MTG

Technische und Strategische Aspekte der PQC Migration

Dr. Falko Strenzke, MTG AG

CAST Workshop PQC, 2025-09-23, Darmstadt

MTG AG

- Gegründet 1995
- Darmstadt, Athen
- ERS Produkte: PKI, KMS, Lifecycle Management, HSM-Integration
- PQC Forschung
- DIN ISO 27001 & ISO 9001 zertifiziert

SecurITy made in Germany
Trust Seal
www.it-sa-trust.de/itsmig

www.mtg.de/de/unternehmen/historie/

MTG

Deutsche Telekom
DB
iskraemeco
theben
Bundesamt für Sicherheit in der Informationstechnik
swissbit
Stromnetz Hamburg
ENX
Bundesnetzagentur
EMH
ciena
schleupen
devolo
entega
CISCO
TREMONDI
Stadtwerke Saarbrücken
VIVAVIS
DECODING THE FUTURE
DARZ
Daten sind wertvoller als Geld
Syna
utimaco
Creating Trust in the Digital Society
thyssenkrupp
bdr
BUNDESDRUCKEREI
inno2grid
Knappschaft Bahn See
LEAR CORPORATION

PQC@Thunderbird

MTG

- BSI-Projekt: Auftragnehmer MTG AG mit TU/e
- Zeithorizont: 12/2021 bis 11/2025
- Standardisierung von PQC in OpenPGP (NIST-PQC-Auswahl)
- Implementierung als Proof-of-Concept
  - ML-KEM+ECC, ML-DSA+ECC, SLH-DSA
  - In Thunderbird (über RNP und Botan)
  - In GnuPG / Libgcrypt
- Beiträge zu Standardisierung in für X.509

EU PQC Transition Roadmap[1]

MTG

- Anfang 2026: Finalisierung der wichtigsten PKI-Standards für PQC
- bis Ende 2026: “First Steps” in Mitgliedsstaaten umgesetzt
  - Cryptographic asset management
  - Quantum risk analysis (Administration und Kritis)
  - ...
- bis Ende 2030:
  - Abschluss PQC-Migration für Hochrisiko-Anwendungen
  - PQC Firmware Updates
  - Start Migration Medium-Risk Anwendungen
- bis Ende 2035:
  - Abschluss PQC-Migration für Medium-Risk Anwendungen

[1] “A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography” Part 1, Version: 1.1, EU PQC Workstream, 11.06.2025

Cryptographic Assets

MTG

ETSI Schema zur Asset-Modellierung [2]

- Asset modelling
  - *cryptographically protected assets*
  - *cryptographic assets*
- Asset dependency map

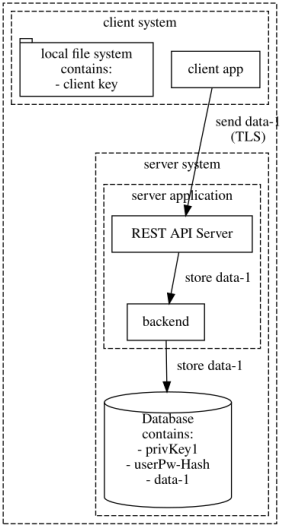
[2] ETSI TR 104 016 V1.1.1 (2024-10) "CYBER; Quantum-Safe Cryptography (QSC); A Repeatable Framework for Quantum-Safe Migrations"

Cryptographic System Modelling

MTG

- Formale Beschreibung von
  - system components
  - *cryptographically protected assets*
  - *cryptographic assets*
  - data flows
- Automatisiert erstellen aus dem Modell:
  - graphische Übersichten
  - Listen, Tabellen
- Automatisierte Prüfungen, ob Policies für Assets eingehalten werden

```
from crymo_elements import Element, StorageLocation,
     Database, FileSystem, Asset, CryptographicKey, Tls
landscape : Element = Element("")
client_sys : Element = Element("client system")
client : Element = Element("client app")
system : Element = Element("server system")
app : Element = Element("server application")
db : Database = Database("Database", technology="mariadb")
server : Element = Element("REST API Server")
backend : Element = Element("backend")

landscape.add_element(system)
landscape.add_element(client_sys)
client_sys.add_element(client)

client_fs = FileSystem("local file system", technology="NTFS
     ")
client_sys.add_element(client_fs)

privKey : CryptographicKey = CryptographicKey("privKey1")
userPw: Asset = Asset("userPw-Hash")
data1: Asset = Asset("data-1")
db.add_asset(privKey)
db.add_asset(userPw)
db.add_asset(data1)
system.add_element(app)
system.add_element(db)
app.add_element(server)
app.add_element(backend)

backend.connect_to(db, description="store data-1")
server.connect_to(backend, description="store data-1")

client_key : CryptographicKey = CryptographicKey("client key
     ")
server_key : CryptographicKey = CryptographicKey("server key
     ")
client_fs.add_asset(client_key)

tls_conn : Tls = Tls(client_key, server_key)
client.connect_to(server, "send data-1", tls_conn)
```



