



# **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**<sub>/100</sub>

NIS2-Bereitschaftsindikator

**58**<sub>/100</sub>

DORA-Bereitschaftsindikator

## 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 für Verwaltungsbussen bis zu 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes (angewendet von der zuständigen Behörde in schwerwiegenden Fällen). Allgemeine Information, keine Beurteilung Ihres spezifischen Haftungsrisikos.*

*DORA — mögliche Zwangsgelder bis zu 1 % des taglichen Gesamtumsatzes pro Tag bei anhaltender Nichtkonformität. Allgemeine Information, keine Beurteilung Ihres spezifischen Haftungsrisikos.*

## Prioritäre Massnahmen

- 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)

Zeitraumen: 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)

Zeitraumen: 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

### RECHTLICHER HINWEIS

Dieses Dokument ist eine automatisierte Post-Quantum-Kryptografie (PQC) Bereitschaftsbewertung und KEIN zertifiziertes Sicherheitsaudit. Alle Feststellungen sind Indikatoren potenzieller Risiken und Nichtkonformitäten auf Basis öffentlich zugänglicher 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 Prüfung eines qualifizierten IT-Sicherheitsspezialisten ergänzt werden. MorozzAI stellt diesen Bericht 'wie er ist' bereit, ohne ausdrückliche oder stillschweigende Garantien hinsichtlich Richtigkeit, Vollständigkeit oder Eignung für einen bestimmten Zweck, und übernimmt keine Haftung für Entscheidungen, die auf seiner Grundlage getroffen werden.