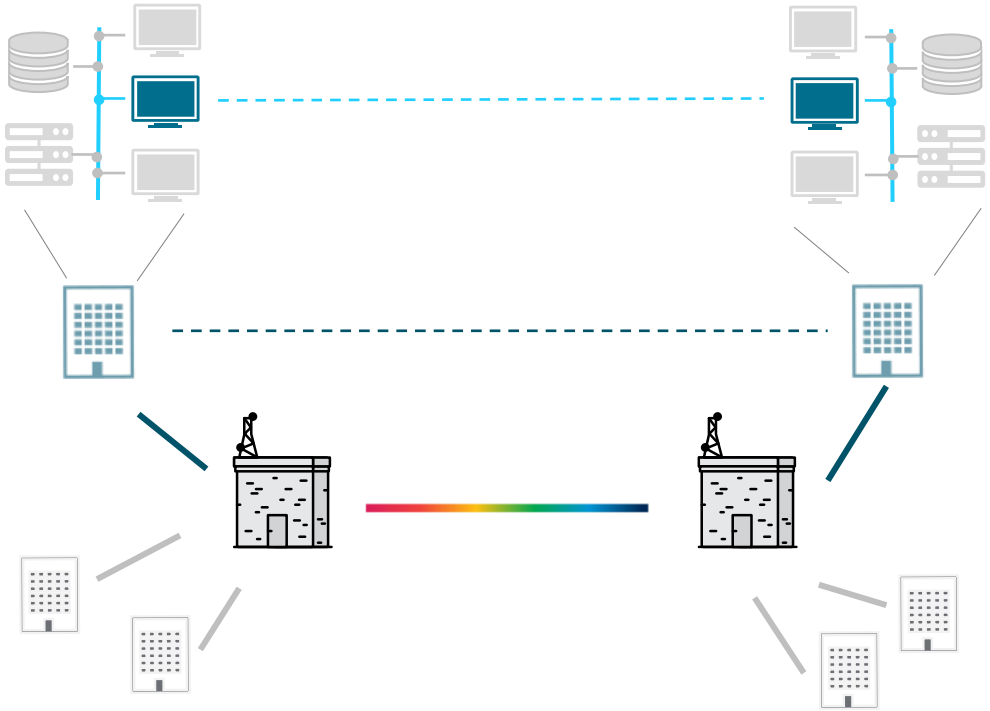
Adva
NETWORK SECURITY

Datensicherheit im Quantenzeitalter

Regulierung, Innovation und Kryptoagilität in Europa

19.1.2026 | OMNISECURE | Dr. Tobias Fehenberger

Ganzheitlicher Schutz in Kommunikationsnetzen



IP Layer 3+ Schutz

Sichere Verbindung von Anwendern mit Anwendungen und Ressourcen

Ethernet Layer 2 Verschlüsselung

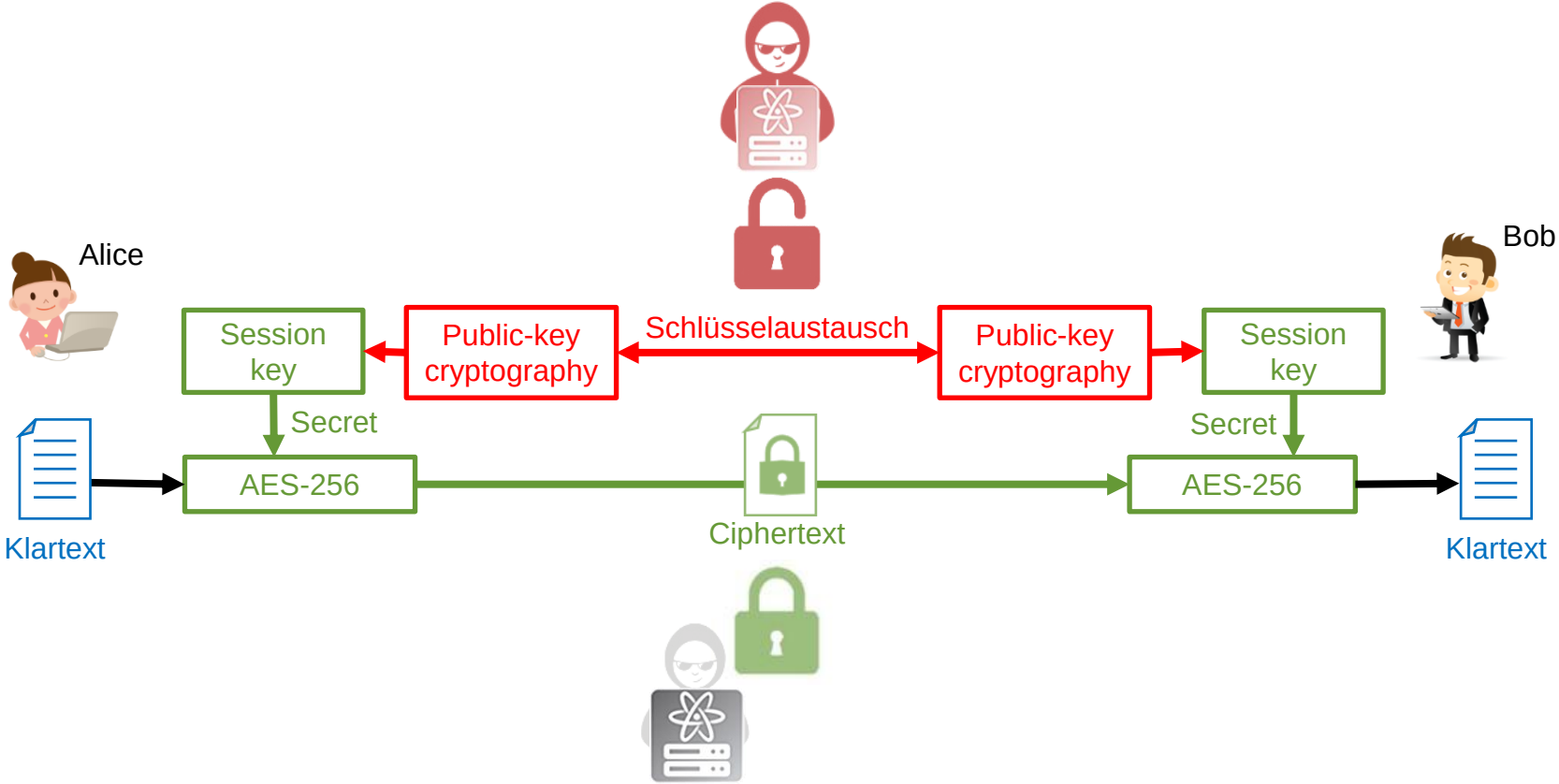
