# PQC-Bereitschaftsbewertung — Technischer Bericht

Auftraggeber: **Bank Krajowy Sp. z o.o.**

Audit-ID: `00000000-0000-0000-0001-000000000001`

Erstellt am: 2026-06-03 19:30 UTC

Modellkonfidenz: **84%**

# Methodik

This technical report has been automatically generated by the PQC Auditor system based on scanning publicly available TLS configurations, HTTP header analysis, and data provided by the client. The analysis was performed using an algorithm classifier (PQC KEM, PQC Signature, Symmetric QR, Hash QR, algorithms vulnerable to Shor's algorithm) and semantic validation via Pydantic schemas.

System: **pqc-analyst-2026-Q2-v2.1**

# Inhaltsverzeichnis

## Risikoubersicht

| 1 | 3 | 1 | 0 | 0 |
|---|---|---|---|---|
| KRITISCH | HOCH | MITTEL | NIEDRIG | UNBEKANNT |

| Komponente | Algorithmus | Empfohlener Ersatz | Aufwand | HNDL-Indikator |
|---|---|---|---|---|
| TLS handshake on bankkrajowy.pl:443 (legacy cipher) | RSA-2048 | REQUIRES_REVIEW:TLS 1.3 with X25519+ML-KEM-768 hybrid key exchange (FIPS 203) | mittel | ja |
| TLS 1.3 modern endpoints (api, mobile, corp) | REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid) | REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid (FIPS 203) — available in Caddy 2.9+, nginx 1.27+, AWS ALB (preview) | gering | ja |
| EJBCA internal PKI — RSA-2048 CA root | RSA-2048 | REQUIRES_REVIEW:ML-DSA-65 CA root (FIPS 204) — requires EJBCA 8.x + PQC-capable HSM firmware | hoch | nein |
| Mobile app certificate pinning (iOS/Android) | ECDSA-P256 | REQUIRES_REVIEW:ML-DSA-65 pinned certificate or hash-based pinning transition strategy | mittel | nein |
| Audit log signing | SHA-1 | REQUIRES_REVIEW:SHA-512 or SHA3-256 for audit log integrity | gering | nein |

## Kryptografische Stuckliste (CBOM)

| # | Komponente | Typ | Algorithmus | Version | Source |
|---|---|---|---|---|---|
| 0 | TLS handshake on bankkrajowy.pl:443 (legacy cipher) | KEY_EXCHANGE | `RSA-2048` | TLS 1.2 | scan |
| 1 | TLS 1.3 modern endpoints (api, mobile, corp) | KEY_EXCHANGE | `REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)` | TLS 1.3 | scan |
| 2 | X.509 certificates (bankkrajowy.pl, api, corp) — DigiCert RSA | SIGNATURE | `RSA-2048` | — | scan |
| 3 | EJBCA internal PKI — RSA-2048 CA root | SIGNATURE | `RSA-2048` | — | intake |
| 4 | Mobile app certificate pinning (iOS/Android) | SIGNATURE | `ECDSA-P256` | — | intake |
| 5 | Data at rest — legacy core banking modules | SYMMETRIC | `REQUIRES_REVIEW:AES-256-CBC` | — | intake |
| 6 | Audit log signing | SIGNATURE | `SHA-1` | — | intake |

## KRITISCH F-001

**Komponente:** TLS handshake on bankkrajowy.pl:443 (legacy cipher)

| | |
|---|---|
| **Algorithmus** | `RSA-2048` |
| **Empfohlener Ersatz** | REQUIRES_REVIEW:TLS 1.3 with X25519+ML-KEM-768 hybrid key exchange (FIPS 203) |
| **Aufwand** | mittel |
| **HNDL-Indikator** | ja |

### Feststellungen

Legacy TLS 1.2 with RSA key exchange on main banking portal bankkrajowy.pl. Financial transaction data and PSD2 authentication credentials are at risk of Harvest-Now-Decrypt-Later attack. RSA-2048 key exchange is quantum-vulnerable (NIST PQC: FIPS 203). DORA Art.9 requires cryptographic protection based on approved data classification.

### Referenzen

- FIPS 203
- REQUIRES_REVIEW:DORA Art.9
- RFC 8446

## HOCH F-002

**Komponente:** TLS 1.3 modern endpoints (api, mobile, corp)

| | |
|---|---|
| **Algorithmus** | `REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)` |
| **Empfohlener Ersatz** | REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid (FIPS 203) — available in Caddy 2.9+, nginx 1.27+, AWS ALB (preview) |
| **Aufwand** | gering |
| **HNDL-Indikator** | ja |

### Feststellungen

TLS 1.3 is enabled on API, mobile, and corporate endpoints, but without post-quantum hybrid key exchange. The X25519-only configuration offers no protection against HNDL attacks on intercepted TLS sessions. Polish National Cybersecurity Strategy 2025-2029 explicitly mandates planning for PQC migration.

