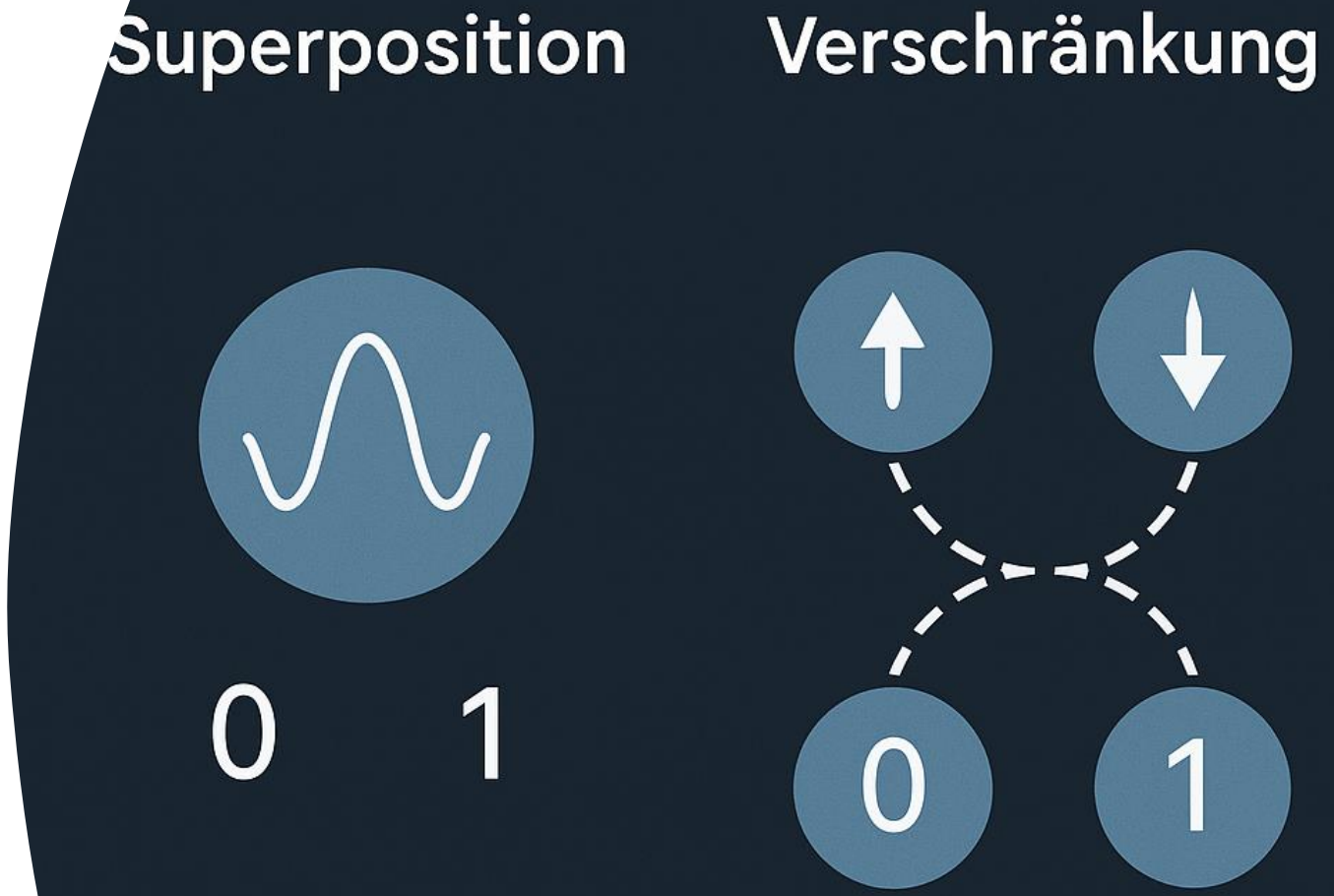
Neue Schlüssel braucht das Amt

Schutz vor Quantencomputern

Arne Tauber – A-SIT
ADV E-Government Konferenz – Wien 4.6.2025

