DFN-CERT

deutsches forschungsnetz

Stand Post-Quanten-Kryptographie aus Sicht eines PKI-Praktikers

85. Betriebstagung | 06.10.2026

Jürgen Brauckmann

Einleitung

Einleitung

- In einigen Jahren: Leistungsfähige Quantencomputer brechen RSA und ECC
- BSI Studie zum Entwicklungsstand Quantencomputer v2.2, 12.2025: *Realisierung eines kryptographisch relevanten Quantencomputers bis 2040 erscheint realistisch.*

  https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Aktualisierung_Studie_Quantencomputer_251219.html

Einleitung

Folgen:

- 2040 ist doch noch lange hin?
- Ja, aber Umstellung **komplex**
  - Neue Algorithmen-Standards für Post-Quantum Cryptography (PQC)
  - Neue Standards für Anwendung dieser Algorithmen
  - Technische Umsetzung in Bibliotheken
  - Umstellung von Anwendungen
  - Migration von Infrastrukturen und Ökosystemen, z.B. PKIs und Föderationen
  - Problem „store now, decrypt later“
  - Problem Langzeitsignaturen
  - Problem Zeitabschätzung Verfügbarkeit Quantencomputer

Einleitung

Algorithmen-Standards NIST 2024:

- FIPS 203 **ML-KEM**
  - Ersatz für RSA-Schlüsseltransport bzw. ECDH-Schlüsseleinigung
  - Pubkey und Ciphertext 1568 Byte bei ML-KEM 1024
- FIPS 204 **ML-DSA**
  - Ersatz für digitale Signaturen mit RSA oder ECDSA
  - Pubkey 2592 Byte, Signaturen 4627 Byte bei ML-DSA-87
- FIPS 205 **SLH-DSA**
  - Konservativere Alternative zu ML-DSA
  - Aber: Deutlich größere Signaturen (8kB-50kB) und deutlich langsamer

Einleitung

Pläne und Empfehlungen:

- NIST IR 8547:
  - Ab **2030** klassische Algorithmen für neue Systeme nicht mehr empfohlen
  - Ab **2035** klassische Algorithmen verboten
- BSI TR-02102:
  - Schlüsseleinigung ohne PQC nur noch bis Ende **2031** empfohlen
  - Für sehr hohen Schutzbedarf Umstellung bis Ende **2030**
  - Klassische Signatur-Algorithmen nur noch bis Ende **2035** empfohlen
  - Derzeit: PQC nur in **Kombination** mit „klassischen" Algorithmen empfohlen
- Google/Cloudflare:
  - 2029 **Abschluss** (!) der PQC Migration

Anwendungsstandards

Anwendungsstandards

CA/B-Forum:

- S/MIME Baseline Requirements seit **2025-08** mit ML-KEM und ML-DSA
- Noch nicht: TLS Baseline Requirements
  - Derzeit noch nicht so relevant, da TLS-Zertifikate nur für Authentifizierung im **Hier und Jetzt** wirksam sind
- Noch keine Zertifikate in der Web-PKI erhältlich
- Einige PKI-Anbieter werben mit internen PKIs mit ML-DSA-Zertifikaten
  - Sinnhaftigkeit derzeit?

Anwendungsstandards

S/MIME:

- CMS:
  - ML-DSA als RFC 9882 seit **2025-10**
  - ML-KEM als RFC 9936 seit **2026-03**
- Thunderbird: Basis-Integration von ML-DSA in NSS läuft
- Outlook: ?

OpenPGP:

- Hybride ML-DSA/ML-KEM in OpenPGP als RFC 9980 seit **2026-06**
- Implementiert in Sequoia PGP, Proton Mail, GnuPG 2.5.23 (mit Flag --allow-9980)

Anwendungsstandards

SAML:

- Problem: xmldsig/xmlenc das letzte Mal **2013** modifiziert
- Draft RFC für Algorithmen-Bezeichner:
  https://datatracker.ietf.org/doc/html/draft-eastlake-rfc9231bis-xmlsec-uris-09
- Viele Konsequenzen. Mindestens:
  - Redirect Binding wg. großer Signaturen nicht mehr sinnvoll
  - AAI Metadaten werden wg. großer Schlüssel explodieren
- **Umsetzungspläne** für Shibboleth/SimpleSAMLphp?

