PQC-Bereitschaftsbewertung — Technischer Bericht

Auftraggeber: **FastPay Sp. z o.o.**

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

Erstellt am: 2026-06-03 19:30 UTC

Modellkonfidenz: **91%**

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

1. Risikoubersicht

2. Kryptografische Stuckliste (CBOM)

3. Feststellungen

4. Massnahmenplan

5. Referenzen und Standards

6. Anhang

Risikoubersicht

0	2	1	0	0
KRITISCH	HOCH	MITTEL	NIEDRIG	UNBEKANNT

Komponente	Algorithmus	Empfohlener Ersatz	Aufwand	HNDL-Indikator
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	gering	ja
JWT RS256 — inter-service authentication tokens	RSA-2048	REQUIRES_REVIEW:ML-DSA-65 JWT signing (FIPS 204) — available in liboqs-go and python-oqs	mittel	ja
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	mittel	nein

Kryptografische Stuckliste (CBOM)

#	Komponente	Typ	Algorithmus	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

HOCH F-001

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

Algorithmus	`REQUIRES_REVIEW:X25519 (classical only, no PQC hybrid)`
Empfohlener Ersatz	REQUIRES_REVIEW:X25519+ML-KEM-768 hybrid key exchange (FIPS 203) — GCP Cloud Load Balancing PQC preview available
Aufwand	gering
HNDL-Indikator	ja

Feststellungen

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.

Referenzen

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

HOCH F-002

Komponente: JWT RS256 — inter-service authentication tokens

Algorithmus	`RSA-2048`
Empfohlener Ersatz	REQUIRES_REVIEW:ML-DSA-65 JWT signing (FIPS 204) — available in liboqs-go and python-oqs
Aufwand	mittel
HNDL-Indikator	ja

Feststellungen

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.

Referenzen

- FIPS 204

Feststellungen — MEDIUM / LOW

MITTEL 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.

Komponente: Cloud HSM ECDSA-P256 — payment authorization signing | **Aufwand:** mittel | **HNDL-Indikator:** nein

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

Massnahmenplan

Schnelle Massnahmen (0-3 Monate)

Zeitrahmen: 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

Hauptmigration (3-12 Monate)

Zeitrahmen: 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

Referenzen und Standards

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

- `REQUIRES_REVIEW:NIST SP 800-131Ar3`

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:

```
d1d98c0169120549718f192ec035e87a28b160c25afef17d84c58b07fb9b02fe
```

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. MorozzAI 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.