PQC Readiness Assessment — Executive Summary

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

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

Generated: 2026-06-03 19:30 UTC

Model Confidence: **91%**

Risk Summary

Regulatory Readiness Indicators

62/100

NIS2 Readiness Indicator

58/100

DORA Readiness Indicator

Indicative Remediation Window: **270** days

Observations

HIGH 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

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.

Component: TLS 1.3 key exchange on all endpoints (fastpay.pl, api, merchant) | **Effort:** small | **HNDL Indicator:** yes

HIGH RSA-2048 → REQUIRES_REVIEW:ML-DSA-65 JWT signing (FIPS 204) — available in liboqs-go and python-oqs

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.

Component: JWT RS256 — inter-service authentication tokens | **Effort:** medium | **HNDL Indicator:** yes

> **MEDIUM** **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

Regulatory Context

Framework	Article	CRITICAL	Related Findings
DORA	`REQUIRES_REVIEW:DORA Art.9(2)`	HIGH	F-001, F-002
TLS key exchange on payment API endpoints uses classical X25519 only. Absence of PQC hybrid key exchange indicates potential non-conformity with DORA Art.9(2) cryptographic key protection requirements for PSD2-regulated payment data.			

> *NIS2 — illustrative upper limit of administrative fines up to €10M or 2% of annual turnover (applied by the competent authority in severe cases). General information, not an assessment of your organisation's specific exposure.*
>
> *DORA — potential periodic penalty payments up to 1% of daily turnover per day of continued non-compliance. General information, not an assessment of your specific exposure.*

Priority Action Plan

1. **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
   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.

REQUIRES_REVIEW:DORA Art.9(2) · REQUIRES_REVIEW:UoKSC Art.10(5)

2. **RSA-2048 → REQUIRES_REVIEW:ML-DSA-65 JWT signing (FIPS 204) — available in liboqs-go and python-oqs** medium
   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.

   REQUIRES_REVIEW:DORA Art.9(2)

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

+ 1 more detailed steps in the technical report

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

+ 2 more detailed steps in the technical report