ISSX IT-Security Swiss Conference

VOGEL IT AKADEMIE

www.issxconference.ch

#issxconference

ISSX

TEMET
end-to-end IT security

Bist Du vorbereitet, wenn Quantencomputer Deine Daten morgen knacken?

André Clerc, TEMET AG

26.06.2025, Pfäffikon SZ

Über den Referenten

André Clerc
Dipl. Inf.-Ing. FH , CISSP,
CAS Project Management

Managing IT Security Consultant
Tätig in der Information Security seit 2000

Kern Kompetenzen

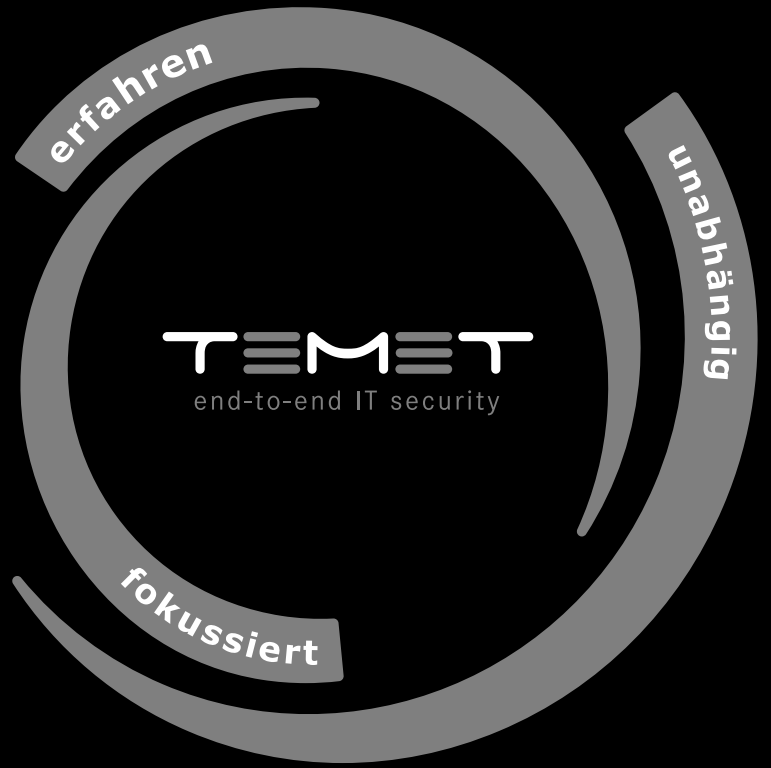
- Security Consulting und Engineering
  Entwicklung von Systemen/Lösungen, welche gegenüber von Böswilligkeit, Fehlern oder Missgeschicken resistent sind
- PKI/M, angewandte Kryptographie
- Kontinuierliche Systemhärtung
- Business Process Modelling (BPMN 2.0)

Engagements

- Founder of About & Beyond Trust Conference
- Author of PKI Education @ SwissSign

TEMET AG

- 14 erfahrene Security Consultants
- Über **250 Jahre** Erfahrung
- **100% unabhängig** – produktneutral und nur unseren Kunden verpflichtet
- Über **155 Kunden** aus unterschiedlichen Branchen
- In der ganzen Schweiz tätig - Sitz im Herzen von Zürich



Wir planen, konzipieren und realisieren Sicherheitsvorhaben und unterstützten unsere Kunden bei der nachhaltigen Gewährleistung ihrer Security.

Quantencomputer brechen RSA & ECC

TEMET
end-to-end IT security

Echte News

QUANTUM INSIDER

Google Researcher Lowers Quantum Bar To RSA Encryption

Research Matt Swayne • May 24, 2025

RSA-2048

Breaking RSA-2048 in a w with a million qu

Insider Brief

- A new study from Google Quantum AI estimates that breaking RSA-2048 encryption could be achieved in under a week using fewer

finanzen.net Depot eröffnen Depot

Home » D... » Google warnt: Quantencomputer könnten Bitcoin- und RS...

QUANTENRESSOURCEN IM BLICK

Google-Studie: Quantencomputer bedrohen RSA- und Bitcoin-Verschlüsselung früher als gedach

03.06.25 23:36 Uhr

Ein Forschungsteam von Google zeigt, dass RSA Verschlüsselungssysteme mit deutlich weniger Quantenressourcen geknackt werden könnten bislang angenommen.