Bandbreitendienste mit geschützten Ende-zu-Ende Verbindungen

Optische Layer 1 Verschlüsselung

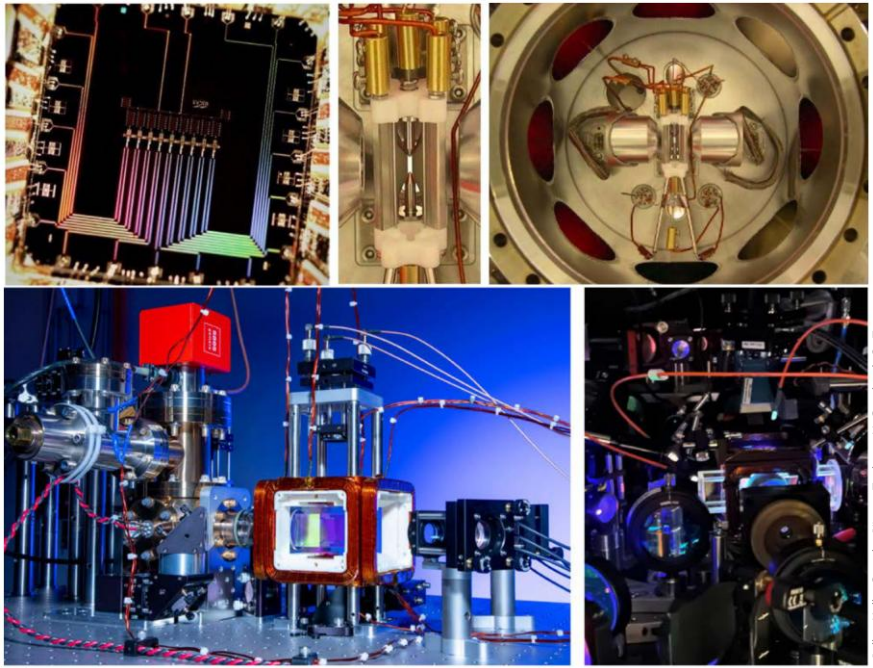
Schutz von optischen Terabit-Verbindungen mit geringster Latenz

Verschlüsselungslösungen für alle Anwendungsfälle

Verschlüsselte Kommunikation



Quantencomputer



Julian Kelly, Google; Jürgen Eschner, U. Saarland; QuEra

BSI Entwicklungsstand Quantencomputer, 2025

Quantencomputer sind bereits heute Realität!