Säulen für PQC-Migration

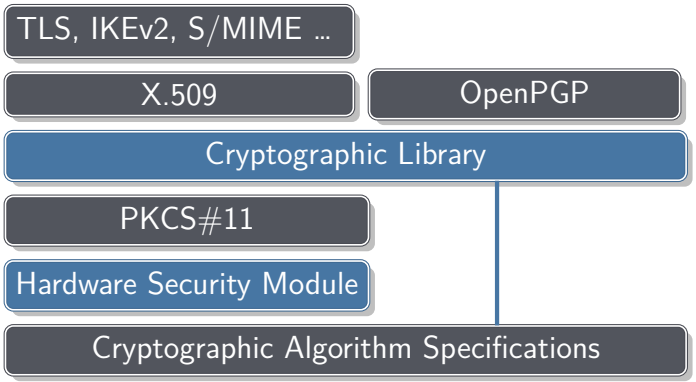
MTG

- Kenne den Ist-Zustand: Asset und Datenfluss Modell
- Antizipiere die Entwicklung bei PQC Standardisierung und Regulation
- Kenne die technischen Anforderungen Deiner Systeme und Einschränkungen bei PQC Verfahren
- Sammle frühe Hands-On Erfahrung
- Entwickle eine Strategie mit Risiko- und Kostenmodell

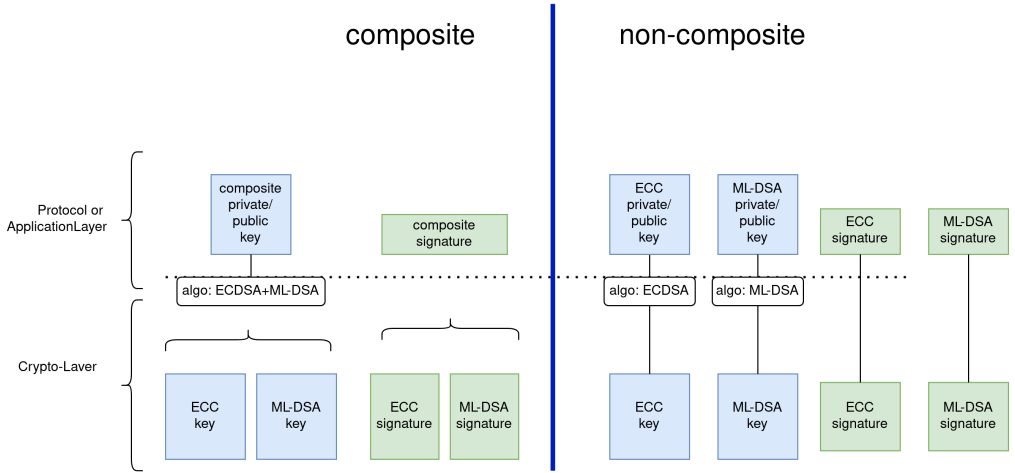
Die Standardisierten PQC-Verfahren

- KEM (Verschlüsselung)
  - ML-KEM
- Signaturen
  - ML-DSA
  - SLH-DSA #
  - XMSS / LMS #

