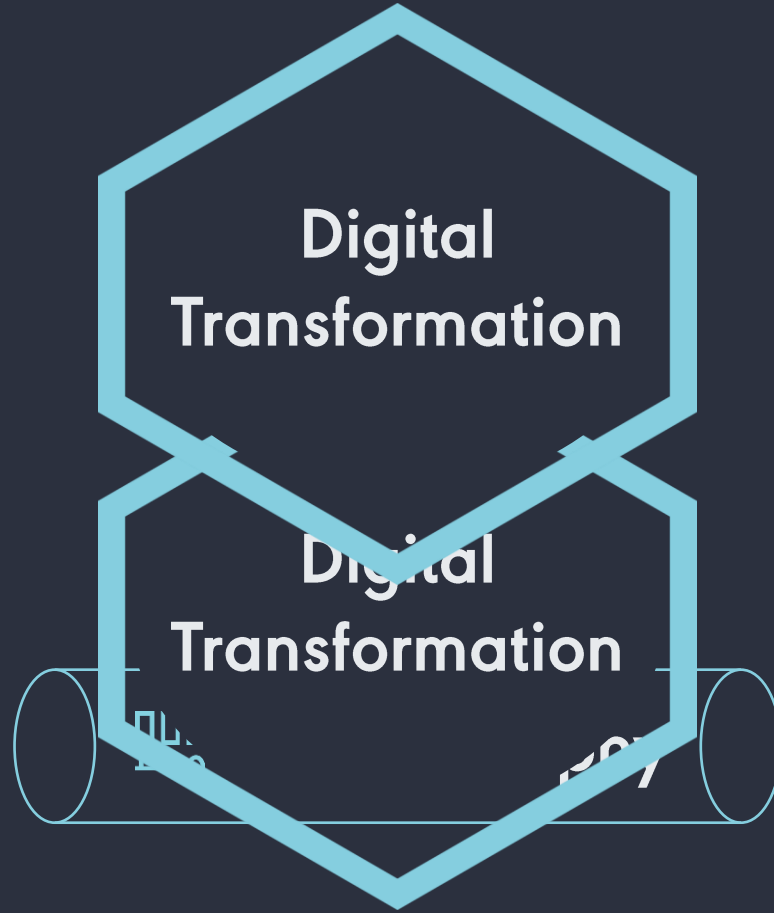
12/06/25

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . +43 (1) 3 555 3-0 . info@cryptas.com

cryptas.com | prime-sign.com
Wien | Graz | Düsseldorf | Hengelo | Stockholm



Digital Transformation



SCOPE / WAS IST BETROFFEN?

— Klassische IT

- Services -> TLS
- Benutzer- / Geräte IDs
- Daten
- Code Signing
- ...

→ Hohe Dynamik / kurze Zyklen

→ Leistungsstarke Systeme

→ Enorme Vielfalt

	User	Devices & Services	Software	Data
Authenticity				
Integrity				
Confidentiality				
Accountability				
Availability				

SCOPE / WAS IST BETROFFEN?

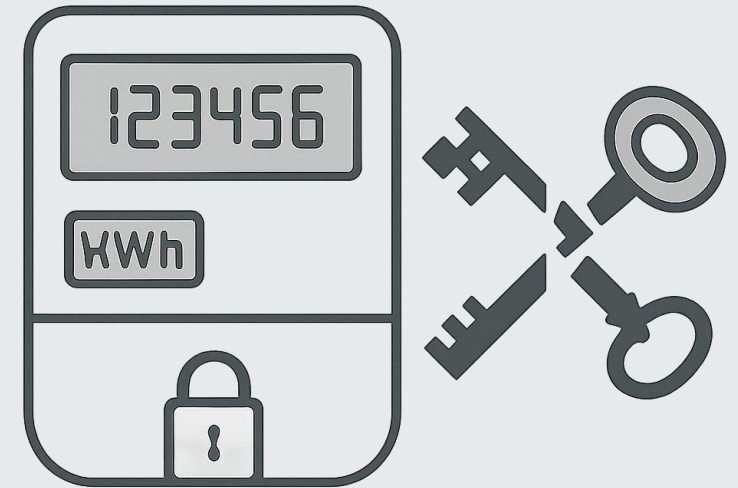
— OT Systeme

- Energieversorgung – z.B. Smart Meters → Roll-Out ~10 Jahre
- Verkehr – z.B. European Train Control System → von 2001 auf 2038 auf 3300km
- Gebäudetechnik - z.B. Zutritt → z.T. mit Umgebung verbunden
- Industrielle Steuerung – z.B. SCADA → Herstellerabhängigkeiten
- ...