Kryptografisch relevante Quantencomputer

Entwicklungsstand Quantencomputer

Bundesamt für Sicherheit in der Informationstechnik

Deutsche Zusammenfassung

BSI-Projektnummer: 477

„Die kontinuierlichen Verbesserungen der Technik […] lassen das Erreichen des Ziels in etwa 15 Jahren realistisch erscheinen."

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2]

4 Jahre

How to factor 2048 bit RSA integers with less than a million noisy qubits

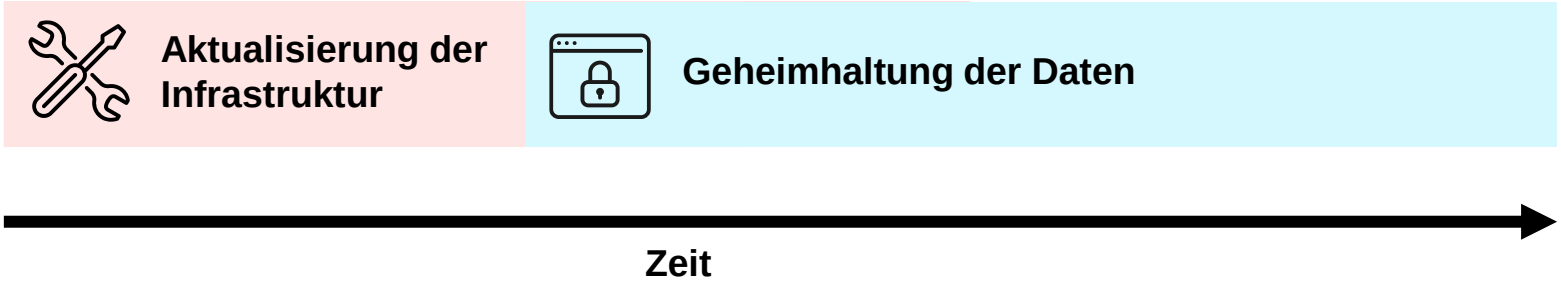
Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA

June 9, 2025

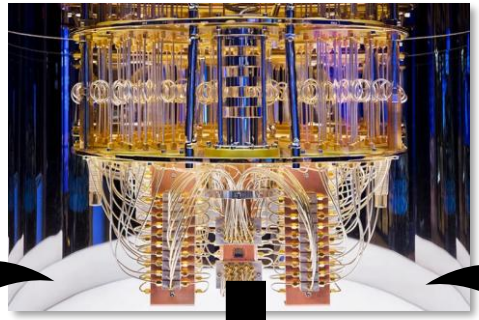
Circa 15 Jahre bis zum „Q-Day"

Das Zeitfenster für Sicherheit schließt sich

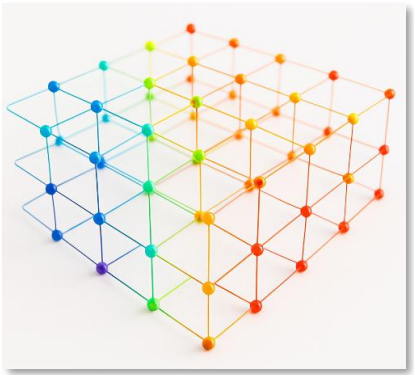


Heute handeln bei sensiblen Daten!

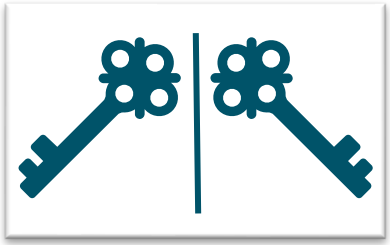
Quantensichere Kryptografie



Post-Quantum Cryptography (PQC)



Verteilung symmetrischer Schlüssel



Quantum Key Distribution (QKD)