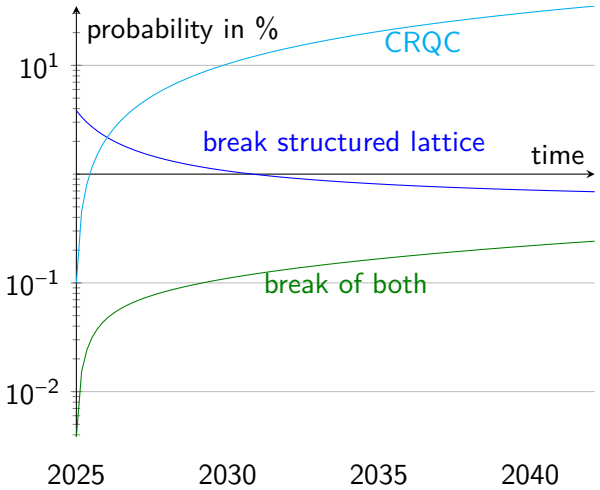
PQC Standardisierung



PQC Hybride

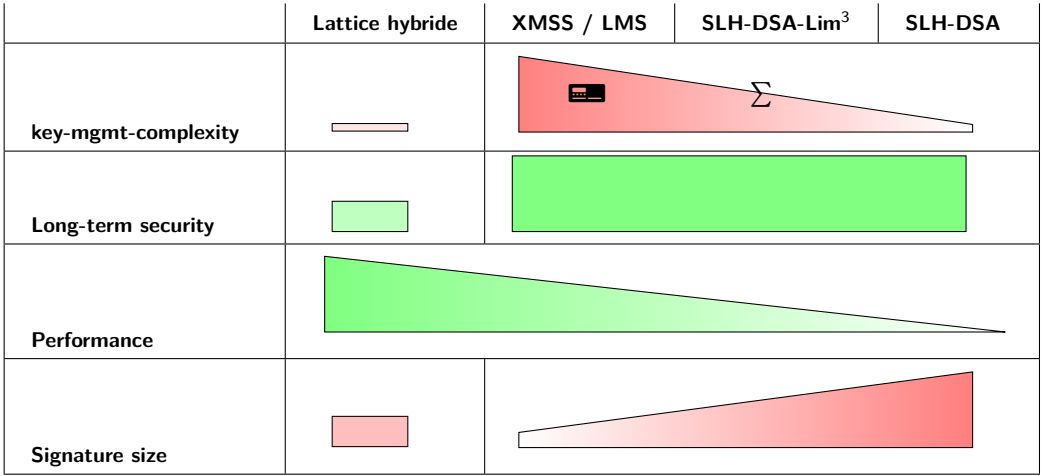

composite
non-composite
Protocol or ApplicationLayer
Crypto-Laver
composite private/ public key
composite signature
algo: ECDSA+ML-DSA
ECC key
ML-DSA key
ECC signature
ML-DSA signature
ECC private/ public key
ML-DSA private/ public key
ECC signature
ML-DSA signature
algo: ECDSA
algo: ML-DSA
ECC key
ML-DSA key
ECC signature
ML-DSA signature

Hybride Structured-Lattice-Verfahren



- ML-DSA+ECDSA
- Problem: Langzeitsicherheit
- CRQC: RSA/ECC fällt weg
- ML-* ausreichend?
- Risiko: Hybrid muss nach Schwächung einer Komponente ausgetauscht werden
  - 🚗🚗 vs. 🚗

Kriterien für PQC Signaturen[4]



[3] SLH-DSA mit kleineren Parametern mit begrenzter Signaturanzahl. Noch nicht standardisiert. SLH-DSA-Lim ist keine offizielle Bezeichnung.

[4] Mit Ausnahme von SLH-DSA-Lim sind dies die Signaturverfahren mit erwarteter kurzfristiger Verfügbarkeit in X.509.

Speichereffizienz: Fast keine PQC Drop-In Replacements bei Signaturen

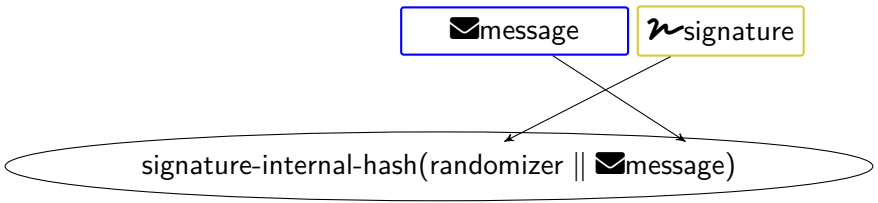
MTG

- Speichereffizienz von Signaturen
  - Kriterium: Muss die Nachricht vollständig im Speicher gehalten werden?
- Relevant für Signatur/Verifikation großer Nachrichten, z.B. Images
- Analyse zu PKCS#11[5]

[5] https://datatracker.ietf.org/meeting/123/materials/slides-123-lamps-falko-discussion-of-pkcs11-v32-proposal-00

Speichereffizienz von Signaturen: Was ist das Problem?

