Szczegółowy raport techniczny audytu PQC

Klient: **FastPay Sp. z o.o.**

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

Wygenerowano: 2026-06-04 13:44 UTC

Pewność modelu: **91%**

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	2	1	0	0
KRYTYCZNY	WYSOKI	ŚREDNI	NISKI	NIEZNANY

Komponent	Algorytm	Zalecana zamiana	Nakład pracy	Ryzyko HNDL
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	mały	tak
JWT RS256 — inter-service authentication tokens	RSA-2048	REQUIRES_REVIEW:ML-DSA-65 JWT signing (FIPS 204) — available in liboqs-go and python-oqs	średni	tak
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	średni	nie

Rejestr komponentów kryptograficznych (CBOM)

#	Komponent	Typ	Algorytm	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

WYSOKI F-001

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

Algorytm	`REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)`
Zalecana zamiana	REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid key exchange (FIPS 203) — GCP Cloud Load Balancing PQC preview available
Nakład pracy	mały
Ryzyko HNDL	tak

Obserwacje

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.

Źródła

- FIPS 203
- RFC 8446

WYSOKI F-002

Komponent: JWT RS256 — inter-service authentication tokens

Algorytm	`RSA-2048`
Zalecana zamiana	REQUIRES_REVIEW:ML-DSA-65 JWT signing (FIPS 204) — available in liboqs-go and python-oqs
Nakład pracy	średni
Ryzyko HNDL	tak

Obserwacje

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.

Źródła

- FIPS 204

Obserwacje — MEDIUM / LOW

ŚREDNI 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.

Komponent: Cloud HSM ECDSA-P256 — payment authorization signing | **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 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

Główna migracja (3–12 mies.)

Termin: 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

Źródła i standardy

- `FIPS 203`
- `RFC 8446`

- `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:

```
d39b2692237830ab47db0702aaec831c8ce494e8be53c7f3a4256674d777e436
```

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.