NIST PQC-Projekt

Dez 2016
Endgültige Anforderungen und Kriterien

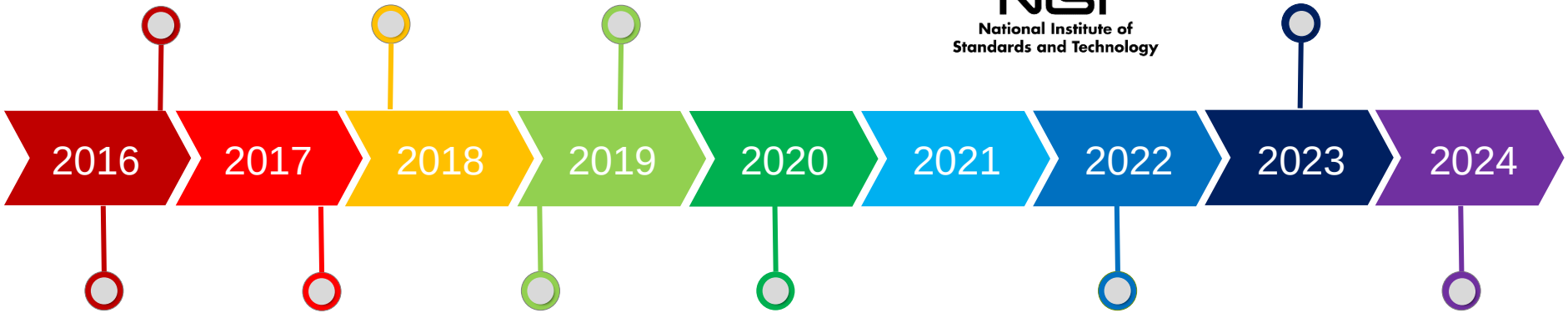
April 2018
1. NIST PQC Workshop

Aug 2019
2. NIST PQC Workshop

2020-2021
Runde 3 Seminare

2023
Entwürfe für Standards veröffentlicht

NIST National Institute of Standards and Technology



Aug 2016
Entwurf der Anforderungen Bewertungskriterien

Nov 2017
Deadline für Einreichungen

Jan 2019
2. Runde gestartet

Jul 2020
Auswahl der Finalisten und Alternativen

Jul 2022
Bekanntgabe der Finalisten zur Standardisierung und Kandidaten für die 4. Runde

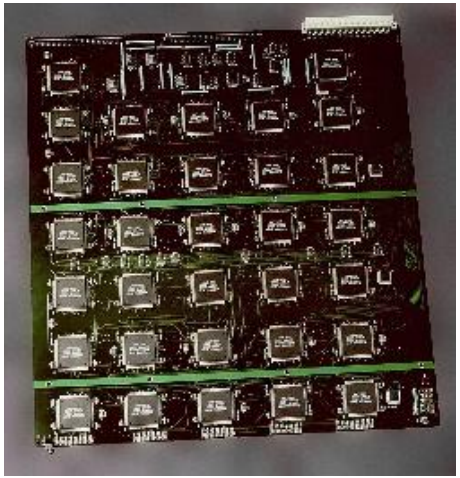
August 2024
Standards finalisiert

PQC: Standards seit 2024

Integration in Kommunikationsprotokolle fehlt teilweise noch

Wie sicher ist PQC gegen klassische Angriffe?

Brute-Force Angriffe

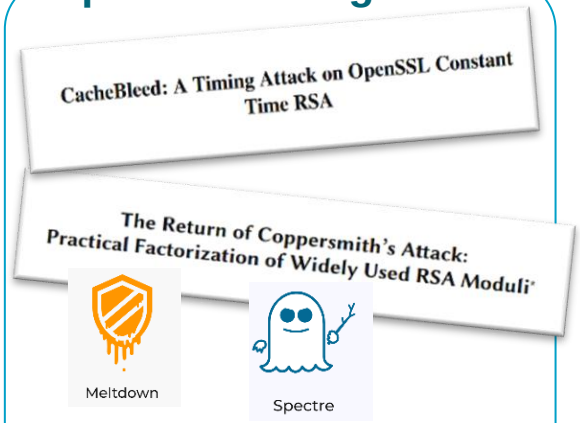


“Deep Crack”
bricht DES (1998)

Mathematische Angriffe

PQC Kandidaten
in 2022 gebrochen

Implementierungsfehler



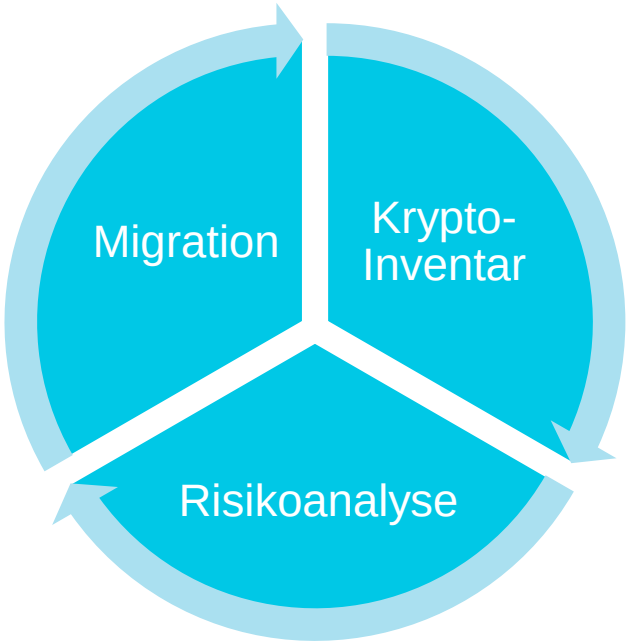
Seitenkanalattacken wird
es wohl immer geben

Kryptoagilität

AG Kryptoagilität

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Kryptoagilität beschreibt einen Prozess bei Herstellern und Anwendern von IT-Systemen, bei dem sicherheitsrelevante kryptografische Komponenten eines IT-Systems als Reaktion auf äußere Einflüsse effizient ausgetauscht werden, ohne die Kernfunktionalitäten zu beeinträchtigen.