- Hash-and-sign Paradigma (RSA, ECDSA) gilt nicht bei PQC
- Internes Hashen mit vorangestelltem Zufallswert (bei Hash-basierten)
- Zufallswert ist in der Signatur enthalten.
- Folge: Bei der Verifikation kann das Hashen der Nachricht erst begonnen werden, sobald die Signatur eingelesen wurde.
  - Folge: Die Nachricht muss vollständig zwischengespeichert werden.



Speichereffizienz von Signaturen: Was sind die Folgen?

MTG

- Ggf. müssen sehr große zu signierende Dateien an HSM geschickt werden
  - SLH-DSA ohne Pre-Hash
  - XMSS / LMS
- Ggf. müssen sehr große zu verifizierende Dateien vollständig im Speicher gehalten werden
  - XMSS / LMS
  - SLH-DSA ohne Pre-Hash
  - Auswirkungen auf Embedded Devices

PQC Verschlüsselung

MTG

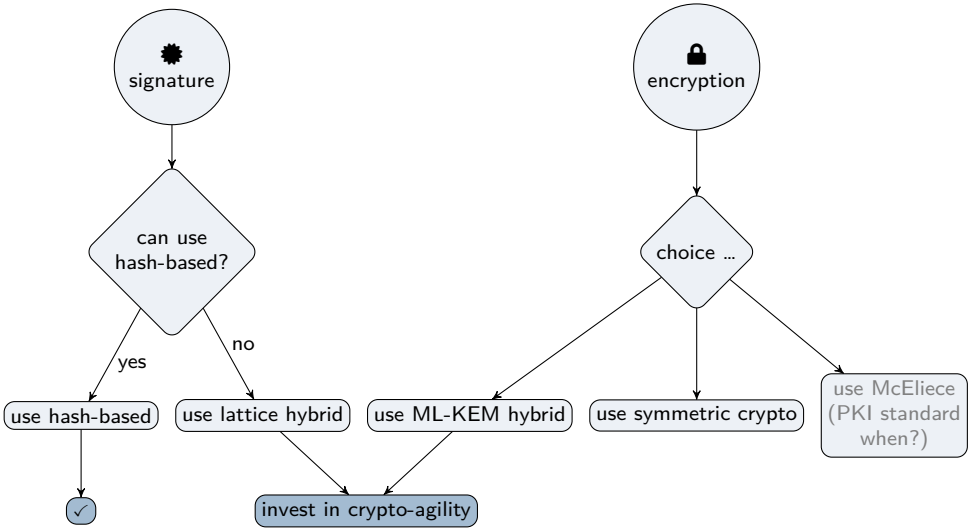
- Nur ein “Europa-taugliches” Standardisiertes PQC-Verfahren: ML-KEM hybride
  - Noch kein X.509 Standard
- Store-now-decrypt-later erfordert schnelles handeln
- Standardisierung von weiteren PQC Verfahren für X.509:
  - in der IETF
  - FrodoKEM ?
  - Classic McEliece ?