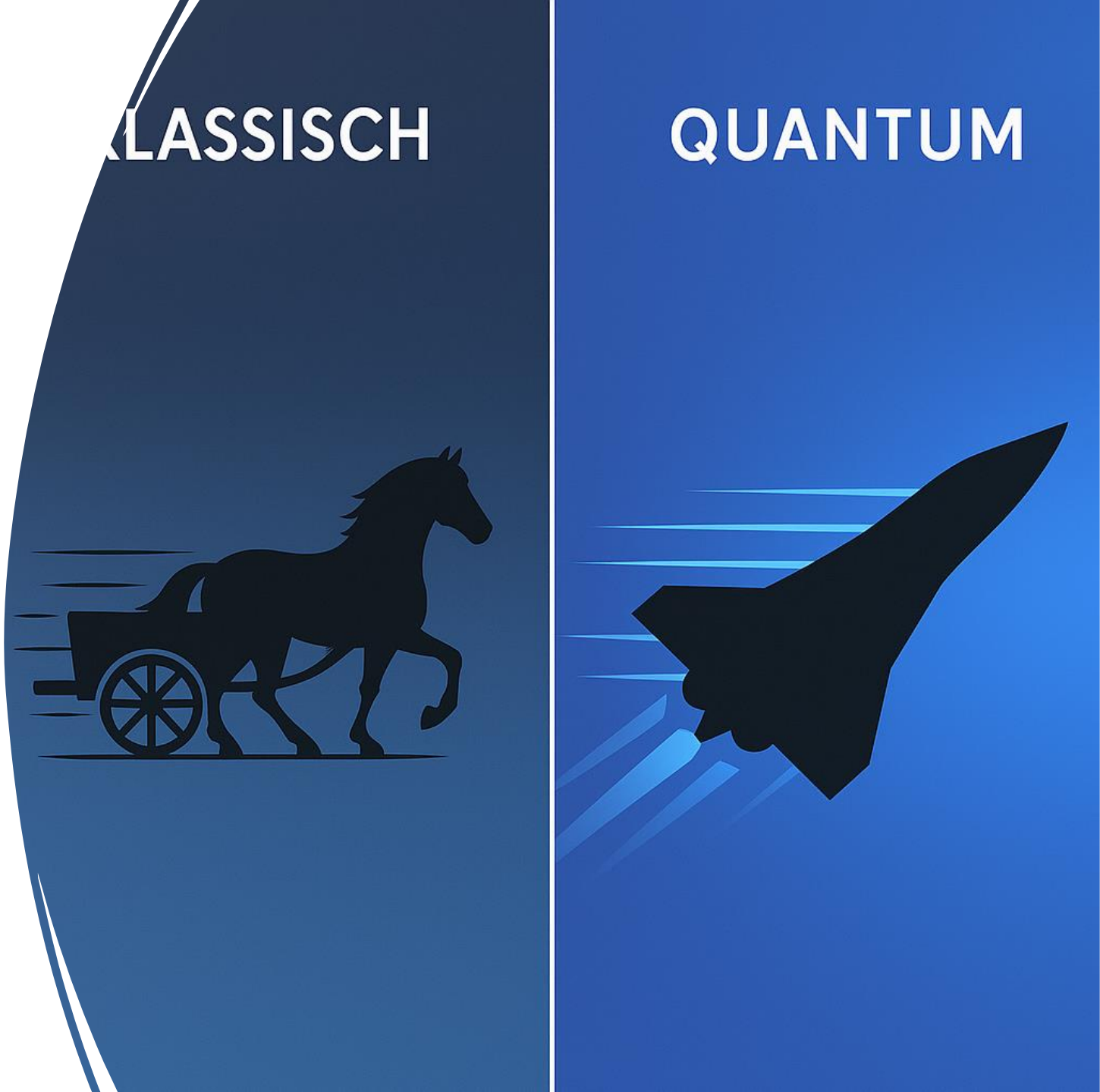
Quantencomputer in 60 Sekunden

- Qubits & Superposition
- Verschränkung = Parallelismus
- Fehlerkorrektur als Hürde



Wie schnell können sie werden?