Viel mehr als ein Software-Update!

Kryptoagilität

Hersteller

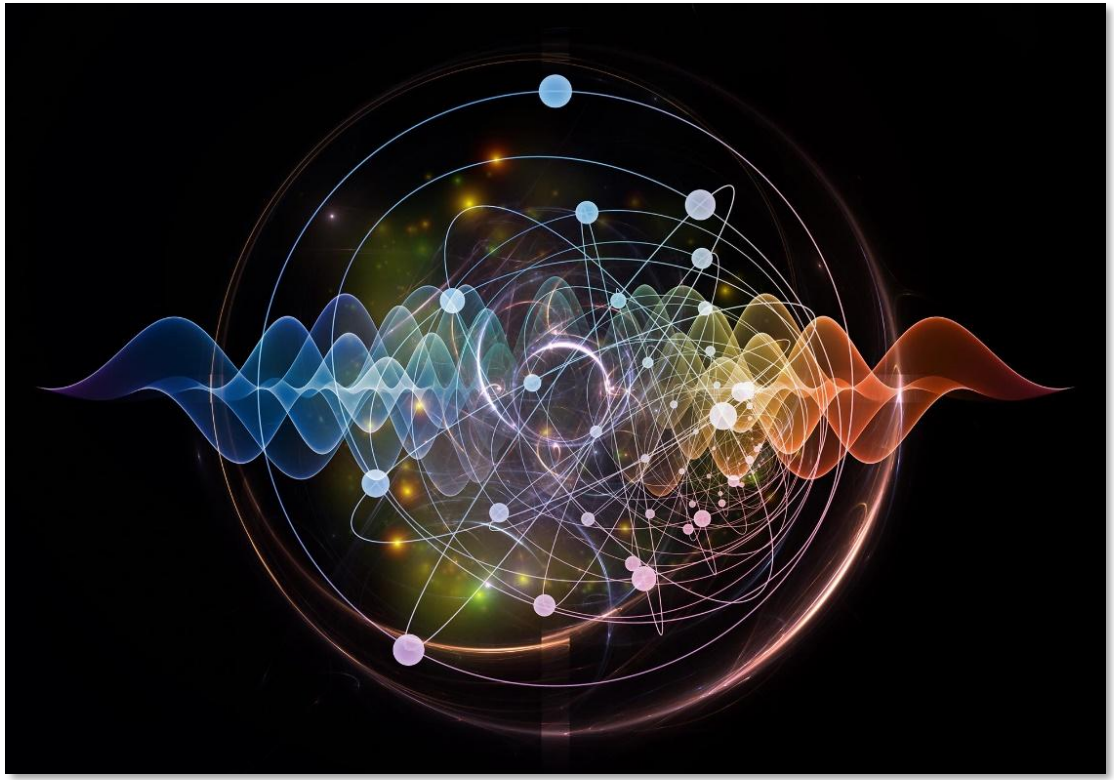
- Modulare und flexible Architektur im Produktdesign
- Konfigurierbarkeit und Austauschbarkeit von kryptografischen Komponenten
- Updatekonzept
- CBOM

Anwender

- Kryptostrategie festlegen
- Anpassung der internen Vorgaben und Prozesse
- Kryptoinventar anlegen
- Risikoanalyse der schützenswerten Assets
- Migration

Komplementäre Anforderungen für Hersteller und Anwender

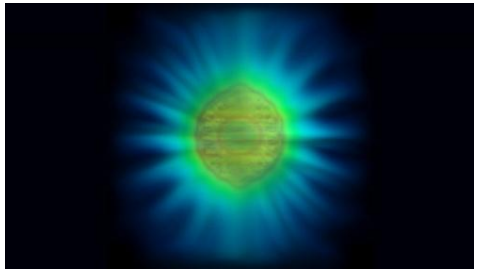
Quantum key distribution (QKD)