### Referenzen

- FIPS 203
- REQUIRES_REVIEW:DORA Art.9

## HOCH F-003

**Komponente:** EJBCA internal PKI — RSA-2048 CA root

| | |
|---|---|
| **Algorithmus** | `RSA-2048` |
| **Empfohlener Ersatz** | REQUIRES_REVIEW:ML-DSA-65 CA root (FIPS 204) — requires EJBCA 8.x + PQC-capable HSM firmware |
| **Aufwand** | hoch |
| **HNDL-Indikator** | nein |

### Feststellungen

Internal EJBCA PKI uses RSA-2048 as CA root. All internal certificates derive from a quantum-vulnerable root. Migration to ML-DSA-65 (FIPS 204) root CA is a multi-month project requiring HSM firmware updates and certificate re-issuance across all internal services.

### Referenzen

- FIPS 204
- REQUIRES_REVIEW:DORA Art.9(2)

## HOCH F-005

**Komponente:** Audit log signing

| | |
|---|---|
| **Algorithmus** | `SHA-1` |
| **Empfohlener Ersatz** | REQUIRES_REVIEW:SHA-512 or SHA3-256 for audit log integrity |
| **Aufwand** | gering |
| **HNDL-Indikator** | nein |

### Feststellungen

Audit log signing uses SHA-1, which is considered cryptographically broken for collision resistance since 2017 (SHAttered attack). While not quantum-specific, this indicates a broader legacy cryptography governance gap and may constitute insufficient controls under DORA Art.9(2). Replace with SHA-256 minimum, SHA-512 recommended.

### Referenzen

- REQUIRES_REVIEW:NIST SP 800-131Ar3
- REQUIRES_REVIEW:DORA Art.9

## Feststellungen — MEDIUM / LOW

### MITTEL F-004: ECDSA-P256 → REQUIRES_REVIEW:ML-DSA-65 pinned certificate or hash-based pinning transition strategy

Mobile app certificate pinning uses ECDSA-P256. While not immediately exploitable (requires quantum computer with Shor's algorithm), pinning to a classical elliptic-curve certificate locks the app into a quantum-vulnerable trust anchor. Updating requires coordinated app store release.

**Komponente:** Mobile app certificate pinning (iOS/Android) | **Aufwand:** mittel | **HNDL-Indikator:** nein

**Referenzen:** FIPS 204, REQUIRES_REVIEW:NIST SP 800-131Ar3

# Massnahmenplan

## Schnelle Massnahmen (0-3 Monate)

Zeitrahmen: 0-3

- Enable TLS 1.3 exclusively on bankkrajowy.pl main portal; disable TLS 1.2
- Deploy X25519+ML-KEM-768 hybrid on all TLS 1.3 endpoints (Caddy or nginx patch)
- Replace SHA-1 audit log signing with SHA-512
- Enable HSTS includeSubDomains and preload on all domains

## Hauptmigration (3-12 Monate)

Zeitrahmen: 3-12

- Plan EJBCA PKI migration: evaluate HSM firmware PQC support (Thales Luna, Utimaco)
- Issue new ML-DSA-65 intermediate CA; begin dual-issuing certificates
- Update mobile app pinning strategy: transition to hash-based or ML-DSA pinned cert
- Migrate data-at-rest encryption from AES-256-CBC to AES-256-GCM across core modules
- Establish cryptographic inventory (CBOM) as living document in DORA ICT risk register

## Langfristig (12-24 Monate)

Zeitrahmen: 12-24

- Complete EJBCA root CA migration to ML-DSA-65 — re-issue all internal certificates
- Decommission all RSA-2048 key material from HSM
- Conduct PQC readiness re-audit to verify migration completeness
- Submit updated cryptographic controls documentation to KNF supervisory record

## Referenzen und Standards

- `FIPS 203`
- `REQUIRES_REVIEW:DORA Art.9`
- `RFC 8446`
- `FIPS 204`
- `REQUIRES_REVIEW:DORA Art.9(2)`

- `REQUIRES_REVIEW:NIST SP 800-131Ar3`

## Prufungsumfang (Scope)

Die Bewertung umfasst: offentlich erreichbare TLS-Endpunkte der vom Auftraggeber angegebenen Domanen, offentliche Zertifikatshistorie uber Certificate-Transparency-Protokolle (crt.sh mit Certspotter-Fallback), HTTP-Sicherheitsheader. Die Bewertung umfasst NICHT: interne oder authentifizierte Netzwerke, Quellcode-Reviews, Penetrationstests, Prufung der Datenklassifizierung, organisatorische Richtlinien.