- Beispiel: RSA-2048+
- Mit klassischen Supercomputern
  - Länger als Alter des Universums
- Cryptopocalypse: mit Quantencomputer in 8 Stunden
  - ~20 Mio logische Qubits
  - Aktuell ~1.000 (phy, ca. 100 log)



Risiko: Digitale Signaturen

- ID Austria / PVP
- Amtssignaturen
- Langzeitarchivierung
- Software-Updates
- Digitale Währungen
- …

Risiko: Verschlüsselung

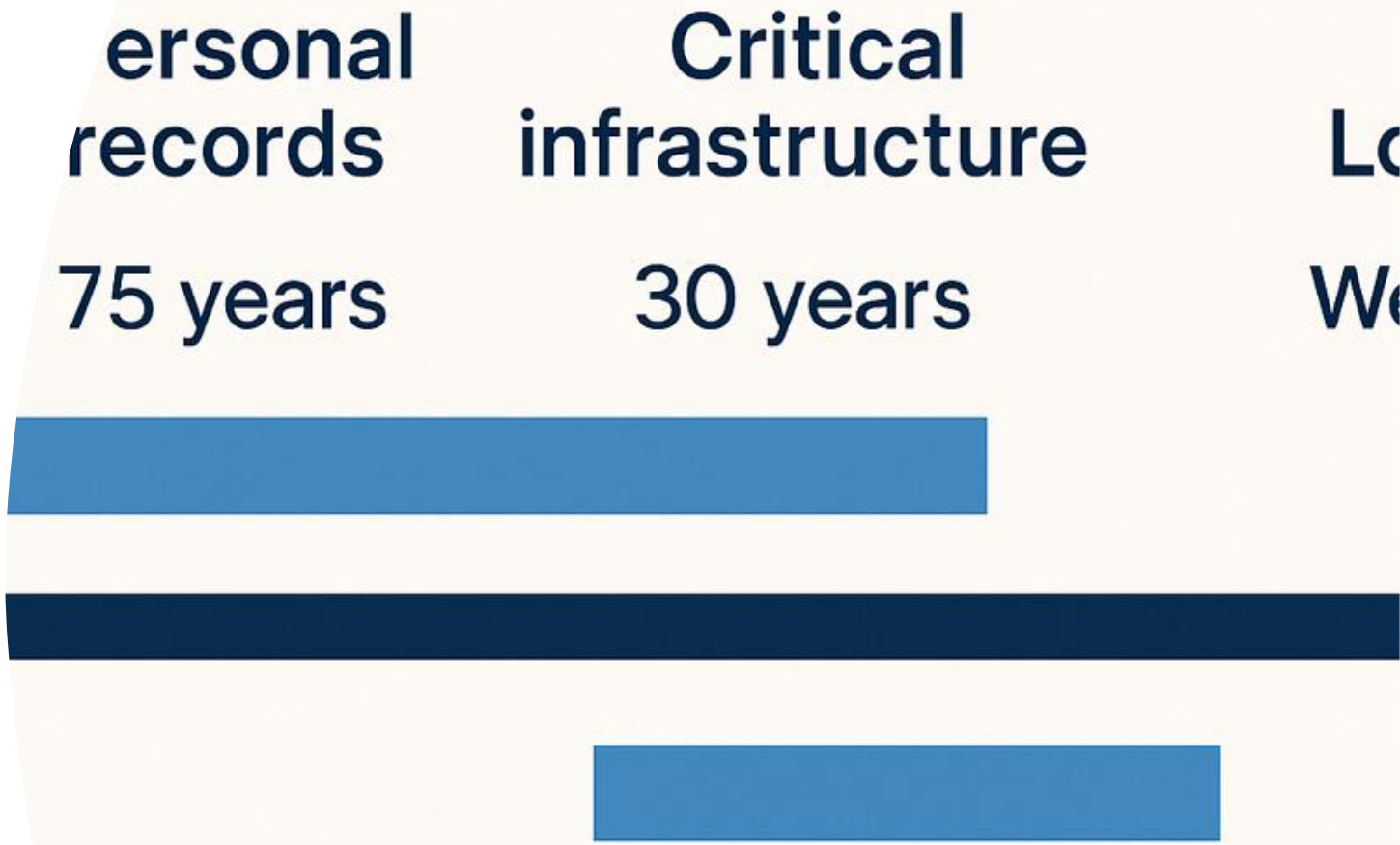
- TLS / VPN / E-Mail
- Klassifizierte Informationen
- Langzeitarchivierung
- Andere: Gesundheits- & Bürgerdaten