QKD: Ausprägungen

DV-QKD

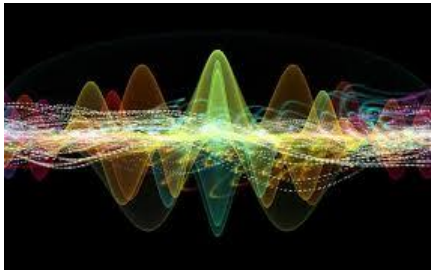
- Etablierteste QKD Variante



DV: discrete-variable

CV-QKD

- Technologien aus der optischen Daten-übertragung



CV: continuous-variable

EB-QKD

- Verwendet verschränkte Photonenpaare

EB: entanglement-based

QKD: Sichtweise der Europäische

Due to current and inherent limitations, QKD can however currently only be
use cases. For the vast majority of use cases where classical key agreement sch
not possible to use QKD in practice. Furthermore, QKD is not yet sufficiently
perspective. In light of the urgent need to stop relying only on quantum-vul
cryptography for key establishment, the clear priorities should therefore be
cryptography and/or the adoption of symmetric keying.

QKD may find some use in a few niche applications, for instance as a defense-in-depth measure on point-to-point links. However, the use of state-of-the art classical cryptography including post-quantum algorithms is by far the preferred way to ensure long-term protection of data, as it is the only technology choice that offers the functional properties needed in modern communication systems.

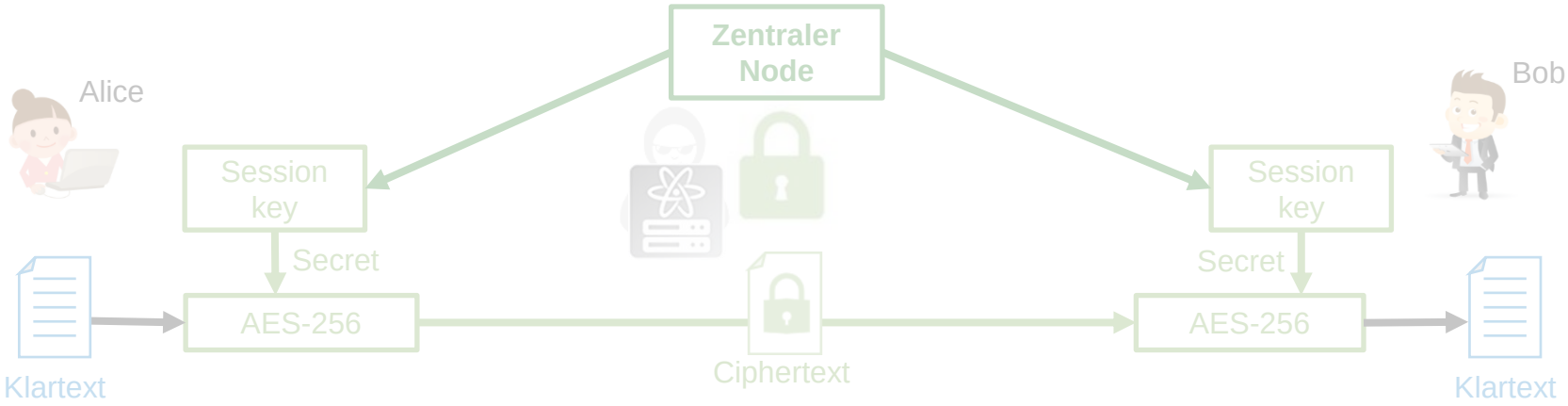
ANSSI, France

NSA continues to evaluate the usage of cryptography solutio
transmission of data in National Security Systems. NSA doe
of quantum key distribution and quantum cryptography for
data in National Security Systems (NSS) unless the limitati

use of QKD for
st sole reliance on
al Infrastructure

UK

Verteilung symmetrischer Schlüssel



! Komplexität **! Abhängigkeiten** **! Angriffsfläche**

Eingebetteter Schlüsselaustausch ist die Zukunft

EU-Verordnungen

NIS2

- Reguliert Organisationen (KRITIS, Telco‘s, IT-Dienstleister)
- Umsetzung von Maßnahmen zur Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit von IT-Systemen
- Umsetzung in Deutschland: Dez 2025

CRA

- Reguliert Produkte und Hersteller
- Teil der CE-Kennzeichnung
- Regelt Anforderungen an Cybersicherheit (Security by Design, SBOM, …)
- Anwendbar: Dezember 2027