New Scientist

Subscribe now

echnology

BM says it will build a practical quantum upercomputer by 2029

he company has unveiled new innovations in quantum hardware and software at researchers hope will make quantum computing both error-proof and useful efore the end of the decade

y Karmela Padavic-Callaghan

10 June 2025

Wieso ist das relevant?

- Moderne digitale Sicherheit beruht u.a. auf Verschlüsselungsalgorithmen, die auf schwierige mathematische Probleme zurückgreift
- **Asymmetrische Kryptografie** (**RSA, ECC, DH**) bildet die Grundlage des heutigen sicheren Internetverkehrs; ist mit heutigen Computern nicht zu knacken (vgl. PKI)
  - Ermöglicht fremden Teilnehmern im Internet, Schlüssel sicher auszutauschen & Identität zu prüfen (Websites, Messaging-Apps, etc.)
  - **Sicherheit fällt** mit der Lösbarkeit der mathematischen Probleme
- **Leistungsfähige Quantencomputer** werden in der Lage sein die mathematischen Probleme zu lösen
  - Schutz der Daten wird mit klassischer asymmetrischer Kryptografie nicht mehr möglich sein

Schutzmöglichkeiten von Daten

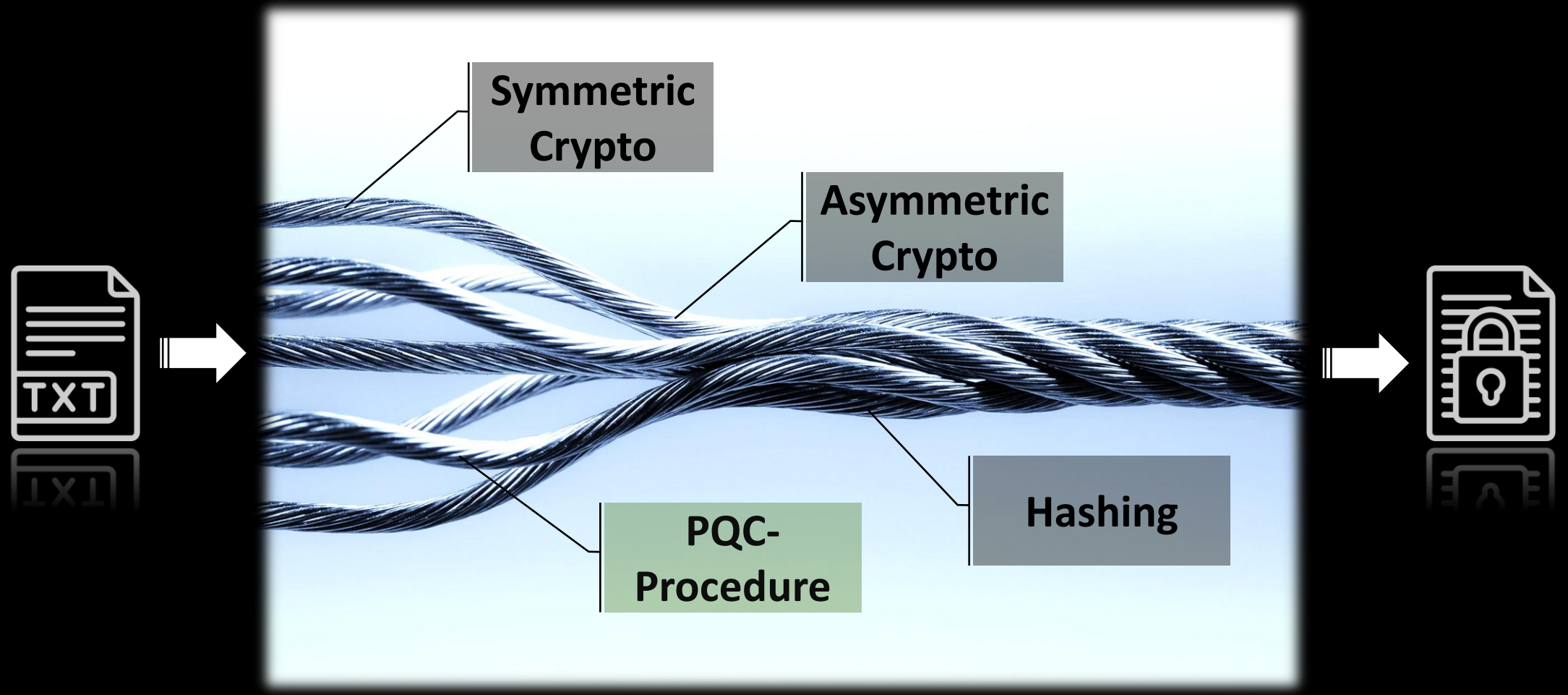
Asymmetrische Kryptographie

- Schlüsselaustausch und Authentisierung im Internet (digitale Zertifikate
- Schlüsselpaar
