

EnteleKRON Security Assessment 2026 | Preflight Audit

Preflight Audit Current Assessment

EnteleKRON

Token, Contract, Security & Architecture Assessment 8 October 2026 Version 1.1

Assessment opinion: **CONDITIONAL / EVIDENCE-GATED**. Architecture and control design are substantially documented. A final production smart-contract opinion remains gated on exact audited commits, deployed bytecode, automated-analysis output, fuzz/invariant evidence, privileged-role configuration and remediation retesting.

1. Audited Asset & Contract Identity

Project / protocol | EnteleKRON (ENTEL KRON) |

Token name | EnteleKRON |

Ticker | ENK |

Current network | Ethereum Mainnet |

Chain ID | 1 |

Standard | ERC-20 |

Contract | 0xC95343B3f8A5af57a9b3B1acFf3D2a7654Fa28F6 |

Decimals | 18 |

Maximum / reserved supply | 100,000,000,000 ENK |

Assessment date | 8 October 2026 |

Sovereign-chain status | Planned; no live EnteleKRON sovereign mainnet asserted by this assessment. |

Future chain direction | Ethereum-secured, EVM-compatible OP Stack L2. |

Future ENK bridge | Not live; dedicated pre-activation audit required. |

2. Current Token / Sale Context

Stage | Price / context | Minimum | Published period |

Stage 1 | \$0.008 | \$10,000 | 1 29 Jul 2026 |

Stage 2 | \$0.010 | Published stage terms | 29 Jul 26 Aug 2026 |

Stage 3 | \$0.012 | \$2,500 | 26 Aug 23 Sep 2026 |

Stage 4 Public Presale | \$0.016 / \$0.020 / \$0.024 / \$0.032 / \$0.040 / \$0.048 | \$500 / \$400 /
Page 1 of 4

\$300 / \$200 / \$100 / no fixed minimum in section 6 | 23 Sep 2026 9 Mar 2027 |

3. Scope & Methodology

Reviewed evidence includes the sovereign architecture definition, native-module specifications, ENK/TVKUSD separation controls, unified financial architecture, current ENK contract identity, deployment-status declarations and historical PFA-2026-000011 as context. The methodology uses immutable scope identification, architecture and trust-boundary analysis, manual security review, automated-analysis/testing evidence where available, severity classification, remediation tracking, deployment verification and final QA. Unexecuted tests are not represented as passed.

4. Architecture Boundaries

Layer | Role | Current state |

Ethereum L1 | Current ENK network and security foundation | Current external network |

OP Stack L2 | Planned EVM execution, bridge and sequencer framework | Planned |

Sovereign modules | Wallet, explorer, identity, proof, SOVRA, EnergieMIND, financial/security layers | Planned / development; module evidence required |

Governance / legal gates | Upgrade, multisig, compliance and activation controls | Defined at design level; deployment evidence required |

5. Threat Model

ID | Threat | Impact | Required controls |

T-01 | Privileged key compromise | Unauthorized state/asset control | Hardened multisig/MPC/HSM, quorum, rotation, monitoring and recovery |

T-02 | Proxy / upgrade abuse | Malicious implementation or storage corruption | Initializer locks, storage-layout checks, restricted upgrades and provenance |

T-03 | Future bridge compromise | Cross-domain asset loss | Standard reviewed stack, dedicated audit, pause and monitoring |

T-04 | Sequencer failure / compromise | Censorship, outage or ordering risk | Hardened keys, failover, monitoring and finality procedures |

T-05 | Sale / accounting error | Wrong price, allocation, vesting or payment state | Exact-decimal accounting, invariants, reconciliation and versioned config |

T-06 | Identity / privacy failure | PII exposure or forged eligibility | No raw PII on-chain, issuer controls, revocation and privacy review |

T-07 | AI authority escalation | Unauthorized financial/governance action | SOVRA recommendation-only boundary and deterministic/human authorization |

T-08 | Oracle / data manipulation | Incorrect external-state decisions | Authenticated sources, freshness bounds, anomaly detection, fail closed |

T-09 | Web/API compromise | Account or allocation/payment manipulation | Server authorization, secret isolation, rate limits, CSP and logs |

T-10 | Supply-chain compromise | Malicious production artifact | Pinned dependencies, SBOM, provenance, signed releases and least-privilege CI |

6. Formal Findings

PF-ENK-2026-01 High Open Production contract assurance package is incomplete for a final code-bound security opinion. Create a release-specific manifest binding repositories, commits, toolchain, addresses, bytecode hashes, tests, coverage, static analysis, fuzz/invariant campaigns and deployment provenance.

PF-ENK-2026-02 High Pre-mainnet gate Future bridge and L2 deployment require dedicated assessment before activation. Review OP Stack deltas, messenger/bridge configuration, admin authority, withdrawals/finality, pause/recovery, sequencer configuration and deployed bytecode.

PF-ENK-2026-03 Medium Evidence required Production signer sets, thresholds, hardware/key policy, recovery and rotation must be cryptographically/deployment verified.

PF-ENK-2026-04 Medium Evidence required ENK supply, allocation, vesting, pricing and TVKUSD-separation invariants require executable CI regression artifacts.

PF-ENK-2026-05 Medium Cross-system The inter-module trust surface requires machine-readable interfaces, authentication/authorization requirements, failure modes and module-specific assessments.

PF-ENK-2026-06 Low Continuous Current-vs-planned public claims should remain machine-checked across ecosystem properties.

7. Production Readiness Gates

Freeze exact production scope and audited commit hashes.

Run and retain static analysis.

Publish unit/integration coverage.

Run stateful fuzz/invariant campaigns.

Bind production bytecode to reviewed source.

Verify all privileged roles and multisig thresholds.

Complete bridge-specific review before ENK migration.

Assess RPC, sequencer, CI/CD, secrets, monitoring and recovery.

Retest all Critical/High/Medium remediation.

Exercise incident response and pause/recovery.

8. Final Opinion

CONDITIONAL / EVIDENCE-GATED. EnteleKRON's current architecture direction is coherent and security-conscious at the design/control level, particularly in Ethereum/current-state clarity, ENK/TVKUSD separation, governance gating, planned OP Stack foundation and limits on autonomous AI authority. A final production smart-contract opinion remains withheld until exact production scope is bound to source, bytecode, testing, privilege, infrastructure and remediation evidence.

[Permanent Preflight record](#) [Download permanent PFA PDF](#) [EnteleKRON home](#)

This is a first-party/common-control technical assessment by Preflight Audit, operated by TVK Labs & Technologies Ltd. It is not an external accreditation, regulatory approval or guarantee that vulnerabilities do not exist. Material changes require reassessment.