Szczegółowy raport techniczny audytu PQC

Klient: **InvestPro MVP Sp. z o.o.**

ID audytu: `00000000-0000-0000-0003-000000000003`

Wygenerowano: 2026-06-04 13:45 UTC

Pewność modelu: **94%**

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

0	1	1	1	0
KRYTYCZNY	WYSOKI	ŚREDNI	NISKI	NIEZNANY

Komponent	Algorytm	Zalecana zamiana	Nakład pracy	Ryzyko HNDL
TLS 1.3 key exchange on investpro.pl and app.investpro.pl	REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)	REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid — enable via Vercel Edge TLS settings or Cloudflare proxy	trywialny	tak
X.509 certificates — Let's Encrypt ECDSA-P256	ECDSA-P256	REQUIRES_REVIEW:When public CAs support ML-DSA: request ML-DSA-65 certificate (FIPS 204). Interim: HSTS + certificate pinning monitoring.	mały	nie
JWT EdDSA (Ed25519) — user session tokens	Ed25519	REQUIRES_REVIEW:ML-DSA-65 JWT signing (FIPS 204) — available via liboqs Python bindings in Supabase edge functions	średni	nie

Rejestr komponentów kryptograficznych (CBOM)

#	Komponent	Typ	Algorytm	Version	Source
0	TLS 1.3 key exchange on investpro.pl and app.investpro.pl	KEY_EXCHANGE	`REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)`	TLS 1.3	scan
1	X.509 certificates — Let's Encrypt ECDSA-P256	SIGNATURE	`ECDSA-P256`	—	scan
2	JWT EdDSA (Ed25519) — user session tokens	SIGNATURE	`Ed25519`	—	intake
3	Data at rest — Supabase + Vercel edge (AES-256-GCM)	SYMMETRIC	`AES-256-GCM`	—	intake

WYSOKI F-001

Komponent: TLS 1.3 key exchange on investpro.pl and app.investpro.pl

Algorytm	`REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)`
Zalecana zamiana	REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid — enable via Vercel Edge TLS settings or Cloudflare proxy
Nakład pracy	trywialny
Ryzyko HNDL	tak

Obserwacje

TLS 1.3 is correctly deployed with modern AEAD cipher suites — an excellent baseline for an 8-person startup. However, key exchange uses classical X25519 only, without ML-KEM-768 hybrid (FIPS 203). Client financial portfolios and personal authentication data transmitted over these sessions are at risk of Harvest-Now-Decrypt-Later attack. Vercel's Edge Network has announced PQC hybrid TLS support; enabling it is a configuration change, not an engineering project.

Źródła

- FIPS 203

Obserwacje — MEDIUM / LOW

ŚREDNI F-002: ECDSA-P256 → REQUIRES_REVIEW:When public CAs support ML-DSA: request ML-DSA-65 certificate (FIPS 204). Interim: HSTS + certificate pinning monitoring.

Let's Encrypt issues ECDSA-P256 certificates, which are quantum-vulnerable in their signing algorithm (Shor's algorithm on elliptic curves). While Let's Encrypt does not yet issue ML-DSA certificates (industry-wide limitation — public CAs awaiting ML-DSA CA/Browser Forum policy), planning for hybrid certificate trust chains is advisable for a regulated MiFID II entity.

Komponent: X.509 certificates — Let's Encrypt ECDSA-P256 | **Nakład pracy:** mały | **Ryzyko HNDL:** nie

Źródła: FIPS 204

NISKI F-003: Ed25519 → REQUIRES_REVIEW:ML-DSA-65 JWT signing (FIPS 204) — available via liboqs Python bindings in Supabase edge functions

JWT session tokens use EdDSA (Ed25519) — currently the strongest available classical signature for this use case. Ed25519 is quantum-vulnerable via Shor's algorithm but has shorter-term risk than RSA/ECDSA due to key size dynamics. Session tokens typically expire within hours, reducing HNDL exposure. Migration to ML-DSA-65 (FIPS 204) can be scheduled within the 12-24 month window.

Komponent: JWT EdDSA (Ed25519) — user session tokens | **Nakład pracy:** średni | **Ryzyko HNDL:** nie

Źródła: FIPS 204

Mapa drogowa

Szybkie zwycięstwa (0–3 mies.)

Termin: 0-3

- Enable X25519+ML-KEM-768 hybrid TLS on Vercel or add Cloudflare proxy with PQC enabled
- Document current cryptographic stack as CBOM — baseline for future audits

Główna migracja (3–12 mies.)

Termin: 3-12

- Evaluate Supabase roadmap for ML-DSA JWT support
- Prototype Ed25519 → ML-DSA-65 migration in staging environment
- Monitor Let's Encrypt and CA/Browser Forum for ML-DSA certificate issuance timeline

Źródła i standardy

- `FIPS 203`

- `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:

```
76ab65d6246de86b7ccf9c516c135d8ed11859198e5b7e471ad583de4303d4f8
```

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.