Anwendungsstandards

OIDC:

- JSON Object Signing and Encryption:
  - ML-DSA als RFC 9964 seit **2026-03**
- Token-Größe wird Problem
  - Migration auf Referenz-Token oder andere Architekturen?
  - Token in Cookies auf **~4k** limitiert
- Landschaft der OIDC clients sehr **heterogen**. Viele verschiedene jwt-Libs.
- Ankündigung für Keycloak ab 2027-3 (27.0.0)

Anwendungsstandards

PDF:

- Übereinkunft auf den PDF Days 2025: PQC soll in die **Spezifikation**
- Zustand PDF-Standardisierung?
- Diverse **Ankündigungen** für Anwendungssoftware

Anwendungsstandards: TLS

- RFC 10024 (2026-08): Hybride **Schlüsselaustauschalgorithmen**
- Fundament für die Verschlüsselung des TLS-Kanals
- ML-KEM für TLS 1.3
  - `X25519MLKEM768`
  - `SecP256r1MLKEM768`
  - `SecP384r1MLKEM1024`
- Sehr **wichtig**, sehr **konkret**, funktioniert **jetzt**!
- Schlüsselaustausch bereits jetzt mit PQC schützenswert
  - „store now, decrypt later“

Anwendungsstandards: TLS

- RFC 10024 **implementiert** in: openssl 3.5, GnuTLS 3.8.8, aktuellen Browsern, aktuellen Webservern, IIS auf Win 11/Server 2025 seit Patchday 14.07.2026
- Oft bereits **automatisch** aktiviert.
- Manuell z.B.:
  - Apache: `SSLOpenSSLConfCmd Curves  \ X25519MLKEM768:X25519:prime256v1:secp384r1`
  - Nginx: `ssl_ecdh_curve  X25519MLKEM768:X25519:secp384r1:prime256v1;`
  - Postfix: `tls_eecdh_auto_curves = X25519MLKEM768, X25519, prime256v1, secp384r1`

SSL Server Test: doku.tid

ssllabs.com/ssltest/analyze.html?d=doku.tid.dfn.de&s=2001%3a638%3ad%3ac104%3a0%3a0%3a0%3a103&hideResults=on&latest

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

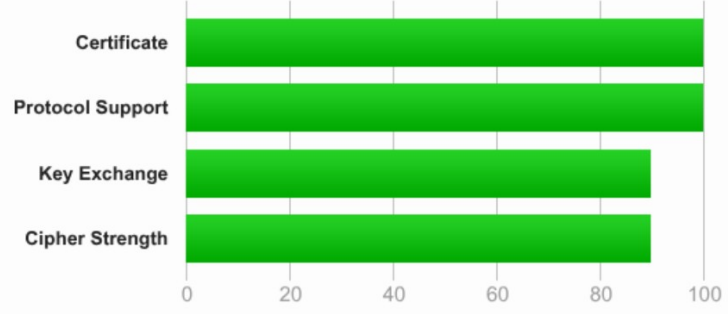
You are here: Home > Projects > SSL Server Test > doku.tid.dfn.de > 2001:638:d:c104:0:0:0:103

SSL Report: doku.tid.dfn.de (2001:638:d:c104:0:0:0:103)

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports PQC (Post-Quantum Cryptography) key exchange.

SSL Server Test: doku.tid

ssllabs.com/ssltest/analyze.html?d=doku.tid.dfn.de&s=2001%3a638%3ad%3ac104%3a0%3a0%3a0%3a103&hideResults=on&latest

Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Cipher Suites

 # TLS 1.3 (suites in server-pr

TLS_AES_256_GCM_SHA384 302) X25519MLKEM768 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_S 56 (0x1303) X25519MLKEM768 (eq. 3072 bits RSA) FS	256
TLS_AES_128_GCM_SHA256 301) X25519MLKEM768 (eq. 3072 bits RSA) FS	128

 # TLS 1.2 (suites in server-pr

TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 (0xc05d) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256 (0xc05c) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH x25519 (eq. 3072 bits RSA) FS	128

Handshake Simulation

Android 4.4.2	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

Anwendungsstandards

OpenSSH:

- Hybride **Schlüsselaustauschalgorithmen** bereits seit 2022
- Ab OpenSSH 9.9 (2024-09): `mlkem768x25519-sha256`
- Seit OpenSSH 10.0 (2025-04): PQC ist **default**
- RFC 10042 (2026-08): Post-Quantum/Traditional Hybrid Key Exchange with the Module-Lattice-Based Key-Encapsulation Mechanism for Use in SSH
- Sehr **wichtig**, sehr **konkret**, funktioniert **jetzt**!