Confidentiality vs. Authentication

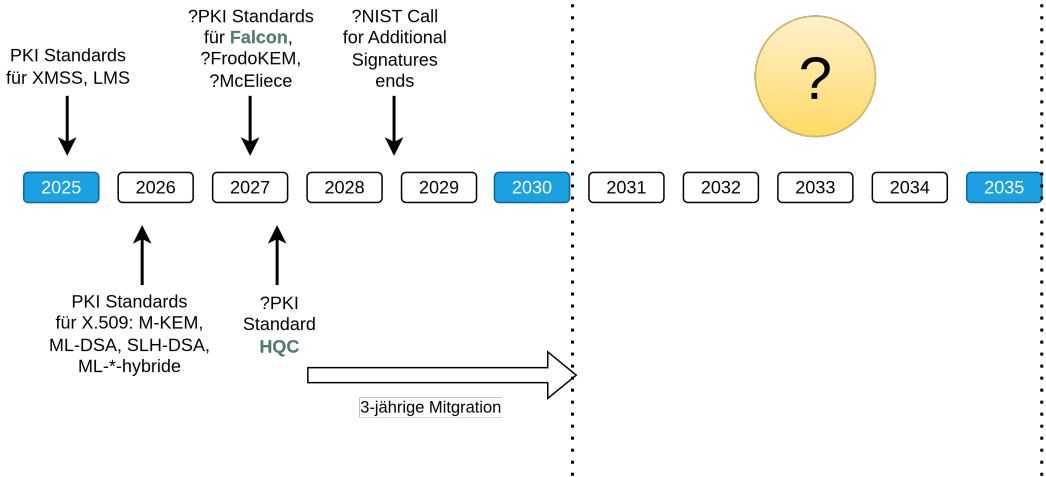
MTG

- Store-now-decrypt-later sorgt für Confidentiality-Problem
  - ggf. bereits verlorenes Rennen
  - Risiko-Abschätzung
- Sichere Authentisierung oftmals wichtiger
  - Beispiel: monetäre Transaktionen
- "Authentisierung muss erst PQC-sicher sein, wenn CRQC existieren"
  - Gilt nur für kryptografische Authentisierung
  - Store-now-decrypt-later gefährdet verschlüsselt übertragene Authentisierungs-Tokens (Passwörter)
  - Zur Migration gehört die rechtzeitige PQ-sichere Erneuerung von Authentisierungs-Tokens

Entscheidungsbäume



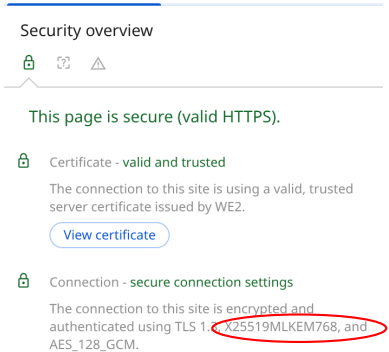
Zeithorizont



TLS mit PQC-Verschlüsselung

MTG

Chromium mit Google Server



PQC VPN

MTG

- Proprietäre PQC-Lösungen verschiedener Hersteller
- IKEv2 with MLKEM in Arbeit bei IETF[6]

[6] draft-ietf-ipsecme-ikev2-mlkem

OpenPGP

MTG

draft-ietf-openpgp-pqc
(in publication process)
BSI, MTG, Proton

algorithms	requ.	security
ML-KEM-768+X25519	**MUST**	192 / 128
ML-KEM-1024+X448	SHOULD	256 / 224
ML-DSA-65+Ed25519	**MUST**	192 / 128
ML-DSA-87+Ed448	SHOULD	256 / 224
SLH-DSA-SHAKE-128s	MAY	128
SLH-DSA-SHAKE-128f	MAY	128
SLH-DSA-SHAKE-256s	MAY	256

draft-ietf-openpgp-nist-bp-comp
(adopted)
BSI, MTG, NIST

algorithms	security
ML-KEM-512+ECDH-**NIST-P-256**	128 / 128
ML-KEM-768+ECDH-**NIST-P-384**	192 / 192
ML-KEM-1024+ECDH-**NIST-P-384**	256 / 192
ML-KEM-768+ECDH-**brpP256r1**	192 / 128
ML-KEM-1024+ECDH-**brpP384r1**	256 / 192
ML-DSA-44+ECDSA-**NIST-P-256**	128 / 128
ML-DSA-65+ECDSA-**NIST-P-384**	192 / 192
ML-DSA-87+ECDSA-**NIST-P-384**	256 / 192
ML-DSA-65+ECDSA-**brpP256r1**	192 / 128
ML-DSA-87+ECDSA-**brpP384r1**	256 / 192

all “MAY”

