Szczegółowy raport techniczny audytu PQC

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

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

Wygenerowano: 2026-06-04 13:44 UTC

Pewność modelu: **84%**

Metodologia

Niniejszy raport techniczny został wygenerowany automatycznie przez system PQC Auditor na podstawie skanowania publicznie dostępnych konfiguracji TLS, analizy nagłówków HTTP oraz danych dostarczonych przez klienta. Analiza została przeprowadzona z użyciem klasyfikatora algorytmów (PQC KEM, PQC Signature, Symmetric QR, Hash QR, algorytmy podatne na algorytm Shora) oraz walidacji semantycznej przez schematy Pydantic.

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

Spis treści

Podsumowanie ryzyka

1	3	1	0	0
KRYTYCZNY	WYSOKI	ŚREDNI	NISKI	NIEZNANY

Komponent	Algorytm	Zalecana zamiana	Nakład pracy	Ryzyko HNDL
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)	średni	tak
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)	mały	tak
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	duży	nie
Mobile app certificate pinning (iOS/Android)	ECDSA-P256	REQUIRES_REVIEW:ML-DSA-65 pinned certificate or hash-based pinning transition strategy	średni	nie
Audit log signing	SHA-1	REQUIRES_REVIEW:SHA-512 or SHA3-256 for audit log integrity	mały	nie

Rejestr komponentów kryptograficznych (CBOM)

#	Komponent	Typ	Algorytm	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

KRYTYCZNY F-001

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

Algorytm	`RSA-2048`
Zalecana zamiana	REQUIRES_REVIEW:TLS 1.3 with X25519+ML-KEM-768 hybrid key exchange (FIPS 203)
Nakład pracy	średni
Ryzyko HNDL	tak

Obserwacje

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.

Źródła

- FIPS 203
- RFC 8446

WYSOKI F-002

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

Algorytm	`REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)`
Zalecana zamiana	REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid (FIPS 203) — available in Caddy 2.9+, nginx 1.27+, AWS ALB (preview)
Nakład pracy	mały
Ryzyko HNDL	tak

Obserwacje

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.

Źródła

- FIPS 203

WYSOKI F-003

Komponent: EJBCA internal PKI — RSA-2048 CA root

Algorytm	`RSA-2048`
Zalecana zamiana	REQUIRES_REVIEW:ML-DSA-65 CA root (FIPS 204) — requires EJBCA 8.x + PQC-capable HSM firmware
Nakład pracy	duży
Ryzyko HNDL	nie

Obserwacje

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.

Źródła

- FIPS 204

WYSOKI F-005

Komponent: Audit log signing

Algorytm	`SHA-1`
Zalecana zamiana	REQUIRES_REVIEW:SHA-512 or SHA3-256 for audit log integrity
Nakład pracy	mały
Ryzyko HNDL	nie

Obserwacje

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.

Obserwacje — MEDIUM / LOW

ŚREDNI 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.

Komponent: Mobile app certificate pinning (iOS/Android) | **Nakład pracy:** średni | **Ryzyko HNDL:** nie

Źródła: FIPS 204

Mapa drogowa

Szybkie zwycięstwa (0–3 mies.)

Termin: 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

Główna migracja (3–12 mies.)

Termin: 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

Długoterminowa (12–24 mies.)

Termin: 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

Źródła i standardy

- `FIPS 203`
- `RFC 8446`

- `FIPS 204`

Zakres audytu (Scope)

Analiza obejmuje: publicznie dostępne punkty końcowe TLS domen klienta, publiczną historię certyfikatów (Certificate Transparency przez crt.sh / Certspotter), nagłówki bezpieczeństwa HTTP. Analiza NIE obejmuje: sieci wewnętrznych, przeglądu kodu źródłowego, testów penetracyjnych, weryfikacji klasyfikacji przetwarzanych danych ani przeglądu polityk organizacyjnych.

Metodologia

Pozyskanie danych: automatyczne skanowanie sslyze 6.x (TLS handshake, cipher suites, certyfikaty), zapytanie do logów CT przez crt.sh z fallbackiem na Certspotter v1 API, sonda HTTP nagłówków bezpieczeństwa. Analiza: klasyfikacja komponentów kryptograficznych w CBOM, mapowanie do taksonomii NIST PQC (FIPS 203 / 204 / 205), ENISA Post-Quantum Cryptography guidance (2024), BSI TR-02102 (2026-01). Mapowanie regulacyjne wykonano na podstawie tekstu NIS2 Directive (EU 2022/2555), DORA (EU 2022/2554), RODO (EU 2016/679). Wszystkie ustalenia mają charakter wskazujący, nie stanowią certyfikowanej opinii audytorskiej.

Ograniczenia

1. Charakter automatyczny analizy: algorytmy i konfiguracje są wyprowadzane z publicznych odpowiedzi serwera. Mogą nie odzwierciedlać wewnętrznej architektury. 2. Kontekst danych: klasyfikacja danych (osobowe, finansowe, medyczne) jest przyjmowana z deklaracji klienta lub zakładana konserwatywnie. Bez niezależnej weryfikacji. 3. Wnioski regulacyjne: wskaźniki potencjalnej niezgodności. Ostateczną opinię o zgodności wydaje wyłącznie certyfikowany audytor lub IOD. 4. Standardy PQC są w fazie aktywnej: rekomendacje oparte na NIST FIPS 203/204/205 (listopad 2024). Niektóre algorytmy (SLH-DSA, Falcon) mogą otrzymać aktualizacje do 2027 roku.

Poziom pewności — interpretacja

Pole «Pewność modelu» (0–100%) to samoocena AI-analityka według dwóch osi: wystarczalność danych wejściowych (pełność skanu + ankiety) oraz spójność wyniku z bazą wiedzy PQC. ≥90% — dane wystarczające, wnioski spójne. 70–89% — dane w większości wystarczające, zalecana ręczna weryfikacja granicznych przypadków. <70% — istotne braki danych; liczbowe oceny sumaryczne (NIS2 / DORA Readiness) zastąpione przez «N/D». Wskaźnik NIE jest oceną prawdopodobieństwa kompromitacji.

Dodatek

SHA-256 raportu:

```
ea4f70c7215003b06b653e25f940c9324340341216084fe823be790491f36b14
```

KLAUZULA PRAWNA

Niniejszy dokument stanowi zautomatyzowaną ocenę gotowości do kryptografii post-kwantowej (PQC readiness assessment), a NIE certyfikowany audyt bezpieczeństwa. Wszystkie ustalenia mają charakter wskazujący na potencjalne ryzyka i niezgodności na podstawie publicznie dostępnych danych technicznych i informacji dostarczonych przez klienta. Dokument nie stanowi (a) porady prawnej, (b) gwarancji bezpieczeństwa, (c) oficjalnej opinii o zgodności z NIS2 / DORA / RODO — taką opinię wydaje wyłącznie certyfikowany audytor. Rekomendacje nie mają statusu nakazu. Zaleca się uzupełnienie raportu ręcznym przeglądem wykwalifikowanego specjalisty ds. bezpieczeństwa informatycznego przed podjęciem decyzji o skutkach prawnych lub finansowych. PQC Auditor dostarcza raport «tak jak jest», bez wyraźnych ani dorozumianych gwarancji dokładności, kompletności lub zastosowania w konkretnych okolicznościach, i nie ponosi odpowiedzialności za decyzje podjęte na jego podstawie.