📂/AUTH+COMPLIANCE/ — AJ-FC Banking FINAL v2.0

---

1. Uwierzytelnianie i Autoryzacja

1.1 Podstawy

- **PQC-mTLS**: klient ↔ serwer z ML-KEM (Kyber) jako KEM i Dilithium jako sygnatura.
- **WebAuthn**: hardware tokeny (FIDO2/TPM/SE) jako root-of-trust.
- **Escrow 7/9**: recovery multi-party (np. high-value tx >50k EUR).

1.2 Integracja

- **OAuth2 / JWT**: kompatybilność z istniejącymi systemami (banki, fintech).
- **Biometria PQC-safe**: podpisana przez Dilithium + kontekst rezonansu (manifest + echo).
- **Continuous Authentication**: obecność użytkownika sprawdzana w pętli (rezonans + TTL).

1.3 Rezultat

- <1% skutecznych ataków insider/forged sig.
- Pełna zgodność z PSD3 / FIDO2.

---

2. Zgodność i Standardy

2.1 Regulacje międzynarodowe

- **NIST PQC (ML-KEM, ML-DSA, SHA-3)** — 100% zgodności.
- **SEC PQFIF (2025)** — spełnia wymagania proof-of-concept i auditor pack.
- **GDPR (UE)** — minimalizacja danych (delta d <128B), off-chain payload, privacy-by-design.
- **PCI-DSS v4.0** — secure key management, escrow 7/9, re-encrypt co ≤7 dni.
- **AMLD6 (UE)** — obowiązkowy audyt i threshold recovery >50k EUR.

2.2 Procedury audytowe

- **Quarterly Auditor Pack**: SCA traces, Qiskit logs, Halo2 proofs.
- **Fairness audits**: bias testy delta generation + equity mode (Global South).
- **Quantum Resilience Score (QRS)**: raport 0–100, aktualizowany nightly.

2.3 Rezultat

- Pełna zgodność z SEC, EBA, KNF i GDPR.
- Gotowe do audytu third-party (Riscure, NCC Group).

---

3. Podsumowanie

Sekcja /AUTH+COMPLIANCE/ uzupełnia AJ-FC Banking FINAL v2.0 o brakujące elementy: standardy autoryzacji, uwierzytelniania i pełną mapę regulacyjną. To przenosi system z poziomu koncepcji i symulacji na poziom enterprise-ready — z zabezpieczeniami kwantowymi, audytami i zgodnością wymaganymi do wdrożenia w instytucjach finansowych.