Kryptografie im Umbruch

Warum sich Organisationen fit machen müssen für das Post-Quantum Zeitalter!

IKT Konferenz 2025

Marko Djordjevic
Senior Strategic Account Executive

Sebastian Zierdt
Technical Sales Consultant

Juni 2025

ENTRUST
SECURING A WORLD IN MOTION

Agenda

- Entrust Vorstellung
- Warum muss gerade jetzt gehandelt werden!
  Die Bedrohung durch Quantencomputer verstehen
  Zeitrahmen & regulatorischer Druck (z. B. NIST, BSI)
  Auswirkungen auf heutige Kryptografie
- Was ist zu tun?
  PQC-Standards & Hybride Übergangslösungen
  Einführung von Cryptographic Posture Management (CPM)
  Aufbau von Crypto-Agility & Automatisierung
- Umsetzung einer PQC Ready Strategie
  Einsatz von CSP, HSMs & PQC Services zur Entdeckung und Migration
  Organisatorische Verankerung & Governance Strukturen
  Handlungsempfehlungen & nächste Schritte

ENTRUST

The World's Most Trusted Brands Trust Us

ENTRUST

Protecting the Identity Lifecycle With Our Core Portfolios

Issuance

- Digital Credentials
- Physical Payment & ID Cards (instant and centrally issued)

Identity Security

- Identity Verification
- Multi-factor Authentication
- Digital Signing

Data Security

- Cryptographic Security Platform
- Integrated PKIs and HSMs
- Certificate, Keys, and Secrets Management

ENTRUST

Building on Our Track Record

$1B+
in revenue

3,100+
colleagues

55+
years of innovation

2k+
partners

150+
countries served

65%
Fortune 500 served

Warum muss gerade jetzt gehandelt werden!

ENTRUST

Die Quantenrevolution

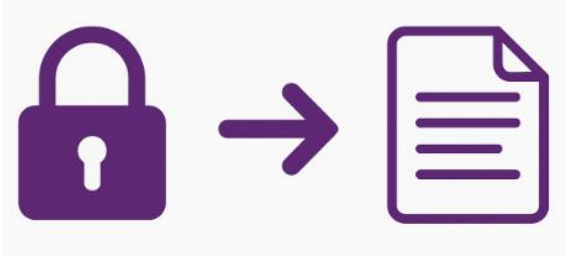
- Quantencomputer werden alles verändern
  - Statt wie ein klassischer Computer mit 1 und 0 (2 Zustände On/Off) zu rechnen arbeiten diese mit Qubits.
  - Qubits können **gleichzeitig mehrere Zustände** annehmen
  - Das macht bisherige für unlösbar gehaltenen mathematische Probleme lösbar!

- Die Gefahr für herkömmliche Verschlüsselungssysteme
  - Viele Verschlüsselungen, die wir heute nutzen für Websites, E-Mail, Daten oder Online banking basieren auf Rechenproblemen für die klassische Computer Jahre wenn nicht Jahrzehnte benötigen würden. Quantencomputer nicht!
  - Betroffen sind davon davon viele klassische Algoritmen und Verfahren
    - RSA & ECC (digitale Signaturen, VPNs, Webseiten)
    - Hash-basierte Verfahren (z.B. bei der Authentifizierung)

ENTRUST

„Harvest now, decrypt later“ – Was heißt das?

- Verschiedene Akteure weltweit speichern Heute verschlüsselte Daten, auch wenn diese stand Heute nicht entschlüsselt werden können!
- Beispiel: Eine verschlüsselte Patientenakte oder vertrauliche Geschäftsdaten werden abgefangen und archiviert.
- Später, wenn Quantencomputer leistungsfähig genug sind, werden diese Daten entschlüsselt – ohne dass Sie es merken.
- Folgen
  - Vertrauliche Informationen von heute sind morgen öffentlich.
  - Signaturen auf Verträgen oder Software könnten nachträglich gefälscht werden.



ENTRUST

Was ist genau betroffen?

- Mögliche Quantenangriffe betreffen viele alltägliche Anwendungen:
  - Webseitenverschlüsselung (TLS/HTTPS)
  - VPN-Zugänge in Unternehmen
  - Signaturen von Dokumenten & PDFs
  - Digitale Identitäten & Ausweise
  - Firmware-Updates & IoT-Geräte

- Dabei sind 3 zentrale Sicherheitsziele bedroht:
  - Vertraulichkeit: Wer darf lesen?
  - Integrität: Wurde etwas verändert?
  - Authentizität: Wer ist der Absender?

ENTRUST

Der Zeitfaktor – Handlungsspielraum wird enger!

- Internationale Behörden wie das **NIST (USA)** und das **BSI (Deutschland)** haben klare Empfehlungen und Migrationspläne veröffentlicht.
- Diese Institutionen fordern Unternehmen auf, ihre kryptografischen Systeme **bis spätestens 2030** auf quantensichere Verfahren umzustellen.
- Was ab 2030 passiert
  - Klassische Algorithmen wie **RSA, ECC** und **DSA** gelten ab dann als **nicht mehr sicher** – selbst mit langen Schlüsseln.
  - Ab **2035** sollen sie laut Entwurf in vielen Standards **nicht mehr zulässig** sein.
- Die Zeit um zu planen und die Umsetzung ist **jetzt**, nicht erst wenn Quantencomputer Realität sind!
  - Wer früh beginnt, kann Risiken reduzieren und regulatorischen Anforderungen gelassen begegnen.