OpenPGP PQC Rollout

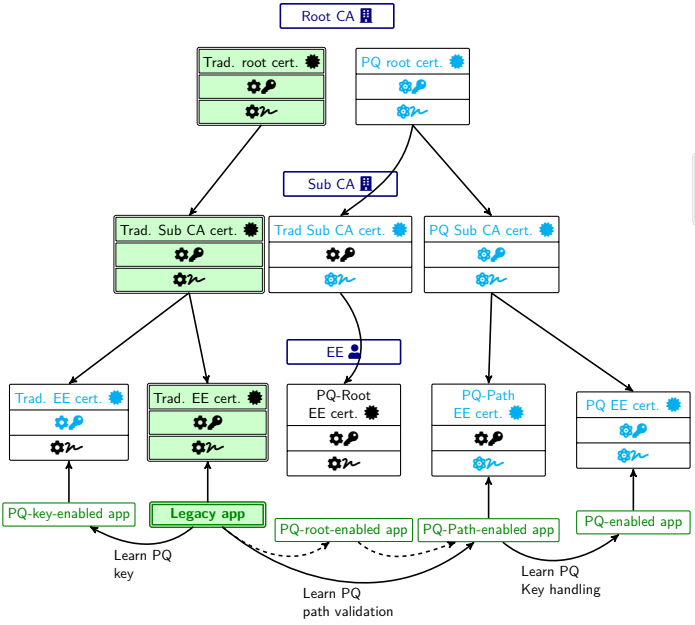
MTG

- OpenPGP Draft mit ML-KEM und ML-DSA hybride, SLH-DSA im Publikationsprozess
- Proton bereitet PQC Rollout vor
- Erste Feldtests:
  - Thunderbird “verschluckt” sich an PQC Artefakten
- Wichtiger Schritt: Graceful failure
  - Legacy Implementierungen mit PQC Artefakten konfrontieren

PQC Migration für PKI

MTG

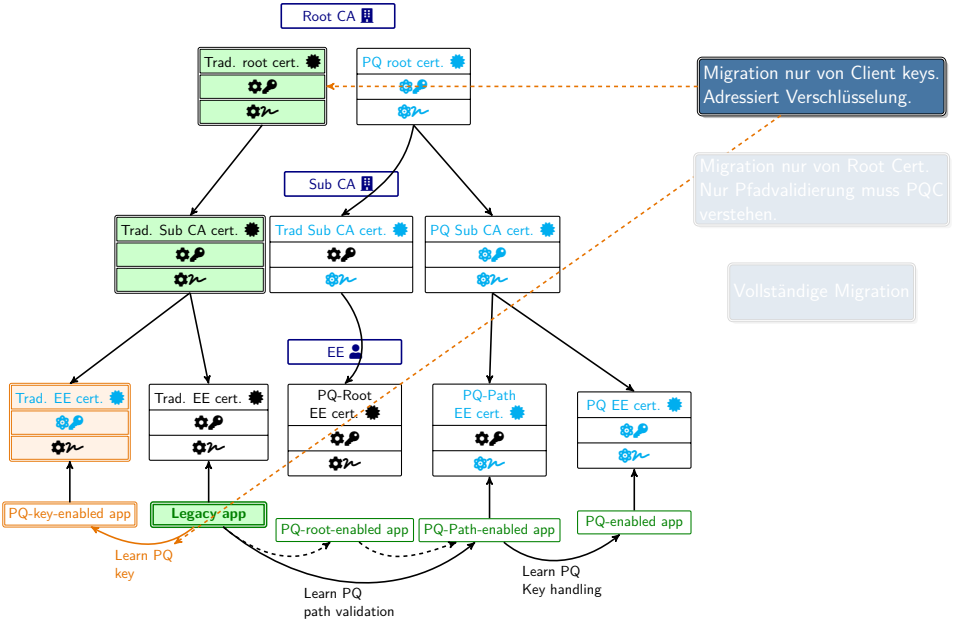
- PKI Migration komplex
- Viele Clients — müssen interoperabel sein
  - mit PKI
  - mit Server-Diensten
  - mit anderen Clients

