PQC Readiness Assessment — Technical Report

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

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

Generated: 2026-06-04 13:45 UTC

Model Confidence: **94%**

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

Risk Summary

0	1	1	1	0
CRITICAL	HIGH	MEDIUM	LOW	UNKNOWN

Component	Algorithm	Recommended Replacement	Effort	HNDL Indicator
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	trivial	yes
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.	small	no
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	medium	no

Cryptographic Bill of Materials (CBOM)

#	Component	Type	Algorithm	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

HIGH F-001

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

Algorithm	`REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)`
Recommended Replacement	REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid — enable via Vercel Edge TLS settings or Cloudflare proxy
Effort	trivial
HNDL Indicator	yes

Observations

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.

References

- FIPS 203

Observations — MEDIUM / LOW

MEDIUM 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.

Component: X.509 certificates — Let's Encrypt ECDSA-P256 | **Effort:** small | **HNDL Indicator:** no

References: FIPS 204

LOW 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.

Component: JWT EdDSA (Ed25519) — user session tokens | **Effort:** medium | **HNDL Indicator:** no

References: FIPS 204

Roadmap

Quick Wins (0–3 months)

Timeframe: 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

Main Migration (3–12 months)

Timeframe: 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

References & Standards

- `FIPS 203`

- `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:

```
76ab65d6246de86b7ccf9c516c135d8ed11859198e5b7e471ad583de4303d4f8
```

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.