Organisationen

Governance

Produkte

HW / SW Design

Cybersicherheit-Standards in der gesamten EU

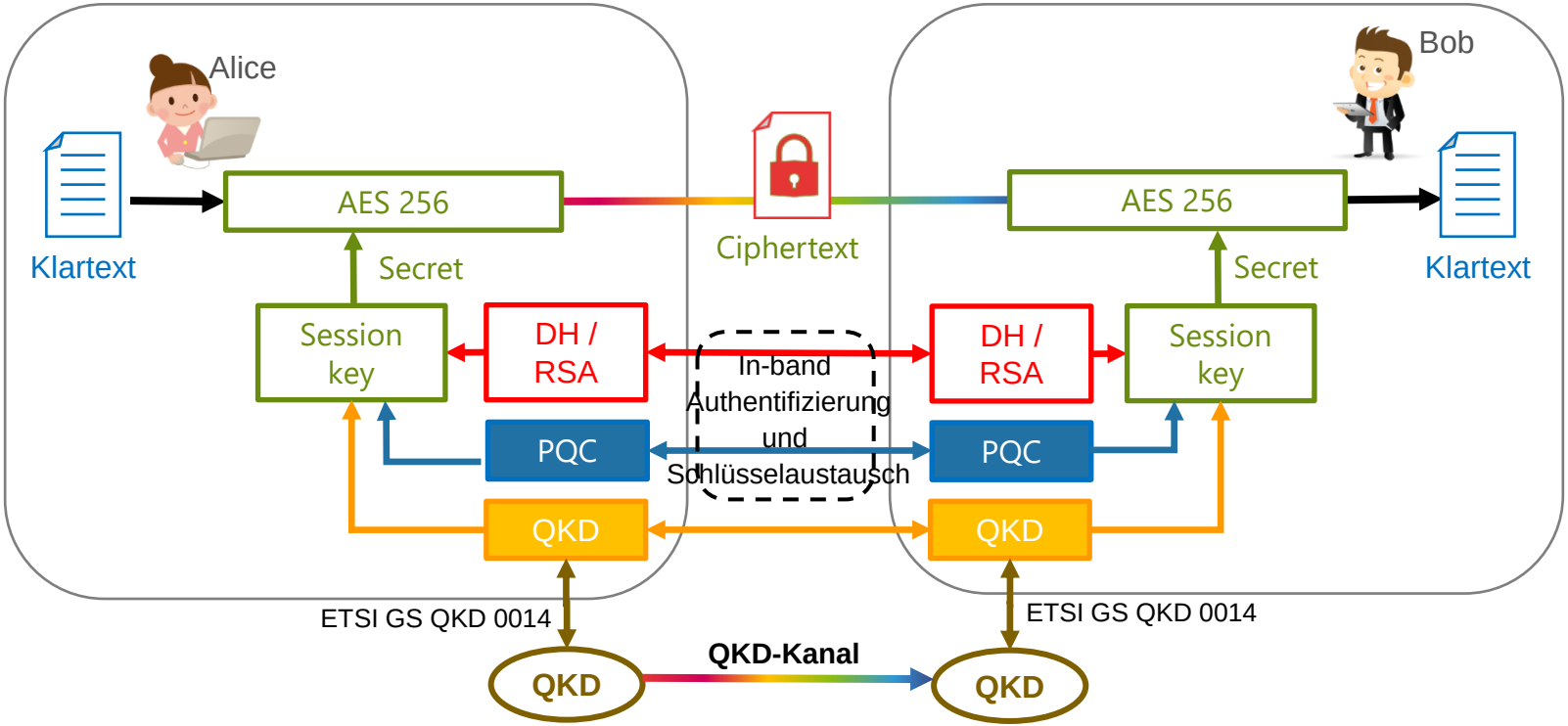
EU-Verordnungen: Spotlight PQC

Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

Klare Zeitlinien für PQC-Migration

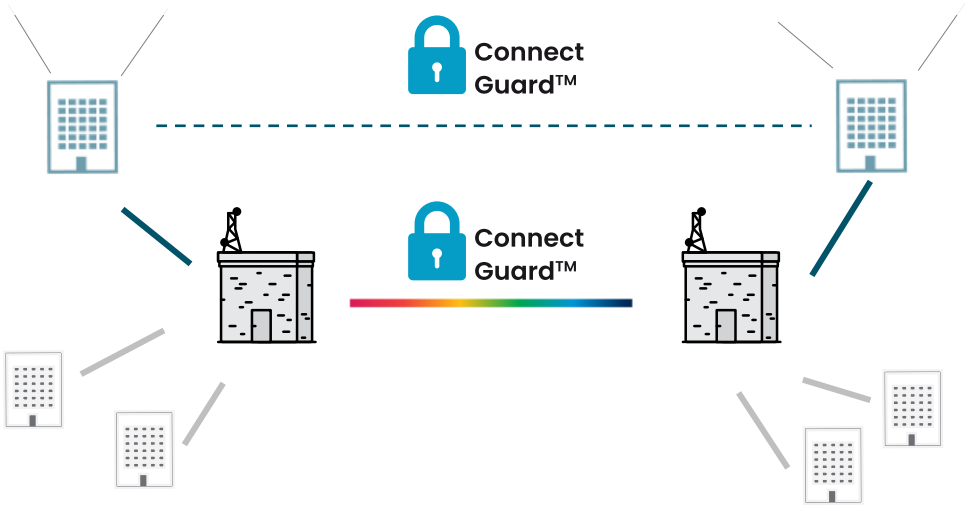
Quantensicherheit



Zukunftssicherer und flexibler Schutz vertraulicher Daten

Ganzheitlicher Netzschutz

Bereits heute echte Quantensicherheit



Ethernet Layer 2 Verschlüsselung

Bandbreitendienste mit geschützten Ende-zu-Ende Verbindungen