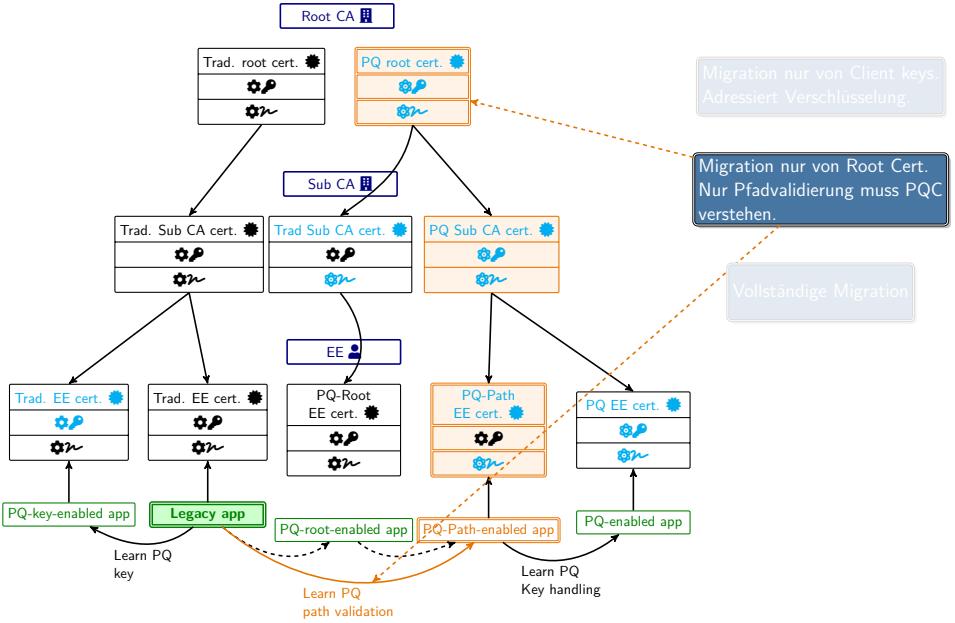


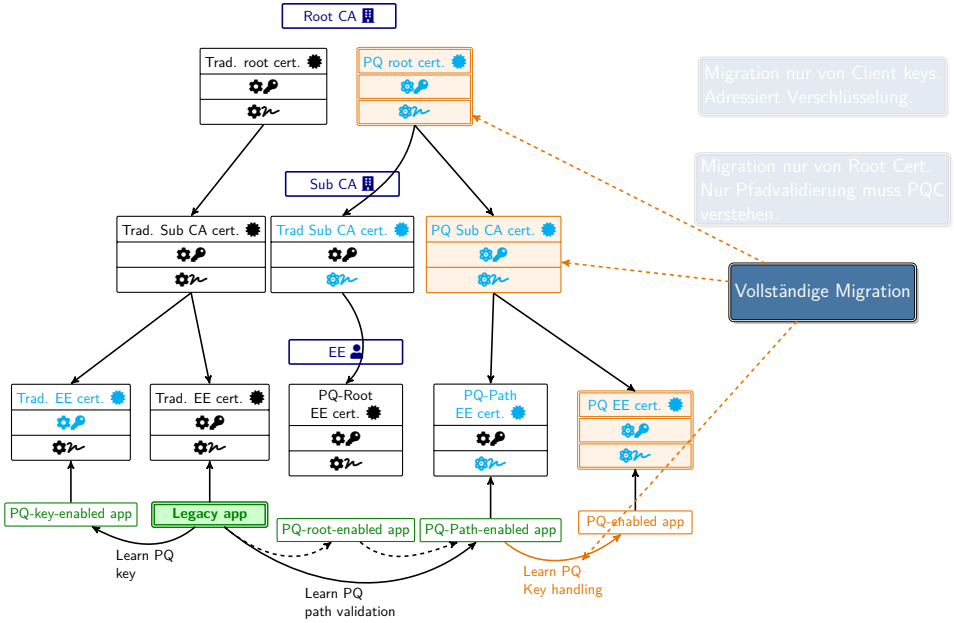
Migration nur von Client keys. Adressiert Verschlüsselung.

Migration nur von Root Cert. Nur Pfadvalidierung muss PQC verstehen.

Vollständige Migration


Root CA
Trad. root cert.
PQ root cert.
Migration nur von Client keys.
Adressiert Verschlüsselung.
Migration nur von Root Cert.
Nur Pfadvalidierung muss PQC
verstehen.
Vollständige Migration
Sub CA
Trad. Sub CA cert.
Trad Sub CA cert.
PQ Sub CA cert.
EE
Trad. EE cert.
Trad. EE cert.
PQ-Root
EE cert.
PQ-Path
EE cert.
PQ EE cert.
PQ-key-enabled app
Legacy app
PQ-root-enabled app
PQ-Path-enabled app
PQ-enabled app
Learn PQ
key
Learn PQ
path validation
Learn PQ
Key handling


Root CA
Trad. root cert.
PQ root cert.
Migration nur von Client keys. Adressiert Verschlüsselung.
Migration nur von Root Cert. Nur Pfadvalidierung muss PQC verstehen.
Vollständige Migration
Sub CA
Trad. Sub CA cert.
Trad Sub CA cert.
PQ Sub CA cert.
EE
Trad. EE cert.
Trad. EE cert.
PQ-Root EE cert.
PQ-Path EE cert.
PQ EE cert.
PQ-key-enabled app
Legacy app
PQ-root-enabled app
PQ-Path-enabled app
PQ-enabled app
Learn PQ key
Learn PQ path validation
Learn PQ Key handling