  - **öffentlicher** Schlüssel zur Verschlüsselung oder Signaturprüfung
  - **privater** Schlüssel zur Entschlüsselung oder Signatur
- *Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH/E), & ECC*
- **Nicht Quantum-safe**

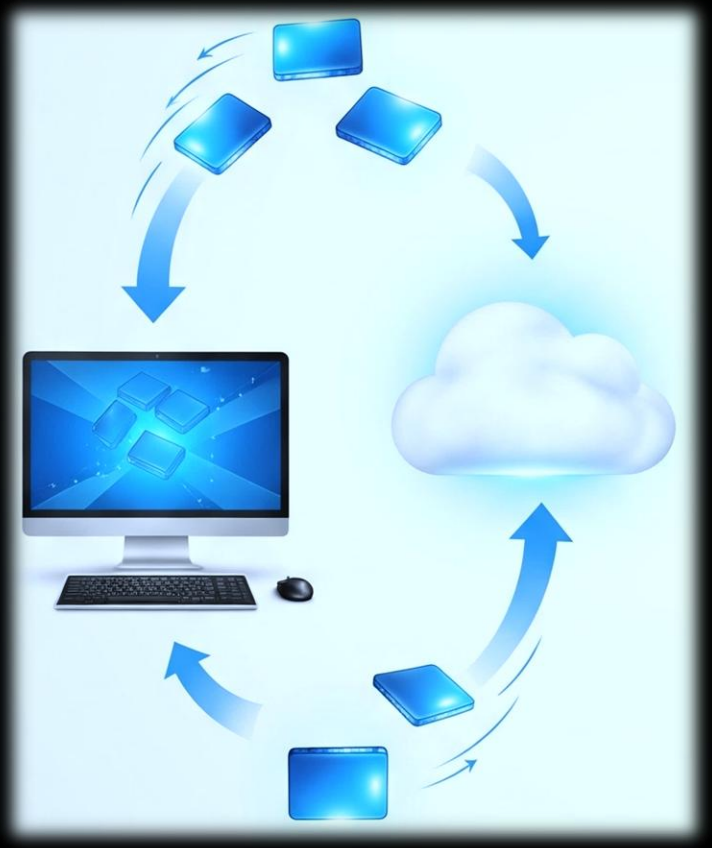
Symmetrische Kryptographie

- Verschlüsselung
- Für die Verschlüsselung grosser Datenmengen
  → Datenstrom, Festplatten, Passwortspeicher, etc.
- *Advanced Encryption Standard (AES, Rijndael), ChaCha20*
- **Qantum-safe**

Hybrider Schutz von Daten



Gefährdete Daten - Handlungsbereiche



- **Vertrauliche (verschlüsselte) Verbindungen** - *Data in Transit*
  - Verbindungen zu Webservern (HTTPS; TCP)
  - Secure E-Mail (S/MIME, PGP)
  - Datagram Transport Layer Security (DTLS)
    - Real-time Communication (WebRTC), VoIP, VPN (OpenVPN), IoT-Kommunikation
  - VPN
    - IPSec
    - WireGuard
  - SSH

Gefährdete Daten - Handlungsbereiche

- **Vertrauliche (verschlüsselte) Daten** - *Data at Rest*
  - Festplatten
  - Dateiserver (Shares)
  - Datenbanken
  - Cloud-Speicherdienste (AWS S3, Azure, Dropbox, Proton Drive,…)
  - Key Stores/Vaults
  - Mobile Geräte, Laptops, Smartphones, Tablets
  - VMs
  - Backup-Medien (Cloud Backup) & Archive
  - ...