Countdown zum „Q-Day“

- Prognosen: 10-15 Jahre
- Harvest-now, decrypt-later
  - Abhören läuft bereits
  - Spätere Entschlüsselung
  - Unsichtbares Risiko
- Frühzeitig Vorsorge treffen

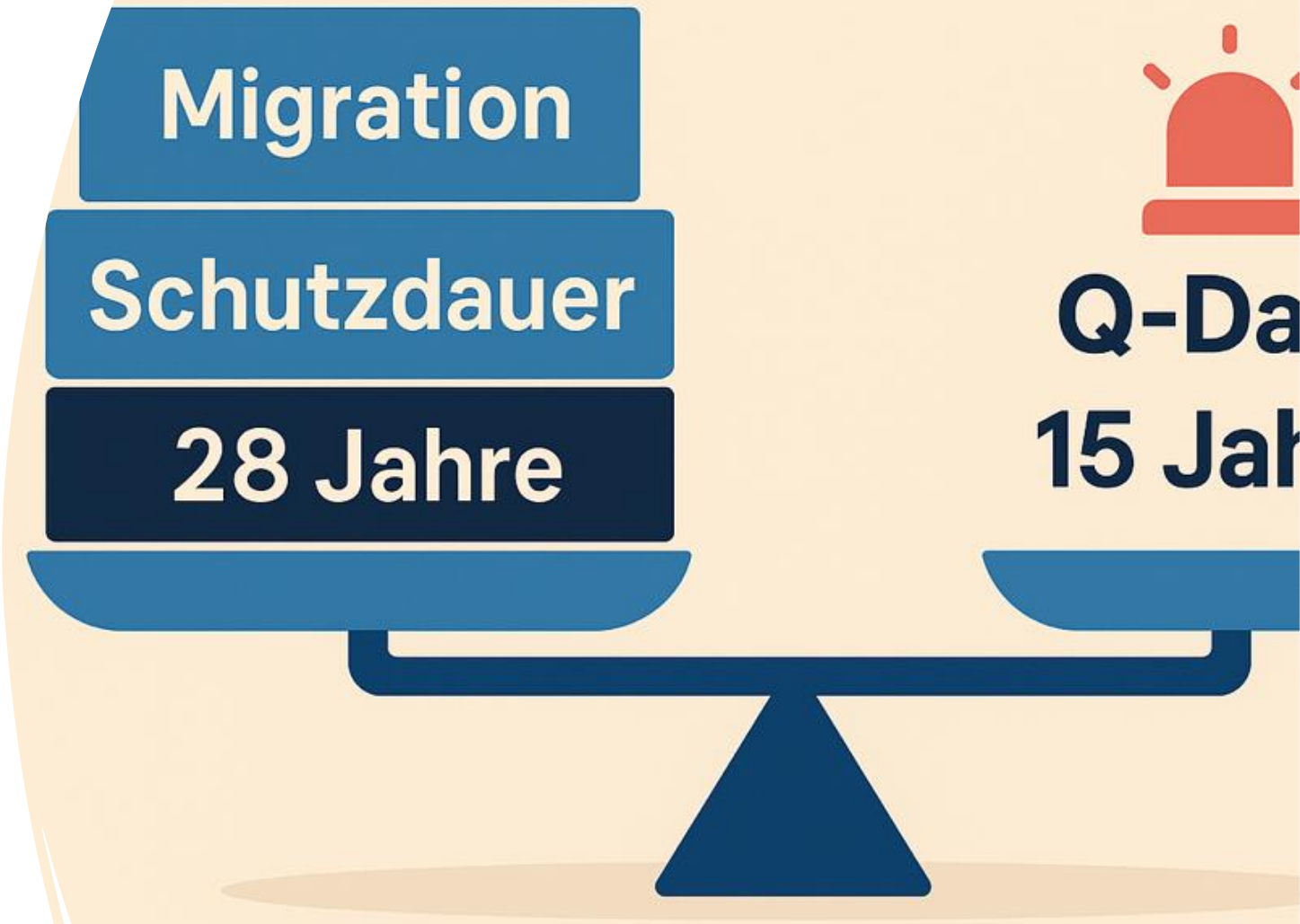
Schutzziel von Daten

- Datenlebenszyklus
  - Logs → Wochen
  - Infrastrukturpläne → 30 J
  - Personenakten → 75 J
- Wert
  - Klassifizierte Informationen
  - Vertrauliche Daten (Gesundheit)
  - Weniger kritische Daten
- Abhängigkeiten meines Schutzes
  - HW mit hoher Lebensdauer



Zeit-zum-Handeln-Gleichung

- Migration + Schutzziel < Q-Day?
- Wenn nein → sofort starten



Was ist Post-Quanten-Kryptografie?

- Keine Quanten-Hardware nötig
- Läuft auf heutiger IT-Infrastruktur
- Mathematischer Abwehrschild
  - „Software Upgrade“
- Ersatz für RSA/ECC
- Quanten-sichere Algorithmen
  - Widerstand gegen Shor & Grover

