TeleTrusT-EBCA "PKI-Workshop" 2025

Berlin, 18.09.2025

"Entwürfe für eine Post-Quanten-PKI"

Dr. Falko Strenzke, MTG

MTG AG

MTG

Gegründet 1995

Sitz in Darmstadt

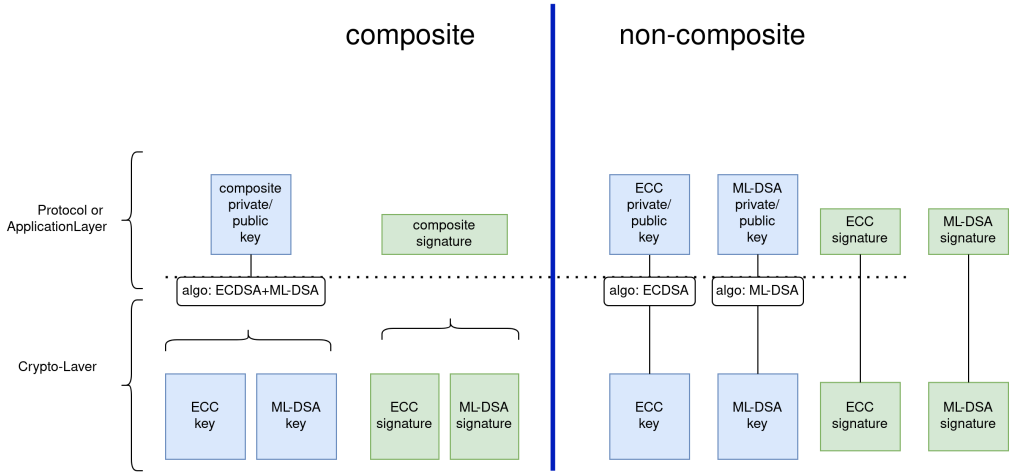
Produkte: PKI, KMS, HSM

PQC Research Projects

Die neuen PQC Algorithmen

- KEM (Verschlüsselung)
  - ML-KEM
    - Composite-Verschlüsselung
- Signaturen
  - ML-DSA
    - Composite-Signaturen
  - SLH-DSA #
    - in Arbeit: SLH-DSA mit alternativen Parametern
  - XMSS / LMS #

Multi-algorithm



Stateful-hash-based Signatures

- Hash-basierte Verfahren: hohe Sicherheit
- tendenziell: große Signaturen
- Status-behaftete Private Keys
  - XMSS, LMS/HSS
  - HSM notwendig
  - Themen: Key backup, Hochverfügbarkeit, etc.
- SLH-DSA: Zustandsloser Private Key
  - Große Signaturen
  - Langsame Signaturerstellung
  - NIST arbeitet an neuen Parametersätzen mit reduzierter Signaturanzahl (z.B. 2^{20}) und kleineren Signaturen

Die neuen PQC Algorithmen – “Europäische Sicht”

	Algo name	Crypto Spec	PKI Spec*	Trust	EU?	Remark
🔒	ML-KEM ▦	NIST ✔	(✔)	low	✖	efficient
	ML-KEM-composite	LAMPS	⧖	medium	✔	efficient
	FrodoKEM ▦	ISO⧖	—	high	?	up to 15KB keys
	McEliece ⁘	ISO⧖	—	high	?	up to 1MB keys
	HQC ⁘	NIST, ≈ 2y	—	high	?	up to 7KB keys
✹	ML-DSA ▦	NIST ✔	(✔)	low	✖	efficient
	ML-DSA-composite	LAMPS	⧖	medium	✔	efficient
	SLH-DSA #	NIST ✔	(✔)	highest	✔	large sig., slow signing
	XMSS #↻	IETF ✔	✔	highest	✔	medium-sized sig.
	LMS #↻	IETF ✔	✔	highest	✔	medium-sized sig.
	Falcon ▦	NIST ≈ ’25	—	low	✖	small signatures

✔ finalized standard
(✔) in publication / finalized by WG
⧖ advanced stage in WG, minor changes still probable
* PKI Specs in LAMPS WG in IETF

▦ lattice-based
⁘ code-based
stateless hash-based
#↻ stateful hash-based

PQC Security Levels

- PQC Security Levels (Symmetric security equivalent)
  - 128 bit
  - 192 bit
  - 256 bit

Non-composite Hybride

- RFC 9763 – Related Certificates for Use in Multiple Authentications within a Protocol
- draft-ietf-lamps-certdiscovery: “A Mechanism for X.509 Certificate Discovery”
  - Agilität bei Algorithmen
  - Verbindung von Signatur- und Verschlüsselungszertifikaten

Entwürfe für eine PQC PKI

- Fragestellungen
  - Was sind typische PKIs?
    - Internet PKI
    - Code-Signing
    - High Security Applications
  - Welche Aspekte sind wichtig?
    - Signaturgröße
    - Laufzeit der Signaturerstellung
    - Langzeitsicherheit
    - Stateful-hash-based (XMSS/LMS)
  - Was wann migrieren?
    - Verschlüsselung – Store-now-decrypt-later ...
    - Wieviel Zeit lassen mit der Umsetzung von PQC Signaturen?
    - Hybride Signaturen mit ML-DSA oder Hash-basierte?
    - Warten auf neue Algorithmen? (SLH-DSA-alt-param, HQC, NIST's new signatures)

MTG

Thank you for your attention

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

MTG AG
www.mtg.de