Gefährdete Daten - Handlungsbereiche

- Bitcoins
- Blockchains
- Digitale Zertifikate und Zertifikatsausgabe Stellen (CAs)
- Geräte und Benutzer Authentifizierung
- Instant Messaging
  - WhatsApp, Viber, Telegram, …
- IoT Kommunikation
- Real-time Communication (RTC)
  - Audio and Video Streams (Zoom, Microsoft Teams, Google Meet, …)
- Sichere E-Mail
- Signierte Verträge, Dokumente und Daten
  - Signierte PDF, SW- & OS-Pakete, Code, Viren-Signaturen, Konfigurationsdateien, …
- Vertrauliche Dokumente und Daten

Potentielles Risiko

Verfügbarkeit
leistungsfähiger Quantencomputer

Sammeln von
vertraulichen Daten

Um diese im Nachhinein
zu entschlüsseln

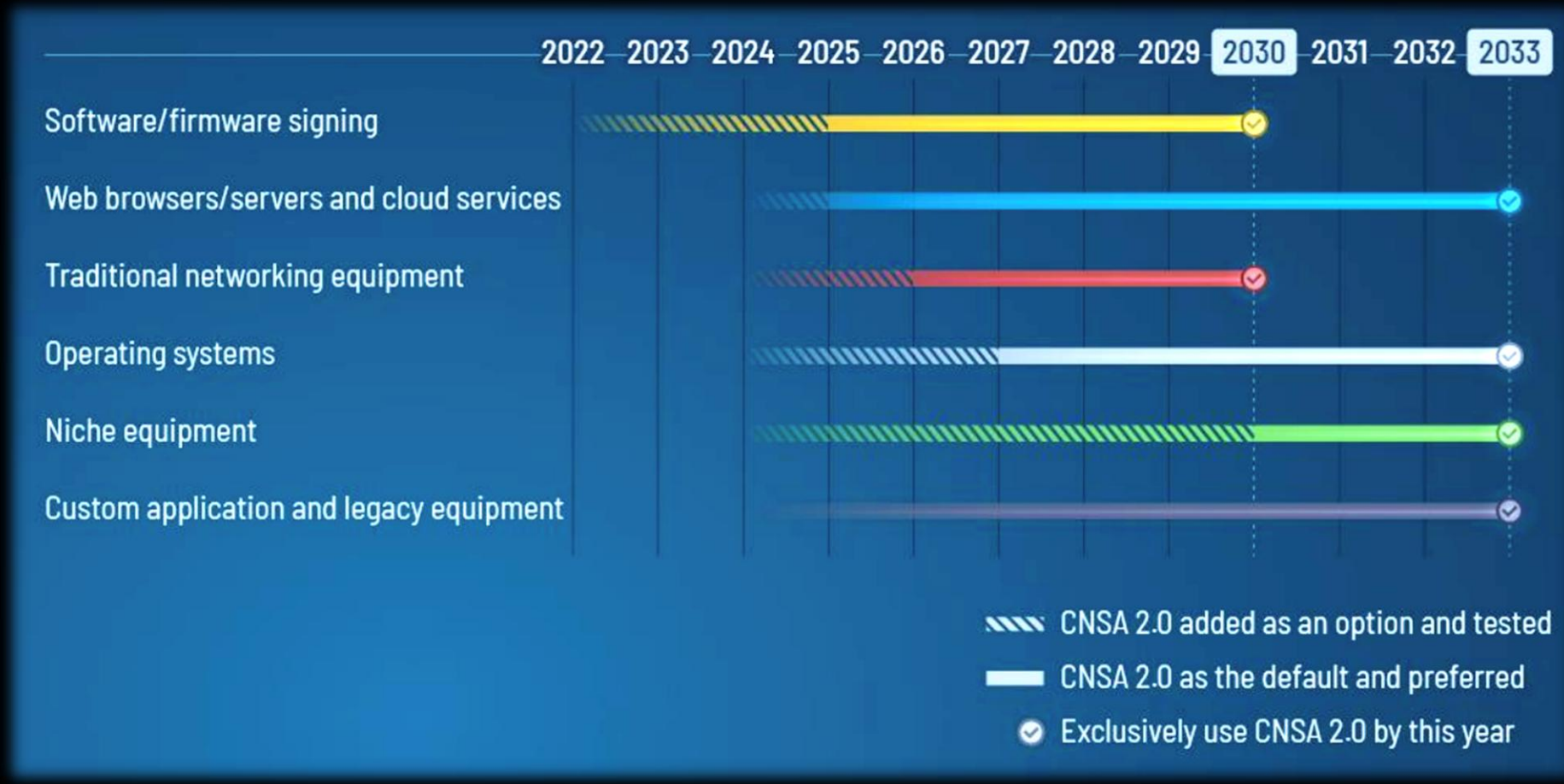
Vertraulichkeit

Integrität

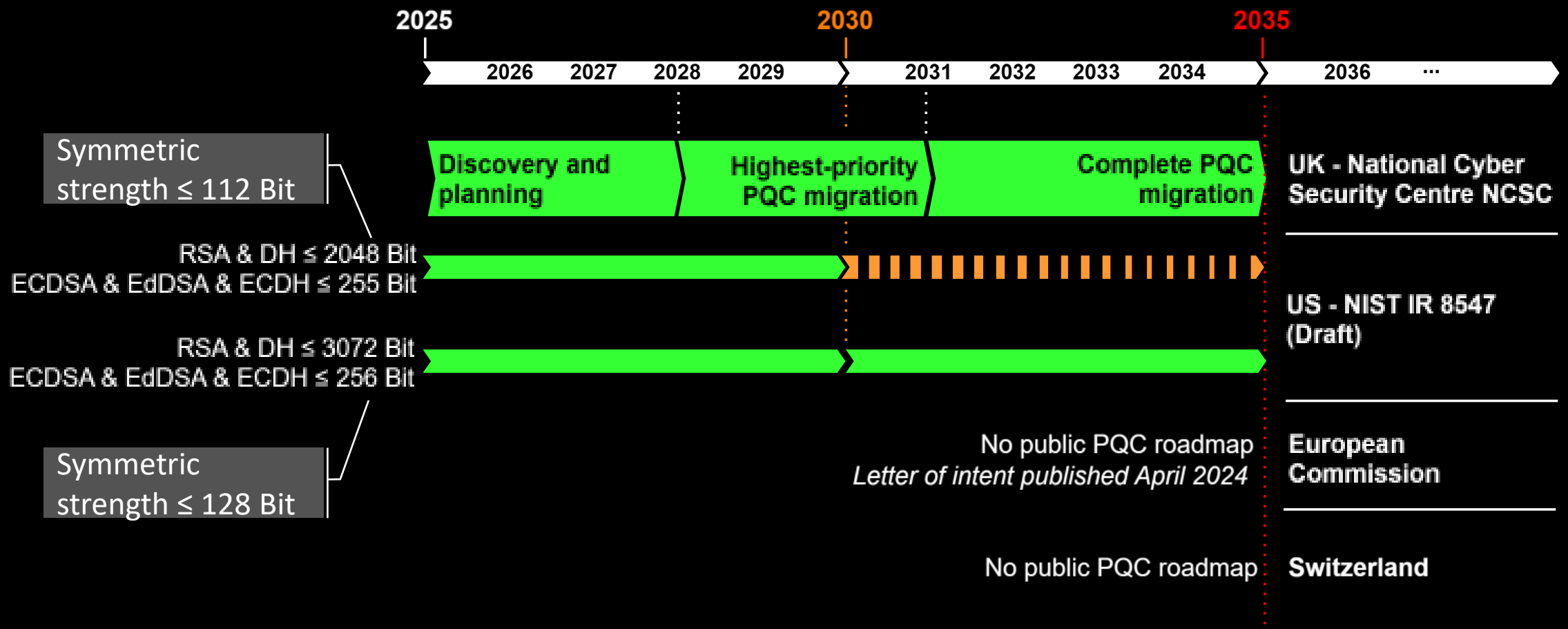
Authentizität

kann nicht mehr
gewährleistet
werden

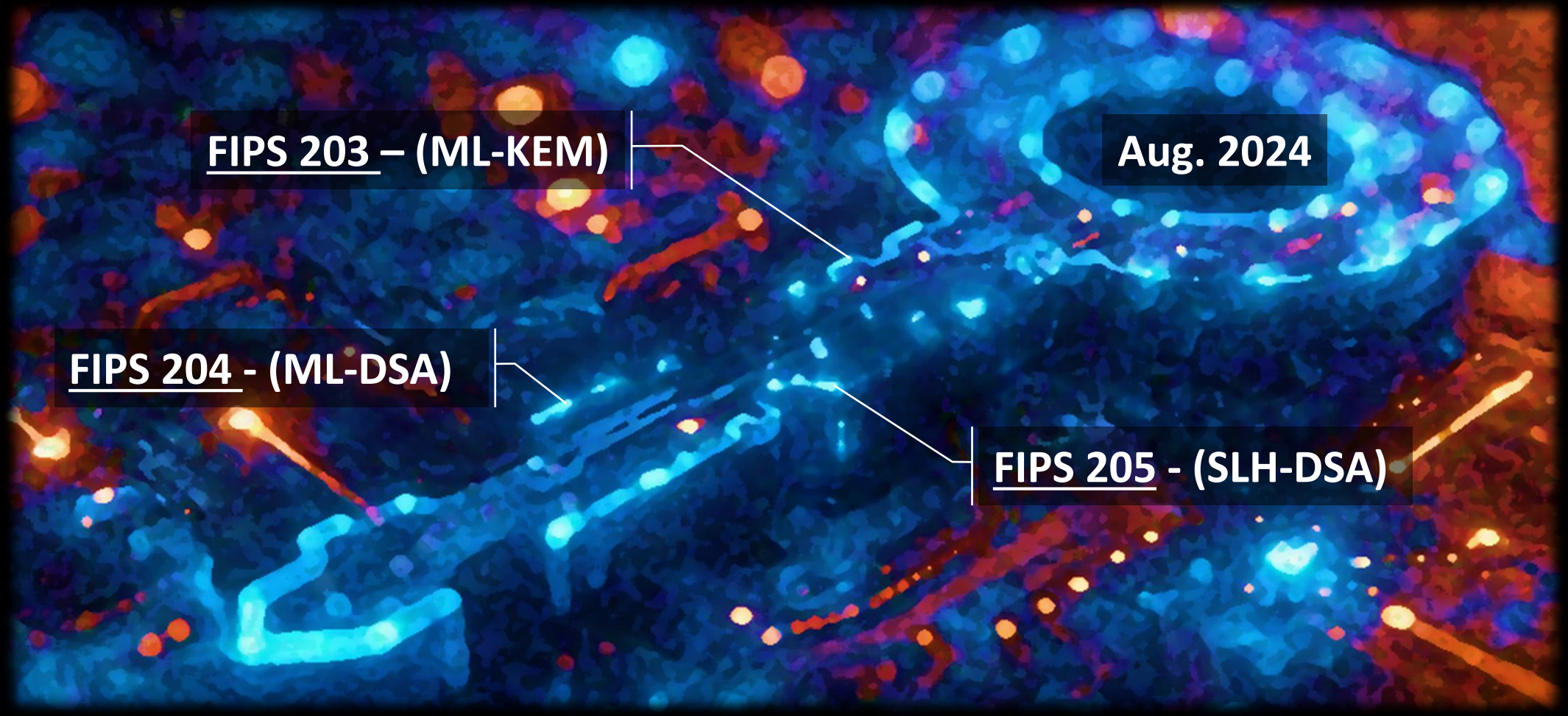
PQC-Roadmaps CNSA 2.0 Timeline



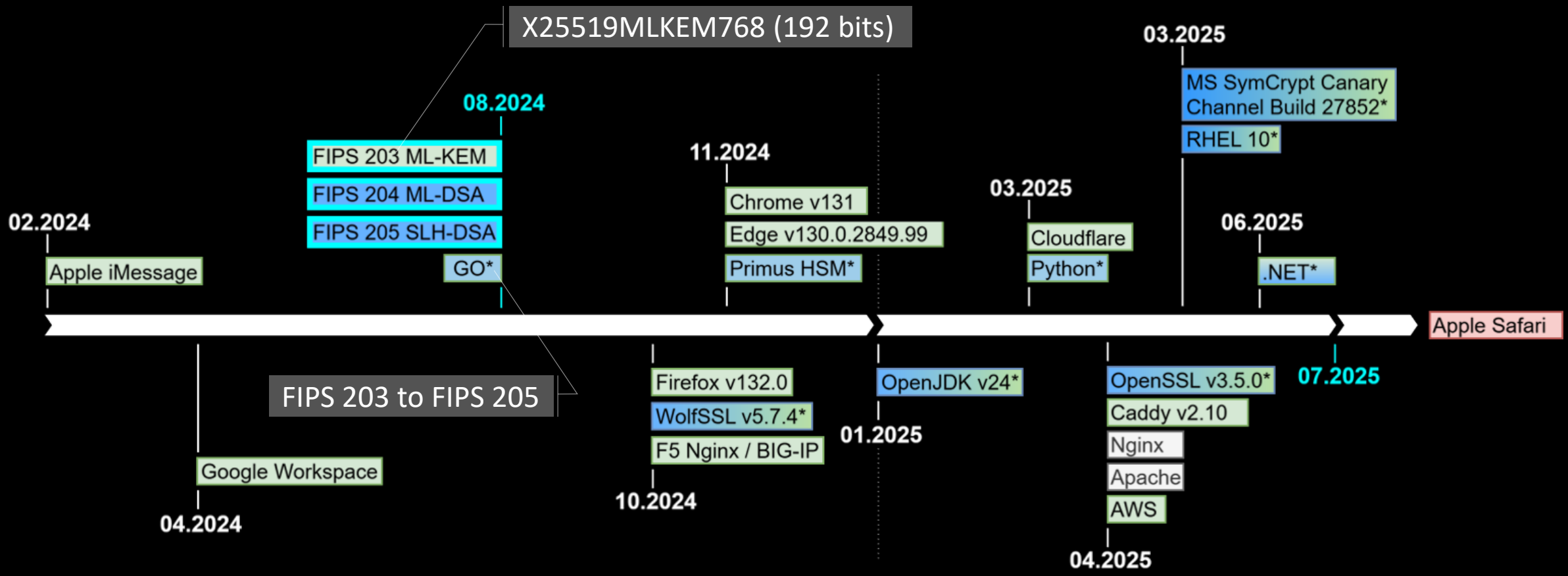
PQC-Roadmaps (Vorschläge)



PQC-Standards sind verfügbar



Produkte mit PQC-Unterstützung



Kann ich zuwarten?

- Zuwarten ist angesichts der Entwicklungen keine strategisch sinnvolle Option
- Panikartiger Aktionismus mit einer Umstellung über Nacht ist nicht angebracht