## Methodik

Datenerhebung: automatisierter sslyze 6.x TLS-Scan (Handshake, Cipher Suites, Zertifikate), Certificate-Transparency-Abfrage uber crt.sh mit Certspotter v1 API Fallback, HTTP-Sicherheits-header-Prufung. Analyse: Kryptografische Komponenten werden in einem CBOM (Cryptographic Bill of Materials) katalogisiert und gegen die NIST-PQC-Taxonomie (FIPS 203, 204, 205), BSI TR-02102 (2024-01), ENISA Post-Quantum Cryptography Guidance (2024) abgeglichen. Regulatorisches Mapping erfolgt gegen den Text von NIS2-Richtlinie (EU 2022/2555), DORA (EU 2022/2554), DSGVO (EU 2016/679) sowie BSI-Grundschutz und BAIT. Alle Schlusse sind Indikatoren und stellen kein zertifiziertes Prufungsurteil dar.

## Einschrankungen

1. Automatisierter Charakter: Kryptografische Primitive und Konfigurationen werden aus offentlichen Serverantworten abgeleitet. Sie konnen die interne Architektur nicht vollstandig widerspiegeln. 2. Datenkontext: Die Datenklassifizierung (personlich, finanziell, medizinisch) wird aus dem Aufnahmeformular ubernommen oder konservativ angenommen. Keine unabhangige Verifikation. 3. Regulatorische Schlusse: Indikatoren moglicher Nichtkonformitat. Ein abschliessendes Compliance-Urteil kann nur von einem zertifizierten Prufer oder Datenschutzbeauftragten erteilt werden. 4. Sich entwickelnde PQC-Standards: Empfehlungen basieren auf NIST FIPS 203/204/205 (August 2024). Einzelne Algorithmen (SLH-DSA, Falcon) konnen bis 2027 aktualisiert werden.

## Konfidenzniveau — Erlauterung

Der Modellkonfidenzwert (0-100 %) ist die Selbstbewertung des KI-Analysten auf zwei Achsen: Ausreichende Eingabedaten (Scan-Vollstandigkeit und Aufnahmeformular) und Konsistenz des Ergebnisses mit der PQC-Wissensbasis. >=90 % - Daten ausreichend, Schlusse konsistent. 70-89 % - Daten uberwiegend ausreichend, manuelle Prufung von Grenzfallen empfohlen. <70 % - Wesentliche Datenlucken; Gesamtbewertungen (NIS2/DORA Bereitschaftsindikatoren) werden durch 'k.A.' ersetzt. Dieser Wert ist KEINE Schatzung der Kompromittierungswahrscheinlichkeit.

# Anhang

Bericht SHA-256:

```
a779da7c716bc032d07f86c5d763edd9e114ac6a5308bcf16df24d411be02757
```

### RECHTLICHER HINWEIS

Dieses Dokument ist eine automatisierte Post-Quantum-Kryptografie (PQC) Bereitschaftsbewertung und KEIN zertifiziertes Sicherheitsaudit. Alle Feststellungen sind Indikatoren potenzieller Risiken und Nichtkonformitaten auf Basis offentlich zuganglicher technischer Daten und vom Auftraggeber bereitgestellter Informationen. Dieses Dokument stellt KEINE (a) Rechtsberatung, (b) Sicherheitsgarantie, (c) formelle Compliance-Stellungnahme zu NIS2 / DORA / DSGVO dar - eine solche Stellungnahme kann nur ein zertifizierter Prufer ausstellen. Empfehlungen sind beratend und nicht vorschreibend. Der Bericht sollte vor Entscheidungen mit rechtlichen oder finanziellen Konsequenzen durch eine manuelle Prufung eines qualifizierten IT-Sicherheitsspezialisten erganzt werden. MorozzAI stellt diesen Bericht 'wie er ist' bereit, ohne ausdruckliche oder stillschweigende Garantien hinsichtlich Richtigkeit, Vollstandigkeit oder Eignung fur einen bestimmten Zweck, und ubernimmt keine Haftung fur Entscheidungen, die auf seiner Grundlage getroffen werden.