Standards & Roadmaps

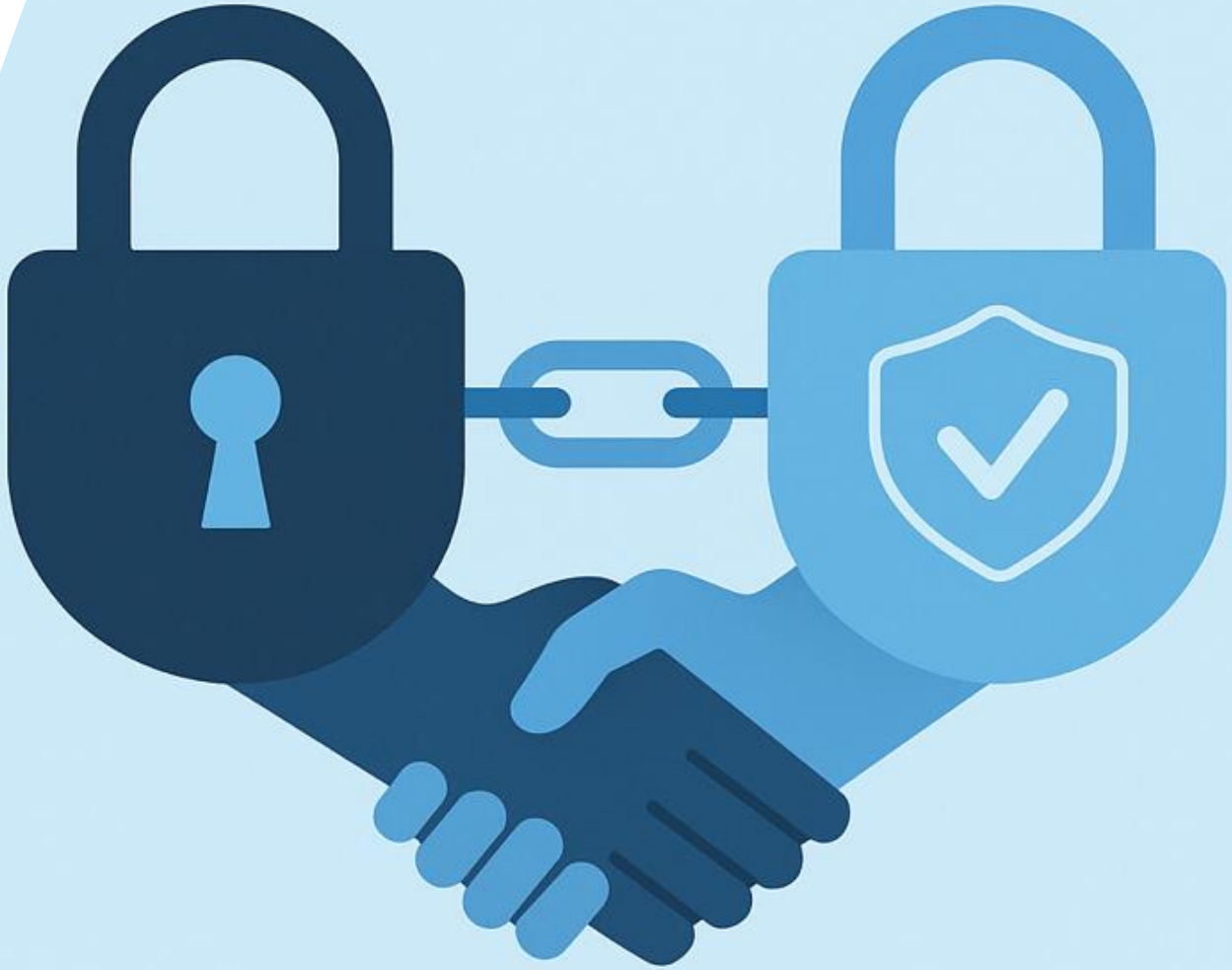
- Algorithmen
  - NIST FIPS 203-205 (2024)
- Leitfäden
  - ENISA, BSI, NCSC, NIST, …
- EU Koordinierte Roadmap (2024)
- Alles nur Theorie?
  - Web-PKI (Google, Cloudflare, …)
  - Integration in Windows 11

Schritt 1: Kryptoinventur

- Betroffene Systeme/Dienste/Daten erfassen
  - SW & HW
  - Algorithmen & Schlüssel erfassen
  - Intern/Extern
  - Supply-Chain
- Kritische Systeme priorisieren