Was ist zu tun?

ENTRUST

PQC-Standards & Hybride Übergangslösungen

- Das US-amerikanische NIST hat drei PQC-Algorithmen als Standard finalisiert:
  - **CRYSTALS-Kyber** (für sichere Schlüsselaustauschverfahren)
  - **CRYSTALS-Dilithium** (für digitale Signaturen)
  - **SPHINCS+** (als hashbasiertes Backup-Verfahren)
- Aber was tun wenn wie Heute **nicht alles PQC Ready ist?**
  - Die Lösung könnte sein: Hybride Kryptografie - Zwei Algorithmen werden kombiniert:
  - Ein klassischer (z. B. RSA oder ECC)
  - Ein quantensicherer (z. B. Kyber oder Dilithium)
- Warum ist das sinnvoll?
  - Der klassische Teil sichert Kompatibilität mit alten Systemen
  - Der PQC-Teil schützt schon heute vor künftigen Quantenangriffen
  - Diese „Hybrid-Zertifikate“ gibt es z. B. schon in X.509-Standards

ENTRUST

Einführung von Cryptographic Posture Management (CPM)

- CPM schafft Übersicht über alle eingesetzten kryptografischen Komponenten:
  - Schlüssel
  - Zertifikate
  - Algorithmen
  - Bibliotheken
  - Protokolle
- Funktionen eines CPM-Frameworks:
  - Automatisierte Erkennung und Inventarisierung
  - Bewertung von Risiken & Compliance-Konformität
  - Lifecycle-Management von Schlüsseln und Zertifikaten
- Ergebnis: Mehr Transparenz & Minimieren operativer Risiken bei der Umstellung auf PQC

ENTRUST

Aufbau von Crypto-Agility & Automatisierung

- Crypto-Agility bedeutet: Kryptografie flexibel & schnell an neue Anforderungen anpassen können→ z. B. bei Algorithmus-Schwächen oder neuen Standards
- Mit den richtigen Automatisierungswerkzeugen lassen sich Schlüsselrotation, Zertifikatswechsel und Risikobewertungeneffizient, sicher und nachvollziehbar durchführen
- So profitieren Sie von einer Crypto-Agility-Plattform:
  - Weniger manuelle Fehler
  - Schnellere Reaktionszeiten
  - Zukunftssichere Sicherheitsarchitektur

ENTRUST

Umsetzung einer PQC Ready Strategie

ENTRUST

Entdecken & Migrieren mit Entrust CSP, HSMs und PQC Services

- Schritt 1: Bestandsaufnahme mit Entrust CSP (Cryptographic Security Platform)
  - Vollständige Erfassung aller kryptografischen Assets (Schlüssel, Zertifikate, Protokolle)
  - Risikobewertung & Priorisierung: Welche Systeme sind besonders kritisch?
- Schritt 2: Testmigration im Entrust PQ-Lab Realitätsnahe Simulation von PQC-Migrationen
  - Einsatz hybrider Zertifikate (z. B. X.509 mit Kyber + RSA)
  - Interoperabilitätsprüfung mit CSP-Komponenten und Applikationen
- Entrust unterstützt mit:
  - Cryptographic Security Platform (CSP)
    - Automatisierte zertifikatsfähige PKI Lösung
    - Key & Secrets Management
    - Compliance Managment
  - PQC ready HSM Platform

ENTRUST

Organisatorische Verankerung & Governance

- Technik allein reicht nicht – Organisation ist entscheidend.
  - Aufbau eines interdisziplinären Krypto-Gremiums (IT, Compliance, Legal, Business)
  - Definition klarer Verantwortlichkeiten & Genehmigungsprozesse Verankerung von PQC-Zielen in der IT-Sicherheitsstrategie
  - Regelmäßige Audits & Aktualisierung des Cryptographic Asset Registers
- Entrust unterstützt mit:
  - PQC Consulting Services & Governance Workshops (PQC Discovery, PQ Lab, …)
  - Strategischer Fahrplan & Reifegradmodelle
  - Unterstützung bei Normen & Compliance (z. B. NIS2, ISO, eIDAS)

ENTRUST

Handlungsempfehlungen & Nächste Schritte

1. Inventarisieren:Starten Sie mit einer umfassenden Kryptografie-Inventur – am besten automatisiert mit einer CPM Lösung.
2. Testen & migrieren:Nutzen Sie das Entrust PQ-Lab, um Migrationen zu erproben und Hybrid-Zertifikate einzuführen.
3. Organisieren:Etablieren Sie klare Rollen, Prozesse und Gremien für den langfristigen Betrieb.
4. Zukunft sichern:Setzen Sie auf Crypto-Agility durch die CSP-Plattform, PQC fähige HSMs und starke Governance.

Wer früh beginnt, schützt nicht nur seine Daten – sondern stärkt Vertrauen, Compliance und Wettbewerbsfähigkeit.

ENTRUST

Crypto Hound - Demo