Empfohlene Algorithmen - Abkündigung RSA

Terminierung_RSA.pdf

Ausgangslage

Quantencomputer könnten RSA und ECC brechen –möglicherweise schon **vor 2030**.

Die Strategie „**Harvest now, decrypt later**“ bedeutet, dass heute verschlüsselte Daten später entschlüsselt werden könnten.

NIST und ETSI empfiehlt daher den **sofortigen Beginn der Migration** zu **Post-Quantum Cryptography (PQC)**.

RSA ist **nicht sofort verboten**, aber sollte **ab 2030 nicht mehr verwendet** werden.

Bis **2035** müssen alle Systeme auf **quantensichere Algorithmen** umgestellt sein.

Empfohlene PQC-Algorithmen sind z.B. **CRYSTALS-Kyber** (KEM) und **CRYSTALS-Dilithium, FALCON, SPHINCS+** (Signaturen).

Empfehlungen

Empfehlungen für Fristen und Algorithmen

Kriterium	**NIST (USA)**	**BSI (Deutschland)**
RSA weiterhin erlaubt bis	**2030 empfohlenes Ende**, **2035 endgültig verboten** [cisa.gov]	**RSA 2000 Bit bis 2023 erlaubt**, danach nur noch **RSA 3000 Bit** empfohlen [bsi.bund.de]
Empfohlene PQC-Algorithmen	CRYSTALS-Kyber, Dilithium, FALCON, SPHINCS+	FrodoKEM, Classic McEliece, Dilithium, SPHINCS+ [bsi.bund.de]
Migrationsziel	Vollständige Ablösung klassischer Algorithmen bis **2035**	**Sensibelste Anwendungen bis 2030** auf PQC umstellen [bsi.bund.de]
Hybridverfahren empfohlen?	Ja, Übergangsweise Kombination klassisch + PQC	Ja, insbesondere für Schlüsselvereinbarung und TLS [bsi.bund.de]
Schlüsselgrößen für RSA	Mindestens 2048 Bit, empfohlen: 3072 Bit oder höher	Ab 2024: **RSA 3000 Bit**, empfohlen: **3072 Bit** [bsi.bund.de]
Post-Quantum Fokus	Sehr hoch, mit konkreten Standards und Zeitplan	Sehr hoch, mit TR-02102 als zentrale Richtlinie und europäischer Abstimmung

Empfehlungen nach Einsatzweck

Anwendungsbereich	**Empfohlene Algorithmen**	**Status**
Symmetrische Verschlüsselung	AES (128, 192, 256 Bit)	Empfohlen
Hash-Funktionen	SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512), SHA-3 (Keccak)	Empfohlen
Digitale Signaturen	ECDSA, EdDSA (Ed25519, Ed448), RSA 2048 Bit	Empfohlen / RSA noch zugelassen
Schlüsselvereinbarung	ECDH, DH mit großen Primzahlen	Empfohlen / DH noch zugelassen
Post-Quantum: KEM	CRYSTALS-Kyber	Empfohlen für PQC
Post-Quantum: Signaturen	CRYSTALS-Dilithium, FALCON, SPHINCS+	Empfohlen für PQC

Zeitliche Umsetzung

2024–2026 – Vorbereitung

- Bestandsaufnahme aller RSA-basierten Systeme
- Sicherheitsbewertung (z.B. Langzeitvertraulichkeit)
- Pilotprojekte mit PQC (CRYSTALS-Kyber, Dilithium)
- Schulungen für Entwickler und Sicherheitsteams
- **Priorität:** Hoch

2026–2029 – Teilweise Migration

- Migration kritischer Systeme (TLS, VPN, E-Mail)
- Hybride Algorithmen (klassisch + PQC)
- PKI-Infrastruktur aktualisieren
- Monitoring der NIST-Standards
- **Priorität:** Sehr hoch

2030–2034 – Vollständige Umstellung

- Keine neuen RSA-Anwendungen mehr
- Migration aller verbleibenden Systeme
- Validierung der neuen Infrastruktur
- Compliance und Dokumentation

- **Priorität:** Kritisch

Ab 2035 – RSA-Ende

- RSA vollständig deaktivieren
- Nur noch quantensichere Algorithmen verwenden
- Regelmäßige Sicherheitsüberprüfungen

- **Priorität:** Pflicht