Root CA
Trad. root cert.
PQ root cert.
Migration nur von Client keys. Adressiert Verschlüsselung.
Migration nur von Root Cert. Nur Pfadvalidierung muss PQC verstehen.
Sub CA
Trad. Sub CA cert.
Trad Sub CA cert.
PQ Sub CA cert.
Vollständige Migration
EE
Trad. EE cert.
Trad. EE cert.
PQ-Root EE cert.
PQ-Path EE cert.
PQ EE cert.
PQ-key-enabled app
Legacy app
PQ-root-enabled app
PQ-Path-enabled app
PQ-enabled app
Learn PQ key
Learn PQ path validation
Learn PQ Key handling

Kosten – Beispiel Signaturen

MTG

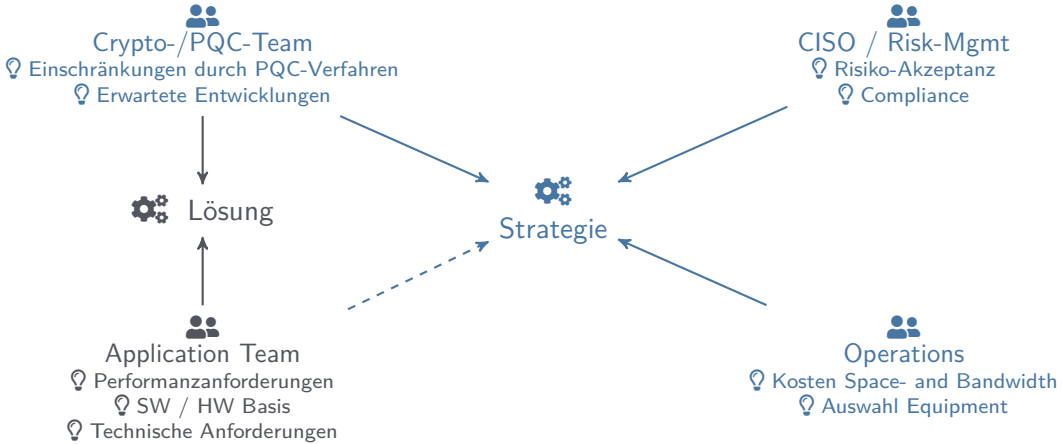
	LMS #⏲ Stateful-hash	**ML-DSA** ▦ Gitter	Einmalige Kosten	Betriebs- und Folgekosten
Key mgmt complexity			HSM-Beschaffung und Integration	HSM-Administration
Crypto-agility requirement			Entwicklungskosten	Erneuter Verfahrenswechsel, neues Rollout
Signature size				Speicherplatz, Bandbreite
Speicherbedarf (große Nachrichten)			Abhängig von Use-case, Hardware-Support, etc.	

Kosten und Strategie

MTG

- Weitere Entscheidungsmöglichkeiten
  - Verzögerte Umsetzung wegen Warten auf zukünftige Verfahren oder Technologien
  - Einsatz von nicht standardisierten Verfahren
  - Wechsel von Sicherheitsprotokollen
  - Re-Engineering von proprietären Applikationsprotokollen
- Strategische Gesichtspunkte
  - Migration ist Compliance- oder Risiko-getrieben?
  - Knowhow-Management

Migration: Aufgabenverteilung und Knowhow-Management



Zieldefinition

MTG

- Was bedeutet es, ein Dienst zu PQC migriert zu haben?
  - Vollständige Umstellung aller direkt und indirekt beteiligten Komponenten
  - Beinhaltet:
    - Nach außen hin sichtbare Kryptografie 🌐
    - Administrationswerkzeuge 🔧
    - Unternehmenskommunikation ✉
  - Denkansatz: “traditionelle Kryptografie bietet Schutz = 0”

Zusammenfassung

MTG

- Strategische Planung erfordert Asset-Modellierung
- Strategische Planung erfordert Kostenmodell
- Kritische Punkte
  - Langzeitsicherheit Gitter-Hybride
  - Performanz / Signaturgrößen Hash-basierte
  - Mangelnde Alternativen bei Verschlüsselung
- Krypto-Agilität als strategischer Invest

MTG

Vielen Dank für Ihre Aufmerksamkeit

Dr. Falko Strenzke
falko.strenzke@mtg.de
+49 6151 8000-24

MTG AG
www.mtg.de