  - **Start** einer überlegten, schrittweisen **PQC-Transition**
- Sensible Daten (Data in Transit) erfordern **dringendes Handeln**

- **Warum jetzt handeln?**
  - Verhindern von ***Harvest Now, Decrypt Later*** *(HNDL)*
  - Lange Transition & Migrationszyklen
  - Standards sind verfügbar
  - Technologie ist verfügbar
  - Internationale Roadmaps (2035)

Start PQC-Transition

TEMET
end-to-end IT security

PQC-Transition

- **Analyse und Inventarisierung**
  → Sofort beginnen
  - Krypto-Inventar erstellen
    - **Externe Kommunikation**
    - **Interne Kommunikation**
    - **Gespeicherte Daten (Data-at-rest)**
    - **Software-Entwicklung**
  - Risikobewertung
  - Krypto-Agilität anstreben

- **Strategie, Planung & Pilotprojekte**
  … Kurz- bis mittelfristig
  - Roadmap entwickeln
  - Hersteller-Kommunikation
  - Testen im «Hybridmodus»

- **Schrittweise Umsetzung**
  … Mittelfristig
  - Externe Systeme zuerst
  - Neue Projekte PQC-Ready machen
  - Interne Systeme und Daten

Quintessenz

PQC-Standards & Migrations-Zeitpläne sind verfügbar

PQC-Technologien sind verfügbar

Anbieter unterstützen PQC

vgl. Cloud

Neue Produkte, SW, etc. sollten PQC unterstützen

PQC-Transition sofort **starten**

Beginne mit Analyse & Inventarisierung

¿ Fragen ?