PQC Readiness Assessment — Technical Report

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

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

Generated: 2026-06-04 13:44 UTC

Model Confidence: **84%**

Methodology

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**

Table of Contents

1. Risk Summary

2. Cryptographic Bill of Materials (CBOM)

3. Observations

4. Roadmap

5. References & Standards

6. Appendix

Risk Summary

1	3	1	0	0
CRITICAL	HIGH	MEDIUM	LOW	UNKNOWN

Component	Algorithm	Recommended Replacement	Effort	HNDL Indicator
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)	medium	yes
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)	small	yes
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	large	no
Mobile app certificate pinning (iOS/Android)	ECDSA-P256	REQUIRES_REVIEW:ML-DSA-65 pinned certificate or hash-based pinning transition strategy	medium	no
Audit log signing	SHA-1	REQUIRES_REVIEW:SHA-512 or SHA3-256 for audit log integrity	small	no

Cryptographic Bill of Materials (CBOM)

#	Component	Type	Algorithm	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

CRITICAL F-001

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

Algorithm	`RSA-2048`
Recommended Replacement	REQUIRES_REVIEW:TLS 1.3 with X25519+ML-KEM-768 hybrid key exchange (FIPS 203)
Effort	medium
HNDL Indicator	yes

Observations

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.

References

- FIPS 203
- RFC 8446

HIGH F-002

Component: TLS 1.3 modern endpoints (api, mobile, corp)

Algorithm	`REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)`
Recommended Replacement	REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid (FIPS 203) — available in Caddy 2.9+, nginx 1.27+, AWS ALB (preview)
Effort	small
HNDL Indicator	yes

Observations

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.

References

- FIPS 203

HIGH F-003

Component: EJBCA internal PKI — RSA-2048 CA root

Algorithm	`RSA-2048`
Recommended Replacement	REQUIRES_REVIEW:ML-DSA-65 CA root (FIPS 204) — requires EJBCA 8.x + PQC-capable HSM firmware
Effort	large
HNDL Indicator	no

Observations

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.

References

- FIPS 204

HIGH F-005

Component: Audit log signing

Algorithm	`SHA-1`
Recommended Replacement	REQUIRES_REVIEW:SHA-512 or SHA3-256 for audit log integrity
Effort	small
HNDL Indicator	no

Observations

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.

Observations — MEDIUM / LOW

MEDIUM 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.

Component: Mobile app certificate pinning (iOS/Android) | **Effort:** medium | **HNDL Indicator:** no

References: FIPS 204

Roadmap

Quick Wins (0–3 months)

Timeframe: 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

Main Migration (3–12 months)

Timeframe: 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

Long Term (12–24 months)

Timeframe: 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

References & Standards

- `FIPS 203`
- `RFC 8446`

- `FIPS 204`

Scope

The assessment covers: publicly reachable TLS endpoints of the client's declared domains, public certificate history via Certificate Transparency logs (crt.sh with Certspotter fallback), HTTP security headers. The assessment does NOT cover: internal or authenticated networks, source-code review, penetration testing, verification of data classification, organisational policies or training programmes.

Methodology

Data collection: automated sslyze 6.x TLS scanning (handshake, cipher suites, certificates), Certificate Transparency lookup via crt.sh with Certspotter v1 API fallback, HTTP security-header probe. Analysis: cryptographic components are catalogued in a Cryptographic Bill of Materials (CBOM) and mapped against NIST PQC taxonomy (FIPS 203, 204, 205), ENISA Post-Quantum Cryptography guidance (2024) and BSI TR-02102 (2026-01). Regulatory mapping is performed against the text of NIS2 Directive (EU 2022/2555), DORA (EU 2022/2554) and GDPR (EU 2016/679). All conclusions are indicators only and do not constitute a certified audit opinion.

Limitations

1. Automated nature: cryptographic primitives and configuration are inferred from public server responses. They may not reflect internal architecture. 2. Data context: data classification (personal, financial, medical) is taken from the client's intake form or assumed conservatively. No independent verification is performed. 3. Regulatory conclusions: indicators of potential non-conformity. Definitive compliance opinion can only be issued by a certified auditor or Data Protection Officer. 4. PQC standards are evolving: recommendations are based on NIST FIPS 203 / 204 / 205 (November 2024). Individual algorithms (SLH-DSA, Falcon) may receive updates through 2027.

Confidence Level — How to Read

The Model Confidence value (0–100%) is the AI analyst's self-assessment on two axes: sufficiency of input data (scan completeness + intake form) and consistency of the result with the PQC knowledge base. ≥90% — data sufficient, conclusions internally consistent. 70–89% — data largely sufficient, manual review of edge cases is recommended. <70% — material data gaps; aggregate scores (NIS2 / DORA Readiness Indicators) are replaced with «N/A». This value is NOT an estimate of breach probability.

Appendix

Report SHA-256:

```
ea4f70c7215003b06b653e25f940c9324340341216084fe823be790491f36b14
```

LEGAL NOTICE & DISCLAIMER

This document is an automated Post-Quantum Cryptography (PQC) readiness assessment, NOT a certified security audit. All findings are indicators of potential risk and non-conformity based on publicly observable technical data and client-provided information. This document does NOT constitute (a) legal advice, (b) a guarantee of security, (c) a formal compliance opinion on NIS2 / DORA / GDPR — only a certified auditor may issue such an opinion. Recommendations are advisory and not prescriptive. The report should be complemented with a manual review by a qualified information-security professional before any decision with legal or financial consequences. PQC Auditor provides this report «as is», without express or implied warranties as to accuracy, completeness or fitness for a particular purpose, and accepts no liability for decisions made on its basis.