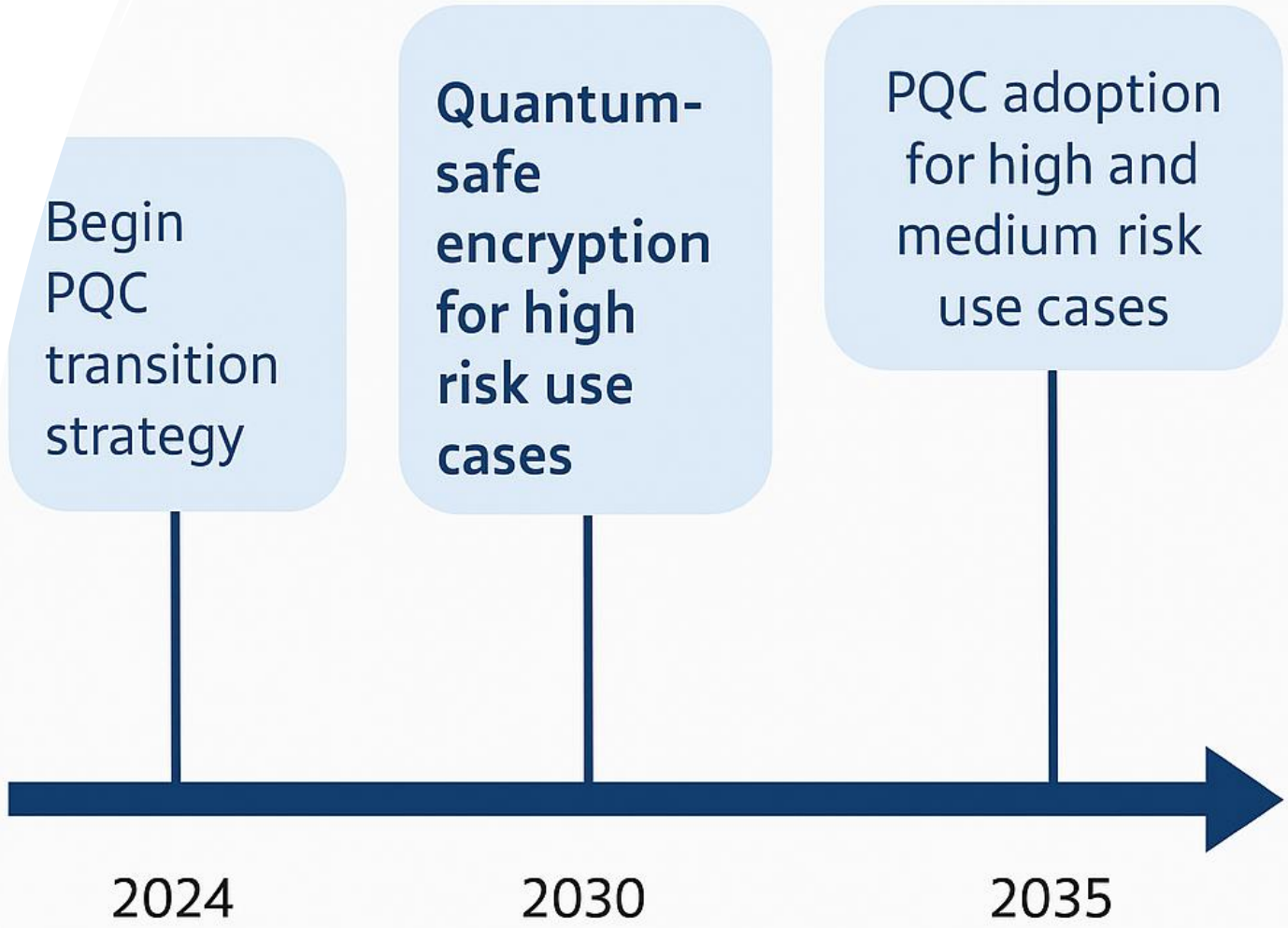
Schritt 2: Migration

- Rahmenbedingungen verstehen
  - Schlüssellängen usw.
- Ansätze
  - Lokale Migration
  - Plattform wechseln
  - Service Einstellen/EOL/Risiko akzeptieren
- Kryptoagilität
  - PKC & PQC Koexistenz
  - PQC + RSA/ECC kombinieren
- Testen / Deployment