Merkle Tree Certificates

Merkle Tree Certificates

- Auswirkungen PQC auf das **Gesamtsystem** Browser, Public CAs, Root-Programme, Zertifikatformate?

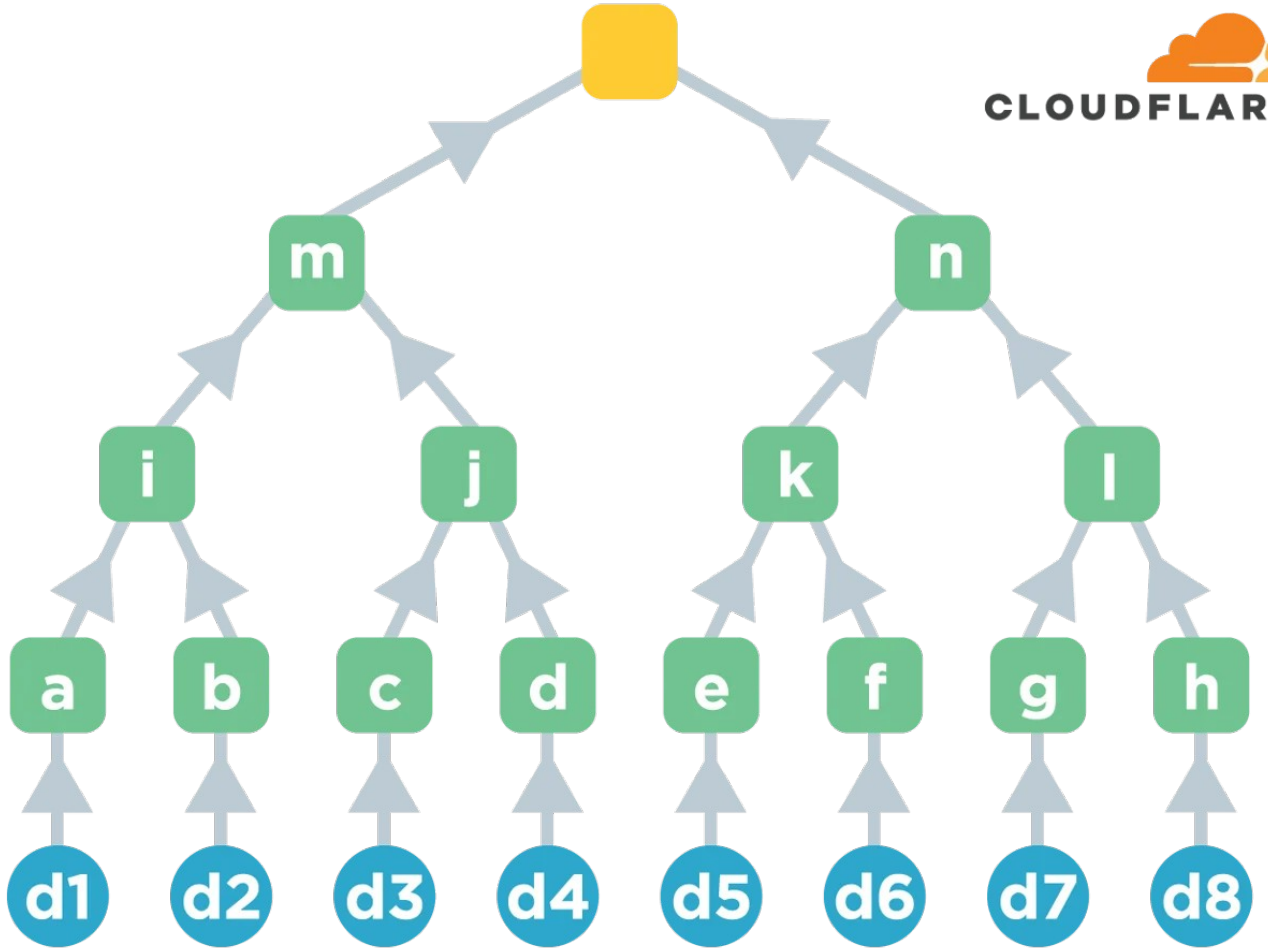
- Problem:
  - PQC nur mit deutlich **größeren** Signaturen: Faktor 10 bis 70.
  - Aktuell in einem TLS-Zertifikat mindestens 3 Signaturen (wg. SCTs/Certificate Transparency)
  - => Zertifikate werden sehr groß: 11KB statt 1kB.
  - => TLS-Handshake wird **riesig**
  - => Internet wird **langsam**
  - (Zusätzlich: Certificate Transparency Logs explodieren mit PQC)