→ Oft schwache Hardware

→ Proprietäre Schnittstellen / Komponenten

→ Große Mengen / Rollout



SCOPE / WAS IST BETROFFEN?

— Sonstige Produkte

- Mobilität – z.B. Connected Car
- Internet of Things – z.B. Heizanlage
- Raumfahrt
- ...

→ Lebenszyklen

→ Erreichbarkeit

→ Unbeachtet



z.B. Voyager 1 + 2:

Seit 1977 unterwegs...

EINORDNUNG / SICHERHEIT

- + Mathematische Sicherheit
- + Qualität der Implementierung
- + Qualität Enrollment
- + Qualität der Schlüsselablage
- + Qualität der Schlüsselanwendung
- + Qualität Life-Cycle-Management



→ Das schwächste Glied bestimmt das Resultat

ZEITACHSE / BEURTEILUNG KRITIKALITÄT

- **Authentifizierung / Identität**

z.B. eID, MFA...

- **Integritätsschutz**

z.B. Digitale Signatur

- **Vertraulichkeit**

z.B. Verschlüsselung – Schutzdauer

- **Verfügbarkeit / Resilienz**

z.B. Hackerangriffe



ZEITACHSE / BEURTEILUNG CHANGE

— Grundsätzlicher Ablauf je Komponente

- 1.) Standardisierung
- 2.) Umsetzung in Produkten
- 3.) Implementierung des Systems
- 4.) Rollout

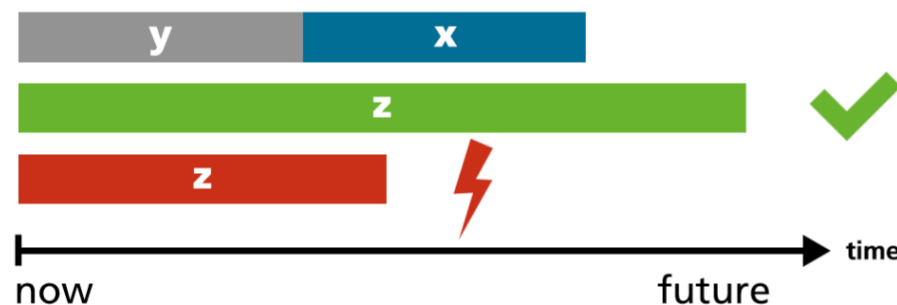
— Abhängigkeiten in der Systemarchitektur

- 1.) Basis / Technologie → z.B. Einrichten einer PQC-PKI
- 2.) Plattformen → Betriebssysteme / Webserver / Infrastruktur
- 3.) Applikationen → Beispiel MDM

ZEITACHSE / PLANUNG

Open question: How big is the threat by quantum computers?

Since it is hard to predict z, the question remains open.



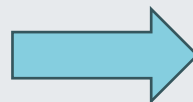
x: time that secrets must remain secret

y: time it takes to deploy quantum-computer secure cryptography

z: time it takes until quantum computers break current cryptography

If z is larger than x+y, we are fine. If it is smaller, we are in danger!

D-DAY / WANN IST ES SO WEIT?



Vergleich 1950er

5200 Röhren

13.000 kg Gewicht

125kW Spitzenleistung

1905 Operationen / s

DIMENSION / VERGLEICH Y2K

- 2-digit Jahreszahl um Speicher zu sparen

1975: 100 USD/kByte

- „Major Topic in 1990s“ → Vergleich Komplexität!

- Kosten / Aufwand

- Alleine US Medicare-Programm ~500 Mio USD
- Kosten gesamt weltweit geschätzt > 500 Mrd EUR



NEXT STEPS / NICHT WARTEN

- **1. Sensibilisierung und Risikobewertung**

Informieren, Assets identifizieren, Risiken Bewerten

- **2. Kryptographische Bestandsaufnahme (Crypto Inventory)**

Erfassen der verwendeten kryptographischen Verfahren, Schlüsselgrößen und Protokollen

Inventarisieren aller Zertifikate und der jeweiligen Einsatzumgebung

- **3. Kryptoagilität sicherstellen**

Anforderungen an Lieferanten über Procurement

- **4. Testen von PQC-Verfahren (Pilotierungen)**

- **5. Roadmap entwickeln und auf Standards achten**