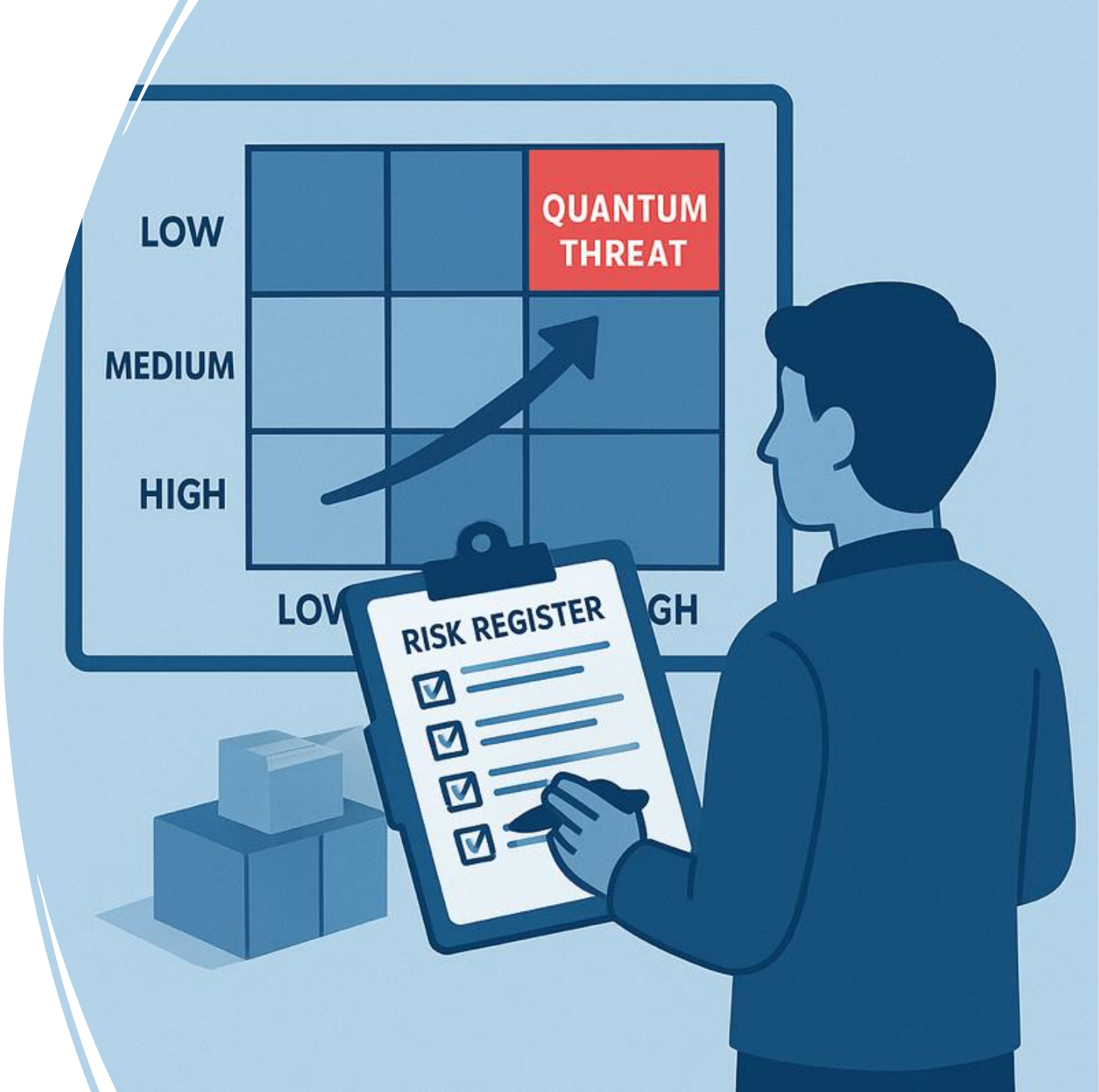
EU Roadmap - Zeitachse

- 2026 – Nationale Roadmaps
- 2030 – Use cases mit hohem Risiko migriert
- 2030 – Use-cases mit niedrig-mittlerem Risiko geplant
- 2035 – Use-case mit mittlerem Risiko migriert



Risikomanagement aktualisieren

- PQC in ISMS integrieren
- 10-Jahres Budget planen



Kernaussagen

- Quantengefahr real
- Umstellung dauert Jahre
- Heute planen

Danke – Fragen?