Merkle Tree Certificates

- Lösungsidee: **Merkle Tree Certificates,**
  IETF WG PKI, Logs, And Tree Signatures (plants)
- Verschmelzung von **X.509** und **Certificate Transparency**
- CAs signieren nicht mehr Zertifikate, sondern betreiben Inclusion Logs
- Zertifikate enthalten keine klassische Signatur, sondern Merkle Tree Certificate Proofs

```
signatureAlgorithm = id-alg-mtcProof (OID 1.3.6.1.4.1.44363.47.0)
```

Merkle Tree Certificates



Bildherkunft: https://blog.cloudflare.com/bootstrap-mtc/

Merkle Tree Certificates

Weitere Eigenschaften:

- Zusätzliche **Rollen** wie Cosigner und Monitore
- Neuer Namensraum für Issuer: trustAnchorId
- Zwei verschiedene Ausprägungen von Zertifikaten:
  - **Standalone**: Mit Signatur für clients ohne aktuelle Infos zum Issuance Log
  - **Landmark-relative**: Ohne Signatur; client benötigt aktuelle zusätzliche Daten zur Verifikation
- Plus ein neues Konzept für **Sperrinformationen** (statt CRL/OCSP)

Merkle Tree Certificates

Konsequenzen:

- **Betriebsweise** PKI-Anbieter ändert sich stark
- Zertifikate der Web-PKI sehen deutlich anders aus
- Clients benötigen für Landmark-relative Zertifikate **aktualisierte Daten** von den PKIs
- Server sollen **beide** Zertifikattypen konfigurieren: Standalone plus Landmark-relative
- Auswirkungen auf selbst-betriebene internal PKIs?

Merkle Tree Certificates

Zustand:

- Standard noch in Entwicklung
- **Machbarkeitsstudien** von Google und Cloudflare bereits Oktober 2025 angekündigt
- Policy-Entwurf von Google für **Chrome Quantum-resistant Root Store** (CQRS)
  - Ab ca. Mitte 2027, getrennt von bestehendem Root Store
  - Initial ausschließlich bestehende Certificate Transparency Log Betreiber in der CA-Rolle

Merkle Tree Certificates

Zustand:

- Apple:
  - Ankündigung **MTC Policy** als Draft Ende Oktober 2026
  - Prognose Start **Q3/2027**
- Let’s Encrypt:
  - Bis **Ende 2026** ein staging environment
  - In **2027** ein production-ready environment
- CloudFlare:
  - Wird CA werden
  - Erste MTC **Q1/2027**

Fazit

Fazit

- PQC nimmt Fahrt auf
  - Konkret bei Ihnen! `X25519MLKEM768` in TLS 1.3!
- CA/B-Forum, PDF, S/MIME, SAML, OIDC: Noch viel Kleinarbeit zu leisten
  - Abwarten und beobachten
- Web-PKI vor tiefgreifendem Umbruch mit Merkle Tree Certificates
  - Auswirkungen auf den PKI-Markt und interne PKIs?

Haben Sie noch Fragen?

- Kontakt:

  DFN-PCA

  dfnpca@dfn-cert.de

  https://www.pki.dfn.de

  https://blog.pki.dfn.de