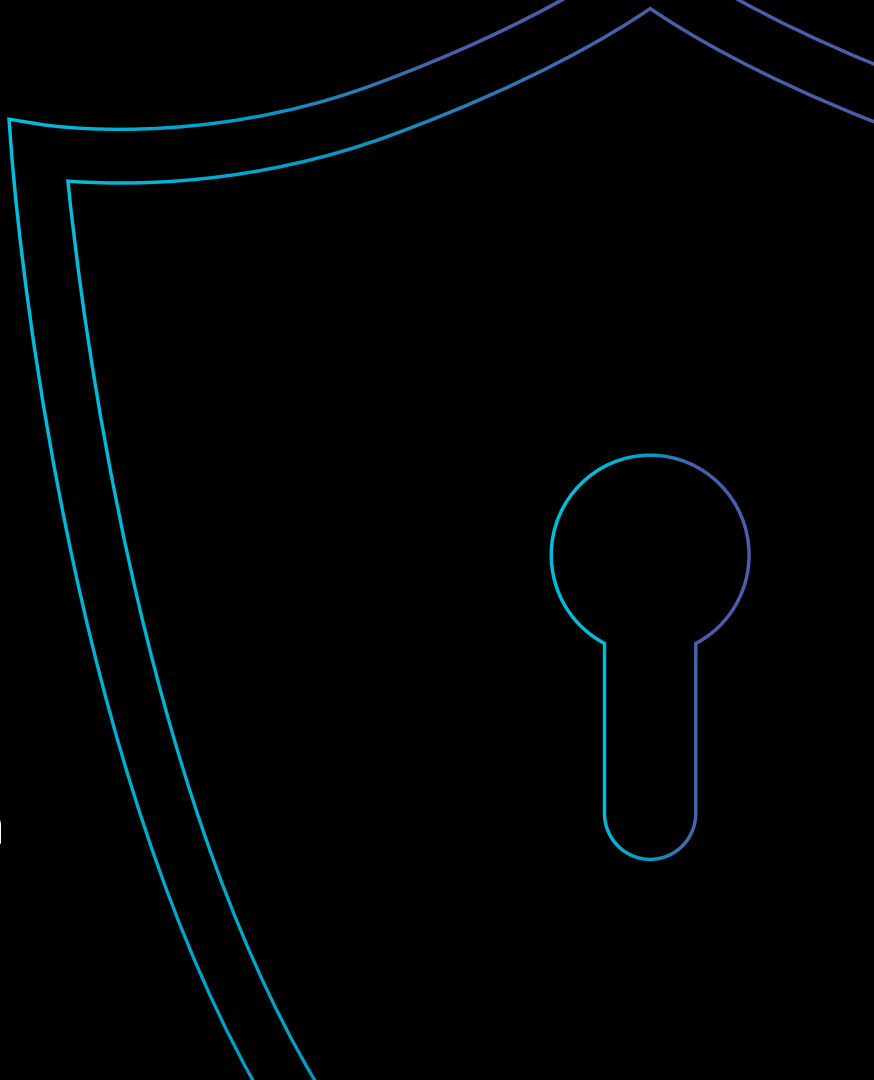
Optische Layer 1 Verschlüsselung

Schutz von optischen Terabit-Verbindungen mit geringster Latenz

Die Bedrohung durch Quantencomputer

- Quantencomputer brechen klassische Schlüsselaustauschverfahren
- Konkrete Angriffsszenarien existieren bereits heute
- Fokus auf PQC-Verfahren
- Untere Netzwerkschichten sind schon heute quantensicher

Migration zu Quantensicherheit kann und muss heute starten!



Danke für Ihre Aufmerksamkeit!

tobias.fehenberger@advasecurity.com