PQC Readiness Assessment — Technical Report

Client: **FastPay Sp. z o.o.**

Audit ID: `00000000-0000-0000-0002-000000000002`

Generated: 2026-06-03 19:30 UTC

Model Confidence: **91%**

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	2	1	0	0
CRITICAL	HIGH	MEDIUM	LOW	UNKNOWN

Component	Algorithm	Recommended Replacement	Effort	HNDL Indicator
TLS 1.3 key exchange on all endpoints (fastpay.pl, api, merchant)	REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)	REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid key exchange (FIPS 203) — GCP Cloud Load Balancing PQC preview available	small	yes
JWT RS256 — inter-service authentication tokens	RSA-2048	REQUIRES_REVIEW:ML-DSA-65 JWT signing (FIPS 204) — available in liboqs-go and python-oqs	medium	yes
Cloud HSM ECDSA-P256 — payment authorization signing	ECDSA-P256	REQUIRES_REVIEW:ML-DSA-65 on GCP CloudHSM (FIPS 204) when production-ready; interim: hybrid ECDSA+ML-DSA	medium	no

Cryptographic Bill of Materials (CBOM)

#	Component	Type	Algorithm	Version	Source
0	TLS 1.3 key exchange on all endpoints (fastpay.pl, api, merchant)	KEY_EXCHANGE	`REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)`	TLS 1.3	scan
1	JWT RS256 — inter-service authentication tokens	SIGNATURE	`RSA-2048`	—	intake
2	Cloud HSM ECDSA-P256 — payment authorization signing	SIGNATURE	`ECDSA-P256`	—	intake
3	TLS 1.3 symmetric encryption (AES-256-GCM, CHACHA20)	SYMMETRIC	`REQUIRES_REVIEW:AES-256-GCM / CHACHA20-POLY1305`	TLS 1.3	scan
4	Data at rest — Cloud SQL (GCP) encrypted volumes	SYMMETRIC	`REQUIRES_REVIEW:AES-256-GCM (GCP managed key)`	—	intake

HIGH F-001

Component: TLS 1.3 key exchange on all endpoints (fastpay.pl, api, merchant)

Algorithm	`REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)`
Recommended Replacement	REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid key exchange (FIPS 203) — GCP Cloud Load Balancing PQC preview available
Effort	small
HNDL Indicator	yes

Observations

TLS 1.3 is correctly deployed across all three domains (excellent baseline). However, key exchange uses classical X25519 only, without ML-KEM-768 hybrid (FIPS 203). Payment transaction metadata transmitted over these connections is at risk of Harvest-Now-Decrypt-Later interception. UKNF-supervised payment institutions are in scope for DORA Art.9(2) cryptographic key protection requirements.

References

- FIPS 203
- REQUIRES_REVIEW:DORA Art.9(2)
- RFC 8446

HIGH F-002

Component: JWT RS256 — inter-service authentication tokens

Algorithm	`RSA-2048`
Recommended Replacement	REQUIRES_REVIEW:ML-DSA-65 JWT signing (FIPS 204) — available in liboqs-go and python-oqs
Effort	medium
HNDL Indicator	yes

Observations

Inter-service JWT authentication uses RS256 (RSA-2048 signing). In a microservices payment architecture, a future quantum attacker forging inter-service tokens would achieve lateral movement across the entire payment processing chain. Migration to ML-DSA-65 (FIPS 204) or Ed25519 as interim is straightforward in Go/Python environments.

References

- FIPS 204

Observations — MEDIUM / LOW

MEDIUM F-003: ECDSA-P256 → REQUIRES_REVIEW:ML-DSA-65 on GCP CloudHSM (FIPS 204) when production-ready; interim: hybrid ECDSA+ML-DSA

Payment authorization signing uses HSM-backed ECDSA-P256 (elliptic curve, quantum-vulnerable via Shor's algorithm). Cloud HSM key migration to ML-DSA-65 requires GCP CloudHSM to support FIPS 204 — currently in preview; production readiness expected Q3 2026. Planning should begin now given HSM procurement and certification timelines.

Component: Cloud HSM ECDSA-P256 — payment authorization signing | **Effort:** medium | **HNDL Indicator:** no

References: FIPS 204, REQUIRES_REVIEW:NIST SP 800-131Ar3

Roadmap

Quick Wins (0–3 months)

Timeframe: 0-3

- Enable X25519+ML-KEM-768 hybrid on GCP Cloud Load Balancer (PQC preview flag)
- Add Permissions-Policy header to complete security header set
- Begin evaluation of liboqs-go for ML-DSA JWT prototype

Main Migration (3–12 months)

Timeframe: 3-12

- Migrate inter-service JWT signing from RS256 to ML-DSA-65
- Update JWT verification across all Go and Python microservices
- Monitor GCP CloudHSM FIPS 204 roadmap; submit change request to UKNF if HSM migration required during DORA audit cycle
- Document cryptographic inventory (CBOM) in DORA ICT risk register

References & Standards

- `FIPS 203`
- `REQUIRES_REVIEW:DORA Art.9(2)`
- `RFC 8446`
- `FIPS 204`

- `REQUIRES_REVIEW:NIST SP 800-131Ar3`

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:

```
d1d98c0169120549718f192ec035e87a28b160c25afef17d84c58b07fb9b02fe
```

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. MorozzAI 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.