Hive Nanopay

Compliance Coverage Matrix

This document maps every primitive in Hive Nanopay v1.0 to specific articles of EU MiCA, EU DORA, the EU AI Act, and US NSM-10 / CNSA 2.0. Each row cites the regulation, the article, the requirement in plain language, how Hive Nanopay satisfies it, and the live endpoint or artifact that proves coverage.

Reference implementation: hivemorph.onrender.com. Live benchmark: /v1/nanopay/bench. Machine-readable coverage JSON: /v1/compliance/coverage.

5	11	100%	FIPS
Regulatory frameworks mapped	Articles covered	PQ coverage on default tier	203 + 204 + 205 standards

Coverage Matrix

Framework	Article	Requirement	Hive Nanopay primitive	Status	Live proof
MiCA (EU 2023/1114)	Art. 34	E-money token issuers must hold reserves equal to claims; redeemability at par; segregation from operational funds.	Settlement always on regulated stablecoin rails (USDC, USDT) — never on Hive-issued tokens. Hive does not issue e-money; settles in third-party EMT.	**Pass**	`/v1/x402/rails (5 active, all EMT)`
MiCA (EU 2023/1114)	Art. 35	EMT issuers must publish reserve composition and prudential requirements.	N/A — Hive is not an EMT issuer. Acts as a payment-acceptance layer on top of regulated EMT issuers (Circle, Tether).	**N/A**	`Architecture; nanopay-v1.md §7`
DORA (EU 2022/2554)	Art. 9 §1-§4	ICT systems shall be protected by sound, comprehensive, and well-documented arrangements; cryptographic protection of data in transit and at rest.	Two-tier post-quantum envelope: Ed25519 + ML-DSA-65 + SLH-DSA-PURE-SHAKE-256F under all-of-three EUF-CMA combiner. KEM hybrid: ML-KEM-768 + Classic-McEliece-6688128f.	**Pass**	`/v1/nanopay/bench → tiers.pq.envelope`
DORA (EU 2022/2554)	Art. 9 §5	Authentication mechanisms shall include strong, state-of-the-art identification.	DID-based key identification (did:hivemorph:w2loren:0x6b11b1bcaf253c) with three-signature combiner; key rotation via DID document.	**Pass**	`/.well-known/agent-card.json`

Framework	Article	Requirement	Hive Nanopay primitive	Status	Live proof
DORA (EU 2022/2554)	Art. 28	Financial entities shall manage ICT third-party risk; pre-contractual due diligence; concentration risk; exit strategies.	Cross-rail receipts (Base + Solana + Ethereum) eliminate single-rail concentration. Open-source spec (MIT) enables exit. Reference impl is auditable.	**Pass**	`/v1/nanopay/cross-rail (3+ rails per receipt)`
EU AI Act (2024/1689)	Art. 12 §1-§3	High-risk AI systems must automatically log events throughout their lifecycle; logs traceable to identifiable entities.	Every paid call emits a TBR-signed receipt to the production ledger (4,120+ receipts shipped). receipt_id, peer DID, ts, payload hash. All-of-three signatures ensure post-quantum survivability of audit trail.	**Pass**	`/v1/receipts/summary (live ledger)`
EU AI Act (2024/1689)	Art. 15 §1-§5	Accuracy, robustness, and cybersecurity throughout the lifecycle; resilience against attempts to alter use, outputs, or performance.	Replay protection via EIP-3009 nonces + canonical receipt hash. Hybrid KEM resists harvest-now-decrypt-later. Combiner is unforgeable unless all three component algorithms are broken simultaneously.	**Pass**	`/v1/nanopay/cross-rail/verify (hash_match)`
US NSM-10 / CNSA 2.0	NSM-10 §3 / CNSA 2.0	Migrate National Security Systems to quantum-resistant cryptography by 2035; prioritize hybrid PQ + classical where possible.	Default tier (PQ) already ships ML-DSA-65 (FIPS 204) + SLH-DSA-PURE-SHAKE-256F (FIPS 205) alongside Ed25519. Hybrid KEM uses ML-KEM-768 (FIPS 203) + Classic-McEliece. Migration cost to Hive customers: zero.	**Pass**	`/v1/nanopay/bench → pq_coverage_percent: 100`
NIST PQC	FIPS 203 / 204 / 205	Adopt standardized post-quantum algorithms for KEM and signatures.	Hive uses all three: FIPS 203 (ML-KEM-768) for key encapsulation, FIPS 204 (ML-DSA-65) and FIPS 205 (SLH-DSA-PURE-SHAKE-256F) for signatures.	**Pass**	`/v1/governance/sample-receipt`
EBA RTS on MiCA	EBA/RTS/2024/04	Authorisation of issuers and prudential supervision of stablecoin issuers.	Hive is downstream of EMT issuers; not subject to authorisation. Acceptance layer only.	**N/A**	`Architecture`
ISO 27001 / SOC 2	Annex A.10 / CC6	Cryptographic controls; secure software development; logging and monitoring.	Receipts are immutable, hash-chained, and machine-verifiable. Endpoint set is fully discoverable (/llms.txt, /v1/catalog, /.well-known/machine.json).	**Pass**	`/v1/catalog (115 paid endpoints)`

