IT CONSULTING & ENGINEERING

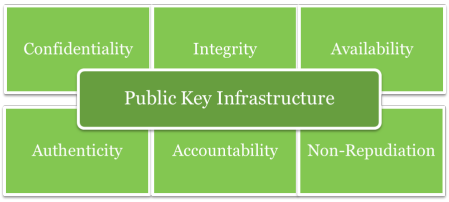
# PUBLIC KEY INFRASTRUCTURE / POST-QUANTUM KRYPTOGRAFIE

NACH DEM EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI) UND DEM INSTITUTE FOR QUANTUM COMPUTING

**Public Key Infrastructures (PKI) bilden die Grundlage für den Schutz von Daten, Systemen und internetfähigen Geräten. Als zentraler Bestandteil moderner Sicherheitsarchitekturen gewährleisten sie Vertraulichkeit, Integrität und Authentizität von Informationen sowie eine kontrollierte Zugriffsverwaltung.**

Digitale Zertifikate, die über eine PKI ausgestellt werden, ermöglichen die Authentifizierung von Benutzern, Geräten und Diensten – sowohl für öffentliche als auch interne Anwendungen.

Grundlage bilden symmetrische und asymmetrische kryptografische Verfahren, die häufig kombiniert eingesetzt werden: Der Schlüsselaustausch erfolgt asymmetrisch, während die eigentliche Datenübertragung symmetrisch verschlüsselt wird.




Aktuelle kryptografische Verfahren sind gegen Angriffe durch klassische Computer – selbst Supercomputer – zuverlässig geschützt. Diese Sicherheit könnte jedoch in Gefahr geraten, sobald leistungsfähige Quantencomputer verfügbar werden.

Mithilfe spezieller Quantenalgorithmen, wären solche Systeme in der Lage, die heutige Verschlüsselung zu brechen. Angreifer könnten so an sensible Daten und Geschäftsgeheimnisse gelangen, Geldflüsse umleiten oder weitere Angriffe vorbereiten. Deshalb empfiehlt es sich, frühzeitig auf Post-Quantum-Kryptografie zu setzen und die eigene Umgebung zeitnah zu schützen.

**Basierend auf langjähriger Praxiserfahrung hat die In&Out AG ein Vorgehen zur Einführung von Public Key Infrastructure (PKI) Lösungen inklusive Post -Quantum Kryptographie.**

**Schutzbedarf und Use Cases identifizieren**

- Benötigte Zertifikatstypen und -mengen festhalten, inkl. der Public-Trusted-Zertifikate
- Aufnahme der eingesetzten Applikationen und Systeme
- Angebundene Umsysteme und externe Partner identifizieren
- Bestehende Automatisierungsprozesse zur Zertifikatserneuerung identifizieren

**Bestehende PKI-Landschaft analysieren**

- Klären, ob die heutige PKI bereits zu Post-Quantum-Verfahren fähig ist
- Bestehen technische Einschränkungen identifizieren
- Existierende Abhängigkeiten zu Applikationen oder Plattformen aufnehmen

**Zielbild und Betriebsmodell definieren**

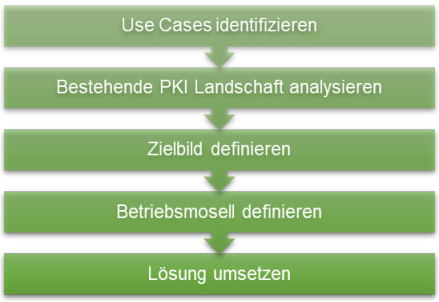
- Ausarbeitung des zukünftigen Target Operating Models
- Definieren, ob die neue PKI-Lösung selbst betrieben oder als Service bezogen werden soll
- Rollen, Verantwortlichkeiten und Schnittstellen zwischen internen und externen Beteiligten definieren

**Migration planen und umsetzen**

- Definieren, ob hybride Zertifikate während der Migrationsphase eingesetzt werden sollen
- Paralleler Betrieb der klassischen und Post-Quantum-Zertifikate
- Einbindung der neuen Root-Zertifikate in die Sicherheitssysteme
- Test der Einbindung aller Anwendungen und Systeme sowie der Automatisierung in die neue Post-Quantum PKI-Lösung

**DAS VORGEHEN:**

Der Leistungsumfang umfasst die Analyse der bestehenden PKI-Lösung und deren Post-Quantum-Bereitschaft sowie die Begleitung bei der Einführung einer neuen PKI-Lösung.




**IHR NUTZEN:**

- Eine PKI-Lösung, die exakt auf die Anforderungen Ihres Unternehmens zugeschnitten ist
- Post-Quantum-Kryptografie für zuverlässigen Schutz vor Angriffen durch Quantencomputer
- Automatisierte Zertifikatserneuerung, angepasst an Ihre spezifischen Prozesse
- Ein klar definiertes Betriebsmodell, das alle relevanten Abteilungen und Partner einbindet
- Eine zukunftsorientierte PKI-Plattform, die neue Anwendungsfälle flexibel unterstützt

**KONTAKTIEREN SIE UNS:**

Wir freuen uns über Ihre Kontaktaufnahme zur fachlichen Vertiefung der Thematik!

Silvio Pelli
Senior IT Consultant
silvio.pelli@inout.ch