PQC-Bereitschaftsbewertung — Technischer Bericht

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

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

Erstellt am: 2026-06-04 13:45 UTC

Modellkonfidenz: **94%**

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

0	1	1	1	0
KRITISCH	HOCH	MITTEL	NIEDRIG	UNBEKANNT

Komponente	Algorithmus	Empfohlener Ersatz	Aufwand	HNDL-Indikator
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	ja
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.	gering	nein
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	mittel	nein

Kryptografische Stuckliste (CBOM)

#	Komponente	Typ	Algorithmus	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

HOCH F-001

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

Algorithmus	`REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)`
Empfohlener Ersatz	REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid — enable via Vercel Edge TLS settings or Cloudflare proxy
Aufwand	trivial
HNDL-Indikator	ja

Feststellungen

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.

Referenzen

- FIPS 203

Feststellungen — MEDIUM / LOW

MITTEL 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.

Komponente: X.509 certificates — Let's Encrypt ECDSA-P256 | **Aufwand:** gering | **HNDL-Indikator:** nein

Referenzen: FIPS 204

NIEDRIG 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.

Komponente: JWT EdDSA (Ed25519) — user session tokens | **Aufwand:** mittel | **HNDL-Indikator:** nein

Referenzen: FIPS 204

Massnahmenplan

Schnelle Massnahmen (0-3 Monate)

Zeitrahmen: 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

Hauptmigration (3-12 Monate)

Zeitrahmen: 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

Referenzen und Standards

- `FIPS 203`

- `FIPS 204`

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:

```
76ab65d6246de86b7ccf9c516c135d8ed11859198e5b7e471ad583de4303d4f8
```

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. PQC Auditor 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.