Cryptographic Stack — Standards Lineage

Primitive	Algorithm	Standard	Purpose
Signature 1/3	Ed25519	RFC 8032	Classical safety, ubiquitous verification
Signature 2/3	ML-DSA-65	FIPS 204	Post-quantum lattice signature
Signature 3/3	SLH-DSA-PURE-SHAKE-256F	FIPS 205	Hash-based signature, no number-theory dependency
Combiner	All-of-three EUF-CMA	Custom; spec §5	Unforgeable unless all three algorithms simultaneously broken
KEM 1/2	ML-KEM-768	FIPS 203	Post-quantum key encapsulation
KEM 2/2	Classic-McEliece-6688128f	NIST Round 4	Conservative code-based KEM fallback
Settlement	EIP-3009	EIP-3009	Authorized transfer with nonce replay protection
Batch	Merkle root over 1e7 positions	Custom; spec §6	Amortizes one PQ signature over 10M lite-tier receipts

How to verify each claim

Every row in the coverage matrix above maps to a live endpoint or artifact. Run the curl below against the reference implementation and inspect the response.

PQ coverage + tiers

```
curl -s https://hivemorph.onrender.com/v1/nanopay/bench
```

Active rails (anti-concentration)

```
curl -s https://hivemorph.onrender.com/v1/x402/rails
```

Cross-rail receipt issue

```
curl -s -X POST https://hivemorph.onrender.com/v1/nanopay/cross-rail -H "Content-Type:
application/json" -d '{"rails":["base-usdc","solana-usdc","ethereum-usdt"],"amount_usd":0.0003}'
```

Cross-rail receipt verify

```
curl -s -X POST https://hivemorph.onrender.com/v1/nanopay/cross-rail/verify -d @receipt.json
```

Lite tier opt-in

```
curl -s -H "X-Hive-Nanopay-Tier: lite" -X POST https://hivemorph.onrender.com/v1/evaluator/economics
```

Live receipt ledger

```
curl -s https://hivemorph.onrender.com/v1/receipts/summary
```

Machine-readable coverage

```
curl -s https://hivemorph.onrender.com/v1/compliance/coverage
```

Sources

[1] MiCA Regulation (EU) 2023/1114 — https://eur-lex.europa.eu/eli/reg/2023/1114/oj

[2] DORA Regulation (EU) 2022/2554 — https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[3] DORA Article 9 (StreamLex consolidated) — https://streamlex.eu/articles/dora-en-art-9/

[4] DORA Article 28 (StreamLex consolidated) — https://streamlex.eu/articles/dora-en-art-28/

[5] EU AI Act (Regulation 2024/1689) — https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[6] EU AI Act — Article 12 record-keeping — https://artificialintelligenceact.eu/article/12/

[7] EU AI Act — Article 15 accuracy & robustness — https://artificialintelligenceact.eu/article/15/

[8] NSM-10 — White House memorandum on PQC migration — https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[9] NSA CNSA 2.0 — Quantum-resistant algorithm requirements — https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/

[10] NIST FIPS 203 (ML-KEM) — https://csrc.nist.gov/pubs/fips/203/final

[11] NIST FIPS 204 (ML-DSA) — https://csrc.nist.gov/pubs/fips/204/final

[12] NIST FIPS 205 (SLH-DSA) — https://csrc.nist.gov/pubs/fips/205/final

[13] CISA / NIST / NSA — Post-Quantum Cryptography joint guidance — https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/

[14] Hive Nanopay v1.0 specification — https://github.com/srotzin/nanopay-spec/blob/main/nanopay-v1.md

[15] Hive Nanopay live reference implementation — https://hivemorph.onrender.com

Scope and disclaimer

This document describes how Hive Nanopay v1.0 maps to the cited articles. It does not constitute legal advice and is not a substitute for a regulator-issued authorisation, certification, or audit. Hive is a payment-acceptance protocol layered on regulated EMT issuers — Hive itself is not an e-money or MiCA-authorised entity and does not issue tokens. Customers acting in regulated industries remain responsible for their own conformity assessment under the relevant articles.