PQC-Bereitschaftsbewertung — Zusammenfassung

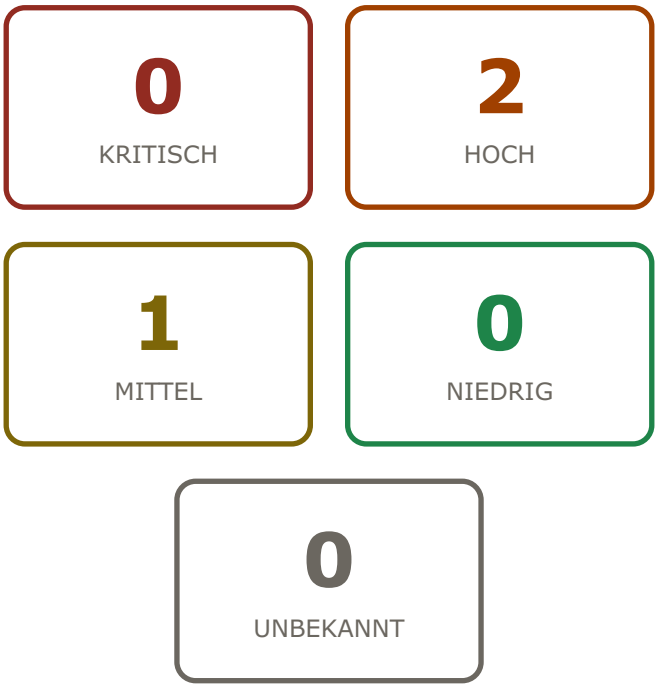
Auftraggeber: **FastPay Sp. z o.o.**

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

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

Modellkonfidenz: **91%**

Risikoubersicht



Regulatorische Bereitschaftsindikatoren

62/100

NIS2-Bereitschaftsindikator

58/100

DORA-Bereitschaftsindikator

Indikativer Behebungszeitraum: **270** Tage

Feststellungen

HOCH 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.

Komponente: TLS 1.3 key exchange on all endpoints (fastpay.pl, api, merchant) | **Aufwand:** gering | **HNDL-Indikator:** ja

HOCH 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.

Komponente: JWT RS256 — inter-service authentication tokens | **Aufwand:** mittel | **HNDL-Indikator:** ja

MITTEL 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

Regulatorischer Kontext

Rechtsrahmen	Artikel	KRITISCH	Verbundene Feststellungen
DORA	`REQUIRES_REVIEW:DORA Art. 9(2)`	HOCH	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 Obergrenze fur Verwaltungsbussen bis zu 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes (angewendet von der zustandigen Behorde in schwerwiegenden Fallen). Allgemeine Information, keine Beurteilung Ihres spezifischen Haftungsrisikos.*
>
> *DORA — mogliche Zwangsgelder bis zu 1 % des taglichen Gesamtumsatzes pro Tag bei anhaltender Nichtkonformitat. Allgemeine Information, keine Beurteilung Ihres spezifischen Haftungsrisikos.*

Prioritare Massnahmen

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** gering

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** mittel
   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)

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

+ 1 weitere detaillierte Schritte im technischen Bericht

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

+ 2 weitere detaillierte Schritte im technischen Bericht